



Tarantella[®] Enterprise II Administration

Instructor Guide

Course Release: 1.0

For Software: Tarantella Enterprise II

©2000 The Santa Cruz Operation, Inc. All rights reserved.

This publication is protected under copyright laws and international treaties.

Information in this document is subject to change without notice and does not represent a commitment on the part of The Santa Cruz Operation, Inc.

SCO documents are provided as is and may include technical inaccuracies or typographical errors. The Santa Cruz Operation, Inc. reserves the right to add, delete, change or modify SCO documents at any time without notice. SCO, the SCO logo, The Santa Cruz Operation, SCO OpenServer, Tarantella, the Tarantella logo and UnixWare are trademarks or registered trademarks of The Santa Cruz Operation, Inc. in the USA and other countries. IXI, X.desktop, Deskworks, Wintif, IXI Panorama, Deskterm, and IXI Desktop are trademarks or registered trademarks of IXI Limited, a subsidiary of The Santa Cruz Operation, Inc. Visionware, Devkit, Vision, Esprit, Kodon, Super.Vision, Visionware Super.Vision, Term.Vision, Visionware Direction, the Visionware logo, Visionware SQL-Retriever, and XVision are registered trademarks of Visionware Limited, a subsidiary of The Santa Cruz Operation, Inc. SuperVision, TermVision, X-Visionware, SQL-Retriever, and Vision Builder are trademarks of Visionware Limited. UNIX is a registered trademark of The Open Group in the United States and other countries. Cheyenne and ARCServe are registered trademarks of Cheyenne Software, Inc. Netscape, Netscape Navigator, Netscape Communications Server, Netscape Commerce Server, Netscape Proxy Server, Netscape FastTrack Server, Netscape Enterprise Server, Netscape SuiteSpot, Netscape Catalog Server, Netscape News Server, Netscape Mail Server, and Netscape Navigator Gold are trademarks of Netscape Communications Corporation. NFS was developed by Legent Corporation (formerly Lachman Associates, Inc.) based on LACHMAN SYSTEM V NFS. LACHMAN is a trademark of Legent Corporation. NFS is a trademark of Sun Microsystems, Inc. TCP/IP was developed by Legent Corporation (formerly Lachman Associates, Inc.) based on LACHMAN SYSTEM V STREAMS TCP, a joint development of Lachman Associates and Convergent Technologies. MPX was developed by Corollary, Inc. VP/ix is a product developed and licensed by Phoenix Technologies, Ltd./INTERACTIVE Systems Corporation. XRemote is a registered trademark of Network Computing Devices, Inc. Oracle is a registered trademark of Oracle Corporation, Redwood City, California. Java is a trademark of Sun Microsystems, Inc. Compaq, Tandem, Integrity, NonStop, NetFlex, ProLiant, ROMPaq, ServerNet, SmartStart, registered in United States Patent and Trademark Office. Intel and Pentium are registered trademarks, and Pentium II Xeon and Pentium III Xeon are trademarks of Intel Corporation. SCO, Veritas, VxFS, and VxVA are registered trademarks of Veritas Software Corporation. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. All other brand and product names are or may be trademarks of, and are used to identify products or services of, their respective owners.

The SCO software that accompanies this publication is commercial computer software and, together with any related documentation, is subject to the restrictions on US Government use as set forth below. If this procurement is for a DOD agency, the following DFAR Restricted Rights Legend applies:

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the US Government is subject to restriction as set forth in subparagraph (c)(1)(ii) of Rights in Technical Data and Computer Software Clause at DFARS 252.227-7013. Contractor/Manufacturer is The Santa Cruz Operation, Inc., 400 Encinal Street, Santa Cruz, CA 95060.

If this procurement is for a civilian government agency, this FAR Restricted Rights Legend applies:

RESTRICTED RIGHTS LEGEND: This computer software is submitted with restricted rights under Government Contract No. _____ (and Subcontract No. _____, if appropriate). It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (g)(3)(i) of FAR Clause 52.227-14 alt III or as otherwise expressly stated in the contract. Contractor/Manufacturer is The Santa Cruz Operation, Inc., 400 Encinal Street, Santa Cruz, CA 95060.

Table of Contents

Lesson 1: Introduction to Tarantella Enterprise II	1-1
Introduction to Tarantella Enterprise II Administration	1-8
Course goal and purpose	1-8
Target audience	1-9
Example Company	1-9
Introduction to Tarantella Enterprise II	1-17
What is Tarantella?	1-17
Benefits of using Tarantella Enterprise II	1-18
Logging into Tarantella Enterprise II	1-21
The Tarantella Enterprise II webtop	1-23
Tarantella Documentation	1-27
On-line References	1-28
Web sites	1-28
News groups	1-29
Typographical Conventions	1-30
Lesson Summary	1-32
Review questions	1-33
Answers to Exercise and Review Questions	1-34
Lesson 2: Installing Tarantella	2-1
Installing the Tarantella Enterprise II Base Product	2-8
Tarantella Enterprise II server requirements	2-8
Distribution media	2-9
Installation procedure	2-10
Removing Tarantella Enterprise II	2-12
Licensing Tarantella Enterprise II	2-13
Web Server Configuration	2-14
Netscape FastTrack Server	2-14
Apache	2-15
Other web servers	2-15
Testing the Installation	2-16
Lesson Summary	2-17
Review questions	2-18
Lab: Installing and Licensing Tarantella	2-20
Overview	2-20
Procedure	2-23
Answers to Exercise and Review Questions	2-25
Lesson 3: Modeling an Organization	3-1
Creating Users and Configuring Applications	3-9
Control Center	3-9

Adding a Tarantella user	3-11
Adding an application	3-14
Deploying the application to a user	3-15
The Tarantella datastore	3-15
Modeling an Organization	3-17
Hierarchal structure	3-17
Inheritance	3-19
The home page attribute	3-20
Creating Objects in Tarantella	3-21
Adding a user	3-21
Adding an application	3-29
Document objects	3-31
Host and Host Group objects	3-31
Moving Objects	3-32
Trash	3-33
Lesson Summary	3-34
Review questions	3-35
Lab: Configuring Tarantella	3-37
Overview	3-37
Procedure	3-39
Answers to Exercise and Review Questions	3-43
Lesson 4: The Tarantella Native Client	4-1
The Tarantella Native Client	4-8
Why does the Native Client exist?	4-8
Installing the Tarantella Native Client	4-9
Running the Native Client	4-11
Logging into the Native Client	4-11
Native Doc Viewer	4-11
Lesson Summary	4-12
Review questions	4-13
Answers to Exercise and Review Questions	4-14
Lesson 5: Printing under Tarantella	5-1
How Tarantella Printing Works	5-7
Configuring a Unix Server for Tarantella Printing	5-8
Configuring a Windows Server for Tarantella Printing	5-9
Submitting Print Jobs under Tarantella	5-10
Lesson Summary	5-11
Review questions	5-12
Answers to Exercise and Review Questions	5-13
Lesson 6: The Tarantella Security Pack	6-1
The Tarantella Security Pack	6-8

Installing the Tarantella Security Pack	6-10
Distribution media	6-10
Installation procedure	6-11
X.509 Certificates	6-12
Obtaining an X.509 certificate for the Tarantella Security Pack	6-13
Supported Certificate Authorities	6-14
Installing an X.509 Certificate.....	6-15
Enabling Tarantella security	6-15
The Control Center	6-16
Testing the Tarantella Security Pack configuration	6-17
Lesson Summary.....	6-18
Review questions	6-19
Lab: Configuring the Tarantella Security Pack.....	6-20
Overview.....	6-20
Procedure	6-21
Answers to Exercise and Review Questions.....	6-33
 Lesson 7: Tarantella Load Balancing	 7-1
Distributing the Load	7-9
Application Server Farms	7-10
Multiple application servers.....	7-10
Balancing applications across multiple application servers	7-11
Creating a Tarantella Array	7-13
Tarantella load balancing	7-13
Arrays of Tarantella servers	7-15
Arrays and web servers.....	7-16
Arrays and the Tarantella URL	7-16
Creating an array of Tarantella servers	7-17
Changing the primary server in an array	7-18
Adding a secondary Tarantella server to an array	7-18
Removing a server from an array	7-19
Dismantling an array of Tarantella servers	7-19
Using a Tarantella Array	7-20
Displaying servers in an array	7-20
Login into a particular Tarantella server in an array	7-20
Balancing the Load across Tarantella Servers	7-21
The load balancing table	7-21
Adding a user to the load balancing table.....	7-23
Removing a user from the load balancing table	7-23
Making a Tarantella server available to a user.....	7-24
Removing a Tarantella server from those available to a user	7-24
Ordering the servers for a user.....	7-25
Lesson Summary.....	7-26
Review Questions	7-27
Lab: Creating an Application Server Farm	7-28

Overview	7-28
Procedure	7-28
Lab: Creating an Array of Tarantella Servers	7-30
Overview	7-30
Procedure	7-31
Answers to Exercise and Review Questions.....	7-36

Lesson 8: Windows Connectivity Pack
8-1

Choosing a Windows Protocol.....	8-9
The “None” protocol.....	8-9
The “SCO Merge” protocol	8-11
The “WinFrame / MetaFrame” protocol.....	8-11
The “WinCenter & UIS” protocol	8-13
The “Local Windows Terminal Server” protocol	8-13
The “Win2000/Terminal Server” protocol.....	8-15
Installing the Windows Connectivity Pack.....	8-16
Distribution media	8-16
Installation procedure	8-17
Licensing issues	8-18
Scalability and performance	8-18
Installing applications	8-19
Application compatibility scripts.....	8-19
Deploying Windows applications under Tarantella	8-20
Installing Windows Terminal Server and Windows 2000	8-21
Windows Terminal Server and Windows 2000 requirements	8-21
Distribution media and creating installation floppies	8-21
Installing Windows 2000 Advanced Server.....	8-22
Installing Windows Terminal Server	8-22
Crucial information for Windows Terminal Server	8-23
Service Pack Installation.....	8-23
Windows Terminal Server administration	8-23
User creation	8-24
Disconnect, logoff and shutdown	8-24
Crucial information for Windows 2000	8-25
Windows 2000 betas	8-25
RDP support.....	8-25
Terminal Server 4.0 compatibility	8-25
Utilities for configuring Terminal Services	8-26
Disabling interactive login.....	8-26
Installation of Terminal Services	8-27
Installation of Print Services for Unix	8-27
Creating user accounts.....	8-28
Using the Windows 2000 “guest” account	8-28
Resetting connections	8-29
Microsoft Terminal Server client.....	8-31

Lesson Summary	8-34
Review questions	8-35
Lab: Installing Windows 2000	8-36
Overview	8-36
Procedure	8-36
Lab: Installing Windows Terminal Server Edition	8-40
Overview	8-40
Procedure	8-40
Lab: Installing Service Pack 5 for Windows Terminal Server	8-44
Overview	8-44
Procedure	8-45
Lab: Installing Internet Explorer 5.0.1	8-46
Overview	8-46
Procedure	8-46
Lab: Office97 Installation	8-47
Overview	8-47
Procedure	8-47
Lab: Creating an Application Object for Microsoft Excel	8-49
Overview	8-49
Answers to Exercise and Review Questions	8-50
 Lesson 9: The X Window System	 9-1
X Window System	9-8
History and philosophy of the X window system	9-8
X application input	9-8
Window managers	9-9
Clipboard	9-9
Fonts	9-10
A Typical X Application	9-11
Xlib	9-11
Xt	9-11
Motif	9-11
Lesson Summary	9-12
Review questions	9-13
Lab: Understanding the X Window System	9-15
Overview	9-15
Procedure	9-16
Answers to Exercise and Review Questions	9-27
 Lesson 10: Customizing Tarantella	 10-1
The Basics You Must Know	10-6
HTML	10-6
Frames	10-7
Tables	10-7
cgi-bin	10-8

RGB colors	10-9
Themes.....	10-11
Login themes.....	10-12
Webtop themes.....	10-13
Icon themes	10-15
Configurable Tarantella Components	10-17
Splash screen.....	10-17
Login screen.....	10-19
The Tarantella webtop.....	10-23
Logging out screen.....	10-31
Logged out screen.....	10-31
The Tarantella Solution Zone.....	10-32
Lesson Summary	10-33
Review questions	10-34
Lab: Modifying the Login Theme	10-36
Overview	10-36
Procedure	10-37
Lab: Modifying the Webtop Theme.....	10-40
Overview	10-40
Procedure	10-41
Answers to Exercise and Review Questions.....	10-46

Lesson 11: The Tarantella 3270 Connectivity Pack	11-1
---	-------------

Installing the Tarantella 3270 Connectivity Pack	11-8
Tarantella 3270 Connectivity Pack requirements	11-8
Distribution media	11-9
Installation procedure	11-9
Using the Tarantella 3270 Connectivity Pack.....	11-13
Lesson Summary.....	11-14

Appendix A: Basic Networking and Tarantella	A-1
--	------------

Network Review	A-9
Media types	A-10
Interfaces.....	A-13
IP datagrams	A-14
IP properties.....	A-15
IP protocols	A-15
Port numbers	A-16
Sequence numbers & acknowledgement numbers	A-17
Encapsulation.....	A-19
Routing.....	A-19
Subnetting	A-19
DNS	A-21
Network protocols.....	A-22
Before Embarking upon Tarantella.....	A-23

Network Utilities Usedby Tarantella Administrators	A-25
ifconfig.....	A-25
ping	A-25
netstat	A-27
tracert	A-29
arp	A-29
nslookup.....	A-31
ipconfig	A-33
winipcfg	A-33
Tarantella Administrator's Tools	A-35
Telneting to a port	A-35
Network sniffers.....	A-36
Using Network Monitor.....	A-37
Lesson Summary.....	A-65
Review questions	A-67
Lab: Gathering Network Information	A-69
Overview	A-69
Procedure	A-69
Lab: Hypothetical Situations	A-71
Situation #1: Checksum Errors	A-71
Situation #2: 100MB File Transfer	A-71
Situation #3: Webserver Configuration Exploration.....	A-72
Situation #4: Maximum Port Number	A-72
Lab: Network Traffic Analysis	A-73
Overview	A-73
Answers to Exercise and Review Questions.....	A-79

1

Introduction to Tarantella Enterprise II

Instructor Guide

Instructor Guide

Lesson 1

Introduction to Tarantella Enterprise II

Introduction

This course is designed for individuals who need to perform routine Tarantella administration tasks on a daily basis. The target audience includes support technicians, developers, engineers, and other technical users who require the ability to perform standard administration tasks.

Objectives

By the end of this lesson, you will be able to:

- Understand the format of this course
- Log into and out of Tarantella
- Use the Tarantella webtop
- Utilize Tarantella help resources

AV 1-1

Instructor Guide

Introduction to Tarantella

- Understanding the format of this course
- Logging into Tarantella
- Using the Webtop
- Logging out of Tarantella
- Locating Tarantella Help



Tarantella®

©The Santa Cruz Operation, Inc.



SCO

Topics

In order to meet these objectives, this lesson discusses:

- Understanding the format of this course — Discusses the topics presented in this course and how the exercises and labs are structured.
- Logging into Tarantella — Discusses how to log into Tarantella as a user.
- Using the webtop — Discusses how to launch applications under Tarantella.
- Logging out of Tarantella — Discusses how to log out of Tarantella.
- Locating Tarantella Help — Discusses the various places to find help in Tarantella.

AV 1-1: Introduction to Tarantella

The first slide describes the overall topics covered in this lesson.

Equipment

The instructor and each student needs the following equipment:

- 1 industry standard Pentium CPU computer running SCO® UnixWare® 7
 - 2GB hard disk (minimum)
 - 64MB RAM (minimum, 96MB or greater recommended)
 - 1 network card
 - 1 (or more) IP address(es)
 - 1 (or more) DNS resolvable name(s)
- 1 industry standard Pentium CPU running Microsoft Windows 95 or 98
 - 2GB hard disk (minimum)
 - 64MB RAM (minimum)
 - 1 network card
 - 1 (or more) IP address(es)
 - 1 (or more) DNS resolvable name(s)
 - Internet Explorer and/or Netscape® Communicator® installed and configured (See <http://tarantella.sco.com/sysreqs> for more info).

The classroom will need to be equipped with the following:

- A connection to the Internet with adequate bandwidth to support the number of students in attendance
- All network infrastructure and equipment (hubs, switches, cables) necessary to inter-connect all of these machines to each other and to the Internet
- 1 (or more) DNS server(s) providing name service. This server must contain all the IP addresses and names used by the student and instructor machines.
- 1 (or more) Windows NT Terminal Server Edition or Windows 2000 Advanced Server system(s)
- 1 printer (minimum) made accessible to the Windows machines by one (or more) of the following methods:
 - A Windows printer share
 - HP Jet Direct
- 1 VGA projector
- White board with markers

1.1 Introduction to Tarantella Enterprise II Administration

The *Tarantella Enterprise II Administration* course covers a range of topics selected to assist technical users in all aspects of administering Tarantella Enterprise II servers. Topics include discussions on installing Tarantella and its add-on packages, customizing Tarantella, and understanding the technologies that form the foundation upon which Tarantella runs.

1.1.1 Course goal and purpose

At the conclusion of this course, students should be able to accomplish tasks such as using Tarantella as an end-user, administering Tarantella servers, installing the various Tarantella components, and customizing the Tarantella login screen and webtop. By the end of the course, students will be able to:

- Login and logout of Tarantella
- Install Tarantella, the Tarantella Security Pack, the Tarantella 3270 Connectivity Pack, and the Windows Connectivity Pack
- Configure applications, documents, users, organization units, and the Tarantella organization
- Access Tarantella via the Native Client
- Configure printing under Tarantella
- Configure application server farms and Tarantella arrays
- Secure Tarantella servers using the Secure Sockets Layer (SSL) capabilities provided by the Tarantella Security Pack
- Customize the Tarantella login screen
- Customize the Tarantella webtop
- Customize the icons used by Tarantella
- Provide access to Windows applications with the Windows Connectivity Pack

1.1.2 Target audience

This is an intermediate level course, aimed at system administrators, support technicians, developers, and engineers. The course pre-requisites include a basic understanding of networking and the X Windows system.

1.1.3 Example Company

Throughout the lessons, exercises, and labs which follow, we will refer to a hypothetical company called Example Company, Inc. In addition, we will refer to the domain *example.com* and machines within that domain. This domain is a registered domain name, however it is not used by an actual organization. Rather, *example.com* is reserved for situations such as those posed by this class where a sample domain name is needed.

Course schedule

This course takes four days to complete. A suggested lesson duration is specified at the beginning of each lesson in this **Instructor Guide**.

The labs included in the course must be completed in order to meet the course objectives.

Suggestions for practice exercises are also included throughout the course. Ample time has been allotted to each lesson to allow for the completion of these exercises.

Training materials

These training materials are used in this course:

- **Instructor Guide** and transparency masters
- **Student Guide**
- Courseware CD-ROM

Software

This class uses the following software:

- Tarantella Enterprise II
- UnixWare 7
- Windows 95 or Windows 98
- Windows Terminal Server Edition or Windows 2000

The *Instructor Guide*

The ***Instructor Guide (IG)*** is organized as follows: Instructor notes are intermingled with text in the ***Student Guide (SG)*** to allow the instructor to easily refer to section content. Page numbers in the ***IG*** do not correspond to those in the ***SG***, however the heading numbers do.

Cross references to other sections within the course materials are included within the text. These cross references generally include the section number or AV number, the section name, and page number. The page number will almost always be different in the ***SG*** than the ***IG***; however, the other components will be the same.

The ***IG*** also contains notes which are instructional aids, including:

AV 1-2: Slide Title

These notes explain the instructional objective of every transparency. The AV number cross references to the number that appears above every slide in the workbook.

GuruNotes

This is extra information not directly presented in the ***SG*** and is intended for more advanced students.

Lesson plan

Each lesson follows a similar approach, or methodology, in the delivery of instruction:

- The suggested lesson duration and instructor preparation notes are provided at the beginning of each lesson when applicable.
- The lesson begins with an overview transparency of the major topics and a list of the lesson objectives.
- The lesson continues with the presentation of lesson topics and the demonstration of lesson tasks.
- Exercises, which allow the students to practice discrete tasks, appear throughout the presentation.
- References appear where appropriate.
- The lesson content concludes with a summary. Use this to reinforce the topics and tasks covered. You should also refer back to the objectives that were presented at the beginning of the lesson.
- Following the content of most lessons are summary exercises, which consist of review questions and labs. The review questions allow the instructor to determine how well the students understood the content, and the labs allow students to apply the material that they learned.

Using the root account in the classroom

When teaching *Tarantella Enterprise II Administration*, the instructor will refer to the use of the **root** account. The power of the **root** account in a UNIX system makes it both important and dangerous in the classroom; allowing students to use the **root** account risks damaging the system.

Why should students use root?

- They will be system administrators, and should learn to use **root** in the classroom before they use it on the job.
- They paid for the course, and often feel **root** privileges are part of what they paid for.
- Many procedures central to system administration are best learned with a hands-on approach.
- Many system administration students have already been system administrators, and expect to use **root**.

Why shouldn't students use root?

- Pranks and tampering can affect the classroom experience.
- Students should be discouraged from using **root** except when absolutely necessary
- Reinstalling a corrupted system wastes class time.
- Some instructors believe that **root** procedures and use can be taught just as well using the LCD display.

What to say to students

- Explain the above concerns.
- Explain your approach, along with its pros and cons.
- Make clear to students their responsibilities if they use the **root** account.

Classroom setup

Install the necessary software, including the operating system and the course software on all the machines.

- Configure a DNS master server on the instructor machine
- Install Tarantella®
- Configure anonymous ftp on the instructor machine
- Enable the web server
- To install the course software, follow these steps:

Step 1. Login as **root**.

Step 2. Insert the CD-ROM into the drive.

Step 3. Mount the CD-ROM:

```
# mount -F cdfs -r /dev/cdrom/cdrom1 /mnt
```

Step 4. Execute the setup program:

```
# sh /mnt/setup
```

Step 5. Unmount the CD-ROM.

```
# umount /mnt
```

- Configure classroom equipment, your own display, and the LCD.
- Problems have been encountered when Microsoft Outlook or Microsoft Outlook Express are running on the Windows clients. Remove these applications if necessary.

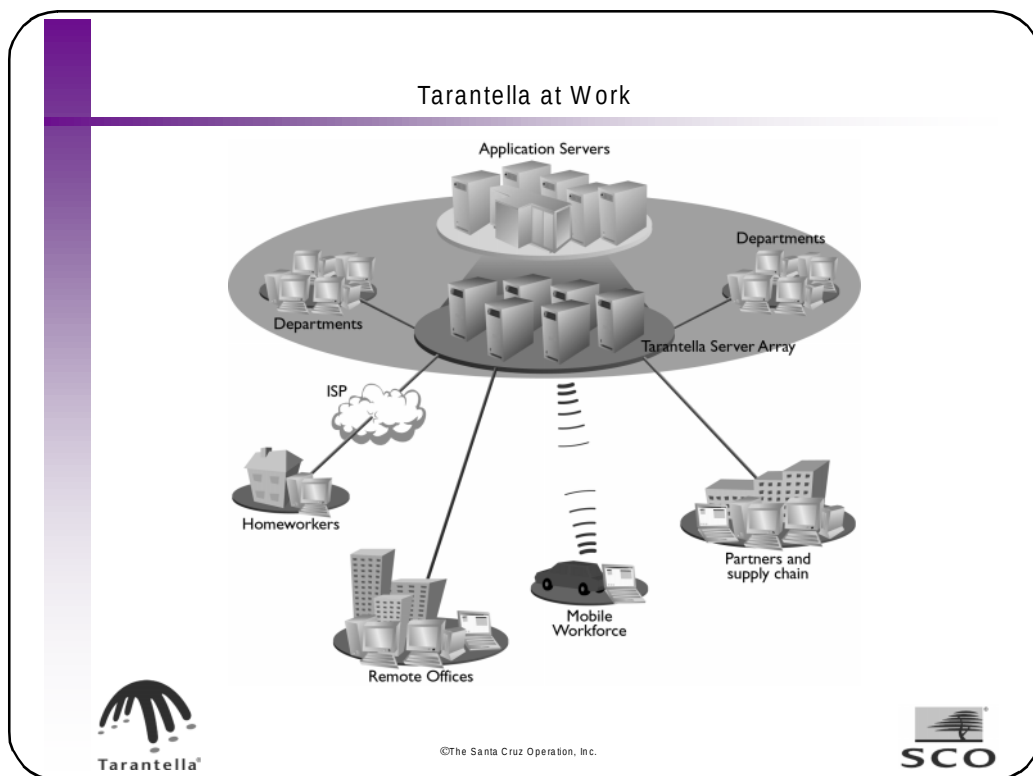
Lesson preparation

- Read the pre-lesson preparation prior to each lesson. Complete any tasks listed in the preparation.
- Read the lesson thoroughly before teaching, and add any additional notes or exercises.
- Read through the appropriate sections of the SCO documentation in support of the lesson topics.

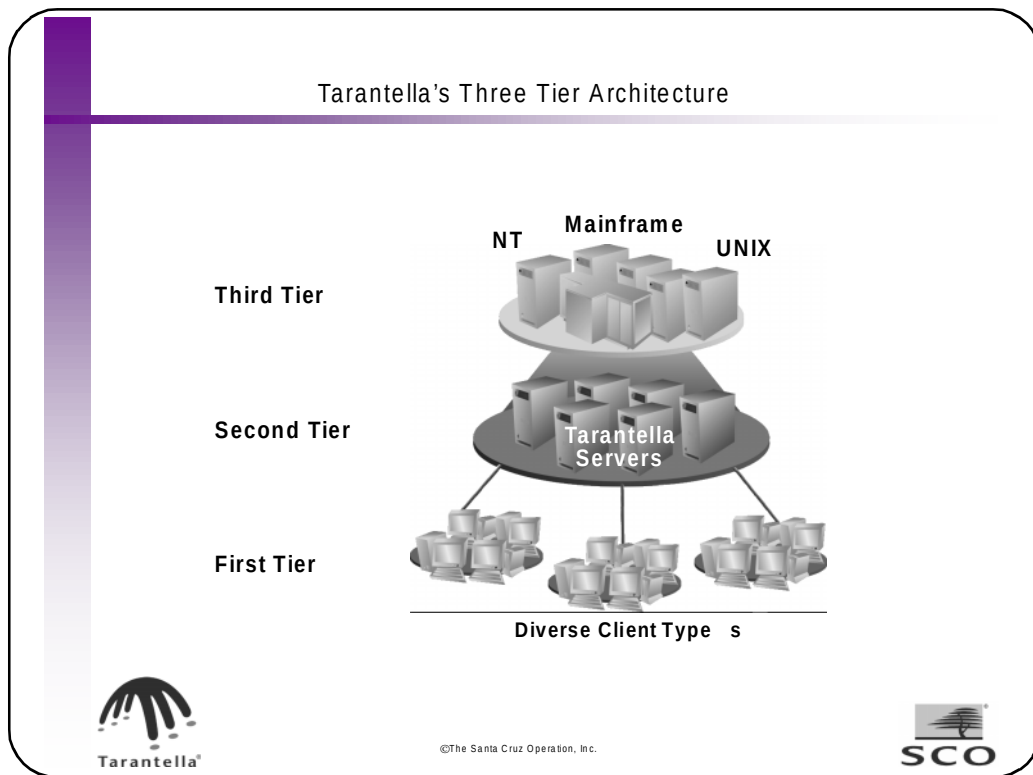
Crash course on what's new in Tarantella Express:

- Allows up to 45 concurrent users
- No Tarantella arrays (2nd tier servers)
- Allows up to 4 application servers (3rd tier servers)
- Installs and configures Apache as part of the Tarantella installation
- *Includes* the Windows Connectivity Pack
- Platform Wizards (aka. PIP—Platform Identity Pack) — Creates Tarantella objects related to the platform on which Tarantella is installed. For instance, the OpenServer PIP creates objects for the **scoadmin** utilities.
- Application Wizards (aka. SIP—Software Installation Pack) — Creates Tarantella objects related to a particular piece of software installed. For instance, the Microsoft SIP creates objects for Word, Excel, PowerPoint, etc.

AV 1-2



AV 1-3



1.2 Introduction to Tarantella Enterprise II

In this section, we describe what Tarantella® Enterprise II is, what it does, how it does it, and what it can do for you. In later lessons, we'll look at Tarantella's capabilities in far greater detail.

AV 1-2: Tarantella at Work

Use this slide to illustrate what Tarantella does.

AV 1-3: Tarantella's Three Tier Architecture

Use this slide to illustrate Tarantella's three tier architecture.

1.2.1 What is Tarantella?

Tarantella instantly web-enables existing mainframe, Unix and Windows applications. It does this without the need for rewriting *any* application code. Furthermore, Tarantella does not require additional software to be installed on clients or application servers.

To accomplish this, Tarantella utilizes a three-tier model in which the Tarantella server resides on the second tier. From this second tier, administrators can centrally control access to applications across multiple sites.

All of the Tarantella software is installed on the second tier. This means that clients and application servers are left unmodified. Tarantella simply drops into your existing network infrastructure.

Since Tarantella Enterprise II runs on a diverse range of clients, you are not required to replace or upgrade your existing clients with new devices.

1.2.2 Benefits of using Tarantella Enterprise II

Non-invasive	Tarantella is a non-invasive solution. No modifications are required on the clients or application servers.
Access	Tarantella provides diverse clients with access to applications running on mainframes, Unix, and Windows. Furthermore Tarantella delivers these applications across everything from a LAN to a dial-up modem connection over Point-to-Point Protocol (PPP).
Resumable Sessions	Tarantella users enjoy the benefit of being able to suspend their work. Rather than exit from all their applications at the end of the day, drive home, dial up the office, and restart all the applications to work from home, users simply log back into Tarantella from home and Tarantella resumes their applications automatically.
Customizable	Tarantella allows administrators to easily customize the appearance of Tarantella and the appearance of the applications launched within Tarantella.

Performance	SCO's Adaptive Internet Protocol (AIP) enables Tarantella to dynamically adjust itself to the performance of the client and the network connection.
Scalability	Tarantella Enterprise II provides excellent scalability by allowing administrators to implement application server farms and Tarantella arrays. Application farms allow Tarantella to launch an application from any of the servers in the application farm. Tarantella arrays allow administrators to have multiple Tarantella servers work cooperatively to centrally manage application deployment.
Security	With the installation of the optional Tarantella Security Pack (TSP), Tarantella encrypts all Tarantella traffic on the network using Secure Sockets Layer (SSL).

 Without the TSP installed, Tarantella passwords are obfuscated (but not encrypted).

AV 1-4

The Tarantella Enterprise II Login Screen



©The Santa Cruz Operation, Inc.



1.2.3 Logging into Tarantella Enterprise II

AV 1-4: Logging into Tarantella Enterprise II

Use this slide to illustrate logging into Tarantella Enterprise II

To log into Tarantella:

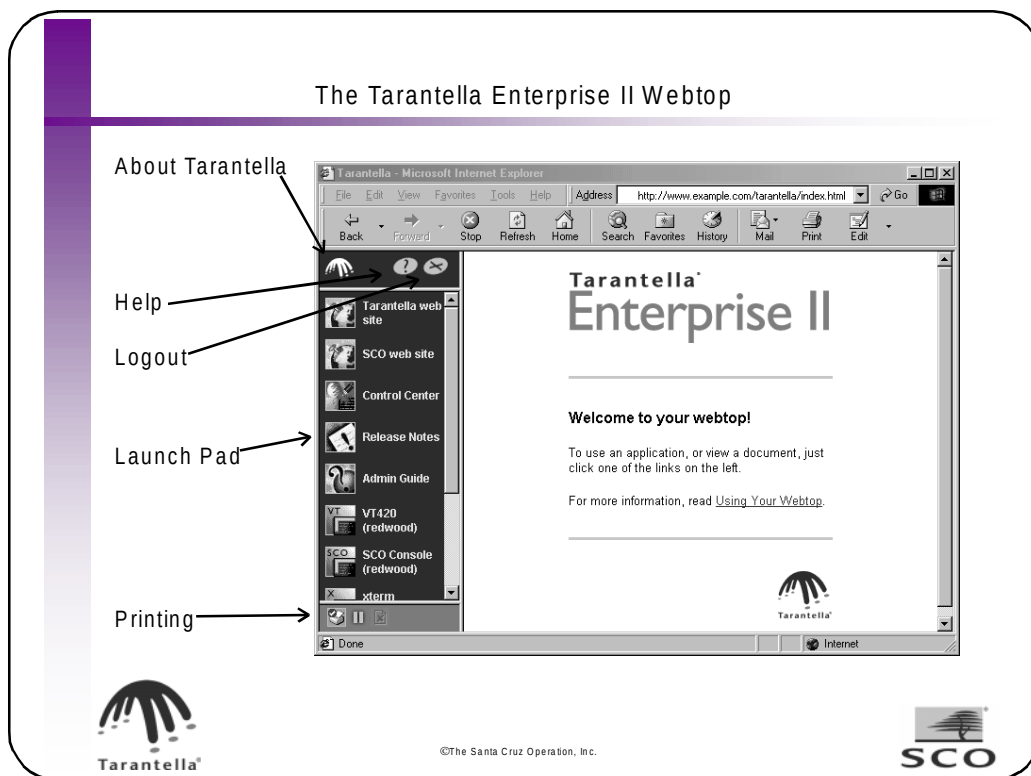
- Step 1. Start a web browser.
- Step 2. Enter the URL **http://server/tarantella**, where *server* is the name of the machine running Tarantella.
- Step 3. Enter your Tarantella user name.
- Step 4. Enter your password.
- Step 5. Click on the **Ok** button.

Exercise: Logging into Tarantella Enterprise II

Log into Tarantella using the server name, user name, and password supplied by your instructor.

AV 1-5

Instructor Guide



1.2.4 The Tarantella Enterprise II webtop

AV 1-5: The Tarantella Enterprise II Webtop

Use this slide to point out the various aspects of the webtop. If presenting the Tarantella Express version of this curriculum, point out the icons created by the PIP and SIP (**scoadmin** and Word, respectively).

The webtop is used to:

- Launch applications

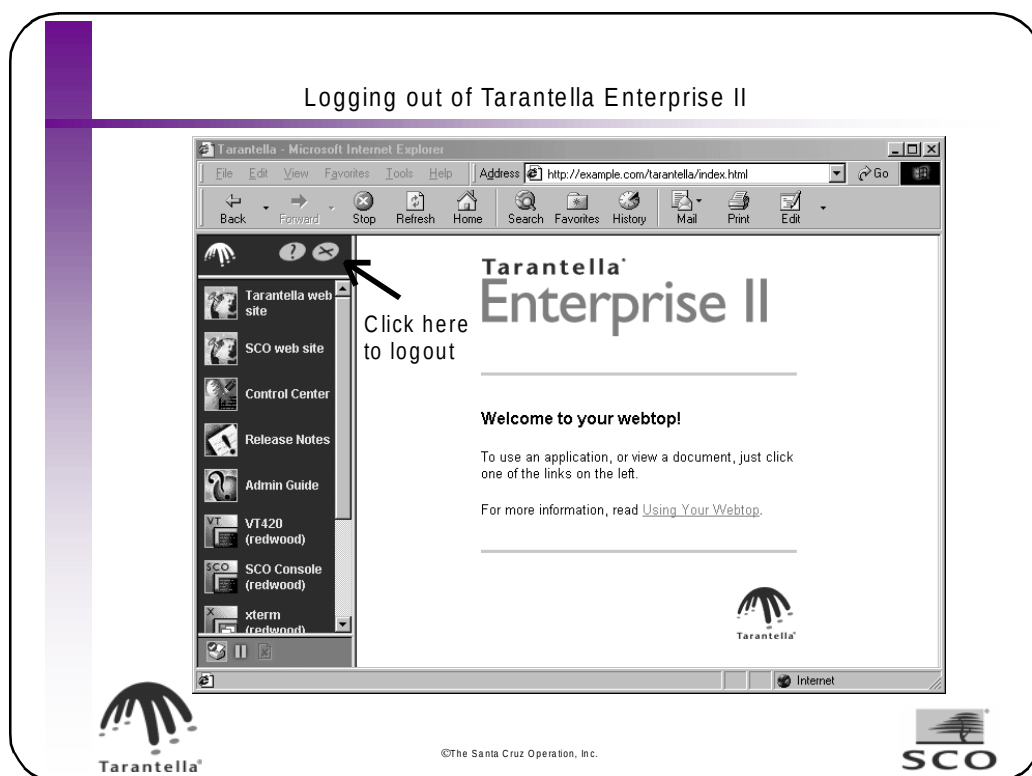
Demonstrate launching an application

- View documents
- Control printers
- Read on-line help

To perform any of these tasks, click on the applicable icon on the webtop.

AV 1-6

Instructor Guide



1.2.4.1 Logging out of Tarantella Enterprise II

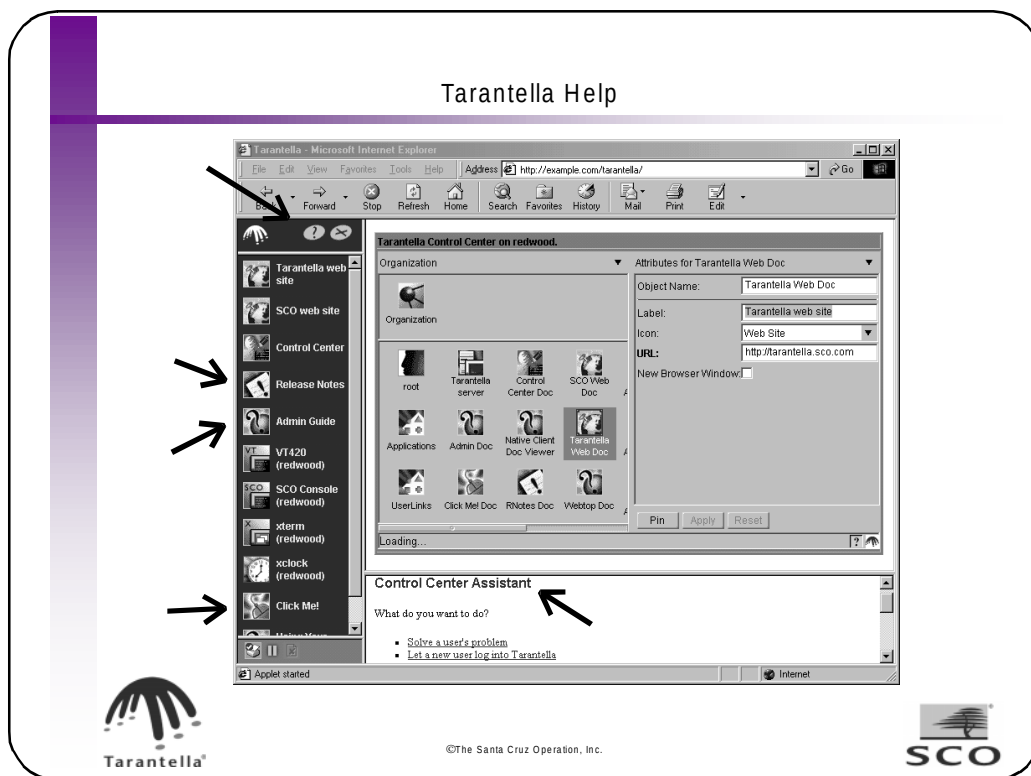
AV 1-6: Logging out of Tarantella Enterprise II

Use this slide to illustrate logging out of Tarantella Enterprise II

To log out of Tarantella, click on the “X” icon on the webtop.

NOTE: Be sure to click on the “X” icon *on the webtop*. Clicking on the “X” in the upper right corner of the browser’s window will close the browser without logging out of Tarantella. Doing this can lead to unintentionally suspended Tarantella sessions.

AV 1-7



1.3 Tarantella Documentation



AV 1-7: Tarantella Help

Use this slide to illustrate the various places where you get help in Tarantella.

References to Tarantella documentation are made throughout the ***Tarantella Enterprise II Administration*** course. This documentation is located on the Tarantella webtop in five areas:

Click Me!	A basic introduction to using Tarantella for end-users.
The “?” icon	Provides a more detailed introduction to Tarantella. Explains using and troubleshooting the webtop in “ <i>Getting Help on using the webtop</i> ”.
Release Notes	Provides late-breaking news about each Tarantella related product installed.
Admin Guide	Includes “How to” articles, technical reference pages, extensive customization information, and more.
Control Center Assistant	An on-line wizard that steps administrators through Tarantella administration tasks.

The Release Notes, Admin Guide, and Control Center Assistant are ordinarily available to Tarantella administrators only.

1.4 On-line References

In addition to the wealth of information provided on-line in Tarantella, you will want to use the following on-line references on the Internet.

Emphasize that the students are going to need to use these resources during the class.

1.4.1 Web sites

http://tarantella.sco.com/info/faq.html	Frequently Asked Questions about Tarantella Enterprise II and Tarantella Express.
http://tarantella.sco.com/knowhow	Contains searchable copies of documentation for all released versions of Tarantella.
http://tarantella.sco.com/tsz	The Tarantella Solution Zone contains hundreds of examples for customizing Tarantella.

The preceding URL will prompt users to register with the TSZ. Once the user has registered, they will be emailed this URL: **http://tarantella.sco.com/tsz/html/en_US**. This is the URL they should use from then on.

http://www.whatis.com	Offers definitions and explanations of computing terms.
http://www.ntfaq.com	Provides information on all aspects of using and administering Windows NT and Windows Terminal Server Edition.
http://www.counterpane.com	Contains security-related articles.
http://www.google.com	A search engine.
http://www.altavista.com	Another search engine.
http://www.ask.com	Another search engine.

1.4.2 News groups

news://pubnews.sco.com/sco.public.tarantella A news group dedicated to discussions on Tarantella products.

1.5 Typographical Conventions

This publication presents commands, filenames, keystrokes, and other special elements as shown here:

lp	Commands, device drivers, programs, and utilities (names, icons, or windows)
<i>/new/client.list</i>	Files, directories, desktops (names, icons, or windows), system, network, and printer names
root	User names
<i>arg</i> or <i>arg</i>	Placeholders (replace with appropriate name or value)
[<i>arg</i>]	Surrounds an <i>option</i> or <i>cmdarg</i> that is not mandatory
<i>arg</i> ...	Indicates multiple occurrences of the <i>option</i> or <i>cmdarg</i>
\$	Command-line prompt for commands executable from the Bourne shell by any user
#	Command-line prompt for commands only executable by the root user from the root account
	Keyboard keys
 	Press  and  keys simultaneously
  	Press all three keys,  ,  , and  , simultaneously
 d	Press  key. With  still depressed, press  .
 0240	Press  key. With  still depressed, press and release in sequence  ,  ,  , and  .
 Q + i	Press  key. With  still depressed, press  . Release both keys and press  .
 Q + I	Press  key. With  still depressed, press  . Release both keys and press   .Exit program?System output (prompts, messages)
tar tv	User input, such as on a command line

“Description”	Field names or column headings (on screen or in database)
Cancel	Button names
Edit	Menu names
Copy	Menu items
File ⇨ Find ⇨ Text	Sequences of menus and menu items
open	Library routines, system calls, kernel functions, C keywords
<code>\$HOME</code>	Environment or shell variables
<code>SIGHUP</code>	Named constants, signals, and kernel parameters
“adm3a”	Data values
<i>employees</i>	Database names and tables
buf	C program structures
<code>b_b.errno</code>	Structure members

1.6 Lesson Summary

This lesson described the basics of Tarantella: how to log in, how to launch applications, how to logout, and how to find help. In the lessons which follow, we delve deeper into Tarantella: how it works and how to configure it.

1.7 Review questions

1. What benefits does Tarantella provide?

Tarantella is non-invasive and customizable. Tarantella provides access to diverse clients and to Unix, Windows, and mainframe applications. Tarantella provides resumable session. The AIP protocol enables Tarantella to dynamically adjust to fit the current bandwidth. Tarantella provides secure communications.

2. How do you log into Tarantella?

You log into Tarantella by typing *http://server/tarantella* in a web browser, where *server* is the name of the Tarantella server.

3. What does the Tarantella webtop enable users to do?

The Tarantella webtop enables users to start applications, view documents, control printers, and read on-line help.

4. How do you log out of Tarantella?

You log out of Tarantella by clicking on the “X” icon on the webtop (not the web browser’s “X” button).

1.8 Answers to Exercise and Review Questions

This section contains the answers to exercises, review questions, and labs presented in this lesson.

Exercise answers

Please consult your instructor if you have any questions about the exercises in this lesson.

Review Question Answers

This section contains the answers to the review questions on page 1-33.

1. Tarantella is non-invasive and customizable. Tarantella provides access to diverse clients and to mainframe, Unix, and Windows applications. Tarantella provides resumable session. The AIP protocol enables Tarantella to dynamically adjust to fit the current bandwidth. Tarantella provides secure communications.
2. You log into Tarantella by typing *http://server/tarantella* in a web browser, where *server* is the name of the Tarantella server.
3. The Tarantella webtop enables users to start applications, view documents, control printers, and read on-line help.
4. You log out of Tarantella by clicking on the “X” icon on the webtop (not the web browser’s “X” button).

2

Installing Tarantella

Instructor Guide

Instructor Guide

Lesson 2

Installing Tarantella

Suggested lesson duration

This lesson should take approximately 1.5 hours to complete including the lab.

Pre-lesson classroom preparation

The classroom network needs to be setup properly (clients installed, DNS updated, etc.). Aside from this, make sure you have the Tarantella media to install from (whether by CD-ROM or via the web).

Instructor preparation

Read the following articles in the **Admin Guide**:

- How to... ⇒ Advanced ⇒ To Uninstall Tarantella
- Reference ⇒ Installation and Setup ⇒ What Setup does
- Reference ⇒ Installation and Setup ⇒ Tarantella installation tree layout
- Reference ⇒ Unix Commands ⇒ The Tarantella uninstall command
- Reference ⇒ Unix Commands ⇒ The Tarantella license command
- Reference ⇒ Licensing ⇒ Licensing overview
- How to... ⇒ Get started ⇒ To configure your webserver for use with Tarantella

Read the Tarantella FAQ at <http://tarantella.sco.com/info/faq.html>.

Introduction

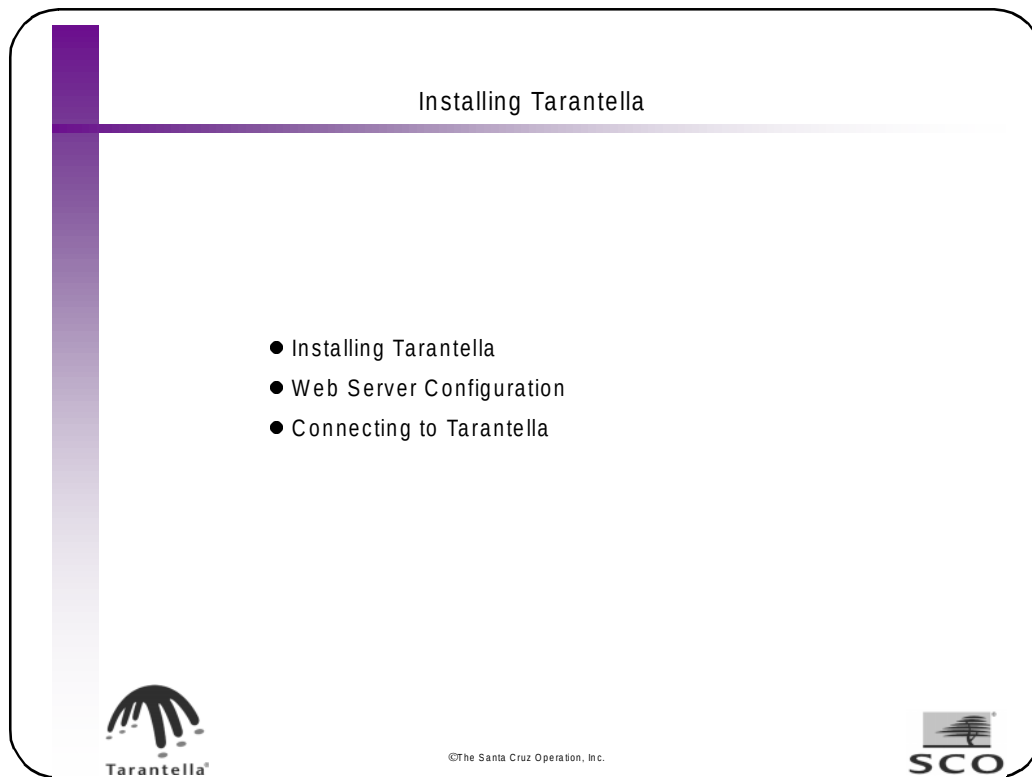
The installation and removal mechanisms in Tarantella Enterprise II have been designed to be reliable and easy to use. To install Tarantella on a server, the administrator should install the Tarantella base software, install any additional Tarantella Packs, and configure the web server.

Objectives

By the end of this lesson, you will be able to:

- Install Tarantella
- Configure the Netscape FastTrack server or Apache for use with Tarantella
- Connect to a Tarantella server

AV 2-1



Instructor Guide

Topics

In order to meet these objectives, this lesson discusses:

- Installing Tarantella — Discusses how to install Tarantella from CD-ROM (or from an archive). Also discussed are procedures for licensing and removing Tarantella.
- Web Server Configuration — Discusses how to configure the Netscape FastTrack Server or Apache for use with Tarantella.
- Connecting to Tarantella — Shows how to connect to a Tarantella server.



AV 2-1: Installing Tarantella

The first slide describes the overall topics covered in this lesson.

2.1 Installing the Tarantella Enterprise II Base Product

The installation and removal mechanisms in Tarantella have been designed to be reliable and easy to use. To install Tarantella on a server, the administrator should install the Tarantella base software, install any additional Tarantella Packs, and configure the web server to allow Tarantella to be accessed.

The Tarantella server software itself installs exclusively on the second-tier.

2.1.1 Tarantella Enterprise II server requirements

The Tarantella Enterprise II server software runs on the following platforms:

Emphasize to students that this is a list of platforms that Tarantella runs on. This is not a list of the platforms that can serve as application servers.

- UnixWare®
- Solaris®
- OpenServer
- AIX
- HP-UX
- Digital Unix (Tru64)
- Linux

As of February 2000, the Linux versions of Tarantella Enterprise II and Tarantella Express are not yet released.

2.1.2 Distribution media

The Tarantella server software is distributed two ways:

Via the web

The Tarantella base product, along with the Tarantella 3270 Connectivity Pack, the Windows Connectivity Pack, and the Tarantella Security Pack can be downloaded from <http://tarantella.sco.com>. Web download is the primary method of distribution.

On CD-ROM

In special instances, SCO distributes the software on CD-ROM. This is not the primary method of distribution.

Table 1: Hints for Using CD-ROMs on SCO Platforms

SCO OpenServer 5	<code>mount -f HS -o ro,lower /dev/cd0 /mnt</code>
SCO UnixWare 7 SCO UnixWare 2.1	<code>/usr/sbin/mount -rF cdfs /dev/cdrom/cdrom1 /mnt</code>

2.1.3 Installation procedure

To install Tarantella:

Step 1. Log in as **root**.

There is no single-user mode requirement.

Step 2. Mount the CD-ROM.

Step 3. Verify that the web server is running. For example, if you are running Netscape® FastTrack Server® on UnixWare 7, execute the following command:

```
# nsfast enable
```

If you fail to do so, Tarantella is unable to automatically set the document directory and the cgi-bin directory for Tarantella under Netscape FastTrack server. You will have to do so manually.

Step 4. Run the following command:

```
sh tta_file.shx
```

where *tta_file.shx* is one of the following file s:

Table 2: Tarantella Enterprise II SHX File Names

Platform	SHX File name
SCO UnixWare® 7+	<i>ttai3un.shx</i>
SCO UnixWare 2.1.2+	<i>ttai3un.shx</i>
SCO OpenServer Release 5.0.2+	<i>ttai3sc.shx</i>
HP-UX 10.20+	<i>ttapahp.shx</i>
IBM AIX 4.2+	<i>ttarsai.shx</i>
SPARC Solaris 2.5.1+	<i>ttaspso.shx</i>

GuruNotes .shx files are a concatenation of a shell script and a compressed datastream. The datastream is in pkgadd format. The .shx shell scripts take care of issuing all of the necessary pkgadd related commands for the particular platform (including installing a functional version of pkgadd, if necessary!).

GuruNotes The file name naming scheme is as follows:

product_name(3 chars)
chipset (2 chars)
operating system(2 chars)

tta = The product's prefix

i 3 = Intel 386

u n = UnixWare

Step 5. Follow the on-screen prompts.

There is no need to start Tarantella after the installation. It has already been started by the installation. Similarly, you needn't do anything to make Tarantella restart upon reboot. The installation sets up Tarantella to automatically start upon reboot.

Installing the Tarantella Security Pack and the Windows Connectivity Packs is performed in the same manner (ie. locate and run the appropriate *.shx file).

2.2 Removing Tarantella Enterprise II

Tarantella is removed using the steps shown in this section. The online documentation should be consulted for further details before the removal is attempted.

- Log in as root on the UNIX system on which Tarantella is to be removed.
- Run this command:

```
/inst_dir/bin/tarantella --uninstall
```

where *inst_dir* is the directory in which Tarantella was installed (usually */opt/tarantella*).

- The Tarantella datastore will not be removed from the system by the uninstall (for upgrade reasons etc.), thus the directory */var/tarantella* and its contents may need to be removed manually.

For more information on how to remove Tarantella, see **How to... ⇒ To Uninstall Tarantella** in the *Admin Guide*.

2.3 Licensing Tarantella Enterprise II

By default Tarantella installs in a 60-day evaluation mode. Tarantella can be used during this trial period. However once the period expires, the Tarantella server will no longer start until it is properly licensed.

There are no functional differences when running in evaluation mode.

To license a Tarantella server, issue the following command:

```
# tarantella license --add license_num
```

where *license_num* is a valid Tarantella license.

The Tarantella license cards supply both a serial number and an activation key. Use the activation key in place of the *license_num* used in the **tarantella license** command above.

Make sure students understand where the tarantella utility lives and how to invoke it even though it does not reside in \$PATH.

Further information on licensing can be found in the Admin Guide. In particular, see Reference ⇒ Licensing ⇒ Licensing Overview.

Contact your reseller or distributor to purchase additional licenses.

2.4 Web Server Configuration

A web server needs to be installed on the same UNIX server as Tarantella. The Tarantella software distribution does not include a web server. A web server should be obtained separately. The two most popular web servers used with Tarantella are the Netscape FastTrack Server and Apache. These two web servers are discussed in this training.

2.4.1 Netscape FastTrack Server

To configure the Netscape web server for use with Tarantella, follow the steps presented in this section of the training. It is assumed that the web server has already been installed.

- Connect to the Netscape Admin Server (see the Netscape documentation).
- Click on **Install a new Netscape FastTrack Server** and accept the default settings.
- Click on **Configure more about your new serve** , press the **Content Mgmt** button, and then click on “**Additional Document Directories**”. Set the URL prefix “<server>/tarantella” to map to `/opt/tarantella` (assuming a default Tarantella installation has been performed). Press the **OK** button and then click on **Save and Appl** .
- Click on the **Programs** button and set the URL “<server>/tarantella/cgi-bin” to map to `/opt/tarantella/cgi-bin`. Press the **OK** button and the click on **Save and Apply**.

The Netscape FastTrack server can be started and stopped with the **nsfast enable** and **nsfast disable** commands, respectively.

2.4.2 Apache

The Apache web server should be configured by following the steps discussed in this section. It is assumed that the web server has already been installed.

- Edit the Apache configuration file *httpd.conf* (usually found in */usr/local/apache/conf*) and add the following lines in the order shown:

In some versions of Apache, the configuration file is called *srm.conf*.

```
ScriptAlias /tarantella/cgi-bin /opt/tarantella/cgi-bin  
  
Alias /tarantella /opt/tarantella
```

There appears to be no restriction on where these lines can be added to the configuration file, but it would seem a good idea to group them with other similar settings. The specified changes are based on a default installation of Tarantella.

- If the web server is not running, start it. Enter: `/usr/local/apache/src/httpd -f /usr/local/apache/conf/httpd.conf` (assuming a default installation of Apache).

NOTE: Newer versions of Apache use **apachectl** to start and stop the web server.

2.4.3 Other web servers

The web server running on the platform where Tarantella is installed must support CGI 1.1. Configuration information about other web servers can be obtained at <http://tarantella.sco.com/knowho>.

CGI 1.1 has been around for quite some time. Most web servers have supported CGI 1.1 since 1993.

To determine what http server is running (if any) on a server, execute “`ps -ef | grep httpd`”. Not only will this help identify the http server, it usually helps to identify the configuration file used by that http server (the arguments to the httpd command usually includes the configuration file name). In the networking chapter, we’ll show how to telnet to the web server and query the server directly.

2.5 Testing the Installation

Test the Tarantella installation by connecting to Tarantella. Connect by typing:

<http://server/tarantella>

where *server* is the name of the Tarantella server.

A login screen will be displayed if the connection is successful.

2.6 Lesson Summary

This lesson described how to install, license, and remove Tarantella. Additionally, this lesson described how to configure a web server to work in conjunction with Tarantella. Finally, this lesson described how to verify a Tarantella installation by connecting to the server via a web browser.

2.7 Review questions

1. On which platforms does the Tarantella server run?

The Tarantella Enterprise II server runs on the following platforms: UnixWare, Solaris, OpenServer, AIX, HP-UX, and Digital Unix (Tru64).

The Tarantella Express server currently runs on OpenServer and UnixWare.

2. Tarantella is installed by running the appropriate *.shx file. How is Tarantella removed?

Tarantella is removed by running:

```
/inst_dir/bin/tarantella uninstall
```

where *inst_dir* is the installation directory into which Tarantella was installed (typically */opt/tarantella*).

3. Which directory should you consider removing after removing Tarantella?

The */var/tarantella* directory remains after the removal of Tarantella. This is done to enable Tarantella to be removed and reinstalled without affecting the Tarantella datastore. In this way you can remove and reinstall Tarantella without affecting your organizational model.

4. What command would you need to issue to add a license to Tarantella?

To license a Tarantella server, you would issue the command “`tarantella license --add license_num`” where *license_num* is a valid Tarantella license.

5. What URL would you use to connect to Tarantella on a machine called `www.example.com`?

The URL is <http://www.example.com/tarantella>.

6. What modifications are necessary on a default installation of Apache?

The Apache configuration file *srm.conf* (usually found in */usr/local/apache/conf*) must be modified to include the following lines (in the order shown):

```
ScriptAlias /tarantella/cgi-bin /opt/tarantella/cgi-bin
Alias /tarantella /opt/tarantella
```

2.8 Lab: Installing and Licensing Tarantella

In this lab, you will perform the steps necessary to install and license Tarantella. After doing so, you will test your Tarantella installation by connecting to the Tarantella server using a web browser.

2.8.1 Overview

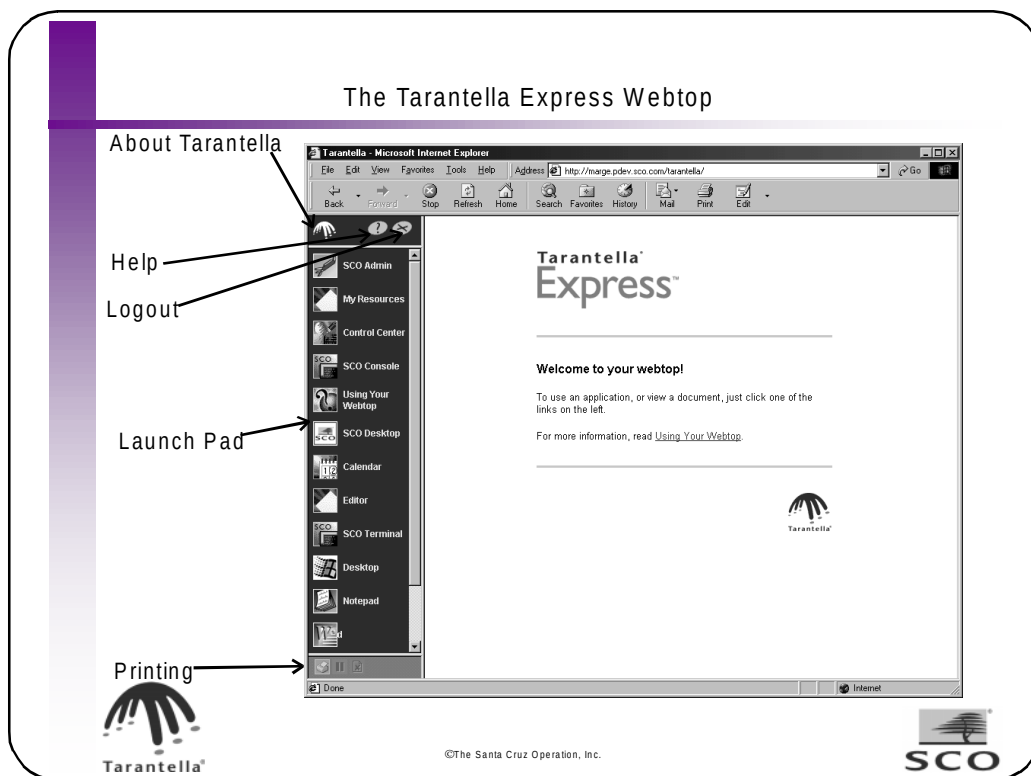
Your tasks in this lab are as follows:

- Install Tarantella
- Configure the web server
- License Tarantella
- Verify the Tarantella server installation by connecting to it with a web browser

The instructor will point you to the location of the tarantella software and license.

Make sure the students know where the software is (CD-ROM, via the web, etc.) and the exact name of the *.shx file that they will be installing. Provide the students with the license(s) that they are to use (if applicable).

AV 2-2



2.8.2 Procedure

Step 1. Log in as root.

Step 2. Verify that the web server is running. For example, if you are running Netscape FastTrack server on UnixWare, execute the following command:

```
# nsfast enable
```

Step 3. The installation of Tarantella will require 50MB in */var/tmp*. Verify that this space is available by executing the following command:

```
# df space
```

If there is insufficient space, you can remedy this problem in either of the two following ways:

- Point the TMPDIR environment variable to a directory which contains sufficient disk space:

```
# TMPDIR=/directory/in/big/enough/filesystem  
# export TMPDIR
```

- Alternatively, unmount the */var/tmp* filesystem:

```
# umount /var/tmp
```

Insufficient space in */tmp* will also cause problems (Tarantella uses a pipe file in */tmp*). The symptoms are 1) the install dies silently or 2) the install fails with "Broken pipe".

Step 4. If directed to do so by the instructor, download the Tarantella *.shx* file for your platform. Otherwise **.shx* file will be provided by the instructor.

Make sure students are clear whether they are getting the Tarantella software from the web, CD-ROM, etc.

Step 5. Execute the **.shx* file by executing the following command:

```
# sh platform.shx
```

where *platform.shx* is replace with the platform specific name of your **.shx* file.

For example, issue the following command on SCO UnixWare 7.1.1 systems:

```
# sh ttai3un.shx
```

Step 6. As shown in AV 2-2, you will be prompted to accept, reject, or read the Software License Agreement.

Assuming that you have read and agree to the Software License Agreement, choose “yes” to accept the Software License Agreement.

AV 2-2: Installing Tarantella

Use this slide to illustrate the Software License Agreement prompt and the Tarantella defaults referenced in Step 6. and Step 7., respectively.

Step 7. As shown in AV 2-2, the installation lists defaults which you can accept or change. Accept the defaults.

Step 8. License Tarantella with the following command:

```
# /inst_dir/bin/tarantella license --add  
license_num
```

where *inst_dir* is the installation directory listed during the installation (see Step 7.) and *license_num* is replaced by a valid Tarantella license.

At this point the students need to map:

- */tarantella* to */opt/tarantella*, and
- */tarantella/cgi-bin* to */opt/tarantella/cgi-bin*

In their web server.

Step 9. Verify that Tarantella is running by connecting to it with a web browser. Use the following URL in the web browser:

<http://server/tarantella>

where *server* is the name of your Tarantella server. Log in and verify that Tarantella behaves as expected.

Step 10. Re-mount the */var/tmp* filesystem if previously unmounted in Step 3.

2.9 Answers to Exercise and Review Questions

This section contains the answers to exercises, review questions, and labs presented in this lesson.

Exercise answers

Please consult your instructor if you have any questions about the exercises in this lesson.

Review Question Answers

This section contains the answers to the review questions on page 2-18.

1. The Tarantella Enterprise II server runs on the following platforms: UnixWare, Solaris, OpenServer, AIX, HP-UX, and Digital Unix (Tru64).

1. The Tarantella Express server currently runs on OpenServer and UnixWare.

2. Tarantella is removed by running:

```
/inst_dir/bin/tarantella uninstall
```

where *inst_dir* is the installation directory into which Tarantella was installed (typically */opt/tarantella*).

3. The */var/tarantella* directory remains after the removal of Tarantella. This is done to enable Tarantella to be removed and reinstalled without affecting the Tarantella datastore. In this way you can remove and reinstall Tarantella without affecting your organizational model.
4. To license a Tarantella server, you would issue the command “`tarantella license --add license_num`” where *license_num* is a valid Tarantella license.
5. The URL is <http://www.example.com/tarantella>.
6. The Apache configuration file *srm.conf* (usually found in */usr/local/apache/conf*) must be modified to include the following lines (in the order shown):

```
ScriptAlias /tarantella/cgi-bin /opt/tarantella/cgi-bin
Alias /tarantella /opt/tarantella
```

3

Modeling an Organization

Instructor Guide

Instructor Guide

Lesson 3

Modeling an Organization

Suggested lesson duration

This lesson should take approximately four (4) hours to complete including the lab.

Pre-lesson classroom preparation

Tarantella must already be installed.

Instructor preparation

Read the following articles in the *Admin Guide*:

Introduction ⇨ Tarantella from a user's perspective

Introduction ⇨ Tarantella from a Tarantella Administrator's perspective

Introduction ⇨ Essential information for Tarantella Administrators

Introduction ⇨ Control Center

Introduction

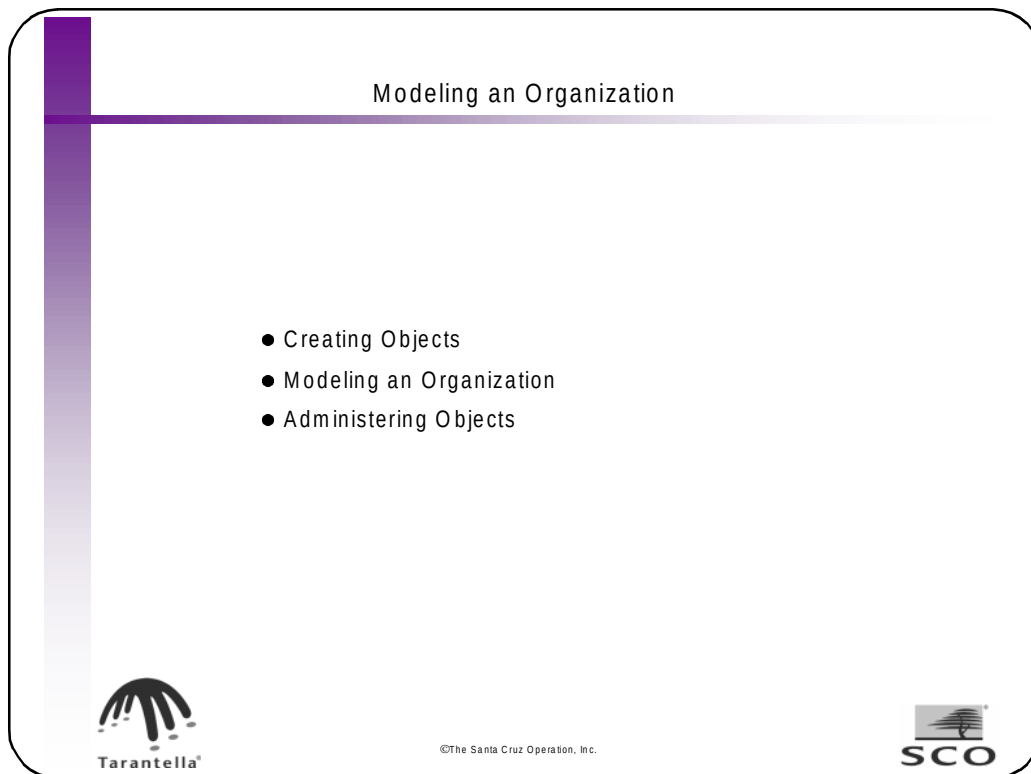
Control Center is the heart of Tarantella and nearly all of administration is done here. Control Center is a graphical administration utility. Conceptually, everything in Control Center is an Object. From the Organizational Units to the Applications to the People. Once you get the hang of navigating through Control Center, administering the Tarantella server is a breeze.

Objectives

By the end of this lesson, you will be able to:

- Create **Organizational Units**, **People**, and **Application** icons
- Allow Unix users and Anonymous users to log in
- Present different webtop content to different people or organizational units

AV 3-1



Topics

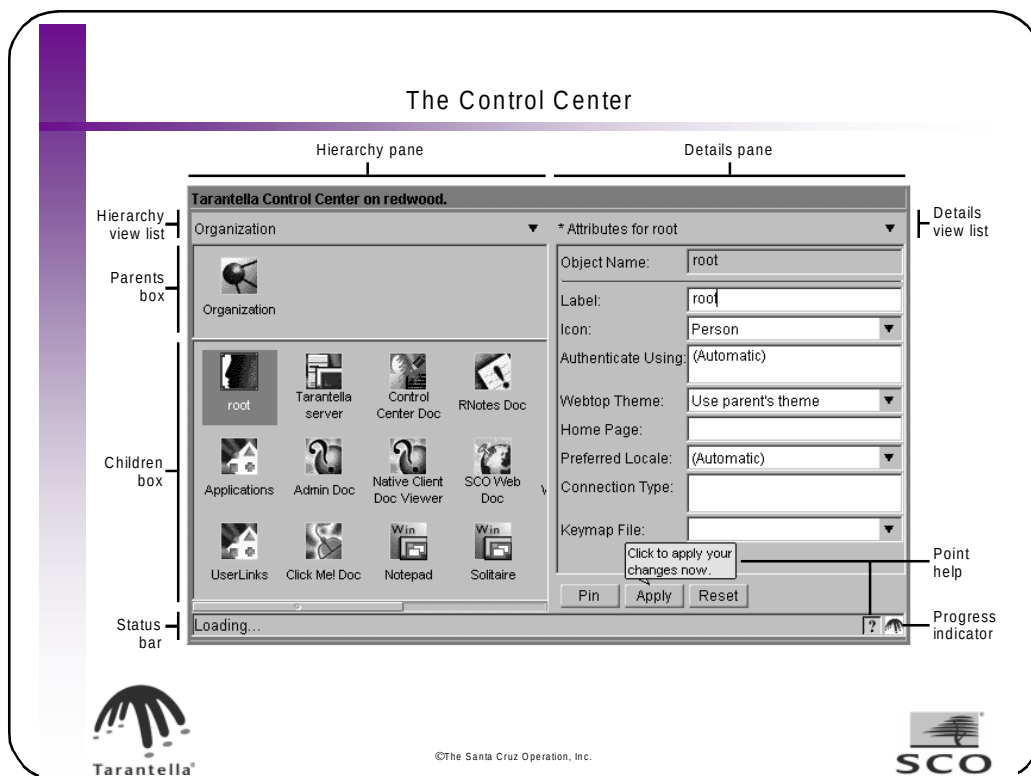
In order to meet these objectives, this lesson discusses:

- Creating objects — Discusses Organizational Unit, Person and Application objects and when to use each.
- Modeling an Organization— Discusses how to use Tarantella's hierarchal structure to implement a model of your organization that is easily administered.
- Administering objects — Discusses using Control Center for creating, moving, deleting objects, modifying security options and session management.

AV 3-1: Modeling an Organization

The first slide describes the overall topics covered in this lesson.

AV 3-2



3.1 Creating Users and Configuring Applications

Tarantella provides an easy to use graphical utility, Control Center, through which you can perform nearly all aspects of Tarantella administration.

3.1.1 Control Center

AV 3-2: Control Center

Use this slide to show the various parts of Control Center utility and their names.

Control Center lets administrators:

Tailor Tarantella to Their Organization	Your organization's resources — people, applications, and documents — are represented by objects in a hierarchy. Use Control Center to create and configure these objects, and structure them in a hierarchy which matches your organization's structure.
Customize Webtops	Use Control Center to configure exactly which links users see on their webtops.
Perform Housekeeping	Use Control Center to keep track of which applications users are running and maintain the password cache.
Configure Servers	Use Control Center to configure options which affect the server as a whole (eg. setting default timeouts or the login theme).

A set of powerful UNIX commands are also available which provide command line equivalents for many Control Center actions.

To run Control Center, simply log into Tarantella as an administrator (eg. the root account) and click on the **Control Center** icon.

Exercise: Running Control Center

Log into Tarantella as root and launch Control Center.

Control-clicking on the Control Center icon instructs Tarantella to launch Control Center in its own web browser

3.1.2 Adding a Tarantella user

Adding a Tarantella user is easy — just right click on the background of the **children box**. You will be presented with a menu. Select **New Object** ⇒ **Person**

Control Center presents a form to be filled out. The fields that need to be filled in include the following:

Object Name	From the user's perspective, the name you set here is the user name that the user will type when logging in. From Tarantella's perspective, this is the name of the object inserted into the Tarantella datastore that will hold all information related to this person.
Label	This is the name that will appear in Control Center on the icon that represents this user.

If the **Label** field is left blank, it defaults to the object name. Users always see the label, not the object name. In the future, the label will be localized with the correct language being displayed.

Authenticate Using	Tarantella has multiple ways of authenticating users: ● Tarantella users are described by a person object in the Tarantella datastore. The Authenticate Using field can be set to one of two values. In the exercise, you set the value to “_user/root”. This instructs Tarantella that when this user logs in, they must authenticate with root's Unix password. This form is used when the Tarantella account name does not match the Unix login name. Alternatively, this field can be set to “(Automatic)”. This instructs Tarantella that the Tarantella account name is the same as the Unix account's name. Again, the user uses the Unix account name when logging into Tarantella. This is used when there is a Unix account whose name exactly matches the Tarantella account name. ● Unix users don't have person objects associated with them. For this type of user, the administrator doesn't create a person object at all. Rather, the user simply logs into Tarantella using their Unix login name and password for their account on the Tarantella server. The Tarantella administrator can enable or disable this feature.
---------------------------	--

- An anonymous user is a user who doesn't have a person object in Tarantella, and doesn't have a Unix account. The Tarantella administrator can enable or disable this feature.

Exercise: Adding a Tarantella User

- | | |
|---------|---|
| Step 1. | In Control Center, right click on the background of the children box. |
| Step 2. | Select New Object ⇒ Person . |
| Step 3. | Type your first name followed by your last name into the Object Name field (eg. John Smith). |
| Step 4. | Type the same name in the Label field. |
| Step 5. | Type “_user/root” in the Authenticate Using field (don't type the double quotes). |
| Step 6. | Click on the Apply button. Be sure to wait until the button letters are grayed out. |
| Step 7. | Log out, then log back into Tarantella using your name and root's password. |

Exercise: Which Type of User Did You Create?

In the previous exercise, you created a user.

What type of user did you create?

A Tarantella user was created.

What password should the user provide when logging in as this user?

The user should provide the root password on the Tarantella server.

Was a person object created for this user.

A person object was created for this user.

Was a Unix account created on the Tarantella server for this new user?

No Unix account was created for this user on the Tarantella server.

3.1.3 Adding an application

Adding an application is just as easy as adding a person — just right click on the background of the **children box**. You will be presented with a menu. Select any of the following:

- **New Object ⇒ SCO Console Application**
- **New Object ⇒ VT420 Application**
- **New Object ⇒ X Application**
- **New Object ⇒ Wyse 60 Application**
- **New Object ⇒ Windows Application**

Installing the Cleo TN3270e connectivity pack adds 3720 applications as a choice in this list. Windows applications, on the other hand, are an available choice whether the Windows Connectivity Pack is installed or not. Adding the WCP provides a new protocol via which to launch Windows applications (ie. RDP through Tarantella)

Exercise: Adding an Application

- | | |
|---------|--|
| Step 1. | In Control Center, right click on the background of the children box. |
| Step 2. | Select New Object ⇒ X Application . |
| Step 3. | Set the Object Name and Label fields to “xeyes”. |
| Step 4. | Set the Application field to “/usr/X/bin/xeyes” (don’t type the double quotes). |
| Step 5. | Click on the Apply button. Be sure to wait until the button letters are grayed out. |

3.1.4 Deploying the application to a user

Before anyone can run the application you just configured, you must first deploy the application to a user.

Exercise: Giving the Application to a User

This exercise assumes that the student is still logged in as their Tarantella user.

- Step 1. Drag-and-drop the icon created in the previous exercise onto your Tarantella person object (ie. the icon with your name).
- Step 2. Log out of Tarantella and log back in. Alternatively, refresh/reload your web browser.
- Step 3. The Launch Pad will now contain a new icon labeled “xeyes”. Click on the icon to launch the application.

3.1.5 The Tarantella datastore

When you add objects such as person objects and applications objects to the organization hierarchy, Tarantella stores this configuration information in the *Tarantella datastore*.

The Tarantella datastore resides in the filesystem on the Tarantella server. The datastore is located in `/var/tarantella/database/database`.

The organization object that appears in the **parents box** in Control Center is stored in the Tarantella datastore as the directory `/var/tarantella/database/database/_ens/Org`.

If you have a person object at the top of the organization hierarchy whose **Object Name** is “root”, there will be a directory called `/var/tarantella/database/database/_ens/Org/root`. The **Object Name** determines the name used for the directory in the Tarantella datastore.

In each of these directories, there is a file called `.object`. This file stores the values for the various attributes you set when creating or modifying an object in Control Center.

Do not modify the `.object` file manually.

Exercise: Exploring the Tarantella Datastore

Change directories to `/var/tarantella/database/database/_ens/Org` and compare what you see in the directory (and its subdirectories) to what you see in Control Center.

You might show students how to examine the `.object` files using the `hd` command.

Exercise: Tarantella Federated Names

In the *Admin Guide*, read **Reference** ⇒ **Miscellaneous information** ⇒ **The Tarantella datastore and TFN names**. In particular, read the section which explains how a user can be identified by a Tarantella Federated Name.

3.2 Modeling an Organization

Now that you understand the basics of how administrators create Tarantella users and applications, we will discuss how to arrange these objects so that they best match your organization. Chances are that your “organization” is your company.

3.2.1 Hierarchal structure

In the preceding exercises, you created a person object and an application object. Both of these we deposited into the **children box**. While this works well for small numbers of such objects, it becomes unwieldy when working with larger numbers of objects.

Tarantella stores all of these objects in a *hierarchy*.

Later we’ll learn about a feature called *marks* which make it easier to work with large numbers of objects in the **children box**. But there is a more fundamental problem that marks alone can’t solve: Depositing all of the objects into the same place will make it extremely inefficient when deploying select applications to large numbers of users.

Just as dividing a company into multiple departments or divisions enables the company to run more efficiently, Tarantella’s *Organizational Units* enable the Tarantella administrator to group the various person and application objects into a more easily administered structure.

 Analogy: The various objects (eg. person, application, document, etc.) you create in Control Center are like *files* in a filesystem. Organizational Units, on the other hand, are like *directories* in a filesystem.

Exercise: Creating a Hierarchy

Step 1. In Control Center, create four new person objects.

The students can use whatever names they want. Furthermore, they can authenticate to whatever Unix account they want.

Step 2. Right click on the **children box**.

Step 3. Select **New Object** ⇒ **Organizational Unit**.

Step 4. Set the **Object Name** and **Label** fields to “San Francisco” (don’t type the double quotes).

Step 5. Click on the **Apply** button. Be sure to wait until the button letters are grayed out.

Step 6. Repeat steps 2 through 5 to create an organizational unit called “Santa Cruz” (don’t type the double quotes).

Step 7. Drag-and-drop two of the person objects you created in step 1 onto the “Us” icon. Drag-and-drop the other two person objects you created onto the “San Francisco” icon.

Step 8. Examine the contents of “San Francisco” by clicking the its icon. Notice that the **parents box** expands to include the “San Francisco” icon. Additionally, the **children box** contents are replaced with the contents of the “San Francisco” organizational unit’s contents.

Step 9. To back out of the “San Francisco” organizational unit, click on the “Organization” icon in the **parents box**.

Step 10. Repeat steps 8 and 9 examining the contents of the “Santa Cruz” organizational unit. Notice that its contents are different from the “San Francisco” organizational unit’s contents.

By creating these organizational units, you have given Tarantella a more hierarchal structure. By nesting organizational units, you can create a tree-like structure that mimics your own organization. Organizational units can be based on geography, departments, or any other categorization you choose.

3.2.2 Inheritance

Objects deeper in the tree inherit the properties and attributes of the objects above.

Exercise: Understanding Inheritance

Step 1. Log out and log into Tarantella as one of the newly created Tarantella users in the “Us.” organizational unit.

Step 2. Examine the applications available on the Launch Pad.

You did not give these applications to the user. How did the user end up with these applications on their Launch Pad? The answer is inheritance.

Step 3. Log back in as a Tarantella administrator and see if you can understand how the user ended up with the applications that appeared on their desktop.

Explain to the students exactly how the user ended up with these applications. Make sure students understand that they may receive applications (and other attributes) from the organization object or organization unit objects.

In general, Tarantella administrators on large systems don’t give applications to particular users. This approach becomes unwieldy with large numbers of users. Instead they create organizational units, place users in the those organization units, and then give applications to the organizational units.

Make sure students understand this point. Explain that they need to remove any applications from the organization’s webtop that they don’t want *everyone* to receive.

3.2.3 The home page attribute

In addition to deploying applications onto a user's webtop, the Tarantella administrator can place an icon for an *organizational unit* or a *person* onto the user's webtop. Instead of launching an application, clicking on the resulting webtop icon will display the web page specified in the organizational unit or person's **Home Page** attribute. This provides an easy means for the Tarantella administrator to inform other users on the system about the various organizational units and people on the system.

For those familiar with the old-fashioned **finger** command in Unix, this is analogous. Unlike **finger** which only knows about users, the **Home Page** attribute lets the Tarantella administrator provide information about people *and* organizational units.

When you drag-and-drop an application object onto a person object, you are *deploying* the application to that person's webtop. Clicking on the resulting webtop icon launches the application.

When you drag-and-drop an application object onto an organizational unit object, you are *deploying* the application to webtops of users in that organizational unit. Again, clicking on the resulting webtop icon launches the application.

On the other hand, when you drag-and-drop a person object onto an organizational unit, you are *moving* the person into the organizational unit. Clicking on the resulting webtop icon does not launch an application. Rather, it displays the specified home page.

You cannot move an organizational unit into another using the drag-and-drop method. Instead, you must be in the organizational unit where you want to create the embedded organizational unit.

Moving a person object into an organizational unit does not place the person on the webtop of the users in that organizational unit. To place a person object on the webtop of the users in an organization unit, you must right click the organizational unit's object, select **Webtop**, then drag-and-drop the person object onto the **details pane**. The same is true for placing an organizational unit object.

Demonstrate the home page attribute to the students. Students understand the home page attribute best when they see it demonstrated.

3.3 Creating Objects in Tarantella

Section 3.1.2 and Section 3.1.3 showed how to create user accounts and applications in Tarantella. In the sections which follow, we re-visit creating person and application objects. Additionally we introduce a new type of object: the document object.

For information about all of the object types supported by Tarantella, read the following article in the *Admin Guide*: **Introduction** ⇒ **Control Center** ⇒ **Type of object**.

3.3.1 Adding a user

In addition to the attributes we set on person objects earlier (Section 3.1.2), Tarantella administrators often change the following attributes:

Webtop theme:

This attribute determines which webtop theme is displayed for a particular user. Tarantella provides the following five choices:

- Standard
- Standard (no icons)
- Horizontal
- Maximum display area
- Use parent's theme

The first four choices are actual webtop themes. Webtop themes control the appearance of the user's webtop. You will see each of these webtops in the following exercise.

"Use parent's theme" instructs Tarantella to set the user's webtop theme to whatever its parent's webtop theme is.

Connection Type:

With the Tarantella Security Pack installed, administrators can enable secure SSL connections on a per-user, per-organizational unit, or organization-wide basis. This will be discussed at length in Lesson 6: "The Tarantella Security Pack."

Exercise: Setting the Webtop Theme

- Step 1. In Control Center, click the icon for the person object corresponding to the Tarantella account that you are currently logged into.
- Step 2. Change the **Webtop Theme** attribute to “Standard”.
- Step 3. Click on the **Apply** button. Be sure to wait until the button letters are grayed out.
- Step 4. Log out and log back in. Alternately, refresh/reload your web browser.
- Step 5. The appearance of the webtop should not have changed (assuming you’re not already leaping ahead of the instructor now that you’ve got the hang of Control Center).
- The webtop didn’t change because this user’s webtop theme already was “Standard”. The webtop theme was being determined from its parent.
- Step 6. Change your user’s webtop theme to “Standard (no icons)”.
- Step 7. Refresh/reload your web browser.
- Step 8. Observe the difference in the webtop appearance.
- Step 9. Repeat step 6 through step 8 using “Horizontal” and “Maximum display area” for the webtop theme.

3.3.1.1 Duplicate user names

What happens when two (or more) Tarantella users have the same user name? If the users have different passwords, then Tarantella determines which user to log in as based on the password supplied. If, on the other hand, the users have the same password, the user will be prompted with a combo box on the login screen which allows the user to specify which user they want to log in as.

 It's not entirely clear to some users that this is a combo box. Set this up for yourself to see what the pull down looks like and you'll see why it's unclear.

3.3.1.2 Other types of users

By default, users must have person objects to log into Tarantella. It is not necessary to create Tarantella person objects for everyone who connects to Tarantella. For that matter, it's not even necessary to have a Unix account. There are two types of users that can use Tarantella without the administrator having to create person objects: Unix users and anonymous users.

Unix users

Administrators can configure Tarantella to allow users to log into Tarantella using a unix account name and password. The only configuration necessary to allow this form of authentication is to enable this feature in Control Center by checking **Server** ⇒ **Security** ⇒ **Allow UNIX Login**.

■ Remind students, if necessary, to get to **Server** via the hierarchy view list.

By default, Unix users belong to the top-level organization. This can be changed by creating an organizational unit anywhere in the tree and setting **Server** ⇒ **Access** ⇒ **UNIX Users' OU** to point to the organizational unit's full object name.

All Unix users receive the same webtop and applications.

Exercise: Allowing Unix User Logins

- Step 1. Configure Tarantella to allow Unix user logins:
- Select **Server** in the Hierarchy View List menu.
 - Click on the **Security** object.
 - Check the **Allow Unix Login** box.
- Step 2. Create an organizational unit for Unix users:
- Select **Organization** in the Hierarchy View List menu.
 - Right click the background of the **children box**.
 - Select **New** ⇒ **Organizational Unit**.
 - Set the **Object Name** and **Label** attributes to “Unix Users” (don’t type the double quotes).
 - Click on the **Apply** button. Be sure to wait until the button is grayed out.
- Step 3. Drag-and-drop the xterm application object onto the Unix Users organizational unit.
- Step 4. Configure Tarantella so that the Unix Users organizational unit is used by Unix users:
- Select **Server** in the Hierarchy View List menu.
 - Click on the **Access** object.
 - Set the **Unix Users’ OU** attribute to the TFN for the Unix Users organizational unit: **.../_ens/Org/Unix Users**
- Step 5. Log out of Tarantella and log back in as a Unix user.
- Step 6. Observe that you can now log in as a Unix user and that the administrator can control what applications Unix users receive.

Anonymous users

When anonymous users login, they don't authenticate with a user name and password. All an anonymous user needs to do to login is to click on the login screen's "Ok" button.

To enable anonymous access, check **Server** ⇒ **Security** ⇒ **Allow Anonymous Login**. Additionally, for added manageability, create a separate Organizational Unit for Anonymous users and change the **Server** ⇒ **Access** ⇒ **Anonymous Users' OU** to that Organizational Unit.

An anonymous user logs in by using a slightly different URL:

<http://server/tarantella/kiosk.html>

where *server* is the name of the Tarantella server.

An anonymous user is given a random name each login. Therefore, features like Session Resumability will not work.

All anonymous users receive the same webtop content.

Exercise: Allowing Anonymous User Logins

- Step 1. Configure Tarantella to allow anonymous user logins:
- Select **Server** in the Hierarchy View List menu.
 - Click on the **Security** object.
 - Check the **Allow Anonymous Login** box.
- Step 2. Create an organizational unit for anonymous users:
- Select **Organization** in the Hierarchy View List menu.
 - Right click the background of the **children box**.
 - Select **New** ⇒ **Organizational Unit**.
 - Set the **Object Name** and **Label** attributes to “Anonymous Users” (don’t type the double quotes).
 - Click on the **Apply** button. Be sure to wait until the button is grayed out.
- Step 3. Drag-and-drop the xclock application object onto the Anonymous Users organizational unit.
- Step 4. Configure Tarantella so that the Anonymous Users organizational unit is used by Unix users:
- Select **Server** in the Hierarchy View List menu.
 - Click on the **Access** object.
 - Set the **Anonymous Users’ OU** attribute to the TFN for the Anonymous Users organizational unit:
.../_ens/Org/Anonymous Users
- Step 5. Log out of Tarantella and log back in as a Unix user.
- Step 6. You can now log in as an anonymous user and the administrator can control what applications anonymous users receive.

3.3.1.3 Tarantella administrators

At installation, root is given administrative rights for Tarantella. Other users can be granted administrative rights. To grant these rights to a user, right click the organization icon in the **parents box** and select **Administration**. The details pane on the right will show the users who are Tarantella administrators. Simply drop a person object onto the details pane to make them a Tarantella administrator.

Students might want to consider making another account that acts as a fallback in case they inadvertently lock themselves out of the root account.

3.3.2 Adding an application

In addition to the attributes we set on application objects earlier (Section 3.1.3), Tarantella administrators often change the following attributes:

Arguments: Many programs require arguments (eg. to specify file names, command line options, etc.). In the application object, you can pass in such arguments via the **Arguments** attribute.

Environment: Unix application objects (eg. SCO Console Application, X Application, etc.) allow you to pass in environment variables through the **Environment** attribute.

Display using: This attribute determines how applications are launched. Choices include:

- **Webtop**
- **New browser window**
- **Independent window**
- **Client window management**

You will see the differences between these in the next exercise.

Resumable: Tarantella allows three choices for application resumability:

- **Always** instructs Tarantella that the application keeps running even after the user logs out and can be resumed when they next log in.
- **Tarantella Session** instructs Tarantella that the application runs until the user logs out of Tarantella.
- **Never** instructs Tarantella that a new instance of the application is launched whenever the application's icon is clicked. The application is not resumable.

Exercise: Displaying Applications

- Step 1. Create a new X application object which runs /usr/X/bin/puzzle. Set the **Display Using** attribute to “Webtop”.
- Step 2. Give the application to a user
- Step 3. Log in as that user. Alternatively, just give the application to yourself and refresh/reload your web browser so that you don’t have to continuously log out and log back in.
- Step 4. Launch the application and observe how it is displayed.
- Step 5. Modify the **Display Using** attribute to “New browser window”.
- Step 6. Log out and log back in (or refresh/reload your web browser if you gave the application to yourself).
- Step 7. Launch the application again. Observe how it is displayed.
- Step 8. Repeat steps 5 through 7 setting the **Display Using** attribute to “Independent window” and “Client window management”.

3.3.3 Document objects

Document objects represent documents which you want to make available to users. Tarantella makes distributing these easy. Distributing a document simply consists of creating a **document object** which contains the URL pointing to the document.

Exercise: Distributing a Document

By now you should be getting the hang of administering Tarantella through Control Center. Create a document object. Set the **URL** attribute to the URL of a document you would like to make available to users (for example, <http://www.sco.com>). Don't forget to give this document to a user! Log in as that user and you will see the document on the user's Launch Pad.

Examine the URL associated with the **Click Me!** document. Notice that this document doesn't have a web address. Rather, it displays a document contained in the Tarantella datastore itself.

 In addition to URLs pointing to HTML documents, document objects can point to .txt files, .pdf files, etc.

3.3.4 Host and Host Group objects

Objects of these types are used in conjunction with Tarantella load balancing. These objects will be discussed in Lesson 7: "Tarantella Load Balancing."

3.4 Moving Objects

Thus far, you have configured Tarantella by dragging-and-dropping objects. This method becomes unwieldy when dealing with large numbers of objects or large hierarchies. As an alternative to the drag-and-drop method, you can *mark* objects that you want to move, making this process even easier than dragging-and-dropping.

To mark an object, simply right click the object and select **Mark**.

To move the marked object:

- Step 1. Right click on the object where you want to move the marked object
- Step 2. Select **Webtop**.
- Step 3. Right click in the details pane and select **Marks**, followed by the object you marked.

Using this same method, you can mark multiple objects and move all of them by selecting **Marks** ⇒ **Add all to webtop** from the menu that appears when you right click the target object's webtop.

What can be moved and where it can be moved depends on the object type.

- Applications can be moved onto Persons, Groups and Organizational Units
- Persons can be moved onto organizations
- Hosts can be moved onto Host Groups
- Host Groups can be moved onto Application Webtops
- Organizational Units can be moved onto other Organizational Units

The on-line documentation says that Organizational Units can be dropped onto other Organizational Units, but this appears to be false. This behavior was allowed in earlier versions of Tarantella.

When an object is moved to another Organizational Unit, the object will become a child of the new organization and not the previous organization. The object will disappear from the **Children View** of the previous Organizational Unit.

3.5 Trash

In Control Center, objects are deleted by right-clicking the object and selecting **Delete**. However, deleting an object doesn't actually remove it. Rather, the object is moved to an area of Control Center called **Trash**.

To view the trash:

- Step 1. Click on the **Default view list** menubar and select **Trash**.
- Step 2. The **Details pane** will display the trash.
- Step 3. From the **Details pane** the objects can be permanently deleted by right clicking the object and selecting "delete".

3.6 Lesson Summary

This lesson discussed how Tarantella can be configured to model the organization where Tarantella is being deployed. This is done in Tarantella by manipulating *objects* using Control Center. Objects discussed included person objects, application objects, group objects, and document objects.

Additionally this lesson discussed Unix users and anonymous users and creating other Tarantella administrators.

3.7 Review questions

1. What tasks does Control Center enable Tarantella administrators to perform?

Control Center enables Tarantella administrators to tailor Tarantella to their organization, customize webtops, perform housekeeping tasks, and modify server configuration settings.

2. What is the purpose of the **Authenticate Using** attribute in person objects?

The Authenticate Using attribute in person objects enables Tarantella administrators to specify to which Unix user account, if any, a particular Tarantella user authenticates.

3. How does Tarantella simplify administration tasks for administrators of large Tarantella servers?

Tarantella allows administrators to organize objects into a hierarchy.

4. What three types of users does Tarantella allow?

Tarantella allows Tarantella users (ie. users for whom a Tarantella person object exists), Unix users (ie. users who have a Unix account but no corresponding Tarantella person object), and anonymous users.

5. How can you make a user an administrator?

You make a user an administrator by right clicking the organization icon in the **parents box**, selecting **Administration**, and drag-and-dropping the user's person object onto the details pane.

6. How do you pass environment variables into applications launched by Tarantella?

You can set environment variables for particular applications by setting that application object's **Environment** attribute.

7. What happens if you delete an object in Control Center?

When you delete an object in Control Center, it is moved to the trash. To actually completely remove the object, you must delete the object from the trash.

3.8 Lab: Configuring Tarantella

This lab has students create numerous person objects and organizational units. If time is short, you can have the students create only a subset of these.

If students create the CDE application object, have students check the CDE application object's **View Host Reply** button and set **Session Ends When** to "Login script completes".

In this lab, you will configure Tarantella for our hypothetical company, Example Company, Inc. This will involve modeling the company in the Tarantella hierarchy, creating person objects, application objects, and organizational units.

3.8.1 Overview

Our hypothetical company, Example Company, Inc., is spread across two geographies:

- North America
- Europe

There are three departments:

- Sales
- Engineering
- Manufacturing

Sales and Engineering are located in North America. Manufacturing, on the other hand, is located in Europe.

The following table details the employees in each department and the login and password for their Unix accounts:

Table 3: Employees and Their Departments

Employee Name	Unix Account Login	Unix Account Password	Department Name
John Stratford	jstratford	apple	Manufacturing
Peter Larson	plarson	banana	Engineering
Suzy Quinn	squinn	cherry	Engineering
Mark Patton	mpatton	date	Sales
John Smith	jsmith	alpha	Sales
Alison McDonald	amcdonald	beta	Engineering
John Smith	johns	gamma	Manufacturing
Samantha Sharp	ssharp	delta	Manufacturing
Tammy Jones	tjones	aardvark	Sales
Julie King	jking	baboon	Sales

The following table details which applications need to be deployed to each department:

Table 4:

Department	Applications	Location
Engineering	X Windows calculator Xedit text editor Real Time Performance Monitor	/usr/X/bin/xcalc /usr/X/bin/xedit /usr/sbin/rtpm
Sales	CDE Desktop Windows calculator "Notepad" text editor	/usr/dt/bin/dtsession c:\windows\calc.exe c:\windows\notepad.exe
Manufacturing	"Notepad" text editor Windows calculator	c:\windows\notepad.exe c:\windows\calc.exe

In addition to the applications above, Peter Larson has requested that he be given the vi text editor (/bin/vi).

Your tasks in this lab are:

- Design a hierarchy that represents this company.
- Implement this hierarchy by creating organizational units and person objects as necessary.
- Create any Tarantella users, Unix users, or anonymous users as necessary. When users log in, they must be able to do so with their full name rather than their Unix account name. For example, John Stratford would log in as “John Stratford” rather than “jstratford”.

■ The users should only create Tarantella users.

- Deploy the applications listed in Table 5. Consult with your instructor if you aren’t certain which type of application object to create for each application.

3.8.2 Procedure

■ These labs are designed to be performed under UnixWare 7.1.0.

Part I: Create the Organizational Units

In Control Center, create two organizational units, “North America” and “Europe” as follows:

- | | |
|---------|--|
| Step 1. | Click on the organization in the parents box to work your way to the top of the tree. |
| Step 2. | Right click on the background of the children box . Select New Object ⇒ Organizational Unit . |
| Step 3. | Set the Object Name and Label to “North America” (don’t type the double quotes). |
| Step 4. | If desired, change the Icon to one of your choosing. |
| Step 5. | Click on the Apply button. Be sure to wait until the button letters are grayed out. |
| Step 6. | Click on the “North America” object that you just created. Notice that the parents box changes is updated to show that you have gone into the North Americal organizational unit. |

- Step 7. Right click on the background of the **children box** and select **New Object** ⇒ **Organizational Unit**.
- Step 8. Set the **Object Name** and **Label** to “Sales” (don’t type the double quotes).
- Step 9. If desired, change the **Icon** to one of your choosing.
- Step 10. Click on the **Apply** button. Be sure to wait until the button letters are grayed out.
- Step 11. Right click on the background of the **children box** and select **New Object** ⇒ **Organizational Unit**.
- Step 12. Set the **Object Name** and **Label** to “Engineering” (don’t type the double quotes).
- Step 13. If desired, change the **Icon** to one of your choosing.
- Step 14. Click on the **Apply** button. Be sure to wait until the button letters are grayed out.
- Step 15. Click on the Organization in the **parents box** to work your way back to the top of the tree.
- Step 16. Repeat the steps above to create the “Europe” and “Manufacturing” organizational units.

Part II: Create the Users

Under Unix, create *Unix* user accounts for each of the Tarantella users in Table 4. How user accounts are created varies from one Unix platform to another, so you will have to read the documentation for your particular version of Unix. A good place to start looking would be to issue the following command:

```
# man -k user | more
```

Consult your instructor if you require help creating the Unix accounts.

 In UnixWare 7.1.0, students can use **scoadmin** ⇒ **account** or **useradd(1M)**.

Create the *Tarantella* person objects as follows:

- Step 1. Click on the organization in the **parents box** to work your way to the top of the tree.

- Step 2. Click on the “Europe” organizational unit in the **children box**.
- Step 3. Click on the “Manufacturing” organizational unit in the **children box**.
- Step 4. Right click on the background of the **children box**, and select **New Object** ⇒ **Person**.
- Step 5. Set the **Object Name** and **Label** attributes to “John Stratford” (don’t type the double quotes).
- Step 6. Assuming that the Unix account that you created for John Stratford is called “johns”, set **Authenticate Using** to “_user/johns” (don’t type the double quotes).
- Step 7. If desired, change the **Icon** and **Webtop Theme** to one of your choosing.
- Step 8. Click on the **Apply** button. Be sure to wait until the button letters are grayed out.
- Step 9. Repeat these steps for each Tarantella user. Be sure to place each user in the organizational unit indicated by Table 4.

Part III: Create and Deploy the Applications

- Step 1. Click on the organization in the **parents box** to work your way to the top of the tree.
- Step 2. Click on the “North America” organizational unit in the **children box**.
- Step 3. Click on the “Engineering” organizational unit in the **children box**.
- Step 4. Right click on the background of the **children box** and select **New Object ⇒ X Application**.
- Step 5. Set the **Object Name** and **Label** attributes to “X Calculator”.
- Step 6. Set the **Icon** and **Display Using** attributes as you see fit.
- Step 7. Set the **Application** attribute to the pathname of xcalc (ie. */usr/X/bin/xcalc*).
- Step 8. Click on the **Apply** button. Be sure to wait until the button is grayed out.
- Step 9. Repeat the steps above for each of the applications listed in Table 5. Don’t forget that John Stratford wants */bin/vi* in addition to the applications he receives as a member of the Manufacturing department.
- NOTE: For Windows applications, set the **Windows Protocol** attribute to “none” (don’t type the double quotes) and check the **Try Local Application** box. This will cause Tarantella to launch the application on the client machine — assuming it exists on the client — rather than on a third tier application server. We will learn how to run Windows applications on third tier servers in Lesson 8: “Windows Connectivity Pack.”

Part IV: Testing Your Work

Once you’ve set up your Tarantella hierarchy, test that you’ve succeeded:

- Check that you can log in as each user. Be sure to use the *Tarantella* user name.
- Check that each user receives the right applications.
- Verify that Peter Larson received */bin/vi* in addition to the applications he receives as a member of the Manufacturing department.

3.9 Answers to Exercise and Review Questions

This section contains the answers to exercises, review questions, and labs presented in this lesson.

Exercise answers

“Which Type of User Did You Create?,” on page 3-13

- What type of user did you create?
A Tarantella user was created.
- What password should the user provide when logging in as this user?
The user should provide the root password on the Tarantella server.
- Was a person object created for this user.
A person object was created for this user.
- Was a Unix account created on the Tarantella server for this new user?
No Unix account was created for this user on the Tarantella server.

Consult your instructor if you have any questions about any of the other exercises in this lesson.

Review Question Answers

This section contains the answers to the review questions on page 3-35.

1. Control Center enables Tarantella administrators to tailor Tarantella to their organization, customize webtops, perform housekeeping tasks, and modify server configuration settings.
2. The Authenticate Using attribute in person objects enables Tarantella administrators to specify to which Unix user account, if any, a particular Tarantella user authenticates.
3. Tarantella allows administrators to organize objects into a hierarchy.

4. Tarantella allows Tarantella users (ie. users for whom a Tarantella person object exists), Unix users (ie. users who have a Unix account but no corresponding Tarantella person object), and anonymous users.
5. You make a user an administrator by right clicking the organization icon in the **parents box**, selecting **Administration**, and drag-and-dropping the user's person object onto the details pane.
6. You can set environment variables for particular applications by setting that application object's **Environment** attribute.
7. When you delete an object in Control Center, it is moved to the trash. To actually completely remove the object, you must delete the object from the trash.

4

The Tarantella Native Client

Instructor Guide

Instructor Guide

Lesson 4

The Tarantella Native Client

Suggested lesson duration

This lesson should take approximately .5 hours to complete including the exercise. There is no lab. Instead, students install and use the Native client in the exercises.

Pre-lesson classroom preparation

The students must have Windows clients, and there must be at least one Tarantella server for the students to log into via the Native Client.

Instructor preparation

Read the following articles in the Admin Guide:

How to... ⇒ Getting users started ⇒ To make the Tarantella Native Client available

How to... ⇒ Getting users started ⇒ To allow native client users to display documents

Introduction

Certain web browsers do not support Tarantella well due to their implementation of Java™. Tarantella provides a Native Client which can be used in place of the web browser. This lesson discusses the installation and use of the Native Client.

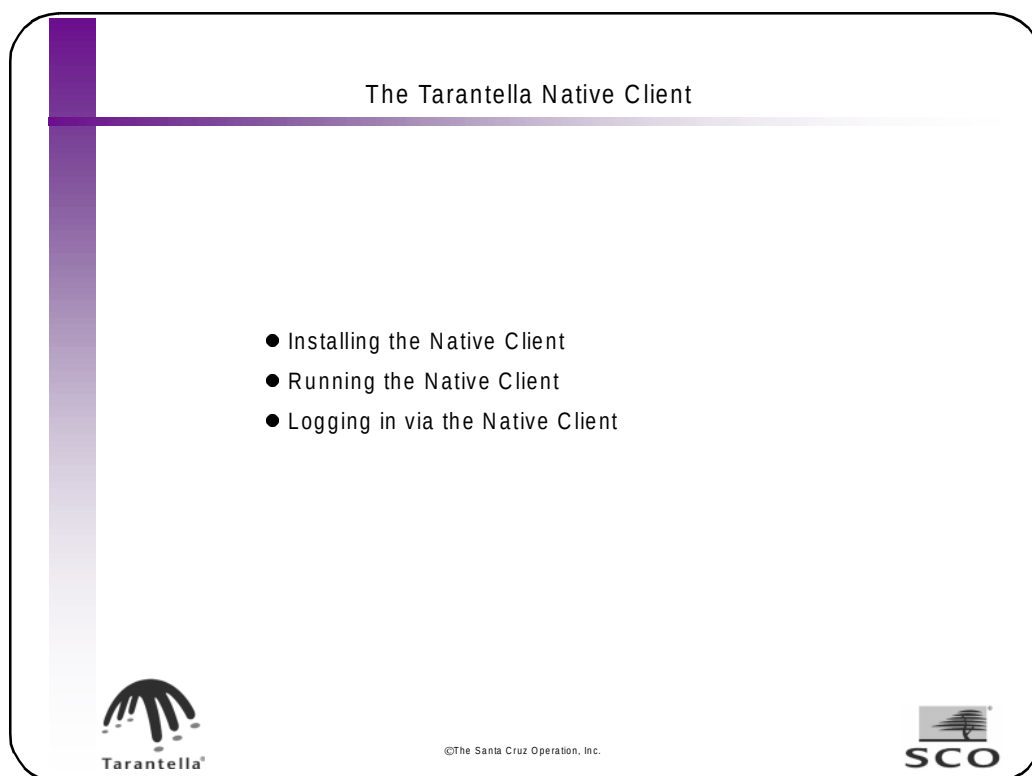
In reality, Tarantella provides more than one Native Client (eg. the 16bit version for Windows 3.1 versus the 32bit version for Windows 95/98/NT).

Objectives

By the end of this lesson, you will be able to:

- Install the Tarantella Native Client on Windows 3.1, 95, 98, or NT
- Run the Native Client
- Connect to Tarantella via the Native Client

AV 4-1



Topics

In order to meet these objectives, this lesson discusses:

- Installing the Native Client— Discusses how to install the Tarantella Native Client.
- Running the Native Client — Discusses how to invoke the Tarantella Native Client.
- Logging in via the Native Client— Explains how to log into a Tarantella server via the Tarantella Native Client.



AV 4-1: Installing Tarantella

The first slide describes the overall topics covered in this lesson.

4.1 The Tarantella Native Client

The Tarantella Native Client enables users to access Tarantella without the need for a Java enabled web browser.

4.1.1 Why does the Native Client exist?

Not all operating systems support Java equally well. For operating systems such as Windows 3.1, supporting Java is problematic at best. Native clients are created on an as-needed basis for the various platforms that Tarantella supports.

Benefits of the Native Client include:

- It needn't be installed on the client itself

That is, you can take the binary, put it on a file server, and let users access it via the network.

- It enables users to use the webtop without requiring a Java enabled web browser
- It works with the Tarantella Security Pack
- It is useful as a “control subject” when troubleshooting
- It is easy to install

4.1.2 Installing the Tarantella Native Client

To install the Native Client, point your web browser to the following URL:

<http://server/tarantella/cgi-bin/install.cgi>

Once on this page, select from either of the following two choices:

16-bit Tarantella Native Client for Windows 3.1

32-bit Tarantella Native Client for Windows 95, 98, NT server, and NT workstation

In Netscape Navigator®:

Step 1. Right click one of the hypertext links.

Step 2. Select “Save Link As...”.

NOTE: There is a known issue with the Netscape FastTrack Server that causes the above procedure to fail. If you are running Netscape FastTrack as your web server and are experiencing problems downloading the Native Client, review the following article in the **Release Notes: Tarantella Express for SCO UnixWare 2.1.2+ or UnixWare 7+**.

To quote the Tarantella Release Notes:

“By default, Netscape web servers treat files with “.exe” extensions as CGI programs to run on the server, rather than files to download to the client. To allow users to download the Tarantella Native Client, you should ensure your web server is configured correctly. You need to edit your web server's *mime.types* file (in the */usr/ns-home/httpd-80/config* directory in UnixWare 7), to remove “exe” as an extension for the “magnus-internal/cgi” type, and add it as an extension for the “application/octet-stream” type.”

After making these modifications, you must restart the Netscape FastTrack server.

In Microsoft Explorer:

Step 1. Right click one of the hypertext links above.

Step 2. Select “Save Target As...”.

This will download a file called either *ttawin16.exe* or *ttawin32.exe*, depending on which hypertext link you click on. These files are self extracting archives. Execute the file you downloaded.

If the Tarantella Security Pack is installed, the names of these files will be *tspwin16.exe* and *tspwin32.exe*.

AV 4-2

Logging into Tarantella via the Native Client

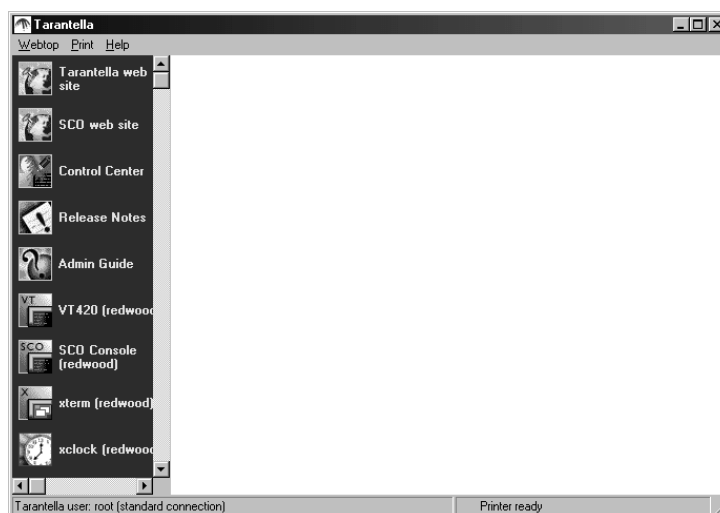


©The Santa Cruz Operation, Inc.



AV 4-3

The Tarantella Native Client Webtop



©The Santa Cruz Operation, Inc.



4.1.3 Running the Native Client

Under Windows 95, 98 or NT, you can execute the resulting binary (ie. the Native Client binary) by selecting:

Start ⇒ Programs ⇒ Tarantella ⇒ Tarantella Native Client

4.1.4 Logging into the Native Client

To log into Tarantella via the Native Client, fill out the login screen shown in AV 4-2. Supply a fully qualified host name, the Tarantella user name, and the password for that user.

AV 4-2: Logging into the Webtop via the Native Client

Use this slide to illustrate logging into Tarantella via the Native Client

The webtop is displayed in the Native Client as shown in AV 4-3.

AV 4-3: .The Tarantella Native Client Webtop

Use this slide to illustrate the webtop under the Native Client. Give a quick demo of the Native Client.

4.1.5 Native Doc Viewer

Tarantella's Control Center utility is a Java applet. Therefore the Native Client cannot run it. In situations like this, the Native Client will automatically invoke the client machine's registered web-browser, if any.

To configure which web browser is launched, in the **Admin Guide**, read **How to... ⇒ Get users started ⇒ To allow native client users to display documents**.

Exercise: Installing the Native Client

Install the Native Client on your client machine (modifying your Netscape web server configuration if necessary). Log into Tarantella via the Native Client.

4.2 Lesson Summary

This lesson described how to install, run, and log in via the Tarantella Native Client. The lesson also discussed a problem related to Netscape's FastTrack server and Tarantella.

4.3 Review questions

1. How do you download the Native Client?

The Native Client is installed as part of the base Tarantella installation. You can install the Native Client by visiting the following URL: `http://server/tarantella/cgi-bin/install.cgi`, where *server* is the name of your Tarantella server.

2. Does the Native Client have to be installed on the clients themselves?

No, the Native Client does not have to be installed on the clients themselves. The Native Client can be made available via a file server accessible to the clients.

3. Does the Native Client work in conjunction with the Tarantella Security Pack?

Yes, the Native Client does work in conjunction with the Tarantella Security Pack.

4.4 Answers to Exercise and Review Questions

This section contains the answers to exercises, review questions, and labs presented in this lesson.

Exercise answers

Please consult your instructor if you have any questions about the exercises in this lesson.

Review Question Answers

This section contains the answers to the review questions on page 4-13.

1. The Native Client is installed as part of the base Tarantella installation. You can install the Native Client by visiting the following URL: *http://server/tarantella/cgi-bin/install.cgi*, where *server* is the name of your Tarantella server.
2. No, the Native Client does not have to be installed on the clients themselves. The Native Client can be made available via a file server accessible by the clients.
3. Yes, the Native Client does work conjunction with the Tarantella Security Pack.

5

Printing under Tarantella

Instructor Guide

Instructor Guide

Lesson 5

Printing under Tarantella

Suggested lesson duration

This lesson should take approximately 2.0 hours to complete including the lab.

Pre-lesson classroom preparation

There must be at least one Unix server and one Windows server, each of which needs a configured printer.

Instructor preparation

Read the following articles in the *Admin Guide*:

How to... ⇒ Add a Tarantella Printer

Troubleshooting and Diagnostics ⇒ Printing ⇒ Configuring application servers for printing

Introduction

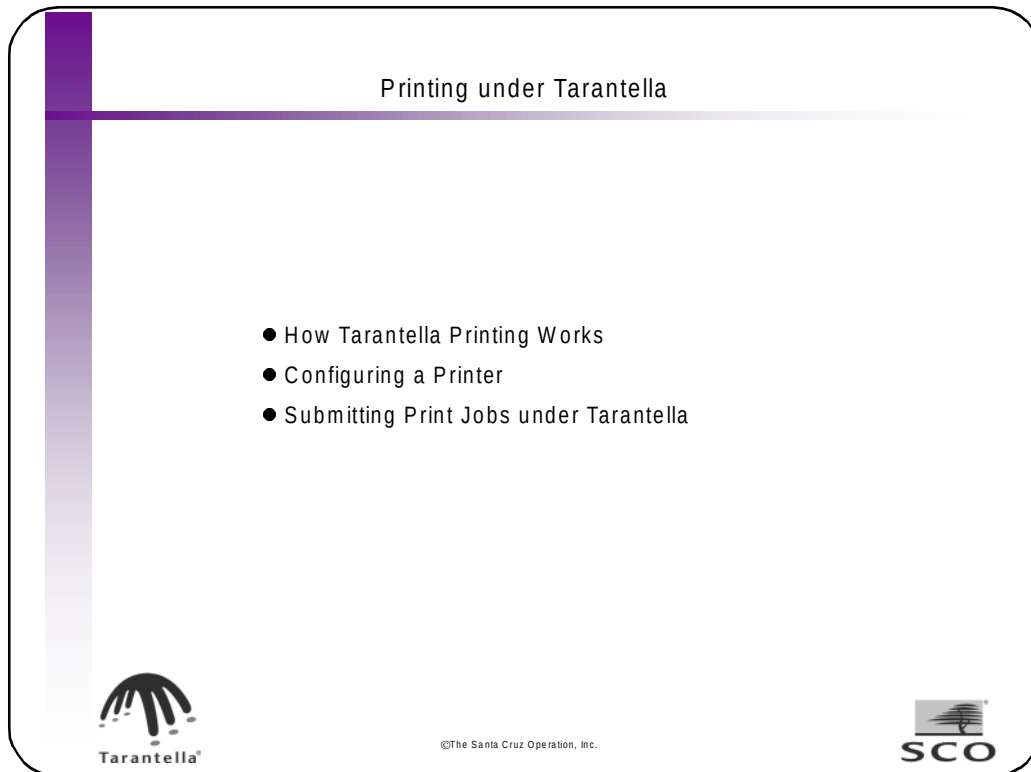
Tarantella's "Follow Me Printing" feature enables users to print from applications running on an application server onto the default printer on the client. In this chapter, we explore how this feature works and how you configure your servers to use it.

Objectives

By the end of this lesson, you will be able to:

- Add a Tarantella printer to a Unix application server
- Add a Tarantella printer to a Windows application server
- Print under Tarantella

AV 5-1



Topics

In order to meet these objectives, this lesson discusses:

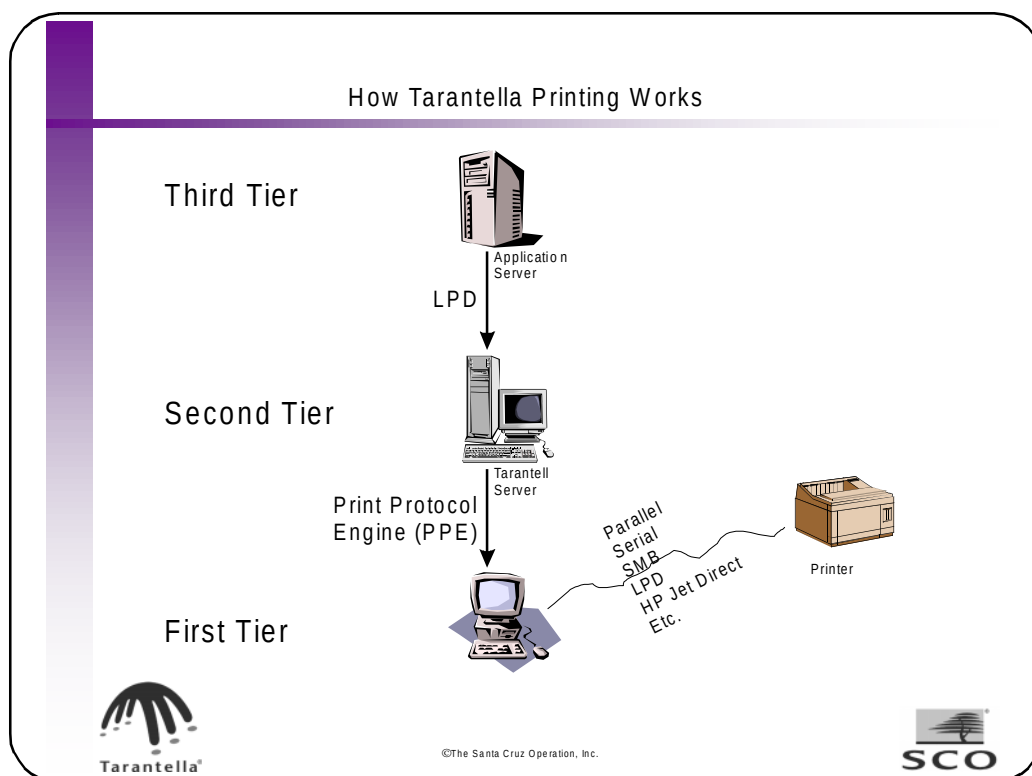
- How Tarantella Printing Works — Discusses how Tarantella gets print jobs submitted on application servers to the client's default printer.
- Configuring a Printer — Discusses how to configure a printer under Tarantella.
- Submitting Print Jobs under Tarantella — Explains how to print from Unix or Windows servers under Tarantella.



AV 5-1: Printing under Tarantella

The first slide describes the overall topics covered in this lesson.

AV 5-2



Instructor Guide

5.1 How Tarantella Printing Works

AV 5-2: How Tarantella Printing Works

Use this slide to illustrate how Tarantella printing works. In particular, show the protocols used by Tarantella and the protocols that the client's printer may use.

As you already know from earlier lessons, Tarantella enables users to launch applications which reside on a variety of application servers. These application servers may be running Unix or Windows.

When a user prints from a client machine, Tarantella's role is to see that the print job is transferred from the application server to the client's default printer.

Tarantella accomplishes this by transferring the print job from the application server to the Tarantella server via LPD.

The Tarantella server hands the print job off to the client using the Print Protocol Engine (PPE).

Once the client has accepted the print job, it's up to the client to print the file. This enables the client to print via Tarantella to any type of printer supported by the client.

Explain the three printer buttons on the webtop.

If you change the default printer on the Windows client, the printer button on the webtop still displays the old default printer. Furthermore, print jobs submitted will appear on the old default printer. You can force Tarantella to recognize the new default printer by simply refreshing/reloading your web browser.

5.2 Configuring a Unix Server for Tarantella Printing

While there is a fair amount of similarity in how different Unix platforms administer printers, there are enough differences to challenge anyone trying to manually configure a printer.

Tarantella eliminates this challenge and makes configuring a printer easy by providing a *single* shell script called *prtinstall.en.sh* which can be run on any of the supported Tarantella platforms.

This shell script knows the details of each Unix platform so that you don't have to bother yourself knowing how to configure printing on each platform. All you have to do is to copy the shell script from a Tarantella server's */inst_dir/bin/scripts* directory (where *inst_dir* is the Tarantella installation directory) onto the application server and then invoke the script as follows:

```
# ./prtinstall.en.sh
```

NOTE: The *prtinstall.en.sh* script is run automatically during the installation of Tarantella. Therefore, it is not necessary to run *prtinstall.en.sh* on the application server if the application server is a Tarantella server.

It is, however, safe to run it multiple times.

To remove the Tarantella printer from an application server, login in as root and type the following:

```
# ./prtinstall.en.sh --uninstall
```

5.3 Configuring a Windows Server for Tarantella Printing

To install a printer on a Windows Terminal Server or Windows 2000 server:

- Step 1. Create an LPR printer on the Windows application server. This is accomplished by telling Windows to create a *local* printer and creating an “LPR” port.

This is the most confusing part of the procedure under Windows for several reasons. First, Windows calls LPD printers LPR printers. Second, you must specify that you want to create a “local printer”. This is because Windows creates a local “port” (similar to LPT1) used to print remotely. When you specify that you want to create a “local printer”, “LPR printer” will be one of the choices.

- Step 2. When configuring the new LPR port:
- For Name or address of server providing lpd, type the DNS name of the Tarantella server where the Tarantella user will log in.
 - For Name of printer or print queue on that server, type “tta_printer”
- Step 3. When prompted whether the printer will be shared with other network users, choose Not Shared.
- Step 4. Choose the printer model and manufacturer that most closely matches your client devices' default printer when prompted. If there's no close match, choose a PostScript printer

For more information on the steps to install a Windows printer are detailed in the online help documentation. In the *Admin Guide*, read **How to... ⇒ Add a Tarantella printer ⇒ To add a Tarantella printer on a Windows application serve .**

Under Windows 2000, you must have “Print Services for Unix” installed for follow-me printing to work. If it is not installed, select **Start ⇒ Settings ⇒ Control Panel ⇒ Add/Remove Programs ⇒ Add/Remove Windows Components ⇒ Other Network File and Print Services ⇒ Details ⇒ Print Services for Unix.**

5.4 Submitting Print Jobs under Tarantella

Printing is easy in Tarantella. All that is necessary to print from an application running under Tarantella is to print from the application!

If you're running a Windows program, select File ⇒ Print... from the application's menu. If you're at a shell prompt in an **xterm**, just use the **lp** command to submit the print job as usual.

In other words, just print from the application in whatever way you ordinarily would. As long as the printer prints to the default printer or prints specifically to a printer called "tta_printer", the print job will print out on the client's default printer.

Exercise: Submitting a Print Job under Tarantella

Launch an application (Unix or Windows) from the webtop and submit a print job.

5.5 Lesson Summary

This lesson described how printing works under Tarantella and how to configure Unix and Windows application servers to print under Tarantella.

5.6 Review questions

1. What is the name of the program that needs to be run on Unix application servers to configure printing under Tarantella?

■ The program that you run on Unix application servers to enable Tarantella printing is called `prtinstall.en.sh`.

2. What protocol does Tarantella use to transfer print jobs from the application server to the Tarantella server?

■ Tarantella uses LPD to transfer the print job from the application server to the Tarantella server.

3. What protocol does Tarantella use to transfer print jobs from the Tarantella server to the client?

■ Tarantella uses the Print Protocol Engine (PPE) to transfer print jobs from the Tarantella server to the client.

4. What is the default name of the Tarantella printer?

■ The default name of the Tarantella printer is "tta_printer".

5.7 Answers to Exercise and Review Questions

This section contains the answers to exercises, review questions, and labs presented in this lesson.

Exercise answers

Please consult your instructor if you have any questions about the exercises in this lesson.

Review Question Answers

This section contains the answers to the review questions on page 5-12.

1. The program that you run on Unix application servers to enable Tarantella printing is called *prtinstall.en.sh*.
2. Tarantella uses LPD to transfer the print job from the application server to the Tarantella server.
3. Tarantella uses the Print Protocol Engine (PPE) to transfer print jobs from the Tarantella server to the client.
4. The default name of the Tarantella printer is “tta_printer”.

6

The Tarantella Security Pack

Instructor Guide

Instructor Guide

Lesson 6

The Tarantella Security Pack

Suggested lesson duration

This lesson should take approximately 1 hour to complete including the lab.

Pre-lesson classroom preparation

You must have already installed the Tarantella Enterprise II base component on each host on which you want to install the Tarantella Security Pack.

Install the Tarantella Security Pack on the instructor's machine so that demos can be performed.

Instructor preparation

Read the following articles in the *Admin Guide*

How to... ⇒ Let your users access Tarantella securely

Reference ⇒ Security

Reference ⇒ Unix Commands ⇒ The Tarantella security command

Introduction

The Tarantella Security Pack is an add-on to Tarantella that protects communications between clients and the Tarantella server. By using the Tarantella Security Pack organizations can confidently extend the reach of applications beyond their internal LAN.

Objectives

By the end of this lesson, you will be able to:

- Install the Tarantella Security Pack
- Obtain an X.509 Certificate from a Certificate Authority
- Install an X.509 Certificate
- Enable Tarantella Security
- Connect to a Tarantella server running the Tarantella Security Pack

AV 6-1

The Tarantella Security Pack

- Installing the Tarantella Security Pack
- Obtaining an X.509 Certificate
- Installing an X.509 Certificate
- Enabling the Tarantella Security Pack



©The Santa Cruz Operation, Inc.

Topics

In order to meet these objectives, this lesson discusses:

- Installing the Tarantella Security Pack — Discusses how to install the Tarantella Security Pack from CD-ROM or via the web.
- Obtaining an X.509 Certificate — Explains how to obtain an X.509 certificate from a Certificate Authority for use with Tarantella Security Pack.
- Installing an X.509 Certificate — Discusses how to install the X.509 certificate generated by a Certificate Authority on a Tarantella server.
- Enabling the Tarantella Security Pack — Details how to turn on the Tarantella Security Pack once the X.509 certificate has been installed.



AV 6-1: The Tarantella Security Pack

The first slide describes the overall topics covered in this lesson.

6.1 The Tarantella Security Pack

The Tarantella Security Pack is an add-on to Tarantella that protects communications between clients and the Tarantella server. By using the Tarantella Security Pack organizations can confidently extend the reach of applications beyond their internal LAN.

A Tarantella server without the Tarantella Security Pack installed uses standard connections for communication between client devices and Tarantella servers. A standard connection transmits all information in cleartext (unencrypted), encoding passwords to deter casual eavesdroppers. This is just as secure as using, for example, the telnet program to communicate between two UNIX hosts.

Actually it's *more* secure than telnet. Whereas telnet sends cleartext passwords, Tarantella obfuscates them using 24-bit encryption.

In environments where very high security is required, these standard security precautions may not be enough. For these situations, the Tarantella Security Pack is available. The Tarantella Security Pack can only help raise security levels as part of an ongoing security strategy. If you use the Tarantella Security Pack, we recommend that you also use HTTPS.

“https” is a unique protocol that is simply SSL underneath HTTP. You need to use “https://” for HTTP URLs with SSL, whereas you continue to use “http://” for HTTP URLs without SSL. The default “https” port number is 443, as assigned by the Internet Assigned Numbers Authority.

A Tarantella server with the Tarantella Security Pack installed can still use standard connections, but also offers SSL (Secure Sockets Layer) connections for communication between client devices and the Tarantella server. An SSL connection provides the following benefits:

Prevents eavesdropping	The Tarantella Security Pack encrypts all information before transmission.
Prevents tampering	The Tarantella Security Pack checks that a message hasn't changed between being sent by a client device and received by the server.
Prevents message forgery	The Tarantella Security Pack requires that the server prove its identity to client devices before communication can take place, and also guards against replay attacks.

The Tarantella Security Pack offers two levels of encryption: strong and standard. Your license for the Tarantella Security Pack determines which type of encryption you use, and it's not possible to change this.

Explain that the license determines the level of security provided.

Steps to installing and configuring the Tarantella Security Pack:

- Install the .shx archive
- Issue the **tarantella security certrequest** command to generate a CSR
- Cut-and-paste the CSR into www.verisign.com or www.thawte.com
- Cut-and-paste the X.509 certificate generated by Verisign/Thawte into the **tarantella security certuse** command
- Set the **Connection Type** attribute on person objects, organizational unit objects, and/or the organization object
- Issue the **tarantella security on** command

Once these steps have been performed, you can log into Tarantella via the web browser. Make certain that the machine portion of the URL used to log in matches the host name specified in the X.509 certificate. For instance, if the X.509 certificate contains the name "apple.example.com", then the following URLs will *not* work:

- <http://localhost/tarantella> Fails because the certificate doesn't specify "localhost"
- <http://apple/tarantella> Fails because the certificate doesn't specify "apple"

Instead you are limited to using the following URL:

- <http://apple.example.com/tarantella> Succeeds because the certificate specifies "apple.example.com"

Alternatively, you *can* use the machines IP address in the URL.

6.2 Installing the Tarantella Security Pack

The installation and removal mechanisms in the Tarantella Security Pack have been designed to be reliable and easy to use. The installation procedure is similar to the procedure detailed in Lesson 2: “Installing Tarantella.”

The Tarantella Security Pack software runs on the following platforms:

- UnixWare 2.1.2+
- UnixWare 7+
- SCO OpenServer 5.0.2+
- SPARC Solaris 2.5.1+
- IBM AIX 4.2+
- HP-UX 10.20+
- Compaq Tru64 UNIX 4.0d+
- Linux

6.2.1 Distribution media

The Tarantella Security Pack software is distributed two ways:

Via the web

The Tarantella Security Pack product (along with other Tarantella products) can be downloaded from <http://tarantella.sco.com>. Web-distribution is the primary method of distribution.

On CD-ROM

In special instances, SCO distributes the software on CD-ROM. This is not the primary method of distribution.

Table 5: Hints for Using CD-ROMs on SCO Platforms

SCO OpenServer 5	<code>mount -f HS -o ro,lower /dev/cd0 /mnt</code>
SCO UnixWare 7 SCO UnixWare 2.1	<code>/usr/sbin/mount -rF cdfs /dev/cdrom/cdrom1 /mnt</code>

6.2.2 Installation procedure

To install the Tarantella Security Pack, follow this procedure:

Step 1. Log in as root.

There is no single-user mode requirement.

Step 2. Mount the CD-ROM.

Step 3. Run the following command:

```
sh tsp_file.shx
```

where *tsp_file.shx* is one of the following file names:

Table 6: The Tarantella Security Pack SHX File Names

Platform	SHX File name
SCO UnixWare® 7+	tspi3un.shx
SCO UnixWare 2.1.2+	tspi3un.shx
SCO OpenServer Release 5.0.2+	tspi3sc.shx
HP-UX 10.20+	tsppahp.shx
IBM AIX 4.2+	tsprsai.shx
SPARC Solaris 2.5.1+	tspspsso.shx
Compaq Tru64 UNIX 4.0d+	tspax01.shx

Step 4. Follow the on-screen prompts.

6.3 X.509 Certificates

A digital certificate is an electronic “passport” that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Tarantella servers use X.509 certificates to prove their identity to clients. Clients use information supplied by the CA to decode the certificate and verify the server's identity.

Before you can use the Tarantella Security Pack, you'll need to provide the Tarantella server with an X.509 certificate. If you're using an array of Tarantella servers, you'll need one certificate for each server on which you install the Tarantella Security Pack.

If you use HTTPS you'll need *two* X.509 certificates -- one for your web server on port 80 and another for Tarantella on port 5307.

The Tarantella Security Pack does *not* enable SSL on the web server.

GuruNotes If you can access the private key, you can use the same certificate for both purposes. The Apache web server lets you do this, but many other web servers don't (eg. Netscape FastTrack Server). You may be able to access the private key needed to decrypt the web server's X.509 certificate. (You might need to decrypt the key first, using the tarantella security decryptkey command.) See the tarantella security certuse command for information about how to do this.

6.3.1 Obtaining an X.509 certificate for the Tarantella Security Pack

A valid X.509 certificate is required before SSL connections are available for Tarantella connections (ie. SSL connections on port 5307). The following are the steps to obtain a Certificate from a Certificate Authority:

Step 1. On your Tarantella server, generate a Certificate Signing Request (CSR) by typing the following command:

```
# tarantella security certrequest --orgname orgname
--country country --state state
```

where *orgname* is the official name of your organization, *country* is your organization's ISO 3166 country code (for example, US or DE), and *state* is the state or province where your organization is located. Double quote any arguments that contain spaces. For example: --state "New Mexico"

Step 2. Send this CSR to a supported Certificate Authority (CA) (eg. VeriSign or Thawte) by filling out the CA's on-line form(s). Consult your CA for details of any additional information they may require and payment information.

■ The easiest way to "send" the CSR is to cut-and-paste it into the web-based form at the CA's website.

Step 3. The CA will then supply you with a certificate which you can use with the Tarantella Security Pack.

- You can include additional information about yourself and your organization in the CSR, if you wish, by using additional attributes with the **tarantella security certrequest** command.
- The **tarantella security certrequest** command generates a new key with which to decode certificates. If you've already used the **tarantella security certrequest** command to generate a CSR and obtain a certificate, running the command again means Tarantella won't be able to decode the old certificate.
- If your CA lets you change the hostname stored in the certificate, make sure the certificate contains a fully qualified DNS name (eg. "seattle.example.com" rather than just "seattle").

■ The **tarantella security certinfo** lets you display information about CSRs and certificates

6.4 Supported Certificate Authorities

The Tarantella Security Pack supports the following Certificate Authorities and certificate types:

- VeriSign Secure Server ID

<http://www.verisign.com>

- Thawte Basic Web Server Certificate

<http://www.thawte.com>

Note, If you want to use an unsupported certificate type or CA with the Tarantella Security Pack, you need to follow the above steps to generate and submit a CSR and must also obtain the root certificate in PEM format for your certificate type. Consult your CA for details on obtaining the root certificate.

6.5 Installing an X.509 Certificate

Once you have obtained an X.509 Certificate from a supported CA, you will need to install it on the Tarantella host. The following is the command to install the Certificate:

```
# tarantella security certuse < /tmp/cert
```

This example assumes that you used the **tarantella security certrequest** command to generate a CSR, which you then sent to a Certificate Authority (CA). The CA returned a certificate to you, which you saved in a temporary file */tmp/cert*.

Alternatively, you can cut-and-paste the certificate.

■ If you cut-and-paste the certificate, omit the “< /tmp/cert” portion of the command above.

6.5.1 Enabling Tarantella security

Once you have installed a Certificate on your Tarantella host, you can enable Tarantella security by typing the following command on your Tarantella host:

```
# tarantella security on
```

This command will enable SSL connections on port 5307. Tarantella will use SSL connections for those users specified by the Tarantella administrator.

■ The command **tarantella security off** disables the Tarantella Security Pack.

6.5.2 The Control Center

The Tarantella Security Pack provides the administrator a large degree of control when configuring security on the Tarantella server. The administrator can set security properties on:

- The organization object
- Organizational unit objects
- Person objects
- Any combination of the above

On each of these types of object, the administrator can specify a set of rules which determine what type of connection:

- Standard
- SSL
- Deny

Furthermore, each of these rules can specify specific conditions under which each type of connection is used based upon the client's and/or server's:

- Name
- IP address
- Subnet

These rules are set by changing an object's "Connection Type" attribute in Control Center.

GuruNotes When a user logs into Tarantella, Tarantella determines which type of connection to use by looking at the user's person object's Connection Type attribute and working its way up until it finds a matching rule.

Demonstrate setting a "Connection Type" in Control Center.

6.5.3 Testing the Tarantella Security Pack configuration

Section , “Part VII: Test the Tarantella Security Pack Configuration,” on page 6-29 will illustrate how to connect to the Tarantella server to test the configuration of the Tarantella Security Pack.

6.6 Lesson Summary

This lesson described how to install the Tarantella Security Pack. Additionally, this lesson described how to obtain and install X.509 Certificates. Finally, this lesson described how to enable the Tarantella Security Pack and how to test it by connecting to the server via a web browser.

6.7 Review questions

1. On which platforms does the Tarantella Security Pack run?

The Tarantella Security Pack runs on the following platforms: UnixWare, Solaris, OpenServer, AIX, HP-UX, and Compaq Unix (Tru64).

2. What are the two levels of encryption offered by the Tarantella Security Pack?

The two levels of encryption offered by the Tarantella Security Pack are 128-bit Strong Cryptography (US and Canada only) and 40-bit Standard Cryptography.

3. Which Certificate Authorities does the Tarantella Security Pack support?

The Certificate Authorities supported by the Tarantella Security Pack are Verisign and Thawte.

4. What benefits does an SSL connection provide over standard connections?

SSL connections provide three benefits over standard connections:

- Prevent eavesdropping — SSL can encrypt all information before transmission.
- Prevent tampering — SSL can check that a message hasn't changed between being sent by a client device and received by the server.
- Prevent message forgery — SSL requires that the server proves its identity to client devices before communication can take place, and also guards against replay attacks.

5. What command do you use to request a CSR?

The command to request a CSR is **tarantella security certrequest**

6.8 Lab: Configuring the Tarantella Security Pack

In this lab, you will perform the steps necessary to install the Tarantella Security Pack. After doing so, you will generate a CSR, request a certificate from a Certificate Authority (CA), install and test the certificate by connecting to the Tarantella with a web browser.

If teaching the Tarantella Enterprise II Administration course, use UnixWare's dtterm throughout this lab so that cut-and-paste will work. If teaching the Tarantella Express Administration course, OpenServer's cut-and-paste capabilities are not as robust. Redirect the CSR in Part II into a temporary file, then use that file as the argument to the `--certfile` option of the `tarantella security` command.

Be aware of how cut-and-paste works in the following utilities:

- dtterm on Unixware uses `CTRL INS` for copy and `SHIFT INS` for paste.
- Netscape Navigator on Windows uses `CTRL C` for copy and `CTRL V` for paste.
- Netscape Navigator on Unix uses `ALT C` for copy and `ALT V` for paste.

Creating a backdoor administrator account case prevent locking yourself out when turning on security.

6.8.1 Overview

Your tasks in this lab are as follows:

- Download the Tarantella Security Pack or obtain it from the instructor
- Install the Tarantella Security Pack
- Generate a CSR by using the `tarantella security certrequest` command
- Obtain an X.509 Certificate from a Certificate Authority.
- Install the Certificate obtained from the Certificate Authority
- Enable Tarantella Security
- Configure Tarantella to use SSL connections
- Verify the Tarantella Security Pack and Certificates have been installed correctly by connecting to it with a web browser

The instructor will point you to where you can obtain the tarantella software and license.

Make sure the students know where the software is (CD-ROM, via the web, etc.) and the exact name of the *.shx file that they will be installing. Provide the students with the license(s) that they are to use (if applicable).

6.8.2 Procedure

Part I: Installing the Tarantella Security Pack

The first item of business is to install the Tarantella Security Pack.

Step 1. If directed to do so by the instructor, download the Tarantella Security Pack .shx file for your platform. Otherwise *.shx file will be provided by the instructor.

Make sure students are clear whether they are getting the Tarantella software from the web, CD-ROM, etc.

Step 2. Execute the *.shx file by executing the following command:

```
# sh platform.shx
```

where *platform.shx* is replaced with the platform specific name of your *.shx file. For example, issue the following command on SCO UnixWare 7 systems:

```
# sh tspi3un.shx
```

Step 3. If you are prompted that there is insufficient space in */var/tmp*, then remedy this problem in either of the following two ways:

- Point the TMPDIR environment variable to a directory which contains sufficient disk space:

```
# TMPDIR=/directory/in/big/enough/filesystem  
# export TMPDIR
```

- Unmount the */var/tmp* filesystem:

```
# umount /var/tmp
```

Once you have remedied this problem, return to Step 2.

The Tarantella Certrequest Command

```
# ./tarantella security certrequest --orgname "Example Co, Inc." --country "US"
--state "California"
```

The certificate's common name (CN) will be: redwood.example.com

This hostname is included in the certificate signing request (CSR) and corresponds to the name of the server that users will connect to.

- If DNS names are used to connect to the server, the hostname above MUST be a fully qualified DNS name.
- If clients are required to connect to the server using an IP address, the hostname above should be the IP address. A DNS record for this IP address SHOULD NOT exist.

For clients to accept the certificate once it's installed, a DNS lookup of the hostname followed by a reverse lookup of the result must return the original hostname.

The hostname to be used in the certificate request is redwood.example.com.

```
Do you want to use this hostname? [yes]
4368 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
....+++++
*****+++++
e is 65537 (0x10001)
```

Verify that this
host name is
correct

Certificate Signing Request (CSR): Summary

```
Subject:
  C=US
  ST=California
  O=Example Co, Inc.
  CN=redwood.example.com
```

The information above will be contained in the CSR.

Create CSR now? [yes]

Send the following Certificate Signing Request (CSR) to a Certificate Authority, such as VeriSign (www.verisign.com). Check with your CA that you're providing all the information they need.

```
-----CUT HERE-----
-----BEGIN CERTIFICATE REQUEST-----
MIIB1zCCAQAQAQAwVzELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbmG1mb3JuaWEx
GTAXBgNVBAQTEEV4Ym1wbGUgQ28sIE1uYy4xGDAwBgNVBAHTD3JlZHVkb2Quc2hv
LmNvbTCBnzANBghk1G9w0BAQEFAAOBjQAwgYkCgYEA1W+qbAh5JTQAQFstxV2b
8JWcYe6wFFJgRt089QAQX0TG0Fdr899yL4hyLqYEjX8HZe/qypV8gbE4LwTmRPSRm
G+IjaNq2EBEAb3qdSuSHY8y2XMOVp/iKZQLQt+bNuneN1bDuyWQeWKA62i70IwPf
zhP0ot0K/qHdGALcteb/gekCAwEAAaAAHAGCSqGSIb3DQEBAUAA4GBAIdhk/Rv
z6ZterZb7I1Tr9gjVU5fyFtCVF/dovBx8RKzFeD3Nb80iD7f1zvxL3UlyBoV/f/k
dC0HmazAD8j3cbGII20vry9BKqbYYGmS1/++35h5RoahIqa8rVltSf7HzCA42t90I
GzUFgpcRpCOWDxAqV62NJ7//DzWEivvONURp
-----END CERTIFICATE REQUEST-----
-----CUT HERE-----
```

Cut-and-paste
this into a file

When you receive your certificate, use 'tarantella security certuse' to install it.

For more information, see 'Tarantella Security Pack overview' in the Tarantella Administration Guide Index.

#



©The Santa Cruz Operation, Inc.



Part II: Generating a CSR

AV 6-2: The Tarantella Certrequest Command

Use this slide to illustrate the `tarantella security certrequest` command.

Once you have installed the Tarantella Security Pack, each host on which the Tarantella Security Pack is installed requires a valid X.509 certificate before SSL connections are available.

Step 1. Log onto the Tarantella server as root, start a dtterm, and generate a CSR by using the **tarantella security certrequest** command:

```
# /opt/tarantella/bin/tarantella security
certrequest --orgname "Example Co, Inc." --country
"US" --state "California"
```

AV 6-2 on page 6-22 shows the output of this command. The output will include the hostname that will be used in the certificate. Verify that the hostname is correct.

- If DNS names are used to connect to the server, the hostname above **MUST** be a fully qualified DNS name.
- If clients are required to connect to the server using an IP address, the hostname above should be the IP address. A DNS record for this IP address *should not* exist.
- For clients to accept the certificate once it's installed, a DNS lookup of the hostname followed by a reverse lookup of the result must return the original hostname.

Step 2. After you accept the hostname, the command generates a CSR. Copy the CSR to the clipboard (ie. highlight the CSR and type `CTRL INS`). You must include the lines which read

“-----BEGIN CERTIFICATE REQUEST-----”

and

“-----END CERTIFICATE REQUEST-----”.

Including additional lines doesn't hurt.

Alternately, copy the CSR to the clipboard.

AV 6-3

The Tarantella Certuse Command

```
# ./tarantella security certuse < /tmp/cert
```

Certificate: Summary

Subject:

C=US
ST=California
O=Example Co. Inc
CN=devnull.uss.sco.com

Issuer:

C=ZA
ST=FOR TESTING PURPOSES ONLY
O=Thawte Certification
OU=TEST TEST TEST
CN=Thawte Test CA Root

Validity:

Not Before: Feb 3 07:45:42 2000 GMT
Not After : Mar 5 07:45:42 2000 GMT

Key and certificate are compatible.

Successfully installed certificate.

#



©The Santa Cruz Operation, Inc.



Part III: Obtaining an X.509 Certificate

- Step 1. Using your web browser, open the following URL:

<http://www.thawte.com>

On the right hand side of the thawte webpage, there will be a link to “Free Trial Certificate”. Click on the link and paste (ie.   under Windows or   under Unix) your CSR into the space provided. Accept all of the defaults, and click the “Generate Test Certificate” button.

You will be asked to verify the information included in the CSR. Once you have verified the information on the screen, a certificate will be generated.

- Step 2. Cut-and-paste the certificate to a file called `/tmp/cert`. Do this by highlighting the certificate in the web browser and typing   under Windows or   under Unix.

Paste the certificate into the dtterm by typing the following:

```
# cat > /tmp/cert
  under Windows or   under Unix
 
```

Alternately, you can do Parts III and IV by doing a cut-and-paste, pasting the certificate directly into the **tarantella security certuse** command instead of pasting it into a file.

Part IV: Installing the X.509 Certificate

AV 6-3: The Tarantella Certuse Command

Use this slide to illustrate the certuse command.

- Step 1. On the Tarantella host, use the **tarantella security certuse** command to install the Certificate:

```
# /opt/tarantella/bin/tarantella security certuse < /tmp/cert
```

Where `/tmp/cert` is the name of the file to which you saved the certificate.

A summary of the certificate information will be displayed (see AV 6-3 on page 6-24), and you will have successfully installed the certificate.

AV 6-4

Enabling Tarantella Security

```
# ./tarantella security on
Tarantella server stopped.
Starting Tarantella 1.41.901 from /opt/tarantella/bin/i3sc0325...
...OK
Checking whether to use secure connections...
Starting Tarantella Security Daemon from /opt/tarantella/bin/i3sc0325...
Secure Daemon exec: listening on 5307 forwarding to 3144

...OK
Tarantella Security Pack now enabled.
# █
```



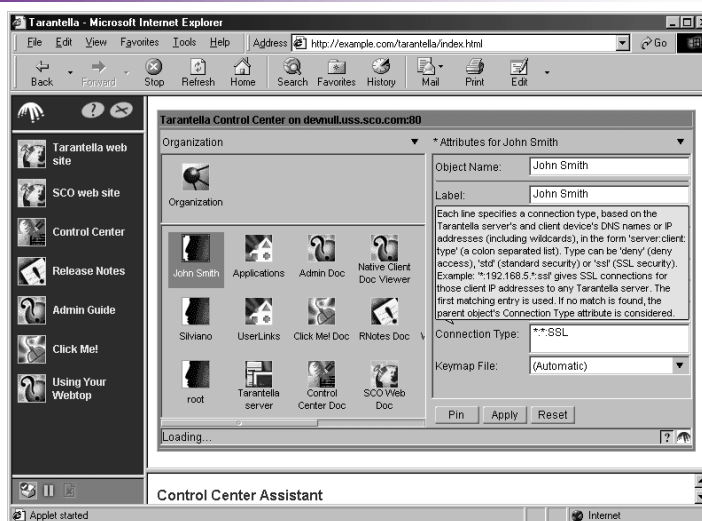
©The Santa Cruz Operation, Inc.



Instructor Guide

AV 6-5

Configuring the Connection Type



©The Santa Cruz Operation, Inc.



Part V: Enabling the Tarantella Security Pack

Enable the Tarantella Security Pack with the **tarantella security on** command. Slide AV 6-4 on page 6-26 shows the output of this command.

AV 6-4: Enabling Tarantella Security

Use this slide to illustrate the **tarantella security on** command.

Part VI: Configuring Tarantella to Use SSL Connections

AV 6-5: Configuring the Connection Type

Use this slide to illustrate setting a person object's connection type in the Control Center. Be sure to emphasize that the same can be done on an organizational unit or the entire organization.

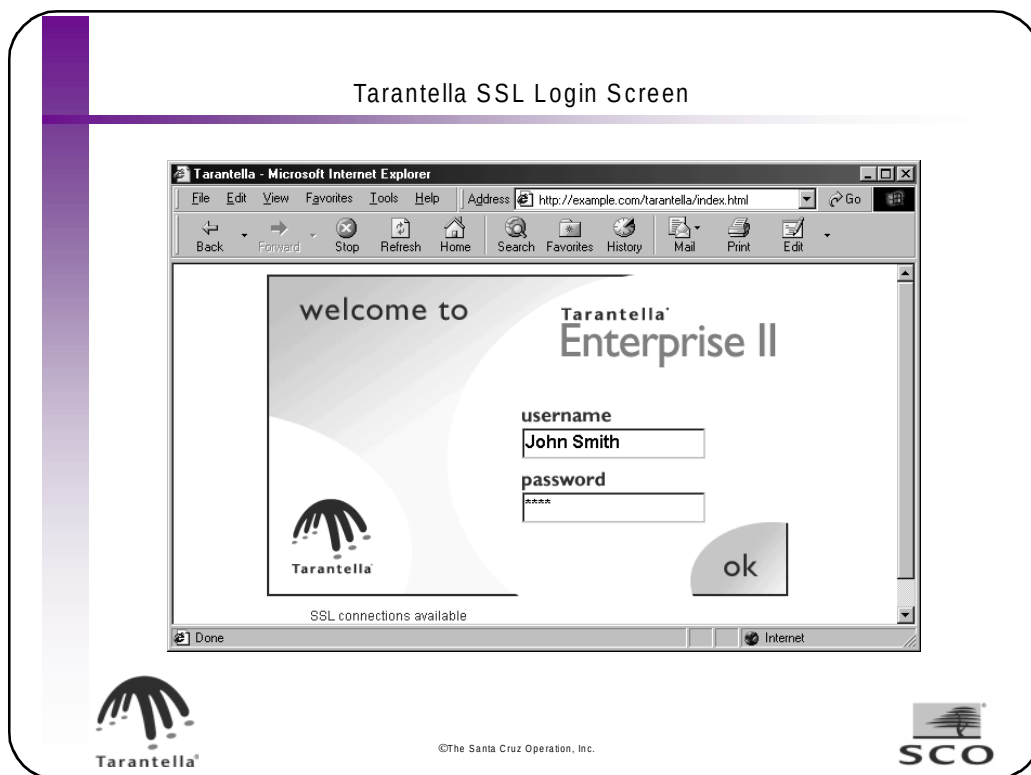
Now that you have enabled the Tarantella Security Pack, you can selectively enable SSL connections on a per person, per organizational unit, or organization wide basis. Simply select one of these three types of objects in the Control Center and set its **Connection Type** attribute to *** : * : SSL**.

Slide AV 6-5 on page 6-26 shows an example of setting the connection type for a person named John Smith.

AV 6-6



AV 6-7



Part VII: Test the Tarantella Security Pack Configuration

Test your installation of the Tarantella Security Pack and Certificate, by connecting to the Tarantella server from a client browser:

<http://server/tarantella>

where *server* is the name of the server upon which the Tarantella Security Pack is installed. Furthermore, the name specified for *server* in the URL *must* match the hostname stored in the X.509 certificate.

NOTE: A security warning will appear (see AV 6-6 on page 6-28). This warning is generated because the certificate you received from the CA was a test certificate. You can safely ignore this warning for this lab. Click on the **accept** button.

AV 6-6: Test Certificate Warning

Use this slide to illustrate the warning dialog that pops up when a test certificate is encountered.

A login screen will appear (see AV 6-7 on page 6-24). Notice on the bottom of the login screen the message stating that SSL connections are available.

AV 6-7: Tarantella SSL Login Screen

Use this slide to point out where the login screen announces SSL logins.

Recall that the Tarantella Security Pack provides the administrator a fine degree of control over which Tarantella users do and don't use an SSL connection. When you log in to a Tarantella server running the Tarantella Security Pack, you can determine whether you are logged in using SSL or a non-SSL connection by placing the cursor between two icons on the launch pad and examining the message on the web browser's status bar.

The lock icon displayed by web browsers such as Netscape Navigator indicate whether HTTPS is being used. The lock icon is *not* an indication of whether Tarantella is using a secure connection.

AV 6-8 on page 6-32 shows a non-SSL connection. AV 6-9 on page 6-32 shows an SSL connection.

AV 6-8: A Non-SSL Tarantella Login

Use this slide to point out where the webtop indicates a standard connection.

AV 6-9: An SSL Tarantella Login

Use this slide to point out where the webtop indicates an SSL connection.

■ As an additional lab, you could have students download the Native Client again. They'll get the TSP version.

AV 6-8

A Non-SSL Tarantella Login



©The Santa Cruz Operation, Inc.



Instructor Guide

AV 6-9

An SSL Tarantella Login



©The Santa Cruz Operation, Inc.



6.9 Answers to Exercise and Review Questions

This section contains the answers to exercises, review questions, and labs presented in this lesson.

Exercise answers

Please consult your instructor if you have any questions about the exercises in this lesson.

Review Question Answers

This section contains the answers to the review questions on page 6-19.

1. The Tarantella Security Pack runs on the following platforms: UnixWare, Solaris, OpenServer, AIX, HP-UX, and Compaq Unix (Tru64).
2. The two levels of encryption offered by the Tarantella Security Pack are 128-bit Strong Cryptography (US and Canada only) and 40-bit Standard Cryptography.
3. The Certificate Authorities supported by the Tarantella Security Pack are Verisign and Thawte.
4. SSL connections provide three benefits over standard connections:
 - Prevent eavesdropping — SSL can encrypt all information before transmission.
 - Prevent tampering — SSL can check that a message hasn't changed between being sent by a client device and received by the server.
 - Prevent message forgery — SSL requires that the server proves its identity to client devices before communication can take place, and also guards against replay attacks.
5. The command to request a CSR is **tarantella security certrequest**

7

Tarantella Load Balancing

Instructor Guide

Instructor Guide

Lesson 7

Tarantella Load Balancing

Suggested lesson duration

If you are teaching the Tarantella Enterprise II version, this lesson should take approximately 3 hours to complete including the lab.

If you are teaching the Tarantella Express version, this lesson should take approximately .5 hours to complete including the lab.

Pre-lesson classroom preparation

You must have already installed the Tarantella base component on each host.

Make sure that every host has the same version of Tarantella installed.

Each host that will become part of an array must have a web server installed and configured to work with Tarantella.

Instructor preparation

Read the following articles in the *Admin Guide*

How to... ⇨ Balance the load across multiple servers

Reference ⇨ Load balancing with arrays

Introduction

Tarantella Enterprise II servers act as application brokers — gateways between client devices and application servers. If many users want to access applications through Tarantella at the same time, a single Tarantella server may become a bottleneck. In addition, if that server is unavailable, users can't access their webtops or run applications.

Load balancing lets you spread your users across multiple servers, rather than having everyone use the same server. Multiple servers provide these benefits:

Increased Performance	More Tarantella servers are available to cope with demand from users.
Increased Robustness	When a Tarantella server is unavailable, other servers take its place.
Scalability	As more users start using Tarantella, you can add Tarantella servers to the array to meet demand.

If you have many users logging into Tarantella at the same time, you should consider using more Tarantella servers.

If you have many users running the same application at the same time, you should consider using more application servers.

Objectives

By the end of this lesson, you will be able to:

- Describe Tarantella Load Balancing
- Describe what is a Tarantella Array
- Describe How a Tarantella Array Works
- Create an array of Tarantella servers
- Describe the Tarantella load balancing table
- Describe Application Server Farms

AV 7-1

Instructor Guide

Tarantella Load Balancing

- Understanding Tarantella Load Balancing
- Understanding Tarantella Arrays
- Application Server Farms
- Understanding the Load Balancing Table



©The Santa Cruz Operation, Inc.

Topics

In order to meet these objectives, this lesson discusses:

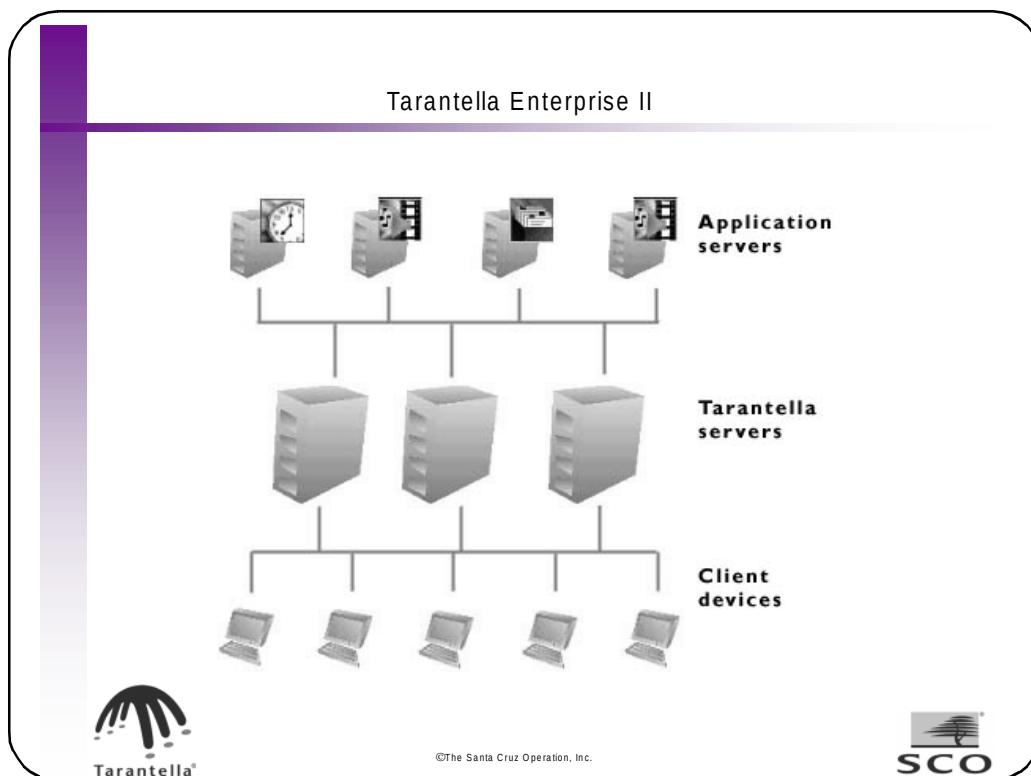
- Understanding Tarantella Load Balancing — Discusses the Tarantella load-balancing feature, which provides a mechanism for distributing users across available Tarantella servers.
- Understanding Tarantella Arrays — Defines the Tarantella arrays, and discusses its use in load balancing.
- Creating an array of Tarantella servers — Discusses the procedure necessary to create, add, delete, and modify arrays.
- Application Server Farms — Discusses the multiple application server features of Tarantella.
- Understanding the Tarantella Load Balancing Table — Discusses the purpose of the load balancing table, adding, removing and modifying of the load balancing table.



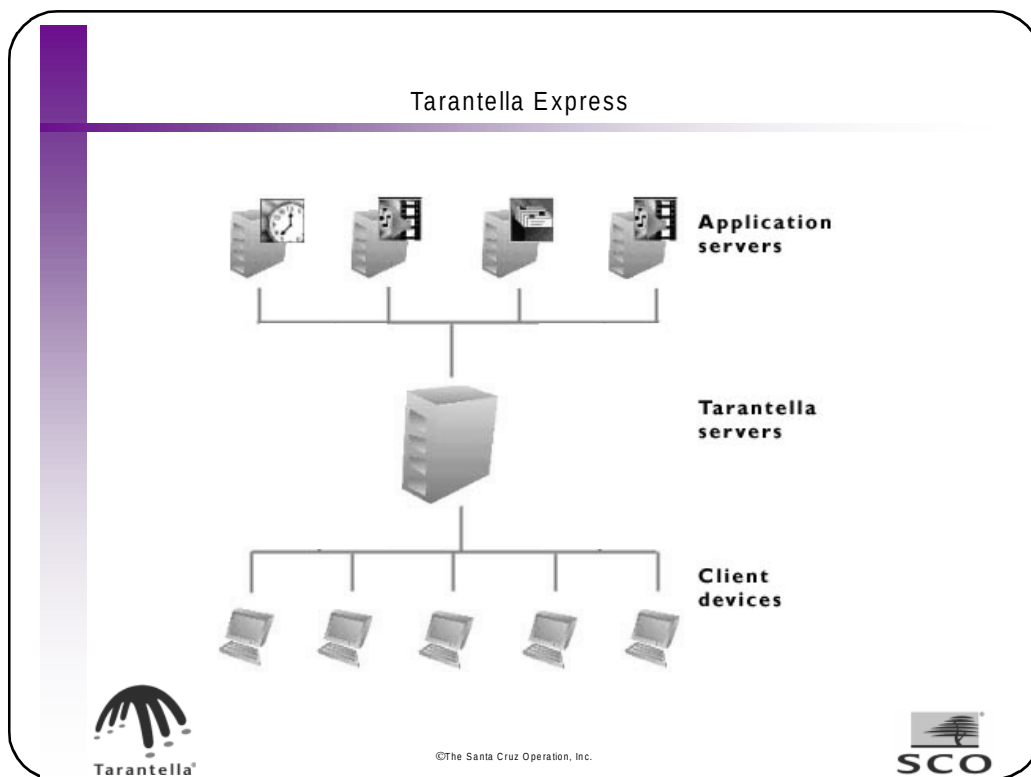
AV 7-1: Tarantella Load Balancing

The first slide describes the overall topics covered in this lesson.

AV 7-2



AV 7-3



7.1 Distributing the Load

AV 7-2: Tarantella Enterprise II

Use this slide to illustrate the Tarantella Enterprise II has *both* Tarantella arrays and application server farms.

AV 7-3: Tarantella Express

Use this slide to illustrate that while Tarantella Express allows application servers, only four application servers are allowed and Tarantella arrays are *not* supported. Tarantella Express users who want more than four application servers or support for Tarantella arrays must upgrade to Tarantella Enterprise II. There is a clear upgrade path to do this.

Tarantella Enterprise II enables the administrator to spread the load across multiple servers in two ways:

- Application Server Farms

Application server farms are comprised of multiple servers, each of which provides the ability to launch the same application or applications. This enables administrators to spread the load.

- Tarantella Arrays

Tarantella arrays are provided to enable administrators to spread the load associated with Tarantella logins. Tarantella arrays are comprised of multiple servers providing Tarantella services. These servers act cooperatively to enable users to log into Tarantella. When a Tarantella user logs into a Tarantella array, the user is authenticated by one of the Tarantella servers in the array. The webtop that the user sees and the applications available to the user are the same regardless which Tarantella server in the array actually authenticates the user.

Whether using application server farms or Tarantella arrays, Tarantella makes all of this invisible to the user.

GuruNotes

Yes, Tarantella Express can have up to four application servers plus the Tarantella server itself can act as an application server.

7.2 Application Server Farms

Running an application on a particular application server (by specifying a DNS name or IP address in the application object's Application Server attribute) can cause a bottleneck.

For instance, if many users want to run the application at the same time, the application server may become overloaded causing a decrease in performance. If the application server is unavailable for any reason (perhaps because of network problems), users won't be able to run that application.

To address this issue, Tarantella lets you balance the application load across multiple application servers. Such a collection of servers is called an application server farm.

7.2.1 Multiple application servers

In order to configure multiple application servers, specify which application servers can run the application. When a user starts the application, Tarantella chooses one of these servers based on which servers are:

Available	If one application server is unavailable, Tarantella will choose another.
Under-used	Tarantella chooses the application server that is running the fewest applications via Tarantella.

To use multiple application servers in this way, you need to:

- Set the application object's **Application Server** attribute to **Use Hosts View**.
- Create a host object for each application server that can run the application.
- Add these host objects to the application object's Hosts view.

If you want to use multiple application servers to run a single application, the application must run in exactly the same way on each application server. This means the application must be installed in the same location on each application server.

7.2.2 Balancing applications across multiple application servers

In order to balance applications across multiple application servers:

- Step 1. Select **Organization** in the Hierarchy View List
- Step 2. Create a host object for each application server you want to run the application on.
- Step 3. Right-click the application object that represents the application you want to run on multiple application servers.
- Step 4. Select **Attributes**. The application object's attributes are shown in the Details pane.
- Step 5. Set the **Application Server** attribute to **Use Hosts View**.
- Step 6. Click **Appl** .
- Step 7. Right-click the application object again, then select **Hosts**. The Details pane shows the application object's Hosts view.
- Step 8. Drag the host objects for the servers you want to run this application from the Children pane into the application object's Hosts view.

When a user starts the application, Tarantella will choose one of the application servers from the application object's Hosts view based on load.

You can use host groups to collect host objects together, then add the host group to the application object's Hosts view.

You can also balance Tarantella sessions across multiple Tarantella servers to provide a faster, more robust service to your users.

Leaving the **Application Server** attribute blank instructs Tarantella to use the second tier machine as the application server.

7.2.2.1 Object attributes

Below is a list of the attributes you can set in Control Center for a host object. If you do not supply entries for each of the object's mandatory attributes, when you click **Appl** , Control Center will prompt you to do so (mandatory attributes appear in bold).

Object Name	The name of the host object in the Tarantella datastore. As with other object in Control Center, this name must be unique.
Label	The object's display name. On webtops this is the label shown for a link. In Control Center this is the tooltip for the object.
Icon	The name of an icon file to be associated with the object. You can choose one of the standard icons from the list of available icons. This list is part of an icon theme. If Tarantella can't find an icon file, it uses the default icon for the object type.
Host Name	The DNS resolvable name or (IP address) of the machine represented by this host object.
Try Tarantella Password	What to do if the user doesn't have a cached password entry.

7.3 Creating a Tarantella Array

Tarantella provides load-balancing services across Tarantella servers. This means that users are distributed across these servers to ensure the best possible overall performance for application access.

Using an array of Tarantella servers instead of a single standalone server helps provide a faster, more robust service to your users.

7.3.1 Tarantella load balancing

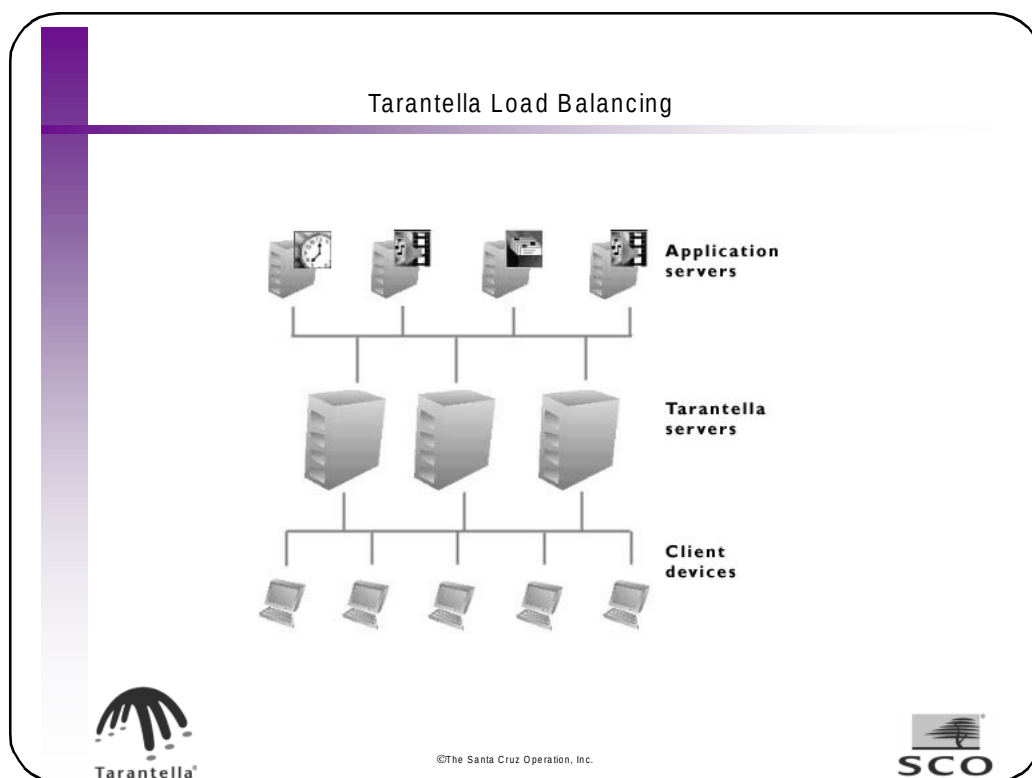
Tarantella software employs a number of default load-balancing mechanisms to distribute user access across the available Tarantella servers. The administrator can adjust the parameters for these mechanisms, if required, in order to 'tune' Tarantella load-balancing for that specific network configuration.

The load-balancing feature provides a mechanism for distributing users across available Tarantella servers. This provides an automated mechanism for distributing users across groups of Tarantella servers. Tarantella seamlessly redirects a user to another server when the initial choice is unavailable and prevents the administrator having to segregate users. Users are still able to enter a single Tarantella URL, for example <http://server/tarantella>.

Tarantella software implements load-balancing by automatically establishing a server preference list for each user, based on its knowledge of the available servers within that array. Each time a user attempts to connect, Tarantella software attempts to connect that user to the first choice server. If the first choice server is not available, it tries to connect the user to the second choice server and so on.

In addition to this, once a Tarantella session is established a server pointer is added to the server preference list. This means that Tarantella always tries to re-connect a user to the server that already has that user's 'resumable' session.

AV 7-4



Instructor Guide

7.3.2 Arrays of Tarantella servers

AV 7-4: Tarantella Load Balancing

Use this slide to illustrate the location of the Tarantella servers in the three-tier architecture.

An array contains one primary Tarantella server and a number of secondary Tarantella servers. The organizational hierarchy of the primary server is replicated to all secondary servers, to ensure users see the same webtop, and can use the same applications no matter which Tarantella server they are actually logged into.

Tarantella servers in an array don't need to run the same operating system — an array containing three different servers (HP-UX, Solaris and UnixWare 7, for example) works just as well as an array containing three identical servers. All the Tarantella servers in an array must be running the same version of Tarantella, however.

The primary Tarantella server is responsible for maintaining the definitive copy of the organizational hierarchy, and distributing it (and any changes made to it) to the secondary servers. To create an array, you first nominate a primary Tarantella server. This server's organizational hierarchy will be used for all Tarantella servers in the array. You can add secondary servers to the array to meet demand from your users or improve the robustness of Tarantella.

The load balancing table determines which Tarantella server a user logs into. You can configure this load balancing table to provide optimum performance for your users.

It's important that users have accounts on all the Tarantella hosts that they might be redirected to. If a user is redirected to a Tarantella server running on a host that user doesn't have an account on, they won't be allowed to log into Tarantella. You can use NIS to ensure that all the hosts in an array use the same user information.

You can run Control Center on any Tarantella server in the array — primary or secondary. However, you can only configure the organizational hierarchy from the primary server.

Only the organizational hierarchy is replicated between servers in an array. Each secondary server has its own emulator sessions, password cache and server configuration. This means that to delete a password cache entry, for example, you need to use Control Center on the appropriate Tarantella server.

Each server in an array must have Allow Port Access enabled to allow replication of the organizational hierarchy between servers.

7.3.3 Arrays and web servers

When Tarantella redirects users to another Tarantella server in an array, it does so by replacing the server name in the Tarantella URL.

For example, if a user logs into Tarantella using the following URL:

<http://boston.example.com/tarantella>

and the load balancing table specifies they should be redirected to seattle.example.com, Tarantella will redirect them to this new URL:

<http://seattle.example.com/tarantella>

This means all the web servers in an array must be configured in a consistent manner.

If a web server is configured to use the HTTPS protocol on port number 85 and is using the document directory “login”, users would supply this URL to access Tarantella:

<https://boston.example.com:85/login>

This time Tarantella redirects them to the following URL:

<https://seattle.example.com:85/login>

If seattle's web server doesn't allow HTTPS connections, doesn't use port 85 or doesn't use login as the document directory, the redirection will fail.

You must configure each web server in an array to use the same:

- Protocol (HTTP or HTTPS, for example)
- Port number
- Document directory
- cgi-bin

7.3.4 Arrays and the Tarantella URL

The Tarantella URL is the URL you give your users for logging into Tarantella. Usually it's of the form <http://server.example.com/tarantella>. Often, this URL points to the primary Tarantella server in an array. When users access this URL, they may be redirected to another server in the array, as described above.

If this server is unavailable (perhaps because of a problem with its network card), users won't be able to access that particular server.

If users know the name of another Tarantella server in the array, they can use that URL to access Tarantella.

A better solution is to let users use the same Tarantella URL (for example <http://tarantella.example.com>) no matter which Tarantella servers are available at any given time.

To do this you should configure your network so that the DNS name you use for the Tarantella URL is shared by all the Tarantella servers in your array, rather than pointing to a single server.

There are a number of ways you can do this:

Use a UNIX host to provide DNS services and configure the **bind** program to map this one DNS name onto the IP addresses of all the Tarantella servers in the array. See the manual page for bind for more information about how to do this.

Configure a router to provide DNS services and map the single DNS name onto the IP addresses of all the Tarantella servers in the array. See your router documentation for more information about how to do this.

7.3.5 Creating an array of Tarantella servers

To create an array of Tarantella servers, on a Tarantella host, execute:

tarantella array join --primary *p_server* --secondary *s_server*...

where *p_server* is a standalone Tarantella server that is to become the primary server in the array, and *s_server*... are standalone Tarantella servers that are to become secondary servers in the array.

- This command creates a new array containing a primary Tarantella server *p_server* and secondary Tarantella servers *s_server*...
- Use either DNS names or IP addresses to specify *p_server* and *s_server*....

WARNING: The existing organizational hierarchy of the new secondary server will be deleted, and replaced (and subsequently kept up-to-date) with the primary server's organizational hierarchy.

To create a new array, *p_server* must be a standalone Tarantella server. You can customize which servers a user may access when they log into Tarantella. You can add additional secondary Tarantella servers to the array at any time.

Tarantella servers in an array don't need to run the same operating system -- an array containing three different servers (HP-UX, Solaris and UnixWare 7, for example) works just as well as an array containing three identical servers. All the Tarantella servers in an array must be running the same version of Tarantella, however.

- All Tarantella servers in an array must use the same port number for their web servers.

7.3.6 Changing the primary server in an array

On a Tarantella host, execute:

tarantella array edit --newprimary *np_server*

where *np_server* is a secondary Tarantella server you want to promote to become the primary Tarantella server in its array.

- This command will fail if *np_server* isn't a secondary server.
- The old primary server will become a secondary server in the array.
- You can use either DNS names or IP addresses to specify *np_server*.

This command prompts a number of times for confirmation, once for each Tarantella server in the array

7.3.7 Adding a secondary Tarantella server to an array

On a Tarantella host, execute:

tarantella array join --primary *p_server* --secondary *s_server*

where *p_server* is the primary Tarantella server in the array you want to add the secondary server to, and *s_server* is the server you want to become a secondary server.

This command adds a secondary server, *s_server* to an existing array of Tarantella servers. You can only specify standalone servers here — you can't add servers to an array if they already belong to another array.

WARNING: The existing organizational hierarchy of the new secondary server will be deleted, and replaced (and subsequently kept up-to-date) with the primary server's organizational hierarchy.

If *p_server* is a standalone server, this command will create a new array with primary server *p_server*, and a single secondary server *s_server* .

You can use either DNS names or IP addresses to specify *p_server* and *s_server*.

7.3.8 Removing a server from an array

On a Tarantella host, type the following command:

tarantella array edit --detach *server*

where *server* is the Tarantella server you want to remove from the array.

You can only remove the primary Tarantella server from an array once you have removed all the secondary servers. The above command will fail if you specify *server* to be the primary server and there are still secondary servers that belong to the array. If you are unsure whether there are any remaining secondary servers, you can find out which Tarantella servers belong to an array.

Tarantella servers which are removed from an array become standalone servers, with an independent organizational hierarchy that starts as a copy of the array's hierarchy.

 This is a great way to duplicate servers!

You can use either DNS names or IP addresses to specify *server*.

7.3.9 Dismantling an array of Tarantella servers

To dismantle an array of Tarantella servers, you must:

- Find out which servers belong to the array.
- Remove all the secondary servers from the array.
- Remove the primary Tarantella server from the array.

You must remove all the secondary servers from an array before you can remove the primary server

7.4 Using a Tarantella Array

This section discusses the different commands associated with using a Tarantella array.

7.4.1 Displaying servers in an array

On a Tarantella host, type the following command:

tarantella array query --summary

This command displays information about the servers that are members of the same array as the UNIX host this command is run on. For each Tarantella server in the array, this command indicates how many users have applications running via that server.

7.4.2 Login into a particular Tarantella server in an array

At times, users want to go to a particular Tarantella server without redirection. For example, changes to the organization in Control Center can only be made from the primary server in the Tarantella array. Therefore, Tarantella administrators must log into the primary server.

Use the following URL to prevent Tarantella from redirecting you to another Tarantella server:

<http://server/tarantella/direct.html>

This is useful if you need to use Control Center to configure the organizational hierarchy for an array. You can only configure the organizational hierarchy for an array by logging into the primary Tarantella, then running Control Center.

You should also use this method if you need to use Control Center to configure the password cache, emulator sessions or server settings for a particular server in an array.

7.5 Balancing the Load across Tarantella Servers

Tarantella server arrays increase performance and availability by spreading the load across multiple servers. This mechanism is configurable by the Tarantella administrator via modifications to the load balancing table.

7.5.1 The load balancing table

Tarantella uses a load balancing table. The table is automatically replicated between all servers in the array, to decide which server to redirect a particular user to when they access Tarantella.

The load balancing table looks like this:

user1: server1 server2 server3 ...

user2: server2 server1 server3 ...

user3: server2 server3 server1 ...

user4: server3 server1 server2 ...

Each entry applies to a single user (identified by a Tarantella Federated Name name), and contains a list of Tarantella servers, in order of preference. One server in each entry is marked as the preferred server. This is the server Tarantella tries to redirect the user to when they log into Tarantella. If the preferred server is unavailable (perhaps because of hardware failure), Tarantella tries each server in the list in turn, until an available server is found. Tarantella then redirects the user to that server, where they are prompted for their password to finish logging in.

 If the server's Can Redirect To Primary attribute is disabled, Tarantella treats the primary server as being unavailable when consulting the load balancing table.

Administrators can add entries to the load balancing table using the **tarantella array distribute** command. If a user doesn't have an entry when they try to log into Tarantella, Tarantella automatically creates one containing all the servers in the array in a random order.

Consider the following load balancing table in an array where boston is temporarily unavailable:

```
.../_ens/Org/IT/rusty: seattle boston=PREF newyork
.../_ens/Org/IT/orange: boston newyork=PREF seattle
```

When **rusty** logs into Tarantella, Tarantella tries the following servers:

boston	It is the preferred server. This server isn't available, so Tarantella carries on looking:
seattle	It is the first in the list. This server is available, so Tarantella stops looking and rusty is redirected to the server “seattle”.

When the user **orange** logs into Tarantella, Tarantella tries the following server:

newyork	It is the preferred server. This server is available, so Tarantella stops looking. The user orange is redirected to the server “newyork”.
---------	--

If a user logs out of Tarantella leaving running emulator sessions, the server that user was last logged into becomes their preferred server. For example, if rusty in the above example leaves running emulator sessions on seattle when he logs out of Tarantella, seattle becomes his preferred server. The entry for **rusty** in the load balancing table will be modified to:

```
.../_ens/Org/rusty: seattle=PREF boston newyork
```

If you let Tarantella create entries for users when required, it will create entries containing all the servers in the array in a random order, ensuring that users are evenly distributed between available Tarantella servers. Initially, the preferred server will be the first server in the list. Tarantella Administrators are free to configure entries in the load balancing table. The **tarantella array distribute** command lets you:

- Add users to the load balancing table.
- Add and remove servers to those available to a user.
- Choose which servers Tarantella tries first for a particular user.

7.5.2 Adding a user to the load balancing table

To add users to the load balancing table, execute:

tarantella array distribute --person *person* --init

where *person* is the user you want to add to the load balancing table.

You can only run this command on the primary Tarantella server.

You can specify the preferred server for this user by changing the **--init** option in the above command to **--init preferred_server**, where *preferred_server* is a DNS name or IP address to specify preferred_server.

This command creates a new entry in the load balancing table for the specified user. The entry contains all the Tarantella servers in the array in a random order.

- Users without an entry can still log in. An entry will be automatically created for them, with a random order of all servers in the array.
- Use a TFN name to specify person, for example `_user / ruby` or `".../_ens/Org/Marketing/ruby"`.

7.5.3 Removing a user from the load balancing table

To remove a user from the load balancing table, execute:

tarantella array distribute --person *person* --exclude

where *person* is the user you want to remove from the load balancing table.

You can only run this command a primary Tarantella server.

Users without an entry can still log in: an entry will be automatically created for them, with a random order of all servers in the array

Use a TFN name to specify person, for example `_user/ruby` or `".../_ens/Org/Finance/ruby"`.

7.5.4 Making a Tarantella server available to a user

To make a server available to a user, type the following command:

tarantella array distribute --person *person* --include *server*

where *server* is the server you want to make available to *person*.

You can only run this command on the primary Tarantella server.

This command adds *server* at a random position in user's entry in the load balancing table. This command will fail if *person* isn't a valid Tarantella user or *server* isn't a Tarantella server in the array.

- Use a TFN name to specify *person*. For example `_user/orange` or `".../_ens/Org/IT/orange"`.
- Use a DNS name or IP address to specify *server*.

7.5.5 Removing a Tarantella server from those available to a user

To remove one of the servers available to a user, type the following command:

tarantella array distribute --person *person* --exclude *server*

where *server* is the server you want to make unavailable to *person*.

You can only run this command on the primary Tarantella server.

This command removes *server* from user's entry in the load balancing table. This command fails if *person* isn't a valid Tarantella user or has running emulator sessions on *server*.

Use a TFN name to specify *person*, for example `_user/rusty` or `".../_ens/Org/IT/rusty"`.

Use a DNS name or IP address to specify *server*.

7.5.6 Ordering the servers for a user

To order the servers for a user, type the following command:

tarantella array distribute --person person --order server1 server2 server3...

where *server1 server2 server3...* are the servers available to *person*.

You can only run this command on the primary Tarantella server.

Use a TFN name to specify *person*, for example `_user/rusty` or `.../_ens/Org/IT/rusty`.

Use a DNS name or IP address to specify *server*

7.6 Lesson Summary

This lesson described how Tarantella load balancing works, described an array of Tarantella servers, and showed you how to create an array of Tarantella servers. Additionally, this lesson described application server farms, and how to balance applications across multiple application servers.

7.7 Review Questions

1. What are the benefits of Tarantella load balancing?

- Increased Performance
- Increased Robustness
- Scalability

2. What is a host object?

A host object represents an application server in the Tarantella datastore. Host objects allow you to balance applications across multiple application servers.

3. What is the command line used to create an array?

```
tarantella array join --primary p_server --secondary s_server ...
```

4. What is the Load Balancing Table used for?

Tarantella uses the load balancing table to decide which server to redirect a particular user to when they access Tarantella.

5. How do you remove a server from an array?

The command to remove a server from an array is **tarantella array edit --detach server**

7.8 Lab: Creating an Application Server Farm

In this lab, you will perform the steps necessary to create an application server farm.

7.8.1 Overview

Your tasks in this lab are as follows:

- Create one host object for each application server
- Set an application object's **Application Server** attribute to **Use Hosts View**.

7.8.2 Procedure

The following steps detail how to create an application server farm.

Part I: Creating the Host Objects

Create a host object for each Tarantella server that will be a member of the array:

Step 1. Log into Tarantella as a Tarantella administrator.

Step 2. Run Control Center.

Create a host object for one of the application servers:

Step 3. Right click on the background of the children box.

Step 4. Select **New Object** ⇒ **Host**.

Step 5. Set the **Object Name** and **Label** attributes to the name of the application server.

Step 6. Set the **Host Name** attribute to the fully qualified domain name of the application server.

Step 7. Click the **Apply** button. Be sure to wait for the button to be grayed out.

Repeat steps 3 through 7 for each application server.

Part II: Configuring the Application to Use the Application Servers

- Step 1. Log into Tarantella as a Tarantella administrator.
- Step 2. Run Control Center.
- Step 3. Right click the **scocon** application object in the children box and select **Duplicate**. This will create a copy of the **scocon** object.
- Step 4. Change the name of the copy by setting the copy's **Object Name** and **Label** attributes to "Fancy scocon".
- Step 5. Change the **Application Server** attribute to **Use Hosts View**.
- Step 6. Click the **Apply** button. Be sure to wait for the button to be grayed out.
- Step 7. Right click the **Fancy scocon** object and select **Hosts**. The details pane now shows the hosts associated with this application.
- Step 8. Drag-and-drop the host objects that you created in Part I onto the details pane.

Part III: Using the Application

Now that you have configured the application (ie. **Fancy scocon**) to use the application servers:

- Step 1. Deploy the application to two Tarantella users
- Step 2. Log in simultaneously as both users
- Step 3. Launch **Fancy scocon** as each user
- Step 4. At the shell prompt, execute the **hostname** command.

 This test should show the two users on different application servers. Alternatively, you can show who is on which application server by looking in **Sessions** in Control Center.

7.9 Lab: Creating an Array of Tarantella Servers

In this lab, you will perform the steps necessary to create an array of Tarantella servers.

7.9.1 Overview

Your tasks in this lab are as follows:

- Choose the servers that will be used to create the array.
- Create the Tarantella array with the **tarantella array join** command.
- Verify that the servers are now part of an array with the **tarantella array query** command.
- Change the primary server in an array with the **tarantella array edit** command.
- Adding a user to the tarantella balance load table with the **tarantella array distribute** command.
- Dismantle the array of Tarantella servers.

Make sure that the servers that will be used to create the array are functioning properly, ie: users can connect to each Tarantella server.

7.9.2 Procedure

Part I: Creating an Array of Tarantella Servers

NOTE: The Tarantella Security Pack needs to be turned off on all servers involved.

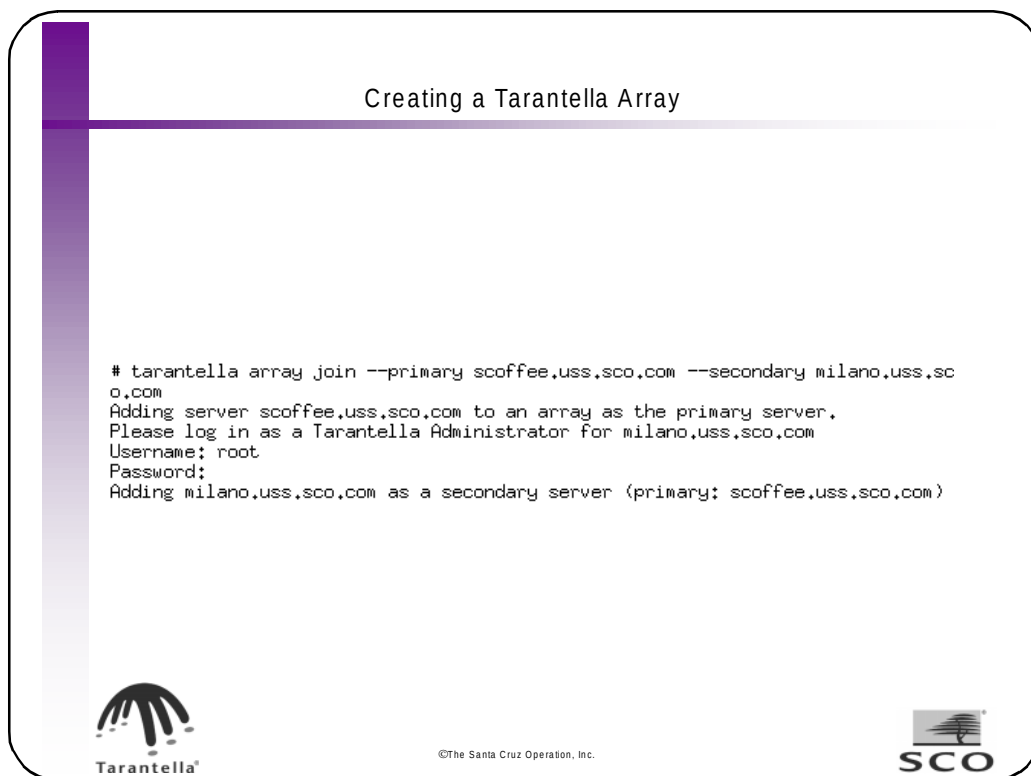
On the Tarantella host that will be designated as the primary server for this particular array, use the **tarantella array join** command to create the array:

```
# tarantella array join --primary redwood.example.com \  
--secondary ash.example.com
```

where *redwood.example.com* is the primary Tarantella server, and *ash.example.com* is the secondary server.

You will be prompted to log in as a Tarantella administrator for the secondary server, at which point you would login as root or the designated administrator login.

AV 7-5



Part II: Verifying that the Servers are Now Part of an Array

AV 7-5: Creating a Tarantella Array

Use this slide to illustrate the **tarantella array join** command.

To verify that the servers are now part of an array, the command **tarantella array query** can be used:

From the Tarantella host where you just created the array, execute:

```
# tarantella array query --summary
```

AV 7-6

Querying a Tarantella Array

```
# tarantella array query --summary
Name                               Users with sessions
scoffee,uss.sco.com (Primary)      0
milano,uss.sco.com                 0
```



©The Santa Cruz Operation, Inc.

Part III: Changing the Primary Server in an Array

In order to change the primary server in an array, on a Tarantella host, execute:

```
# tarantella array edit --newprimary milano.uss.example.com
```

This command converts a secondary server in an array to the primary server on an array. The old primary server should now be a secondary server in the array.

Part IV: Adding a User to the Load Balancing Table

AV 7-6: Querying a Tarantella Array

Use this slide to illustrate the **tarantella array query** command.

To add a user to the load balancing table, on the primary Tarantella host, execute:

```
# /opt/tarantella/bin/tarantella array distribute --person  
person --init
```

where *person* is the name of the user you are adding to the balance load table.

Use **tarantella array query --server *server*** to show the contents of the current load balancing table.

Part V: Dismantling an Array of Tarantella Servers

To dismantle the array of Tarantella servers, you will need to do the following steps:

Step 1. Find out which servers belong to the array. Execute:

```
# tarantella array query --summary
```

Step 2. Remove ALL of the secondary servers from the array. Execute:

```
# tarantella array edit --detach server
```

where *server* is the name of the server to be removed from the array.

Step 3. Once you have removed all of the secondary Tarantella array servers, you can proceed to remove the primary Tarantella array server with the same command as described on step 2.

7.10 Answers to Exercise and Review Questions

This section contains the answers to exercises, review questions, and labs presented in this lesson.

Exercise answers

Please consult your instructor if you have any questions about the exercises in this lesson.

Review Question Answers

This section contains the answers to the review questions on page 7-27.

1. Some of the benefits of Tarantella load balancing are:
 - Increased Performance
 - Increased Robustness
 - Scalability
2. A host object represents an application server in the Tarantella datastore. Host objects allow you to balance applications across multiple application servers.
3. `tarantella array join --primary p_server --secondary s_server ...`
4. Tarantella uses the Load Balancing table to decide which server to redirect a particular user to when they access Tarantella.
5. The command to remove a server from an array is **`tarantella array edit --detach server`**

8

Windows Connectivity Pack

Instructor Guide

Instructor Guide

Lesson 8

Windows Connectivity Pack

Suggested lesson duration

This lesson should take approximately four hours to complete including the lab.

Pre-lesson classroom preparation

The system on which Windows Terminal Server is installed on should have at least 96MB of RAM. Each student should also have their own laptop or secondary Windows machine.

It is easiest if all of the machines in the classroom are capable of booting from the CD-ROM. If this is not possible, then three (four for Windows 2000) floppies are needed for each machine incapable of booting from CD-ROM.

Install Windows NT Server 4.0 Terminal Server Edition and Service Pack 5.

Instructor preparation

Although a Tarantella machine is not needed for this lesson, there needs to be at least one Tarantella server available at the end of the lesson (perhaps the instructor's machine). Do not convert all of the machines in the classroom to Windows Terminal Server or Windows 2000.

The lesson requires that the students know their machine name, IP address, subnet mask and DNS server. If their machines have an ISA networking card or a non-recognized networking card, then the parameters (IRQ, Base address, etc.) will need to be provided to the student.

Introduction

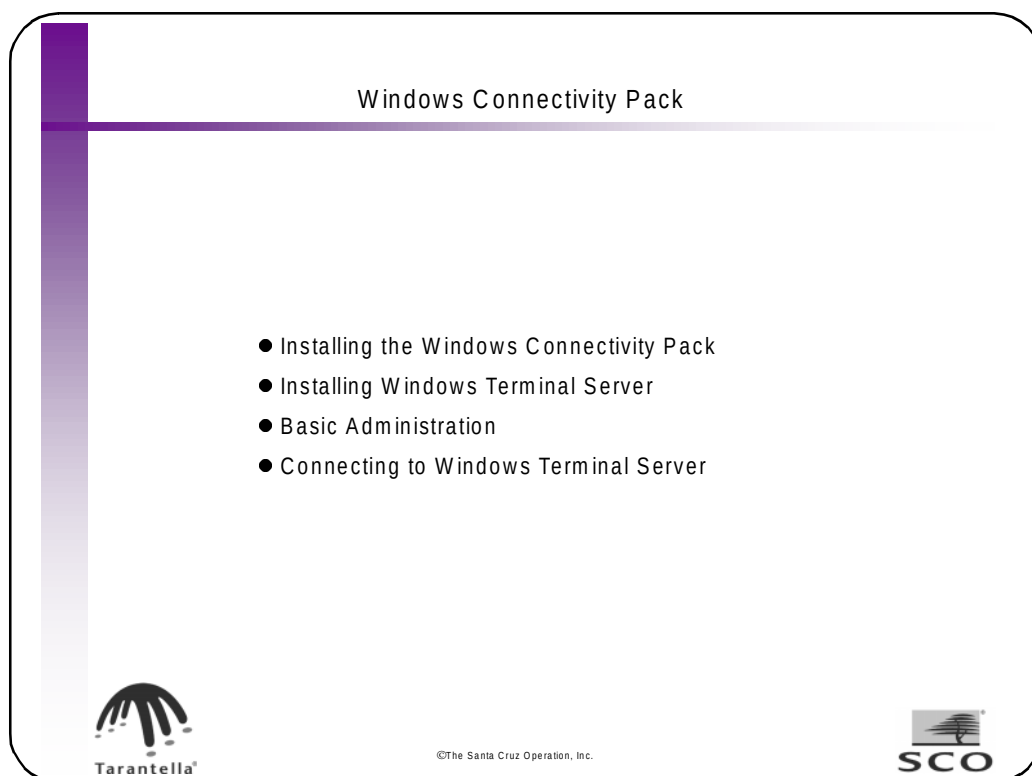
Many customers want Windows interconnectivity. The Windows Connectivity Pack is designed to provide this connectivity. To use the Windows Connectivity Pack effectively, it is important that Tarantella administrators at least become familiar with the Microsoft servers being used in the corporate workplace. This chapter explains installation, basic administration and connectivity of Windows Terminal Server and Windows 2000.

Objectives

By the end of this lesson, you will be able to:

- Install Windows Terminal Server Edition and Windows 2000
- Add applications, users, and perform other basic Terminal Server administration tasks
- Connect to a Windows Terminal Server from a Microsoft Terminal Server Client
- Configure Windows application object in Tarantella to enable users to launch Windows applications from Tarantella

AV 8-1



Topics

In order to meet these objectives, this lesson discusses:

- Installing the Windows Connectivity Pack — Discusses how to install the Windows Connectivity Pack onto a Tarantella server.
- Installing Windows Terminal Server — Discusses how to install Windows Terminal Server from CD-ROM (with or without floppies).
- Basic Administration — Discusses application installation and user creation. Points out which client connectivity programs are most useful to an administrator.
- Connecting to Windows Terminal Server — Shows how to install Microsoft Terminal Server Client and connecting to the Windows Terminal Server.

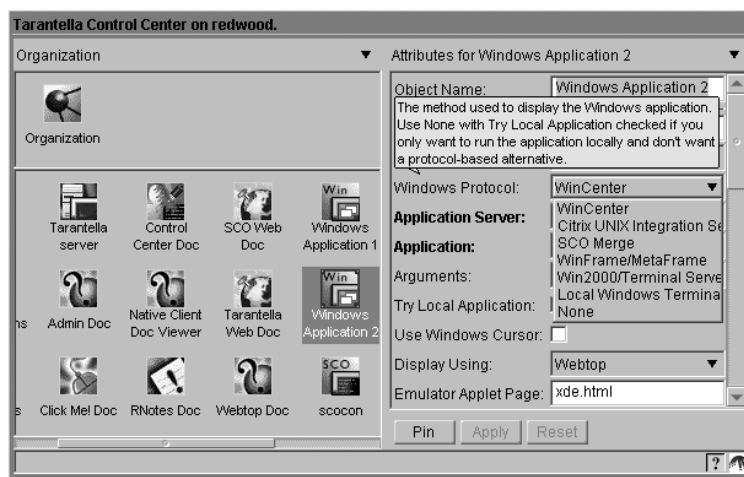


AV 8-1: Installing Tarantella

The first slide describes the overall topics covered in this lesson.

AV 8-2

Selecting a Windows Protocol



©The Santa Cruz Operation, Inc.



AV 8-3

The "None" Protocol

Second Tier



AIP

First Tier



Application runs locally on client



©The Santa Cruz Operation, Inc.



8.1 Choosing a Windows Protocol

AV 8-2: Selecting a Windows Protocol

Use this slide to illustrate where, in Control Center, you select the protocol to use when running a Windows application. Point out the six different protocols.

One of the design goals of Tarantella is to broker Windows programs. In response to the ever-shifting Windows market place, Tarantella now has six different protocols to choose from when brokering a Windows application.

8.1.1 The “None” protocol

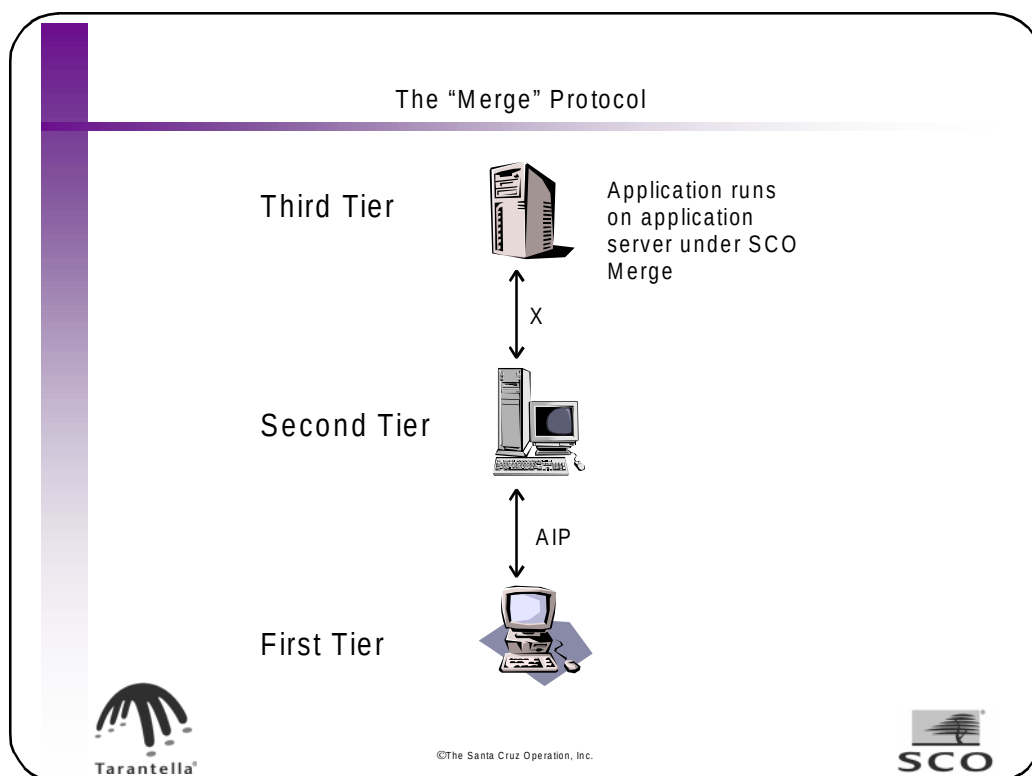
AV 8-3: The “None” Protocol

Use this slide to illustrate the “None” protocol.

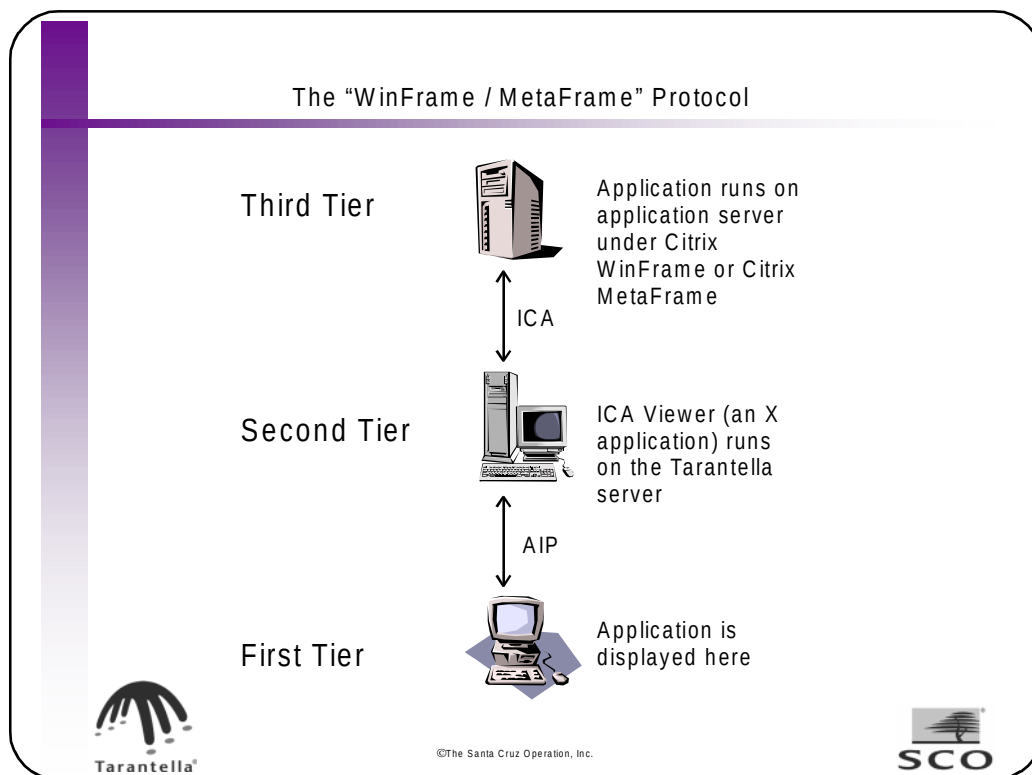
Use this protocol to run Windows programs that reside on the Windows client itself. When the user activates the application, the Tarantella server runs that application on the client. This is illustrated in AV 8-3 on page 8-8.

This protocol is used in conjunction with the “Try Local Application” checkbox on the windows application attributes form. In other words, if you chose “None” as your Windows protocol, you additionally need to check the “Try Local Application” checkbox.

AV 8-4



AV 8-5



8.1.2 The “SCO Merge” protocol

AV 8-4: The “SCO Merge” Protocol

Use this slide to illustrate the “SCO Merge” protocol.

Use this protocol to run an application on a UNIX server under SCO Merge.

8.1.3 The “WinFrame / MetaFrame” protocol

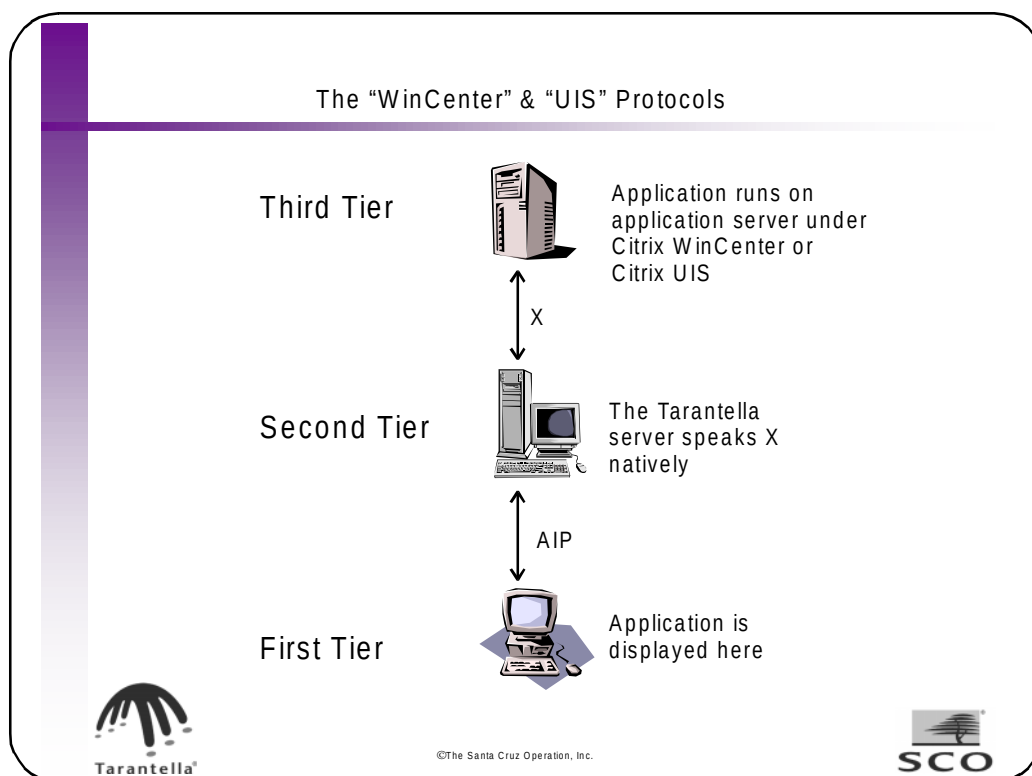
AV 8-5: The “WinFrame / MetaFrame” Protocol

Use this slide to illustrate the “WinFrame / MetaFrame” protocol.

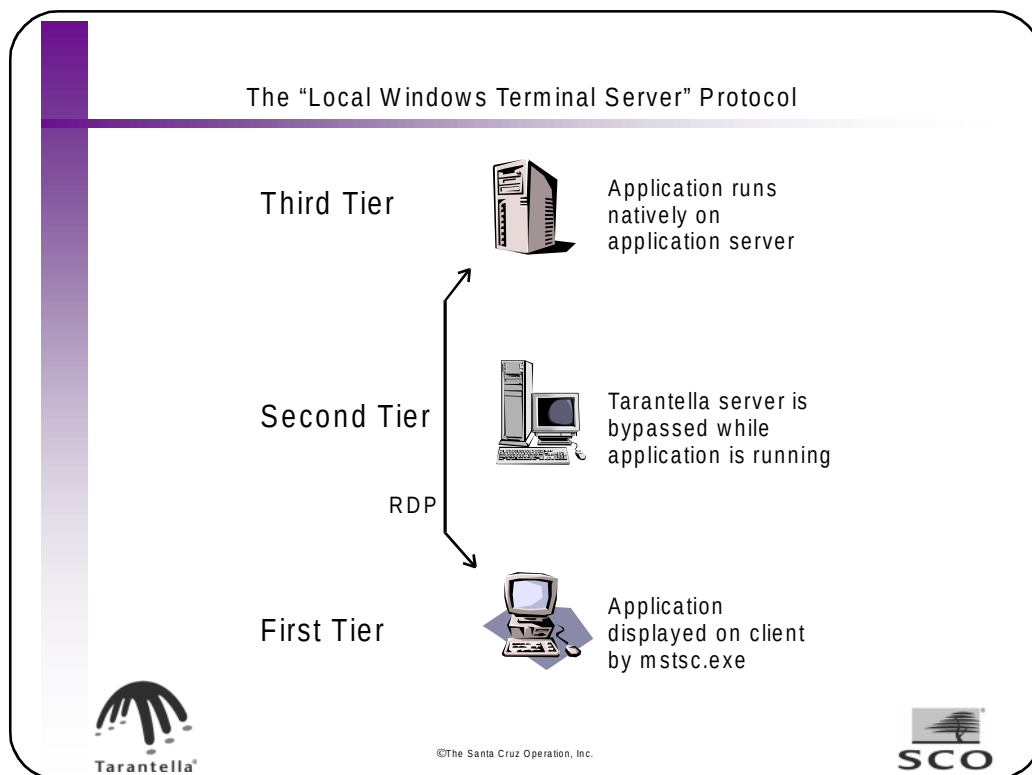
Use this protocol to run an application under Citrix WinFrame or MetaFrame.

Citrix WinFrame and Metaframe enable Windows applications running on an application server to be displayed on another machine running the *ICA viewer*. The ICA viewer is an X application. By running the ICA viewer on the Tarantella server, Tarantella is able to speak *ICA* to the application server and display the application on the Windows client via the AIP protocol.

AV 8-6



AV 8-7



8.1.4 The “WinCenter & UIS” protocol

AV 8-6: The “WinCenter / UIS” Protocol

Use this slide to illustrate the “WinCenter” and “UIS” protocols in Section 8.1.4 and Section 8.1.5 .

Use this protocol when the Windows application is being run under either of the following products:

- NCD WinCenter
- Citrix/NCD UNIX Integration Service (UIS)

Since WinCenter and UIS speak X, displaying them on the Windows client via Tarantella is just as easy as displaying any other X application.

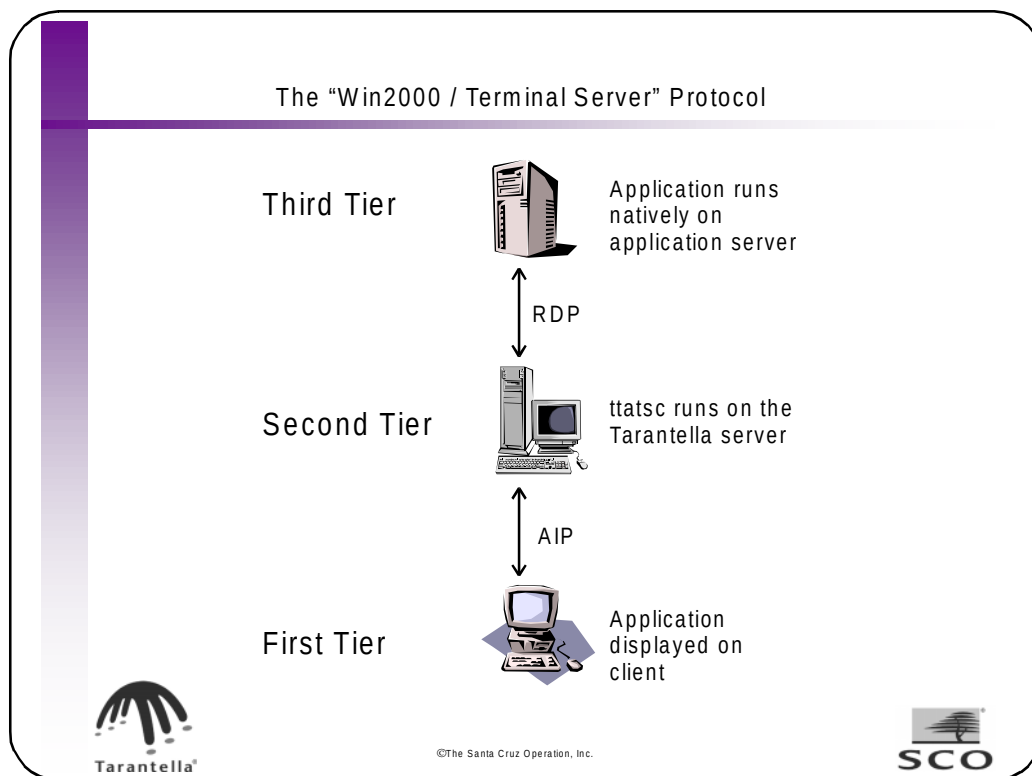
8.1.5 The “Local Windows Terminal Server” protocol

AV 8-7: The “Local Windows Terminal Server” Protocol

Use this slide to illustrate the “Local Windows Terminal Server” protocol.

Use this protocol when the Windows client already has *mstsc.exe* installed. This executable uses Microsoft’s Remote Desktop Protocol (RDP) to communicate directly to the application server. Tarantella only initiates the connection between the Windows client and the Windows server.

AV 8-8



Instructor Guide

8.1.6 The “Win2000/Terminal Server” protocol

AV 8-8: The “Win2000/ Terminal Server” Protocol

Use this slide to illustrate the “Win2000/ Terminal Server” protocol.

This protocol allows the first and third tiers to remain untouched. There is no need for the Microsoft Terminal Server Client or a third party product on the application server. This protocol is added to the Windows Protocols pull down menu in Control Center when the Windows Connectivity Pack is installed.

Make sure students understand how the “Win2000/Terminal Server” is added to the pull down menu.

Use the Windows Connectivity Pack when:

- Load balancing is required
- Better compression is required

Citrix sets up the parameters for compression when the session is initiated. Imagine you and 500 of your co-workers show up at 8:00 a.m. You start hitting the Windows server via Citrix all at once. Therefore your bandwidth is considered limited. This means you are considered a low bandwidth connection for the rest of the day.

- Encryption is required

WCP and TSP can work together. RDP supports low and medium (not high) encryption between the 2nd and 3rd tiers. The full TSP strength encryption can be used between the 1st and 2nd tiers.

The Windows Connectivity Pack installs a new binary on the Tarantella server called *ttatasc*. This program speaks RDP to the Windows server and communicates with the client via Tarantella’s AIP protocol.

A few limitations of the WCP:

- Tarantella’s third tier load balancing doesn’t take into account disconnected Windows Terminal Server sessions (it orphans them)
- Cursors are made monochrome and mapped onto available Java cursors
- You cannot use an X window manager

8.2 Installing the Windows Connectivity Pack

The installation and removal mechanisms in the Windows Connectivity Pack have been designed to be reliable and easy to use. The installation procedure is essentially same as the procedure detailed in Lesson 2: “Installing Tarantella.”

The Windows Connectivity Pack software runs on the following platforms:

- UnixWare 2.1.2+
- UnixWare 7+
- SCO OpenServer 5.0.2+
- Compaq Tru64 UNIX 4.0d+
- SPARC Solaris 2.5.1+
- IBM AIX 4.2+
- HP-UX 10.20+

8.2.1 Distribution media

The Windows Connectivity Pack software is distributed two ways:

Via the web

The Windows Connectivity Pack product (along with other Tarantella products) can be downloaded from <http://tarantella.sco.com>. Web-distribution is the primary method of distribution.

On CD-ROM

In special instances, SCO distributes the software on CD-ROM. This is not the primary method of distribution.

Table 7: Hints for Using CD-ROMs on SCO Platforms

SCO OpenServer 5	<code>mount -f HS -o ro,lower /dev/cd0 /mnt</code>
SCO UnixWare 7 SCO UnixWare 2.1	<code>/usr/sbin/mount -rF cdfs /dev/cdrom/cdrom1 /mnt</code>

8.2.2 Installation procedure

To install the Windows Connectivity Pack, follow this procedure:

Step 1. Log in as root.

There is no single-user mode requirement.

Step 2. Mount the CD-ROM.

Step 3. Run the following command:

```
sh wcp_file.shx
```

where *wcp_file.shx* is one of the following file names:

Table 8: Windows Connectivity Pack SHX File Names

Platform	SHX File name
SCO UnixWare® 7+	wcpi3un.shx
SCO UnixWare 2.1.2+	wcpi3un.shx
SCO OpenServer Release 5.0.2+	wcpi3sc.shx
HP-UX 10.20+	wcppahp.shx
IBM AIX 4.2+	twcprsai.shx
SPARC Solaris 2.5.1+	wcpspso.shx
Compaq Tru64 UNIX 4.0d+	wcpaxo1.shx

Step 4. Follow the on-screen prompts.

Now that the Windows Connectivity Pack is installed, “Windows 2000/Terminal Server” is the default windows protocol which creating Windows application objects in Control Center.

Exercise: Installing the Windows Connectivity Pack

Install the Windows Connectivity Pack on your Tarantella server. Once installed, verify that “Win2000 / Terminal Server” is the default windows protocol when Windows application objects are created.

8.2.3 Licensing issues

The Windows Connectivity Pack uses only one license per product (as implemented by Microsoft’s RDP protocol). You must still comply legally with Microsoft’s licensing policies. Furthermore, you need licenses for whatever applications you are running.

8.2.4 Scalability and performance

When using the Windows Connectivity Pack, there are no additional requirements on the Windows Terminal Server.

Up to 10Mb of graphics caching could occur on the Tarantella server.

This 10Mb cache limitation is no worse than the Windows Terminal Server client and is a feature of the RDP protocol.

CPU usage is minimal but proportional to the amount of incoming graphics.

There is latency due to the extra hop involved.

8.2.5 Installing applications

When you install an application under Windows Terminal Server or Windows 2000, Microsoft requires that you use the **Add/Remove Programs** utility to install the application. Failure to do so will result in the application only being available to the administrator.

In Windows 2000, you can often recover gracefully if you forget to use **Add/Remove Programs**. If, for instance, you unintentionally let the application install from the autorun script on the CD-ROM, you can go into **Add/Remove Programs**, select the application from the list of applications, and click the **Change** button. Note, however, that if the button says “Change / Remove”, clicking the button will *remove* the application.

The requirement to run **Add/Remove Programs** is imposed by Microsoft, not Tarantella. You have to use **Add/Remove Programs** with similar products such as Citrix.

8.2.6 Application compatibility scripts

Some applications such as Microsoft Office 97 provide an “application compatibility script” which must be run in order to make the application multi session ready. An example of running is given in Section 8.13 on page 8-47.

Not all applications provide an application compatibility script. Consult your application’s documentation to see whether an application compatibility script is required.

The requirement to run the application compatibility scripts is imposed by Microsoft, not Tarantella. You have to run the application compatibility scripts with similar products such as Citrix.

8.2.7 Deploying Windows applications under Tarantella

Creating application objects under Tarantella for Windows applications is similar to creating application objects for other application types. When using the Windows Compatibility Pack:

- Step 1. In Control Center, right-click on the background of the **children box**.
- Step 2. Select **New Object** ⇒ **Windows Application**.
- Step 3. Set the **Object Name**, **Label**, and **Icon** attributes as usual.
- Step 4. Set the **Windows Protocol** attribute to **Win2000/Terminal Server**.
- Step 5. Set the **Application Server** attribute to the fully qualified DNS-resolvable name of the Windows server.
- Step 6. Set the **Application** attribute to the pathname of the application (using “\” as the path delimiter).

Alternatively, set the **Application** attribute to “-” to have the application object display the Windows desktop.
- Step 7. Specify any arguments as needed in the **Arguments** attribute.
- Step 8. Check **Use Windows Cursor** .
- Step 9. Set the **Display Using** attribute as desired.
- Step 10. Click **Appl** .
- Step 11. Deploy this Windows application object.

8.3 Installing Windows Terminal Server and Windows 2000

The installation of Microsoft's NT-based products has not changed much in five years. The installation of Windows Terminal Server and Windows 2000 is very much like Windows NT 3.51. What has been added is device driver information and a few questions that are specific to a terminal server and licensing.

8.3.1 Windows Terminal Server and Windows 2000 requirements

Windows Terminal Server and Windows 2000 are multi user platforms. Hosting multiple users and running such a graphically intensive operating system puts a heavy load on the system memory. The server should have at least 96MB of RAM.

With only 64MB of RAM, system resources become overtaxed and various subsystems fail to run properly. This course can be finished with an under-configured machine, certain errors will arise but the bulk of the concepts and materials can be completed.

8.3.2 Distribution media and creating installation floppies

Both Windows Terminal Server and Windows 2000 come on a single bootable CD. If the machine is unable to boot from the CD-ROM, there are one of two likely problems occurring:

- The machine supports bootable CD-ROMs but is improperly configured.
- The machine does not support bootable CD-ROMs

If the machine supports booting from CD-ROM but is improperly configured, invoke the computer's CMOS setup utility to change the applicable BIOS setting(s). CMOS setup utilities vary from manufacturer to manufacturer. Consult your hardware manual for information about your computer's CMOS setup utility.

 Be prepared to assist students in setting up booting from CD-ROM if the machines support this feature.

If the machine does not support bootable CD-ROMs, you can create a set of floppies by following these steps:

Step 1. Insert the Windows Terminal Server or Windows 2000 CD-ROM into the drive on a Windows machine.

Step 2. Assuming your CD-ROM is D:, select **Start** ⇒ **Run**

Step 3. For Windows Terminal Server, type: `D:\i386\winnt.exe /ox`

For Windows 2000, type: `D:\bootdisk\makeboot a:`

This will bring up a DOS window and ask for high-density floppies. These floppies will become the install disks for the server.

8.3.3 Installing Windows 2000 Advanced Server.

The process for performing a complete installation of Windows 2000 Advanced Server is outlined in the lab in Section 8.9 on page 8-36.

If you are using Windows 2000 in the classroom, have the students perform the lab before proceeding. Make sure they do not perform the following labs:

- Installing Windows Terminal Server (Section 8.10 on page 8-40)
- Installing Service Pack 5 for Windows Terminal Server (Section 8.11 on page 8-44)
- Installing Internet Explorer 5.0.1 (Section 8.12 on page 8-46)

8.3.4 Installing Windows Terminal Server

The process for performing a complete installation of Windows Terminal Server is outlined in the lab in Section 8.10 on page 8-40.

In addition to performing the basic installation, you should also perform the steps outlined in the labs in Section 8.11 on page 8-44 and Section 8.12 on page 8-46. These labs install Service Pack 5 for Windows Terminal Server and Internet Explorer, respectively.

Have the students do the labs before proceeding.

8.4 Crucial information for Windows Terminal Server

This section details the information that you need to know as a Tarantella administrator when working with Windows Terminal Server.

8.4.1 Service Pack Installation

Service Pack 5 for Windows Terminal Server needs to be installed to enable Tarantella to work correctly with RDP. Instructions for installing Service Pack 5 are given in Section 8.11 on page 8-44.

If students installed Windows Terminal Server during the lab, have them perform the Service Pack installation lab in Section 8.11 on page 8-44.

8.4.2 Windows Terminal Server administration

While there are numerous utilities in Windows Terminal Server, only a few are relevant to RDP. All of these utilities can be found by selecting **Start** ⇒ **Programs** ⇒ **Administrative Tools (Common)**.

Terminal Server Administration

This is one of the more useful utilities to Tarantella administrators using Microsoft's RDP services. You can view what processes a user is running by clicking on the user. Information about the RDP protocol information can be determined with this utility.

Terminal Server Connection Configuration

The security section is probably the only section to be frequently used here. However, if there are several cards or protocols (RDP and ICA), this program can help segregate traffic.

User Manager for Domains

A very useful program and is discussed in the next section.

8.4.3 User creation

One of the most common tasks performed on a multi user machine is the creation of users. To create users in Windows Terminal Server:

- Step 1. Log in as **Administrator**.
- Step 2. Start the **User Manager for Domains**.
- Step 3. Choose **User** ⇒ **New User** .
- Step 4. Enter the name and password.
- Step 5. Choose **Config**.
- Step 6. Change “on a broken or timed-out connection” to **reset**.

Both Tarantella and Windows Terminal Server can handle session resume. Whereas Tarantella calls this “session resumability” Windows Terminal Server calls this “session disconnection.” To save resources on the Terminal Server, let Tarantella handle the resumability.

- Step 7. Click **Add**.
- Step 8. Click **Close**.

8.4.4 Disconnect, logoff and shutdown

There are several different ways to quit a Windows Terminal Server session.

- | | |
|------------|--|
| Disconnect | Start ⇒ Disconnect . This will log the user out but leave the programs running. When the user logs in again, they will be at the same spot and screen as when they disconnected. |
| Logoff | Start ⇒ Logoff . This will log the user off and close the users running applications. |
| Shutdown | This will shutdown the entire server. You can shutdown the system by selecting Start ⇒ Windows NT Security ⇒ Shutdown . |

Alternately, you can type **CTRL** **ALT** **DEL** at the console to display the Windows NT Security window and then select **Shutdown**.

8.5 Crucial information for Windows 2000

This section details the information that you need to know as a Tarantella administrator when working with Windows 2000.

8.5.1 Windows 2000 betas

The Windows 2000 betas are not supported by Tarantella.

8.5.2 RDP support

When using the “Win2000/Terminal Server” protocol (see Section 8.1.6 on page 8-15) in Tarantella, you must use a version of Windows 2000 which supports RDP (Remote Desktop Protocol). For instance, Windows 2000 Advanced Server supports RDP, whereas Windows 2000 Professional Edition does not.

8.5.3 Terminal Server 4.0 compatibility

During the installation of Windows 2000, the “Terminal Services Setup” screen prompts whether you want:

- “Permissions compatible with Windows 2000 Users” or
- “Permissions compatible with Terminal Server 4.0 Users”

You must select the latter.

8.5.4 Utilities for configuring Terminal Services

There are three utilities used for configuring Terminal Services under Windows 2000:

Terminal Services Client Creator	Used for creating setup floppies used to install the Microsoft Terminal Server Client (see Section 8.6 on page 8-31).
Terminal Services Configuration	Used to configure various settings for RDP connections. This utility is described in the follow sections.
Terminal Services Manager	Used to control RDP sessions. This utility enables the Windows administrator to send messages to RDP users, disconnect RDP users, reset RDP sessions, and perform other administrative tasks.

8.5.5 Disabling interactive login

Windows 2000 forces interactive login by default. Even if the password used by Tarantella for the authentication between the second- and third-tier servers is correct, Windows 2000 still prompts the user to enter a password. To turn off interactive login:

- Step 1. **Start ⇒ Programs ⇒ Administrative Tools ⇒ Terminal Services Configuration.**
- Step 2. Double-click **RDP-Tcp** under the Connection column.
- Step 3. Under the **Logon Settings** tab, check **Use client-provided logon information.**
- Step 4. Uncheck **Always Prompt for Password.**

 Alternatively, you can leave Always Prompt for Password checked to allow users to log into different Windows 2000 accounts.

8.5.6 Installation of Terminal Services

During the installation of Windows 2000, you are given the opportunity to install Terminal Services. It is this component that installs RDP. If you fail to install Terminal Services during the installation of Windows 2000, you can install it after the installation:

- Step 1. Log in as **Administrator**.
- Step 2. Select **Start ⇒ Settings ⇒ Control Panel ⇒ Add/Remove Programs ⇒ Add/Remove Windows Components**.
- Step 3. Check **Terminal Services**.
- Step 4. Click **Next**.
- Step 5. Choose **Application server mode** on the “Terminal Services Setup” screen.
- Step 6. Click **Next**.
- Step 7. Click **Finish**.

8.5.7 Installation of Print Services for Unix

If you plan to use Tarantella’s follow-me printing feature from Windows 2000, you must install “Print Services for Unix”:

- Step 1. Log in as **Administrator**.
- Step 2. Select **Start ⇒ Settings ⇒ Control Panel ⇒ Add/Remove Programs ⇒ Add/Remove Windows Components**.
- Step 3. Highlight **Other Network File and Print Services**.
- Step 4. Click **Details...**
- Step 5. Check **Print Services for Unix**.
- Step 6. Click **OK**.
- Step 7. Click **Next**.
- Step 8. Click **Finish**.

8.5.8 Creating user accounts

To create user accounts in Windows 2000:

- Step 1. Log in as **Administrator**.
- Step 2. Select **Start** ⇒ **Programs** ⇒ **Administrative Tools** ⇒ **Computer Management**.
- Step 3. Double-click **Local Users and Groups**.
- Step 4. Highlight **Users**.
- Step 5. Select **Action** ⇒ **New User...**
- Step 6. Provide the information requested.
- Step 7. Uncheck **User must change password at next logon**.
- Step 8. Uncheck **Account is disabled**.
- Step 9. Click **Create**.

8.5.9 Using the Windows 2000 “guest” account

Windows 2000 automatically creates a “guest” account. However the guest account is not configured for use under RDP. To make the guest account available via RDP:

- Step 1. Log in as **Administrator**.
- Step 2. Select **Start** ⇒ **Programs** ⇒ **Administrative Tools** ⇒ **Terminal Services Configuration**.
- Step 3. Double-click **RDP-Tcp** under the Connection column.
- Step 4. Under the **Permissions** tab, click **Add...**
- Step 5. Highlight **Guest**.
- Step 6. Click **Add**.
- Step 7. Click **OK**.

8.5.10 Resetting connections

Windows 2000 has a feature much like Tarantella's session resumability feature. Under Windows 2000, sessions can be "disconnected." Tarantella cannot connect to disconnected sessions.

If you plan to have only Tarantella brokered connections to Windows 2000:

- Step 1. Log in as **Administrator**.
- Step 2. Select **Start** ⇒ **Programs** ⇒ **Administrative Tools** ⇒ **Terminal Services Configuration**.
- Step 3. Double-click **RDP-Tcp** under the Connection column.
- Step 4. Under the **Sessions** tab, check the *second* checkbox labeled **Override user settings**.
- Step 5. Check **End Session**.
- Step 6. Click **OK**.

Making the changes detailed above will prevent Windows 2000 from creating disconnected sessions.

If you plan to have non-Tarantella connections to Windows 2000 (eg. RDP client connections from *mstsc.exe*) you can allow Windows 2000 to disconnect sessions, but it is recommended that you specify a period of time after which to reset disconnected sessions:

- Step 1. Log in as **Administrator**.
- Step 2. Select **Start** ⇒ **Programs** ⇒ **Administrative Tools** ⇒ **Terminal Services Configuration**.
- Step 3. Double-click **RDP-Tcp** under the Connection column.
- Step 4. Under the **Sessions** tab, check the *first* checkbox labeled **Override user settings**.
- Step 5. Select a value for **End a disconnected session** (eg. 1 Hour). This will allow users a period of time to re-connect. More importantly, this will prevent Tarantella users from creating sessions that will never reconnect.
- Step 6. Under the **Sessions** tab, uncheck the *second* checkbox labeled **Override user settings**.
- Step 7. Check **End Session**.
- Step 8. Click **OK**.

8.6 Microsoft Terminal Server client

Make sure the students understand that *mstsc.exe* is not necessary when using Tarantella. This section is provided to allow students to see what users see when they use Microsoft's way of connecting to Windows Terminal Services.

The Microsoft Terminal Server Client (also known as *mstsc.exe*) is the program that Microsoft expects people to use to access systems running Windows Terminal Server Edition and Windows 2000. This utility isn't required when using Tarantella's "Win2000/Terminal Server" protocol (see Section 8.1.6 on page 8-15).

While *mstsc.exe* is not needed under Tarantella, it is useful to see *mstsc.exe* in action in order to understand the advantages of Tarantella.

To install *mstsc.exe* from the Windows Terminal Server CD-ROM:

- Step 1. Insert the Windows Terminal Server CD-ROM into your Windows client.

 If an installation window pops up, close the window. *Do not* install Windows Terminal Server on your Windows client.
- Step 2. **Start** ⇒ **Run** ⇒ **Browse** and browse to the CD-ROM to
 \CLIENTS\TSCLIENTS\WIN32\I386\DISK1\SETUP.EXE
- Step 3. Click the **Open** button.
- Step 4. Click the **OK** button.
- Step 5. Accept all of the defaults.

Make sure that the students understand that the procedure above is for administrators who have the Windows Terminal Server Edition CD-ROM. This CD-ROM is taken directly to the client machine.

The procedure following, on the other hand, is for administrators who have access to a Windows 2000 server with Terminal Services installed. This procedure is used to create two (or more) floppies on the Windows 2000 system and then taken to the client machine for installation.

Alternatively, you can create setup floppies under Windows 2000:

- Step 1. On a Windows 2000 server, select **Start** ⇒ **Programs** ⇒ **Administrative Tools** ⇒ **Terminal Services Client Creator**
- Step 2. Select “Terminal Services for 32-bit x86 windows”.
- Step 3. Specify which floppy drive to use.
- Step 4. Indicate if you want the floppies formatted.
- Step 5. Click the **OK** button.
- Step 6. The floppy creator tool prompts for you to insert the first floppy. Click the **OK** button.
- Step 7. The floppy creator tool prompts for you to insert the second floppy. Click the **OK** button.
- Step 8. Click the **OK** button when the tool reports that the floppies have been successfully created.
- Step 9. Insert the floppies into the floppy drive on the Windows client.
- Step 10. Click **Start** ⇒ **Run...**
- Step 11. Type “a:\setup.exe”.
- Step 12. Click the **Continue** button.
- Step 13. Enter your name and organization.
- Step 14. Click the **OK** button.
- Step 15. Click the **OK** button to confirm your information.
- Step 16. Click the **I Agree** button to accept the license agreement.
- Step 17. Click the “large button” to start the installation.
- Step 18. Click the **Continue** button.
- Step 19. Insert the second floppy when prompted and click the **OK** button.
- Step 20. Click the **OK** button.

Now that you have installed the Microsoft Terminal Server Client using either of the procedures outlined above, you can run the Terminal Server Client:

Step 1. **Start ⇒ Programs ⇒ Terminal Server Client ⇒ Terminal Server Client**

Step 2. In the dialog box, enter the IP Address or machine name of the Windows Terminal Server and Click the **Connect** button.

NOTE: Using the Microsoft Terminal Server Client there are only three resolutions possible. In contrast, Tarantella is not limited to these three resolutions.

Exercise: Install Microsoft Terminal Server Client and Attach to the Windows Terminal Server

Install the Microsoft Terminal Server Client and connect to a server running Windows Terminal Server Edition or Windows 2000 using various resolutions.

8.7 Lesson Summary

This lesson described how to install Windows Terminal Server and applications as well as basic administration and client connectivity. What has just been completed is generally what is done in a Microsoft-oriented corporate installation. All the clients would have Microsoft Terminal Server Clients installed and the servers would be Windows NT Terminal Server Edition. This methodology enhances the fat client paradigm since it requires specialized software on each Windows client.

8.8 Review questions

1. How many different windows protocols does Tarantella support (including None).

There are six Windows protocols: None, SCO Merge, WinFrame/MetaFrame, WinCenter/UIS, Local Windows Terminal Server and Win2000/Terminal Server.

2. If you have lost the floppies necessary for installing Windows Terminal Server or Windows 2000, how do you make new ones?

For Windows Terminal Server - D:\i386\winnt.exe /ox
For Windows2000 - D:\bootdisk\makeboot a:

3. How many different resolutions does the standard Microsoft Terminal Server Client have? Does Tarantella suffer from this same limitation?

Three. 640x480, 800x600, 1024x768. Tarantella can have any arbitrary resolution.

4. When logging into Windows NT Terminal Server Edition for the first time, what is the username to be used (assuming the machine is not a domain member)?

The name to use when first logging in is Administrator.

8.9 Lab: Installing Windows 2000

 This lab can be performed as an instructor led demo.

In this lab, you will install Windows 2000 Advanced Server onto your application server.

8.9.1 Overview

Your tasks in this lab are twofold:

- Create the boot floppies required by the installation (see Section 8.3.2 on page 8-21) or set up your machine to boot from CD-ROM
- Install Windows 2000

The instructor will point you to where you can obtain the necessary software.

8.9.2 Procedure

In this lab we assume that you are booting from CD-ROM. If this is not the case, see Section 8.3.2 on page 8-21 for information on creating installation floppies.

In addition, this lab makes the following assumptions:

- Your system requires no SCSI or RAID drivers
- You are using the entire disk for Windows 2000

To install Windows 2000 Advanced Server, follow this procedure:

- | | |
|---------|--|
| Step 1. | Insert the Windows 2000 Advanced Server CD-ROM (and boot floppy #1 if you are installing from floppy). |
| Step 2. | Boot the machine |
| Step 3. | The installation reports “Setup is inspecting your computer’s hardware configuration...”. |
| Step 4. | The installation prompts “Press  if you need to install a third party SCSI or RAID driver...”. Do not press  . |
| Step 5. | The installation reports “Setup is loading files” multiple times. |

- Step 6. The installation reports “Setup is starting Windows 2000”.
- Step 7. The installation reports “Setup program has detected that you are about to install Windows 2000”. Press **ENTER** to continue
- Step 8. The installation prompts “To set up Windows 2000 now, press ENTER.”. Press **ENTER** to continue.
- Step 9. The installation displays the Windows 2000 licensing agreement. Press **F8** to accept the license agreement.
- Step 10. The installation displays the fdisk table. If necessary, delete existing partitions using the **D** **ENTER** **L** key sequence.
- The non-intuitive **L** helps avoid problems should someone hold down the **D** key accidentally.
- Step 11. You are returned to the fdisk table. Type **C** to create a partition.
- Step 12. Enter size of partition in megabytes.
- Step 13. Type **ENTER**.
- Step 14. Type **ENTER** to install.
- Step 15. Select “Format this partition using the NTFS file system”.
- Step 16. Type **ENTER** to continue
- Step 17. This installation reports “Setup is copying files...”.
- Step 18. The installation reports “Please wait while setup initializes Windows 2000”.
- Step 19. Type **ENTER** restart the computer
- Step 20. The installation prompts “Please insert the Compact Disc labeled ‘Windows 2000 Server CD-ROM’ into your CD-ROM drive (E:) and the click OK.”
- Step 21. The installation reports “Welcome to the Windows 2000 Setup Wizard”.
- Step 22. Click **Next**.
- Step 23. The installation reports “Installing Devices”.
- Step 24. The installation displays the “Regional Settings” screen.

- Step 25. Click **Next**.
- Step 26. The installation displays the “Personalize Your Software” screen.
- Step 27. Enter your name and organization.
- Step 28. Click **Next**.
- Step 29. The installation displays the “Licensing Modes” screen. Choose “Per server” with 25 connections
- Step 30. Click **Next**.
- Step 31. The installation displays the “Computer Name and Administrator Password” screen.
- Step 32. Provide the information requested and click **Next**.
- Step 33. The installation displays the “Windows 2000 Components” screen.
- Step 34. Check “Terminal Services”.
- Step 35. Click **Next**.
- Step 36. The installation displays the “Date and Time Settings” screen.
- Step 37. Click **Next**.
- Step 38. The installation displays the “Terminal Services Setup” screen.
- Step 39. Select “Application server mode” (not “Remote administration mode”).
- Step 40. Click **Next**.
- Note that this screen says, “Use Add/Remove Programs in Control Panel to install programs for use in application server mode”. This is a requirement imposed by Microsoft.
- Step 41. The installation displays the “Terminal Services Setup” screen.
- Step 42. Select “Permissions compatible with Terminal Server 4.0 Users” (not “Permissions compatible with Windows 2000 Users”)
- Step 43. Click **Next**.
- Step 44. The installation reports “Installing Components”.

- Step 45. The installation reports “Performing Final Tasks”.
- Step 46. The installation reports “You have successfully completed Windows 2000 Setup.”
- Step 47. The installation reportst “If there is a CD in your drive, remove it.”
- Step 48. Click **Finish**.

NOTE: Do not perform labs Section 8.11 on page 8-44 and Section 8.12 on page 8-46 on Windows 2000 servers.

8.10 Lab: Installing Windows Terminal Server Edition

In this lab, you will install Windows Terminal Server onto your application server.

8.10.1 Overview

Your tasks in this lab are two-fold:

- Create the boot floppies required by the installation (see Section 8.3.2 on page 8-21) or set up your machine to boot from CD-ROM
- Install Windows Terminal Server

The instructor will point you to where you can obtain the necessary software.

8.10.2 Procedure

In this lab we assume that you are booting from CD-ROM. If this is not the case, see Section 8.3.2 on page 8-21 for information on creating installation floppies.

To install Windows Terminal Server, follow this procedure:

- Step 1. Insert the Windows Terminal Server CD-ROM (and boot floppy #1 if you are installing from floppy).
- Step 2. Boot the machine.
- Step 3. If installing from floppies, follow the instructions for inserting the floppies.
- Step 4. Type  “To setup Windows Terminal Server Now”.
- Step 5. Type  to accept the CD controller.
- Step 6. Type  to agree to the licensing agreement
- Step 7. Type  to accept the default list of hardware and software.

When setting up a production server, attention to the proper mouse and video card are necessary. For the class, the defaults should work.

 If the defaults are not correct for your classroom hardware, tell the students where they need to veer from the defaults.

Step 8. If there is a partition on the drive already (most likely the Unix partition) then delete it via the key sequence **D** **ENTER** **L**.

The non-intuitive **L** helps avoid problems should someone hold down the **D** key accidentally.

Step 9. Create a 2 Gigabyte partition by typing **C** **2** **0** **0** **0** **ENTER**.

GuruNotes In Windows Terminal Server, there is still a 2GB limit on a partition. There are ways around it, but for this lesson, it is best to avoid issues and just set up a 2GB partition.

Step 10. Type **ENTER** to install Windows Terminal Server on the partition.

Step 11. Select **NTFS** then type **ENTER**.

The drive will now start formatting.

With Windows Terminal Server, the default is FAT, but a FAT filesystem will not work for our purposes as it has limited security amongst other issues.

Step 12. Once the formatting is complete the you will be asked for the installation directory. Press **ENTER** to accept the default of **\WTSRV**.

Step 13. Press **ESC** to skip the secondary examination. This will save time in the classroom. The secondary examination should be performed on production servers.

The files will be copied from CD-ROM to the hard drive. This takes some time.

Step 14. After the copying is complete, eject the CD-ROM (and floppy) then press **ENTER** to reboot the machine.

The system will boot by itself. It will convert the filesystem from FAT to NTFS. It will reboot again by itself. The rest of the installation is done in graphical mode.

Yes, you heard right. We selected "NTFS" during the install, but Windows did "FAT" anyway. Go figure.

Step 15. Insert the CD-ROM when prompted and click **OK**.

Step 16. The installation will display an overview page of the next three steps. Click **Next** to start gathering the information.

Step 17. Enter a **Name** and an **Organization** and click **Next**. This is just an information field but can not be easily changed, so when installing in a production environment, choose wisely.

Step 18. Choose **PER SEAT**.

■ “Per Seat” is the easiest option for our purposes.

Step 19. Choose **5** (or thereabouts) for the quantity of clients. There is no immediate checking for licenses and this quantity will work for this lesson. In a production environment, the appropriate number of licenses need to be purchased.

Step 20. You instructor will tell you what to name your machine. Enter this name in the field labeled **Computer Name**.

Step 21. Click **Next** to accept the Stand Alone Server

Step 22. Use **root** as the password.

Step 23. Choose **NO** to avoid creating an Emergency Recovery floppy. This floppy is not needed here in the classroom, but in a production system, **YES** should be chosen.

Step 24. Click **Next** to accept the default software.

Step 25. Click **Next** to install Internet Explorer.

Step 26. The next step is the networking. Click **Next** to start the installation.

Step 27. Click **Next** to have the computer on the network.

Step 28. Click **Next** to *not* install Internet Information Server (Microsoft’s web server).

Step 29. Click **Start Search** to start the autodetection of the networking card.

If none are found then ask the instructor for assistance.

Step 30. Accept the defaults for the card, protocols and services.

If you are prompted for the network card’s parameter, ask the instructor for assistance.

■ In a production environment, uncheck the IPX/SPX protocol if it is not in use at the site. Having only one protocol cuts out any infrequent but difficult multi-protocol issues.

- Step 31. Choose **No** to *not* use DHCP.
- Step 32. Under the IP Address Tab, fill in the IP address, subnet mask and default gateway. This information will be provided by the instructor.
- Step 33. Under the DNS Tab, fill in the Domain Name and DNS server IP address. This information will be provided by the instructor.
- Step 34. Click **OK**.
- Step 35. A dialog box will pop up saying that WINS is not configured. Click **Yes** to continue on *without* setting up WINS.
- Step 36. Accept the default services, start the network and accept **Workgroup** as the workgroup name. Then click **Finish**
- Step 37. Choose the appropriate Time Zone, then click **Close**.
- Step 38. Accept the defaults for the display adapter and settings.
- The system will continue copying data.
- Step 39. Eject the CD when the copying is complete.
- Step 40. Click **Restart**.

Let the system boot up automatically. The system will automatically install Internet Explorer and then reboot again. It will then configure Internet Explorer which can take a while. When it is complete, the login screen will appear and the system is ready to use.

8.11 Lab: Installing Service Pack 5 for Windows Terminal Server

After installing Windows Terminal Server, you must install Service Pack 5.

NOTE: Perform this lab on Windows Terminal Server installations only. Do not perform this lab on a Windows 2000 server.

8.11.1 Overview

Your task is to install the Service Pack onto Windows Terminal Server. This software will be provided by your instructor.

8.11.2 Procedure

Step 1. Log onto the Windows Terminal Server system as **Administrator** with the password used earlier (**root**).

Uncheck the “Show Welcome Screen” and click **Close**.

Step 2. The instructor will provide you with the CD-ROM with the latest Service Pack. Insert this CD-ROM.

 The Service Pack is located on the Enterprise II CD-ROM.

Step 3. Choose **Start** ⇒ **Settings** ⇒ **Control Panel** ⇒ **Add/Remove Programs**

In the multi user NT environment, the installation of a program *must* be done via the **Add/Remove Programs** utility. Otherwise, the program will only be installed for the Administrator. Furthermore, certain registry settings may not be set properly.

Step 4. Click **Install**.

Step 5. Click **Browse** and browse to the \WTSSP5 folder on the CD-ROM.

Step 6. Choose *wtsi386* and click **Open**.

Step 7. Windows will insert the filename into the command line. Click **Next**.

Step 8. Click **Next** to install the service pack for all users

Step 9. Check the **Licensing Agreement**.

Step 10. *Uncheck* **Backup Files**. This is simply to save time in the classroom.

Step 11. Click **Install**.

Step 12. When the installation completes, click **Restart**.

8.12 Lab: Installing Internet Explorer 5.0.1

Windows Terminal Server provides an out of date version of Internet Explorer. In this lab you will upgrade Internet Explorer to 5.0.1 so that the web browser on the Windows Terminal Server can be used as a client to Tarantella.

NOTE: Perform this lab on Windows Terminal Server installations only. Do not perform this lab on a Windows 2000 server.

8.12.1 Overview

Your task is to install Internet Explorer 5.0.1 onto Windows Terminal Server. This software will be provided by your instructor.

8.12.2 Procedure

- Step 1. Log onto the Windows Terminal Server system as **Administrator**.
- Step 2. The instructor will provide you with the CD-ROM with the latest Internet Explorer. Insert this CD-ROM.
- Step 3. Choose **Start** ⇒ **Settings** ⇒ **Control Panel** ⇒ **Add/Remove Programs**.
- In the multi user NT environment, the installation of a program *must* be done via the **Add/Remove Programs** utility. Otherwise, the program will only be installed for the **Administrator**. Furthermore, certain registry settings may not be set properly unless you use the **Add/Remove Programs** utility.
- Step 4. Click **Install**.
- Step 5. Click **Browse** and browse to the `\ie5download` folder on the CD-ROM.
- Step 6. Choose `ie5setup` and click **Open**.
- Step 7. Windows will insert the filename into the command line. Choose **Next**.
- Step 8. Choose **Next** to **Install For All Users**.
- Step 9. Click **Accept** to accept the license agreement.
- Step 10. Choose **Typical** software installation.
- Step 11. When the copying completes, click **Finish** to restart the computer.

8.13 Lab: Office97 Installation

In this lab, you will make Office97 available on the Windows Terminal Server.

8.13.1 Overview

Install Office97 on the Windows Terminal Server. Office 97 provides an application compatibility script which you are required by Microsoft to run.

Your instructor will provide you with the necessary software.

8.13.2 Procedure

- | | |
|----------|--|
| Step 1. | Log onto the system as Administrator . |
| Step 2. | Insert the Office97 CD-ROM. The autorun script on the CD-ROM will automatically launch an installation program. |
| Step 3. | Close the window <i>without</i> installing the application. Otherwise, only the Administrator will have access to the programs. |
| Step 4. | Choose Start ⇒ Settings ⇒ Control Panel ⇒ Add/Remove Programs
Windows should automatically find the <i>setup.exe</i> program on the CD-ROM. |
| Step 5. | Click Next to accept <i>setup.exe</i> . |
| Step 6. | Click Next to install for all users. |
| Step 7. | Click Continue . |
| Step 8. | Enter a <i>Name</i> and <i>Organization</i> and click OK to accept them. |
| Step 9. | Accept the ProductID and default installation folder. |
| Step 10. | Click Typical installation. |
| Step 11. | Click Continue to accept the defaults. |
| Step 12. | When everything is copied, click Finish . |
| Step 13. | Reboot the system. |

Step 14. Microsoft Office 97 provides an application compatibility script which you are required to run. When the system reboots, log in as **Administrator** and select **Start** ⇒ **Run** ⇒ **Browse**.

Step 15. Browse to **C:\WTSRV\Application Compatibility Scripts\Install** and run the *Office97.cmd* program.

This program is a simple script that fixes up issues that arise from the fact that multiple users will be using the Office programs.

You can view the comments in the *Office97.cmd* to see what it does and why.

Step 16. An edit box will pop up with a file that asks to be modified. Put in **W:** after the **Set RootDrive=**. The last line should read:

Set RootDrive=W

For reasons unknown, when converting this curriculum to PDF format the **W:** (double-u colon) above only shows up as **W**. The **Set RootDrive** command must be set to **W:**.

If students mistakenly type **W** instead of **W:**, you can fix up the registry by running *regedit*. Search for all occurrences of **W** and change them to **W:**. The usual precautions when editing the registry should be taken.

Alternatively you can edit the *office97.key* file created by the application compatibility script with wordpad, change the occurrences of **W** to **W:**, save the changes, then double click the *office97.key* file to apply the changes to the registry.

Step 17. Select **File** ⇒ **Save**.

Step 18. Select **File** ⇒ **Exit**.

The script will continue with the W: drive used as the users' drive.

Installing Office 2000 is similar. The only major difference is that Office 2000 does not provide (or require) an application compatibility script.

8.14 Lab: Creating an Application Object for Microsoft Excel

In this lab, you will create an application object to enable Tarantella users to access Microsoft Excel.

8.14.1 Overview

- Step 1. Log into Tarantella as **root**.
- Step 2. Create a Windows application object for Excel:
- Right-click the children box.
 - Select **New Object** ⇒ **Windows Application**.
 - Set the **Object Name** and **Label** attributes to “Excel”.
 - Set the **Application Server** attribute to the fully qualified domain name of the Windows application server.
 - Set the **Windows Protocol** attribute to **Win2000/Terminal Server**.
 - Set the **Application** attribute to *C:\Program Files\Microsoft Office\excel.exe*.
 - Check **Use Windows Cursor** .
 - Click the **Apply** button. Be sure to wait till the button is grayed out.
- Step 3. Deploy the “Excel” application object that you created.
- Step 4. Refresh/reload the web browser.
- Step 5. Excel should now appear on the launch pad. Launch Excel.

8.15 Answers to Exercise and Review Questions

This section contains the answers to exercises, review questions, and labs presented in this lesson.

Exercise answers

Please consult your instructor if you have questions about the exercises in this lesson.

Review Question Answers

This section contains the answers to the review questions on page 8-35.

1. There are six Windows protocols: None, SCO Merge, WinFrame/MetaFrame, WinCenter/UIS, Local Windows Terminal Server and Win2000/Terminal Server
2. For Windows Terminal Server : `D:\i386\winnt.exe /ox`
For Windows2000: `D:\bootdisk\makeboot a:`
3. Three. 640x480, 800x600, 1024x768. Tarantella can have any arbitrary resolution.
4. The name to use when first logging in is **Administrator**.

9

The X Window System

Instructor Guide

Instructor Guide

Lesson 9

The X Window System

Suggested lesson duration

This lesson should take approximately 2.5 hours to complete including the lab.

Pre-lesson classroom preparation

The classroom network needs to be setup properly (clients installed, DNS updated, etc.). Tarantella should be installed and configured. Students should have access to a UNIX console or xterm through Tarantella as well as directly through UNIX.

Instructor preparation

Read the following articles in the *Admin Guide*:

How to... ⇒ Configure application objects for your X environment ⇒ To run a CDE session

Reference ⇒ Objects and attributes ⇒ X Application objects

You might also find the following helpful:

O'Reilly and Associates "*The Definitive Guide to the X Window System -- Volume 3M: X Window System User's Guide*" by Valerie Quercia & Tim O'Reilly

<http://www.x.org/>

Introduction

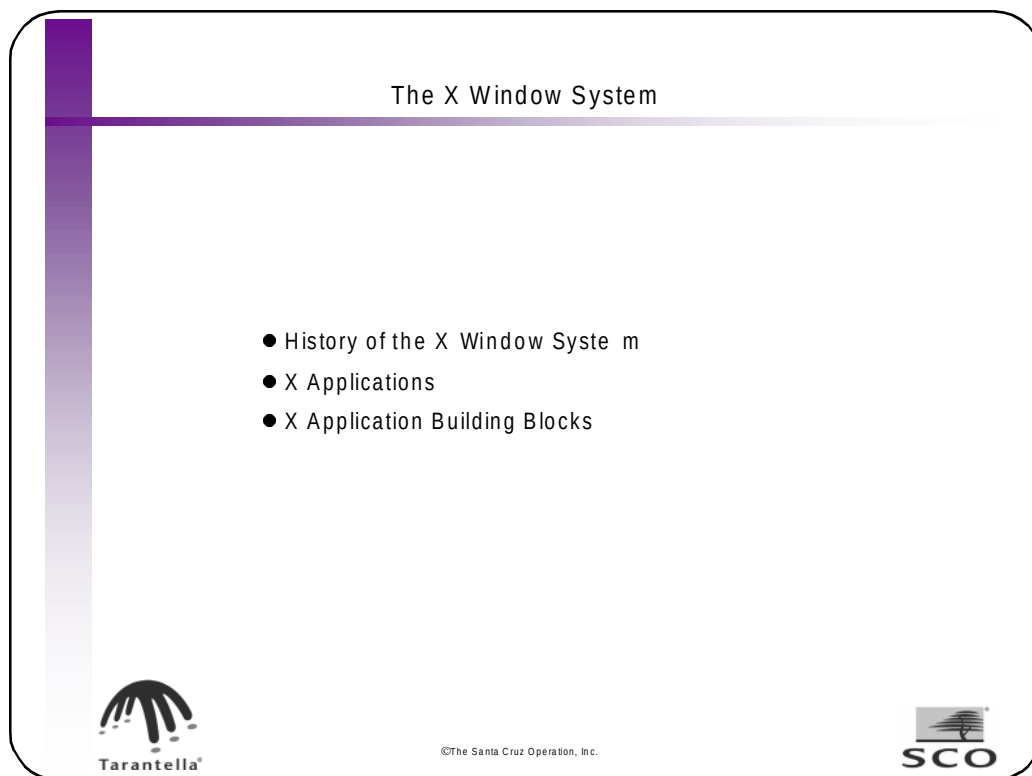
The X Window System plays an integral part in Tarantella's connectivity to UNIX applications. A basic understanding of how the X Window System (or "X" for short) works greatly enhances an administrator's ability to understand and create X application objects using Control Center.

Objectives

By the end of this lesson, you will be able to:

- Describe some of the basic mechanisms that affect the functionality of an X application
- Have a working knowledge of how X applications are built
- Use several X utilities to modify X applications as well as change the way an X client behaves

AV 9-1



Topics

In order to meet these objectives, this lesson discusses:

- History of the X Window System — Discusses the philosophy behind the development of the X Window System
- X Applications — Discusses the basic mechanisms behind X applications
- X Application Building Blocks — Discusses the different components that are involved in the development of an X application.

AV 9-1: The X Window System

The first slide describes the overall topics covered in this lesson.

9.1 X Window System

The X protocol was developed to fill the need to provide a graphical user interface primarily for the UNIX operating system. X provides for the display and management of graphical information.

The key difference between X and other GUI-based operating systems, such as Windows, is in the structure of the X protocol. Whereas Windows displays graphical applications local to the PC, the X protocol distributes the processing of applications by specifying a client-server relationship at the application level.

9.1.1 History and philosophy of the X window system

The X Window System is a TCP/IP based graphics window system developed at MIT. It was designed based on the following principles:

- Mechanism not policy

Meaning that X provides mechanisms for doing things but does not force you to follow a particular style. As an example, consider the Mac. On the Mac, the menu is on the top of the screen. The menu is always on the top of the screen. X, on the other hand, gives you the capability of creating a menu, but it doesn't dictate how/where you create the menu. Similarly, on the Mac, you have one button on your mouse. That's it. X, on the other hand, supports various numbers of buttons on the mouse.

- Atoms
- Selections
- Properties

Atoms, Selections, and Properties are discussed in Section 9.1.4 on page 9-9.

9.1.2 X application input

X applications accept *input* from the X server telling it that there is something that it needs to act upon. This *input* is usually in the form of pressing a key on the keyboard or moving the pointer (mouse). There are specific functions that are used to interpret keyboard *inputs*:

Keysyms

These are actual keyboard symbols that map numeric scancodes to keys on the keyboard. They pull their information from the *XKeysymDB*.

Modifiers	These keys are used to modify the action of other keys. These keys are often used to invoke commands of some sort, such as window manager functions. Some common modifier keys include the <i>Alt</i> , <i>Ctrl</i> , and <i>Shift</i> keys. These keys are recognized by X programs as <i>maps</i> to physical keys on the keyboard.
-----------	---

9.1.3 Window managers

The X Window System uses a special type of client application to control its windowing environment. This client is called the window manager and can vary from client to client. The window manager allows the user to move, resize, circulate, and iconify windows on the display. In UnixWare, the CDE is the window manager being used.

■ Discuss with students other window managers (eg. mwm, pmwm, kde, fvwm95, etc.).

9.1.4 Clipboard

Most X clients exchange information via *properties*. The advantage of the selection mechanism is that it allows data from one client to be converted to a different format so that it can be used by another client. When text is selected, it is owned by the client from which it has been copied. Once it is pasted into another window, that new window becomes the owner of the selection.

Selection	Text copied into memory using the mouse pointer is saved into a global buffer that is globally available to all other X applications. This data is located on the client and not the server.
Property	An X window has associated <i>properties</i> consisting of a name, a type, a data format, and some data. These are intended as a general-purpose data storage and intercommunication mechanism for clients. Each property name is associated with a corresponding unique integer value known as an atom.

9.1.5 Fonts

A font is a style of text character. Many X clients allow you to specify the font used to display text in the window, in menus, and labels, or in any other text fields. Fonts are generally divided into families. These families can be changed according to fourteen different criteria such as size, weight, name, point size, etc.

To understand fonts under X, you need to understand the following concepts:

Wildcards	An asterisk (*) is used to represent any part of the font name string. If the wildcarded font name matches more than one font, the server will use the <i>first</i> one that matches. The names are sorted in simple alphabetical order and as a result, wildcarding the font weight would result in a font with a <i>bold</i> weight rather than a <i>medium</i> weight.
Font Search Path	Fonts are stored in three directories by default. They are <i>/usr/lib/X11/fonts/misc</i> , <i>/usr/lib/X11/fonts/75dpi</i> , and <i>/usr/lib/X11/fonts/100dpi</i> . Other directories can be added to the font search path, or its order can be rearranged using xset with the fp option.
<i>fonts.dir</i> and <i>fonts.alias</i>	The <i>fonts.dir</i> file is located in the same directory as the font files. The <i>fonts.dir</i> files acts as a database for the X server. The <i>fonts.alias</i> files can be created in any directory in the font search path. In this file you can associate fonts with alternative names of your own choosing. When the X server searches the directories in the default font search path, it uses both the <i>fonts.dir</i> and <i>fonts.alias</i> files to locate the fonts it needs.

9.2 A Typical X Application

We will now examine three building blocks of a typical X application:

Xlib	The X library is a programming interface to the X Window System.
XT (intrinsics)	The X Toolkit Intrinsics is a library which determines the resources an X application will use.
Motif	Motif is a toolkit that determine the “look and feel” of an X application.

9.2.1 Xlib

All a client program needs to do to use the X display is to open up a connection with the server and then send X protocol requests to it. To simplify sending these, an extensive library of numerous display subroutines is provided. The X library (also known as *xlib*) provides this functionality.

- Primitives
- Manages Connection to X server
- Manages windows

9.2.2 Xt

The *X Toolkit Intrinsics* is a library built upon the lowest programming level API or *Xlib*. This library provides the functionality from which the *widget* sets are built. Widgets are user interface objects such as menus, command buttons, dialog boxes, and scrollbars. Xt uses *resources* to customize these widgets.

9.2.3 Motif

Motif is a set of user interface guidelines developed by the Open Software Foundation (OSF) which specifies how an X Window System application should “look and feel”. Motif includes the Motif Toolkit which enforces a policy on top of the X Toolkit Intrinsics. Motif has been internationalized.

9.3 Lesson Summary

This lesson described the basics of the X Window System. In this lesson, we took a high level look at how the X Window System accepts input, uses the clipboard, the window manager, how fonts are used, and the building blocks of X applications.

9.4 Review questions

1. What is the basic philosophy behind the X Window System and what principles is it based on?

The basic philosophy of the X Window System is “mechanism not policy” and it's built on the principles of atoms, property and selection.

2. How does the X client accept keyboard input from the X server?

Keyboard inputs are interpreted using keyboard symbols and modifiers which access the *keysyms*. These associations can be changed using the *xmodmap* application.

3. How does the X Window System use the Clipboard?

X clients exchange information using “*selections*” which are saved into a global buffer made available to all X applications. Once text has been selected, it keeps the *properties* of the original client until it is pasted into a new application window where it will assume the properties of the new client.

4. What are the default files and directories that the X server uses to locate fonts?

The default font search paths are */usr/lib/X11/fonts/misc*, */usr/lib/X11/fonts/75dpi*, and */usr/lib/fonts/100dpi*. The database file, *fonts.dir*, and the alias file, *fonts.alias* are also used by the X server to locate different fonts. The *fonts.dir* file is located in the same directory as the fonts themselves, and the *fonts.alias* file must be located in the font search path.

5. What are the three building blocks of typical X applications and how are they related to each other?

A typical X application would be built using the Motif Toolkit to create the “look and feel”. The Motif Toolkit enforces a policy on top of the X Toolkit Intrinsics (Xt) which is layered upon the X library or Xlib which provides policy subroutines to the X server.

9.5 Lab: Understanding the X Window System

In this lab, you will familiarize yourself with various X utilities. You will learn how to use these various X applications to create and modify a resource database. You will also learn how to alter the function of your X client's keyboard modifiers and the differences between the Tarantella X server and the standard UnixWare X server.

9.5.1 Overview

Your tasks in this lab are:

- Determine the differences between the Tarantella X server and the standard UnixWare X server using the command **xdpyinfo**. Familiarize yourself with the use of the command **xset**.
- Create a resource database so that whenever the X application **xedit** is started, the background of the "Save" button is red and its text is presented using *18 point bold Lucida font*. Repeat the above while in a CDE session. When you exit CDE, it saves any resources that are still loaded on the screen. Which database are they saved to? You will find the **editres** and **xfontsel** commands useful.
- Using the **xmodmap** application alter the *keysyms* so that the *shift* key and the *caps lock* keys are switched. Once you have modified the keys, verify their functionality by trying to produce the following: ") (* & ^ % "

Make sure that the students know how to use the man pages. They may also have problems determining the correct path for the commands (eg. */usr/bin/X11/* versus */usr/X/bin/*).

For CDE, they will need to save their **xedit** changes to the *.dtpfile* file in their home directory. They will have to restart their client session in order to see their changes when they restart **xedit**.

If a student runs into problems returning their **shift** and **caps lock** keys to their original functionality, they can set them back to their defaults by restarting the X client.

9.5.2 Procedure

The sections following explain step by step how to carry out the tasks in this lab.

These labs are designed to be performed under UnixWare.

Part I

For this exercise, you will use MWM instead of CDE.

Step 1. On the UnixWare graphical login screen, choose **Options** ⇒ **Sessions** ⇒ **Failsafe Session**.

We're merely doing this to simplify the graphical environment.

Step 2. Log in as **root**.

Step 3. If an xterm is not started automatically, launch one by right clicking the background of the screen and choosing "New Window".

Step 4. In the xterm, execute the **xdpyinfo** command:

```
# xdpyinfo | more
```

If **xdpyinfo** is not found, **\$PATH** is probably set incorrectly. The **xdpyinfo** command is located in */usr/X/bin* under UnixWare.

- Step 5. Log into Tarantella and open an xterm. Execute the same command from within the Tarantella xterm.

```
# xdpinfo | more
```

What differences do you notice between the xdpinfo commands in Step 4. and Step 5.?

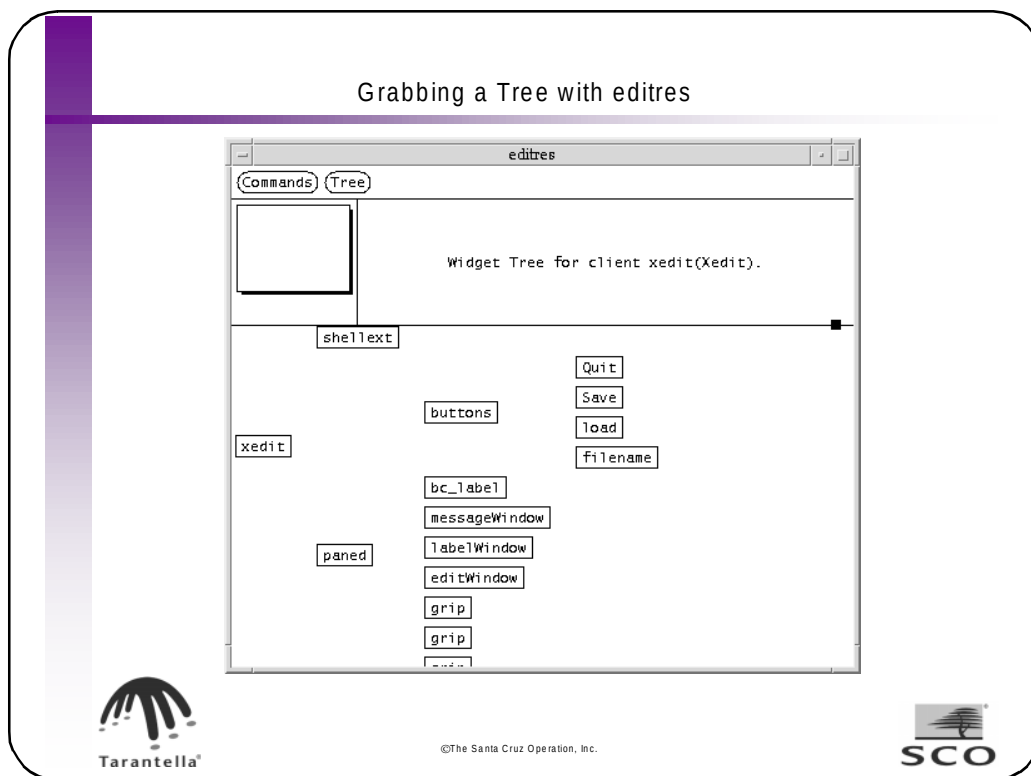
Some of the differences the students should notice are the vendor release numbers, MIT in the UNIX server vs. GLX in the Tarantella server. Tarantella will use NATIVE_WND and will have different vendor extensions so that X clients can talk to additional X servers. In addition to these, there are different visuals, color depths, font paths, and dpi settings.

- Step 6. In either xterm, execute **xset** by executing the following command:

```
# xset 2>&1 | more
```

The output will list some of the functionality that can be changed and controlled using the **xset** command.

AV 9-2



Part II

Step 1. Log into CDE as **root**.

Step 2. From an **dtterm**, open the application **xedit**:

```
# xedit &
```

Step 3. From the **dtterm**, execute the following command:

```
# editres &
```

Both applications should open up in separate windows.

Step 4. Load the **xedit** widget tree into **editres**.

- Bring the **editres** window into focus by pointing your mouse and clicking anywhere in the **editres** window.
- On the **editres** menu, select **Commands** ⇒ **Get Tree**.
- Your pointer will turn into a cross hair. Use it to click on the **xedit** window. The **editres** window will display the **xedit** widget tree as shown in AV 9-2 on page 9-18.

AV 9-2: Grabbing a Tree with editres

Use this slide to show students what the editres screen looks like after grabbing a resource tree.

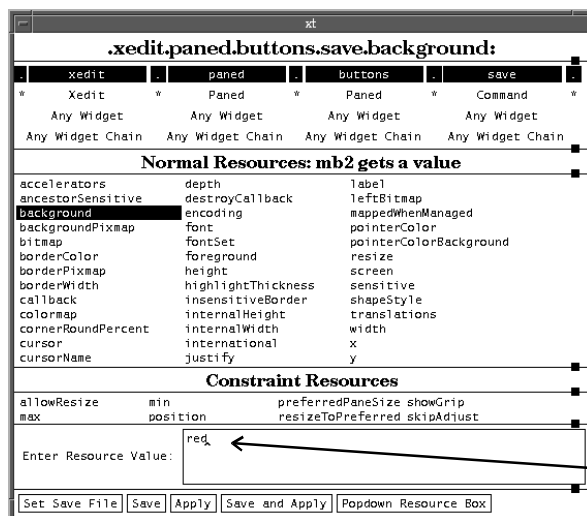
Step 5. Display the Xt resources for **xedit** using **editres**:

- Click on the box that says “Save” in the **editres** window. The box will become highlighted in black.
- Select **Commands** ⇒ **Show Resource Box** on the **editres** menu.

The **xt** window will pop up containing all of the available resources for the **Save** button.

AV 9-3

Changing the Save Button Color with editres

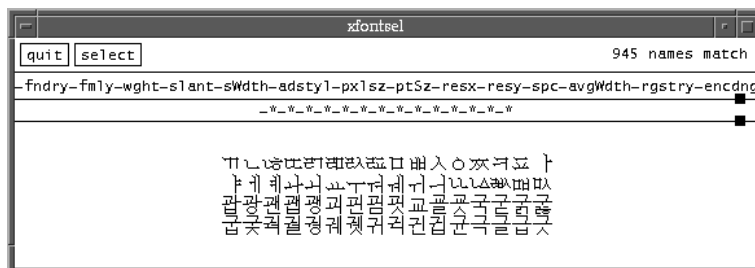
Type
"red"

©The Santa Cruz Operation, Inc.



AV 9-4

Selecting Fonts with xfontsel



©The Santa Cruz Operation, Inc.



Step 6. Change the color of the **Save** button to red.

- Click on the word “background”. It should become highlighted.
- In the box located to the right of “Enter ResourceValue:” type the word “red.” AV 9-3 shows where to enter the value “red.”

AV 9-3: Grabbing a Tree with editres

Use this slide to show where the student should enter the color “red”.

- Click on the **Save and Apply** button directly below the text box.
- A new **fileDialog** window will appear prompting you to enter the name of a file in which to save **xedit**’s resources. Save the resource to a file called *.dtprofile*.
- If you did this step correctly, the **Save** button in **xedit** should have turned red.

Step 7. Change the font weight and style using **xfontsel** and **editres**:

From the **dtterm** window, execute **xfontsel** using the following command:

```
# xfontsel &
```

AV 9-4: Selecting Fonts with xfontsel

Use this slide to illustrate the **xfontsel** command.

A picture of **xfontsel** is shown in AV 9-4.

GuruNotes Each of the asterisks represents a modifiable characteristic of that particular font.

Step 8. Select the font family by clicking on “fmly” and choosing “lucida”.

Step 9. Select the font weight by clicking on “wght” and choosing “bold”.

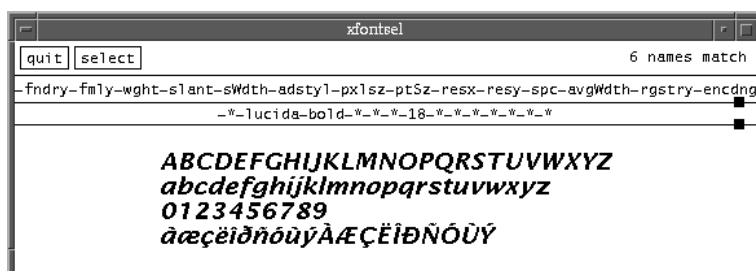
GuruNotes The value for weight may be expressed differently depending upon the X server being used (i.e. **b** for **bold**, **r** for **regular**).

Step 10. Select the pixel size by click on “pxlsz” and choosing “18”.

The result should look similar to AV 9-5 on page 9-22.

AV 9-5

Selecting Fonts with xfontsel

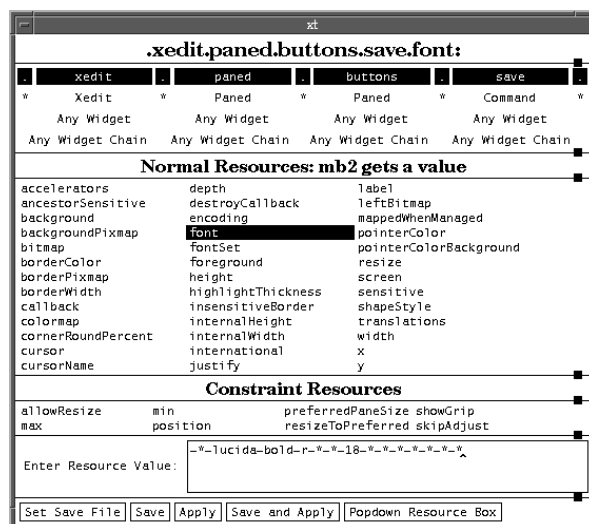


©The Santa Cruz Operation, Inc.



AV 9-6

Changing Fonts with editres



©The Santa Cruz Operation, Inc.



GuruNotes

If you leave slant set to asterisk, the asterisk will act as a wildcard and select the first available slant style. “Italic” before “regular” (remember that font characteristics are listed in alphabetical order). Therefore if you want the font to display as **regular** text, you’ll have to set slant to “**r**”.

- Click on the **select** button which will store your font selection into your X client’s buffer.
- Return to the **xt** window (still being displayed from **editres** and click on **font** in the **Normal Resources** window.
- Click your mouse in the **Enter Resource Value** window. If you click both mouse buttons at the same time, the font name should be pasted into the window from your X client’s buffer. If the paste fails, simply type “**-*-lucida-bold-r-*-18-*-**-*-***” in manually. Click the “save and apply” button. The results should look similar to AV 9-6:
- If you did this step correctly, the **Save** button in **xedit** should have turned changed to Lucida bold regular 18 point.

The settings for the CDE session that you’re running are saved in the user’s home directory in `$HOME/.dt/sessions/current/dt.session`.

AV 9-5: Selecting fonts with xfontsel

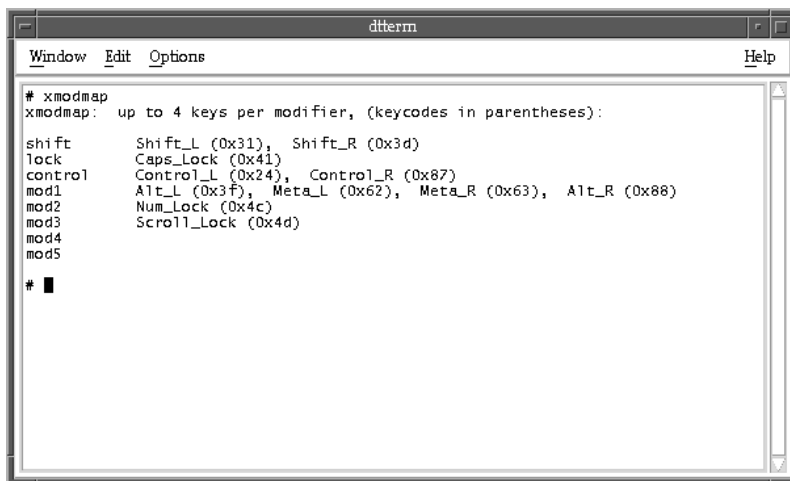
Use this slide to illustrate the **xfontsel** command.

AV 9-6: Changing Fonts with editres

Use this slide to illustrate **editres**.

AV 9-7

Examining Key Mappings with xmodmap



```
# xmodmap
xmodmap: up to 4 keys per modifier, (keycodes in parentheses):

shift      Shift_L (0x31), Shift_R (0x3d)
lock       Caps_Lock (0x41)
control    Control_L (0x24), Control_R (0x87)
mod1       Alt_L (0x3f), Meta_L (0x62), Meta_R (0x63), Alt_R (0x88)
mod2       Num_Lock (0x4e)
mod3
mod4       Scroll_Lock (0x4d)
mod5

# █
```



©The Santa Cruz Operation, Inc.



Part 3

AV 9-7: Examining Key Mappings with xmodmap

Use this slide to illustrate the **xmodmap** command.

In this portion of the lab, you will examine and then modify the default keyboard settings.

Step 1. Observe the current *keysyms* using **xmodmap**. Execute:

```
# xmodmap
```

AV 9-7 shows the output of the **xmodmap** command.

Step 2. Using the **xmodmap** application, alter the *keysyms* so that the **shift** key and the **caps lock** keys are switched.

GuruNotes

The **xmodmap** program is used to edit and display the keyboard modifier map and keymap table that are used by client applications to convert event keycodes into *keysyms*. It is usually run from the user's session startup script to configure the keyboard according to the individual's preferences.

- In a **dtterm**, create a file called “*xlab*”.

```
# vi xlab
```

Point students unfamiliar with **vi** to the graphical text editor.

- In this file, type the following **xmodmap** script:

```
!  
! Swap Caps_Lock and Shift_L  
!  
remove lock = Caps_Lock  
remove shift = Shift_L  
keysym Shift_L = Caps_Lock  
keysym Caps_Lock = Shift_L  
add lock = Caps_Lock  
add shift = Shift_L
```

GuruNotes

If you want to change the binding of a modifier map, you must also remove it from the appropriate modifier map.

- Execute the **xmodmap** script by using the following command:

```
# xmodmap xlab
```

- Step 3. You can verify that this command worked by trying to type the \$ % ^ & keys. You must now use the **CapsLock** key to get these keys to show up on your screen. Notice that the left shift key functions as the Caps Lock key. The right shift key does not behave as Caps Lock because the **xmodmap** script said nothing about remapping the right shift key.

The keysyms can be set back to their original state by restarting the xclient, or by running Part 3 with the following script

```
!  
! Swap Caps_Lock and Shift_L  
!  
remove lock = Caps_Lock  
remove shift = Shift_L  
keysym Caps_Lock = Shift_L  
keysym Shift_L = Caps_Lock  
add lock = Caps_Lock  
add shift = Shift_L
```

Due to a restriction with Java, Tarantella can't tell the difference between the left and right shift keys. Consequently Tarantella only reports the left shift key as being present. However, both shift keys act as the left shift key.

9.6 Answers to Exercise and Review Questions

This section contains the answers to exercises, review questions, and labs presented in this lesson.

Exercise answers

Please consult your instructor if you have any questions about the exercises in this lesson.

Review Question Answers

This section contains the answers to the review questions on page 9-13.

1. The basic philosophy of the X Window System is “mechanism not policy” and it’s built on the principles of atoms, property and selection.
2. Keyboard inputs are interpreted using keyboard symbols and modifiers which access the *keysyms*. These associations can be changed using the *xmodmap* application.
3. X clients exchange information using “*selections*” which are saved into a global buffer made available to all X applications. Once text has been selected, it keeps the *properties* of the original client until it is pasted into a new application window where it will assume the properties of the new client.
4. The default font search paths are */usr/lib/X11/fonts/misc*, */usr/lib/X11/fonts/75dpi*, and */usr/lib/fonts/100dpi*. The database file, *fonts.dir*, and the alias file, *fonts.alias* are also used by the X server to locate different fonts. The *fonts.dir* file is located in the same directory as the fonts themselves, and the *fonts.alias* file must be located in the font search path.
5. A typical X application would be built using the Motif Toolkit to create the “look and feel”. The Motif Toolkit enforces a policy on top of the X Toolkit Intrinsics (Xt) which is layered upon the X library or Xlib which provides policy subroutines to the X server.

10

Customizing Tarantella

Instructor Guide

Instructor Guide

Lesson 10

Customizing Tarantella

Suggested lesson duration

This lesson should take approximately 3 hours to complete including the lab.

Pre-lesson classroom preparation

In the lab, you will need to provide the students with the file *excologin.tar* from the courseware CD-ROM. Be prepared to distribute this file to the students.

Instructor preparation

Read:

Admin Guide ⇒ Advanced Customization ⇒ Applet parameters and methods ⇒ Login applet ⇒ Applet Parameters

Introduction

Tarantella is highly customizable. Tarantella is built on common web programming interfaces like HTML, so Tarantella is easy to customize to fit the style of your corporate web pages.

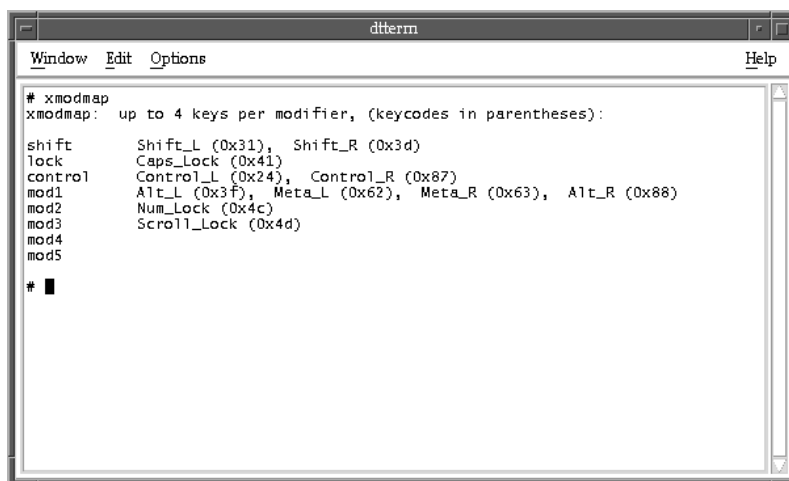
Objectives

By the end of this lesson, you will be able to:

- Create a new login theme
- Create a new webtop theme

AV 10-1

Examining Key Mappings with xmodmap



```
dtterm
Window Edit Options Help
# xmodmap
xmodmap: up to 4 keys per modifier, (keycodes in parentheses):

shift      Shift_L (0x31), Shift_R (0x3d)
lock       Caps_Lock (0x41)
control    Control_L (0x24), Control_R (0x87)
mod1       Alt_L (0x3f), Meta_L (0x62), Meta_R (0x63), Alt_R (0x88)
mod2       Num_Lock (0x4c)
mod3       Scroll_Lock (0x4d)
mod4
mod5
# █
```



©The Santa Cruz Operation, Inc.



Topics

In order to meet these objectives, this lesson discusses:

- Web Programming Basics— Discusses the basic portions of web programming that you must know to customize Tarantella. This discussion includes HTML, frames, cgi-bin, and RGB colors.
- Themes — Discusses Tarantella's login and webtop themes.
- Customizable Files— Shows which files are customizable in Tarantella and how to modify these files.

FYI — Most of the Tarantella client, including the launch pad, is compiled with Java 1.02 for compatibility with the widest range of browsers. Java 1.02 does not support animated gifs. The print applet is compiled with Java 1.1 which does support animated gifs. As Java 1.02-only browsers are increasingly rare, Tarantella will cease to support them in future releases and then the launch pad will support animated gifs.

AV 10-1: Customizing Tarantella

The first slide describes the overall topics covered in this lesson.

10.1 The Basics You Must Know

Because Tarantella is built upon common web technologies, Tarantella is easy for web-savvy developers to customize. Modifying the appearance of Tarantella to conform to the appearance of your web site requires you to understand the basic web technologies that have been around for several years.

10.1.1 HTML

Hypertext Markup Language (HTML) is a document format used on the web. HTML is comprised of plain text in conjunction with *tags* (eg.) which enable web page developers to control the format and layout of a web page, include graphics in a web page, and to hyperlink to other web pages.

Tarantella uses HTML to construct the web pages for the webtop, the login screen, the help screens, etc.

Tutorials on HTML abound on the web. For more information on HTML, visit any of the following links:

- <http://www.ncsa.uiuc.edu/General/Internet/WWW/HTMLPrimer.html>
- http://directory.netscape.com/Computers/Data_Formats/Markup_Languages/HTML
- <http://gort.ucsd.edu/dt/html/htmlwatch.html>
- <http://werbach.com/barebones>

10.1.2 Frames

Frames enable web page developers to divide web pages into separate regions. These regions are optionally scrollable and resizable. Frames can be nested:

```
<FRAMESET COL="50%, 50%">
  <FRAMESET ROW="50%, 50%">
    <FRAME SRC="http://tarantella.sco.com">
    <FRAME SRC="http://www.sco.com">
  </FRAMESET>
  <FRAMESET ROW="33%, 33%, 33%">
    <FRAME SRC="http://www.sco.com/ta">
    <FRAME SRC="http://www.sco.com/downloads">
    <FRAME SRC="http://www.sco.com/skunkware">
  </FRAMESET>
</FRAMESET>
```

Tarantella uses frames to construct the webtop screen (see AV 10-6 on page 10-22).

For information on frames, see any of the URLs listed in Section 10.1.1, “HTML” .

10.1.3 Tables

In addition to enabling web page developers to create tables of information, tables can be used to properly align multiple graphic images into what appears to be a single graphic.

Tarantella uses tables to construct the login screen (see on page 10-16).

It is not always apparent that a table is being used. This is because web pages set the <TABLE> tag's BORDER= value to 0. Changing the BORDER= value to a non-zero number is useful in understanding the layout of a multi-file graphic.

For information on tables, see any of the URLs listed in Section 10.1.1, “HTML” .

10.1.4 cgi-bin

Hypertext links in HTML utilize cgi-bin to call external programs to perform a variety of tasks. cgi-bin scripts typically generate HTML code which is passed to and displayed by the web browser.

Tarantella uses cgi-bin scripts to perform a variety of tasks. These include, but are not limited to, the following:

- Displaying the help screens
- Determining which printing protocol to use with the client web browser
- Installing the various Java archives required
- Displaying the webtop.

For more information on cgi-bin, visit the following URLs:

- <http://hoohoo.ncsa.uiuc.edu/cgi/overview.html>
- <http://www.dataex.com/members/support/cgi.html>

10.1.5 RGB colors

One of the easiest ways to quickly change the appearance of Tarantella is to change the colors it uses. The sample code includes references to colors in the *.html* files.

The colors used by Tarantella are set three different ways:

- The HTML <BODY> tag
- Apple parameters
- Graphics files

10.1.5.1 Setting colors via the HTML <BODY> tag

Much of the time, Tarantella sets the color scheme by setting the <BODY> tag in a *.html* file.

Consider the following code snippet from */opt/tarantella/webtops/en_US/standard/left.html*:

```
<body bgcolor="#0000FF" text="#000000" link="#FFFF00" vlink="#CCCC00"
alink="#FFFFFF">
```

This code sets various color attributes for the launch pad. The colors are indicated in hexadecimal RGB format. Seasoned web page developers will be intimately familiar with setting colors in this manner.

Point out to students that setting the <BODY> tag as shown above will change the background, text, link, etc. colors of the launch pad's frame. But that frame is covered by a Java applet. Set only the **bgcolor** attribute differently, refresh the browser, and it will become readily apparent that the Java applet occupies most of the frame.

You might quiz the students what the effect would be of the <BODY> tag above. Students are likely to say that the **text=** portion will result in setting the color of the labels used in the launch pad frame. This is incorrect. The colors used by the Java applet running the launch pad frame are set via applet parameters.

10.1.5.2 Setting colors via applet parameters

Some modifications that you will make to Tarantella's color scheme aren't set through the HTML `<BODY . . . >` tag. In several instances (eg. *left.html*), Tarantella-specific parameters are used to pass colors to the various Tarantella applets:

```
<param name="LabelColor" value="FFFFFF">
<param name="ObjectBackgroundColor" value="0000FF">
<param name="ObjectTopShadow" value="000080">
<param name="ObjectBottomShadow" value="8080FF">
<param name="HostBackgroundColor" value="0000FF">
```

These parameters are documented in the Admin Guide in ***Advanced Customization*** ⇒ ***Applet parameters and methods*** ⇒ ***Login applet*** ⇒ ***Applet Parameters***.

10.1.5.3 Setting colors in graphic files

In some instances (eg. the graphics used on the login screen, the icons used on the print status frame, etc.), the colors used by Tarantella aren't set via `<BODY>` tags or applet parameters at all. Rather, the colors are set in graphic files.

Where as colors set via `<BODY>` tags and applet parameters can be modified using a text editor, the graphic files must be edited with a graphical editor.

10.2 Themes

There are three types of Tarantella themes: login, webtop, and icon. Together these define a basic (or not so basic) visual design for every aspect of a user's interaction with Tarantella.

Generally, a theme is a collection of files stored in a directory. The name of the directory is the name of the theme (you use this name in Control Center when configuring which theme to use).

Some sample themes are supplied with Tarantella. You can create your own. Themes control the look and feel of Tarantella. We recommend that you don't modify any of the themes supplied with Tarantella. Instead, make a copy of the theme and work on the copy.

NOTE: It is assumed that the Tarantella installation directory is `/opt/tarantella`. Throughout this lesson, `/inst_dir` refers to the Tarantella installation directory.

Make sure the students understand that wherever they see `/inst_dir`, they should substitute the name of the Tarantella installation directory (usually `/opt/tarantella`).

Themes are not replicated across arrays automatically. You must do so manually.

10.2.1 Login themes

The login theme determines the appearance of the login screen on the Tarantella server. Login themes:

- Are stored in `/inst_dir/login/en_US`

For example, the standard login theme is stored in `/opt/tarantella/login/en_US/standard`.

- Are constructed with HTML, frames, and graphics files
- Use the **login** applet supplied with Tarantella

Tarantella comes with one login theme, the **standard** login theme. To modify the login theme:

- | | |
|---------|--|
| Step 1. | Copy the standard login theme directory to a different name in the same directory. |
| Step 2. | Make the desired modifications to the files in the new directory |
| Step 3. | Select the new login theme in Control Center by selecting Server view and change the Login Theme attribute of the Access object to the name of the newly created directory. |

For more information on the login applet, in *Admin Guide* see **Advanced Customization** ⇒ **Applet parameters and methods** ⇒ **Login applet**.

GuruNotes The login theme does *not* control the logout screens. The logout screens are controlled by the webtop theme.

10.2.2 Webtop themes

Webtop themes control the overall layout of the users' webtops. Webtop themes:

- Are stored in `/inst_dir/webtops/en_US`
- Are constructed using HTML and graphics files.
- Are configured using Control Center by editing the Webtop Theme attribute of an organization object, an organizational unit object, or a person object.

Tarantella supplies four webtop themes: **standard** (the default), **horizontal**, **noicon**, and **maximum**. To create your own webtop theme, copy the **standard** webtop theme directory to a different name in the same directory. Make the desired modifications to the files in the new directory. Then select the new webtop theme in Control Center for any combination of the organization object, organizational unit objects, or a person objects.

Exercise: Changing Webtop Themes

Setting the organization's webtop theme:

- Step 1. In Control Center, change your organization's webtop theme to **horizontal**.
- Step 2. Log out of Tarantella and log back in as the administrator
- Step 3. Observe the difference in the appearance of the webtop theme

Setting a particular user's webtop theme:

- Step 1. Select a user's person object in Control Center
- Step 2. Change the webtop theme attribute for that person to **noicon**
- Step 3. Log out of Tarantella, log back in as the person you selected
- Step 4. Observe the difference in the appearance of this person's webtop theme
- Step 5. Log out as this person and log back into Tarantella as the administrator
- Step 6. Observe that the administrator's webtop theme has not changed (ie. it still uses the **horizontal** webtop theme).

The purpose of this exercise is two-fold: First, we want to show the students how to change webtop themes. Second, we want to make sure that students understand that each of the webtop themes is separate from the others (ie. setting the organization to the webtop theme to **horizontal** and then the person's webtop theme to **noicon** did *not* result in the person having a horizontal launch pad with no icons). Emphasize these points if necessary.

10.2.3 Icon themes

Icon themes determine the appearance of the webtop icons.

Icon themes:

- Are stored in the `/inst_dir/images/en_US/size`, where *size* is the icon size.

For example, the standard icon theme is stored in `/opt/tarantella/images/en_US/32/standard`.

- Are configured on a per webtop theme by setting the webtop tray applet's `IconTheme` parameter.

For example, the standard webtop theme sets its icon theme to **standard** by setting the **IconTheme** parameter in `/opt/tarantella/webtops/en_US/standard/left.html` and `/opt/tarantella/webtops/en_US/standard/AdminTools.html` to `standard`. The changes to `left.html` and `AdminTools.html` change the icons used on the launch pad and in the Control Center, respectively.

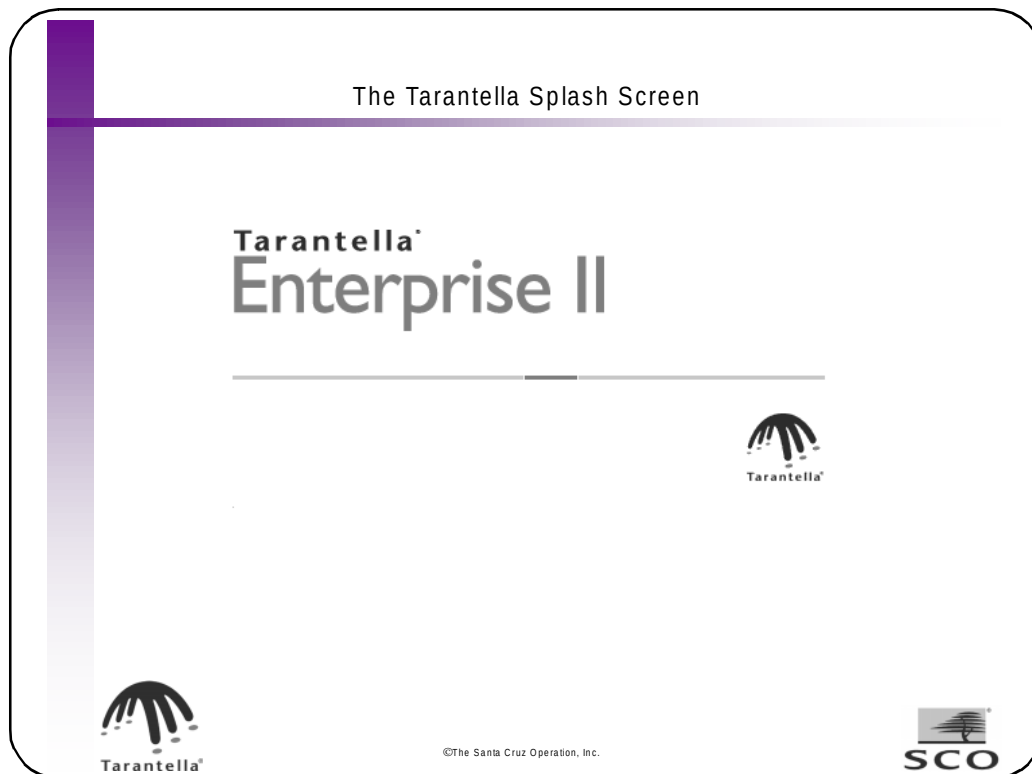
GuruNotes The `IconTheme` parameter is a parameter to the `asad` applet.

- You can create your own icon themes by copying `/inst_dir/images/en_US/size/standar` and modifying the copy

Tarantella comes with one icon theme, the **standard** icon theme. To create your own icon theme, copy the **standard** icon theme directory to a different name in the same directory. Make the desired modifications to the graphics files in the new directory. Then select the new icon theme by setting the `IconTheme` parameter in your webtop theme's `AdminTool.html` and `left.html`.

This, of course, assumes that the developer hasn't changed the names of `AdminTool.html` and `left.html` in the process of modifying the webtop to suit their preferences.

AV 10-2



10.3 Configurable Tarantella Components

In the sections which follow, we will discuss how to modify the various configurable screens displayed by Tarantella:

- The Spash Screen
- The Login Screen
- The Main Screen
- The Logout Screen

10.3.1 Splash screen

AV 10-2: The Tarantella Splash Screen

Use this slide to explain the Tarantella splash screen

AV 10-2: shows the default splash screen for Tarantella. The splash screen is displayed while Tarantella initializes the login sequence.

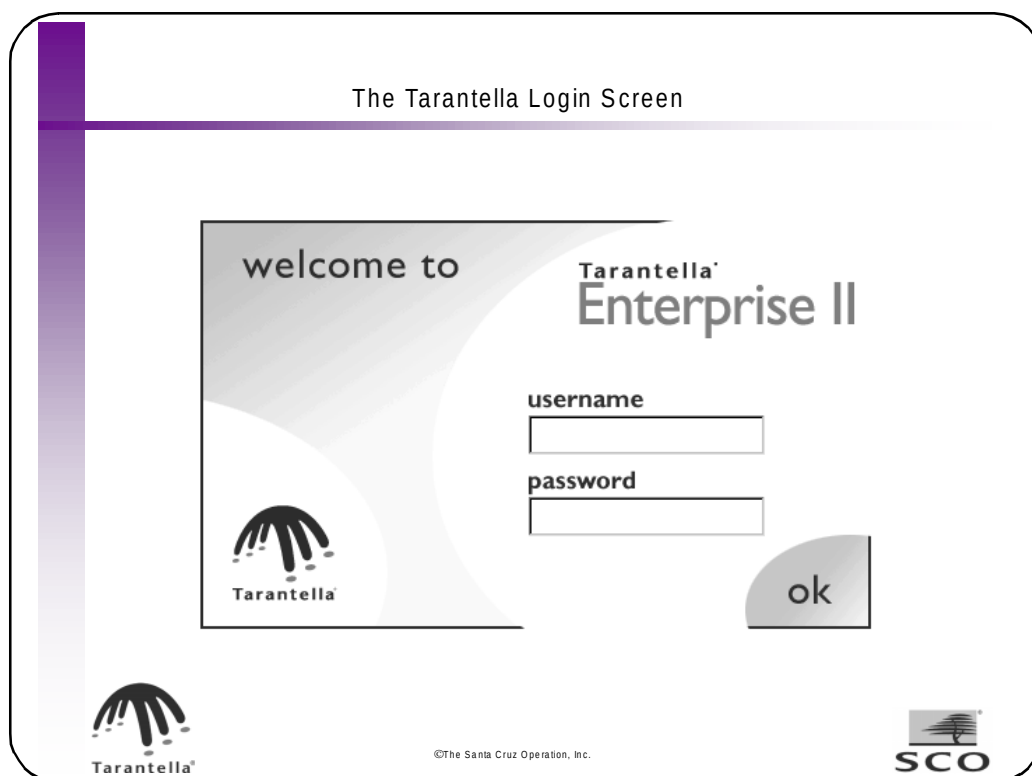
The splash screen is implemented for the default login by the file `/inst_dir/login/en_US/boot/splash.html`, where `inst_dir` is the Tarantella installation directory (usually `/opt/tarantella`).

The following graphics files are used in by the splash screen:

<code>/inst_dir/webtops/art/eiilogo_big.gif</code>	This is the logo on the top of the splash screen.
<code>/inst_dir/login/boot/working.gif</code>	This is the animated "working" gif on the splash screen.
<code>/inst_dir/login/webtops/ttalogo_small.gif</code>	The small tta logo in the lower right corner of the splash screen.

This, of course, assumes that the developer hasn't changed the names of `AdminTool.html` and `left.html` in the process of modifying the webtop to suit their preferences.

AV 10-3



10.3.2 Login screen

AV 10-3: The Tarantella Login Screen

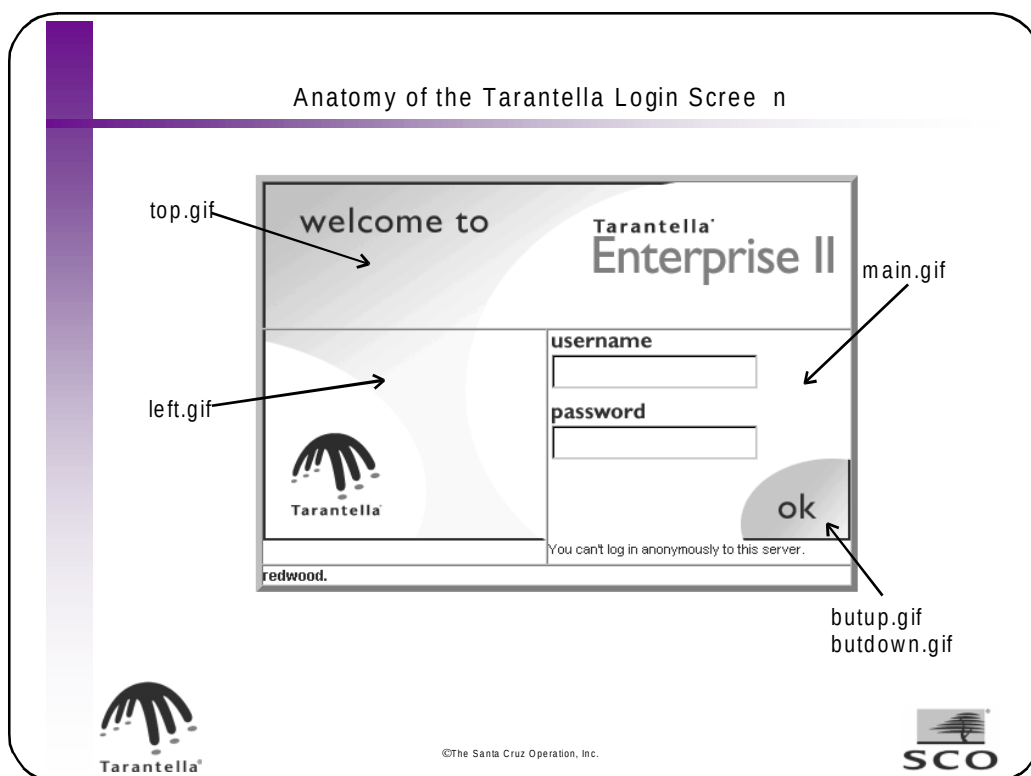
Use this slide to explain the Tarantella login screen

These files control the appearance of the various login screens:

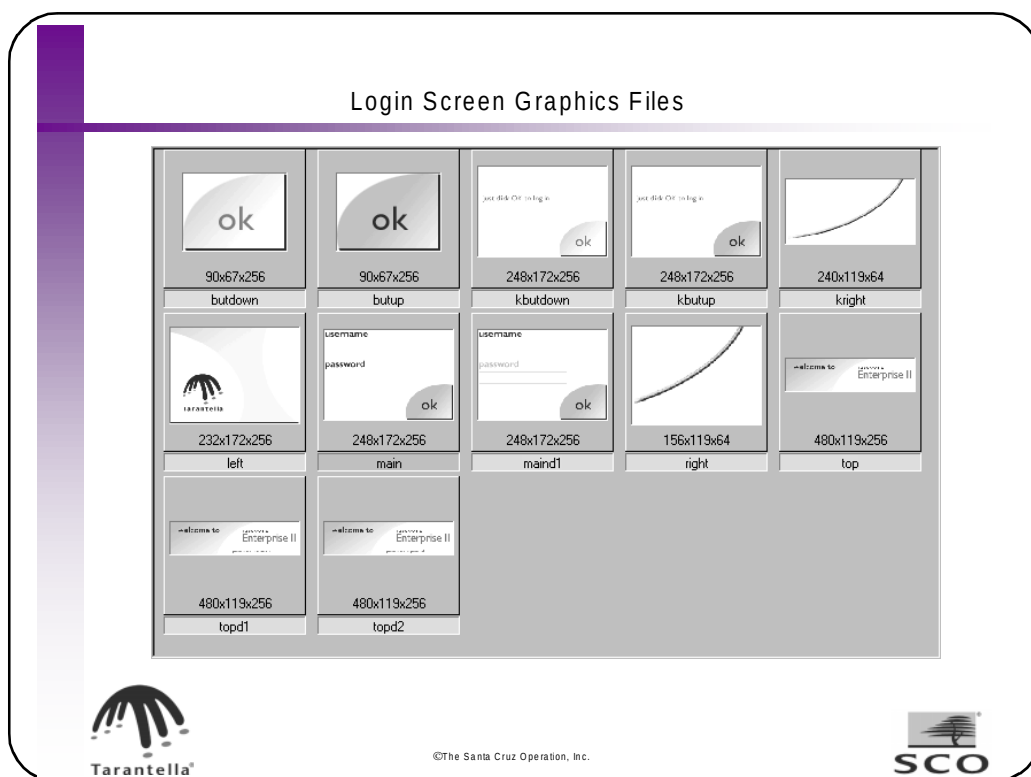
<i>/inst_dir/login/en_US/theme/index.html</i>	This file controls the appearance of the login screen.
<i>/inst_dir/login/en_US/theme/kiosk.html</i>	This file controls the appearance of the anonymous login screen.
<i>/inst_dir/login/en_US/theme/distrib1.html</i>	This file controls the appearance of the login screen for systems in Tarantella arrays.
<i>/inst_dir/login/en_US/theme/distrib2.html</i>	Like <i>distrib1.html</i> , this file controls the appearance of the login screen for systems in Tarantella arrays. Whereas <i>distrib1.html</i> controls the login screen when the user types in their user name, <i>distrib2.html</i> controls the login screen when the user is prompted for their password.
<i>/inst_dir/login/en_US/theme/direct.html</i>	This file controls the appearance of the login screen for systems in Tarantella arrays. Whereas <i>distrib1.html</i> and <i>distrib2.html</i> “distribute” users across Tarantella servers, <i>direct.html</i> enables users to log in directly the server of their choice.

The login screen (shown in slide AV 10-3:) is highly configurable. It can be configured by editing the HTML code that determines its layout and the graphics it uses and by modifying the parameters the HTML code passes to Tarantella’s login applet. Be sure to read in ***Admin Guide***.

AV 10-4



AV 10-5



10.3.2.1 The login screen graphics files

AV 10-4: Anatomy of the Tarantella Login Screen

Use this slide to explain the layout of the Tarantella login screen.

GuruNotes The technique which was used to produce this picture (ie. changing the value of the **border** parameter in the file `/inst_dir/login/en_US/standard/index.html` to a non-zero value) can be used anywhere in Tarantella where frames are used to view the layout of the frames used.

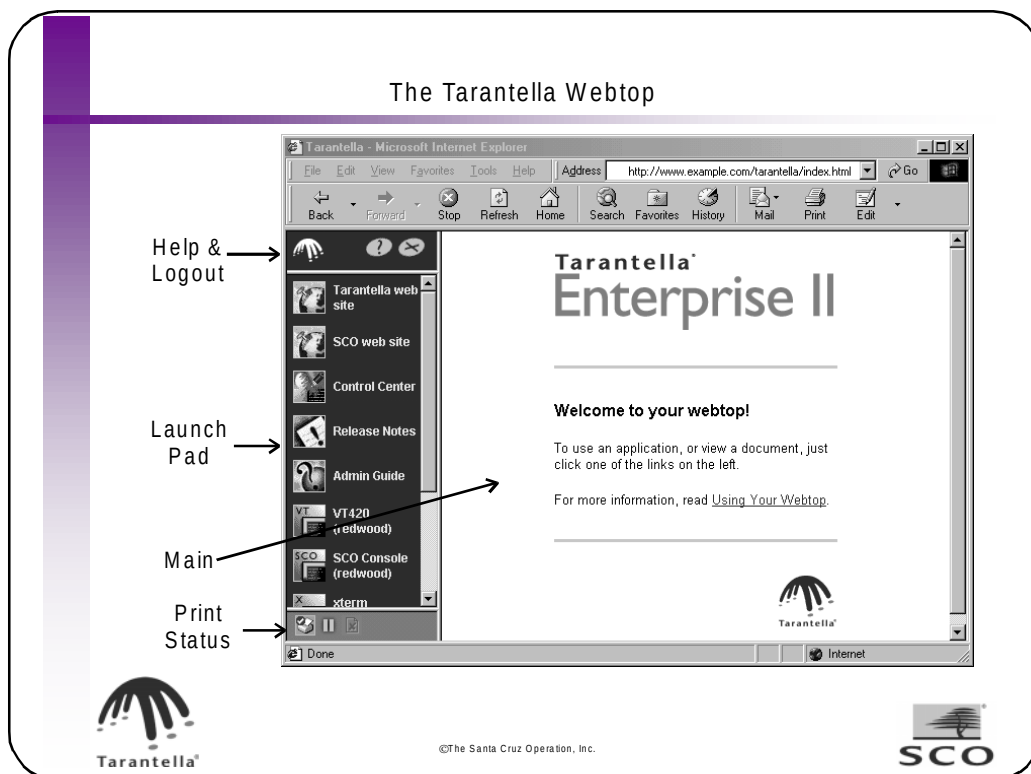
AV 10-5: Login Screen Graphics Files

Use this slide to explain the graphics files used by the login screen. In addition to explaining *top.gif*, *left.gif*, *main.gif*, *butup.gif*, and *butdown.gif*, be sure to explain the graphics files used in conjunction with *kiosk.html* and *direct.html* (Anonymous and direct logging in).

<i>top.gif</i>	This graphic file appears on the top of the login screen in the default login screen.
<i>left.gif</i>	This graphic file appears on the left side of the login screen in the default login screen.
<i>main.gif</i>	This graphic file appears to the right side of <i>left.html</i> in the default login screen. The graphic file shows up under the text boxes which query users for their user name and password.
<i>butup.gif</i>	This graphic file appears in the lower right hand portion of the default login screen. It is the button that users click on to log in to Tarantella.
<i>butdown.gif</i>	This graphic file appears in the same location as <i>butup.gif</i> , but is displayed when the user clicks on the button.

Make sure that the students understand that there is no requirement to use the default layout for the login screen or even the file names above.

AV 10-6



10.3.3 The Tarantella webtop

The Tarantella Webtop is comprised of the following components:

- The Main Frame
- The Launch Pad
- The Print Frame
- The Help/Logout Frame

AV 10-6: The Tarantella Webtop

Use this slide to point out the launch pad, the help/logout frame, and the main frame in the Tarantella webtop.

The HTML code which defines the layout of the frames used by the webtop and their contents is `/inst_dir/webtops/en_US/theme/index.html`, where *theme* is the name of the webtop theme being used.

10.3.3.1 The main frame

The main frame can be used to display welcome messages, documents, web pages, and applications.

The main frame is implemented in the default webtops by the file `/inst_dir/webtops/en_US/theme/right.html`, where *theme* is the name of the webtop theme being used.

Aspects you may wish to modify:

- The color scheme used
- The graphics files displayed

AV 10-7

The Tarantella "asad" Applet

```

<ttapplet archive="asad" name="Tarantella Webtop" code="SmartIconHost" width="%%
%CALCWIDTH%" height="%%CALCHEIGHT%">

<!-- Don't touch these parameters: -->
<param name="ObjectCount" value="%%OBJCOUNT%">
<param name="AsadPort" value="%%ASADPORT%">

<!-- Following parameters may be configured, but don't delete them: -->
<param name="ObjectWidth" value="%%OBJWIDTH 127%">
<param name="ObjectHeight" value="%%OBJHEIGHT 34%">

<!-- Following parameters may be configured, or omitted: -->
<param name="LayoutStyle" value="%%LAYOUTSTYLE vertical%">
<param name="ObjectGap" value="%%OBJGAP 10%">
<param name="TopMargin" value="%%TOPMARGIN 0%">
<param name="BottomMargin" value="%%BOTTOMMARGIN 0%">
<param name="LeftMargin" value="%%LEFTMARGIN 5%">
<param name="RightMargin" value="%%RIGHTMARGIN 0%">
<param name="IconToLabelGap" value="8">
<param name="BorderWidth" value="1">
<param name="IconTheme" value="standard">
<param name="TargetFrame" value="DisplayFrame">
<param name="ShowLabel" value="true">
<param name="ShowIcon" value="true">

```



©The Santa Cruz Operation, Inc.



One of the quickest and easiest ways to make Tarantella appear to be an integral part of your corporate network is to point the main frame at the company's home page instead of *right.html*. In the file */inst_dir/webtops/en_US/theme/index.html*, change the line which reads:

```
<frame src="right.html" name="DisplayFrame" scrolling="auto">
```

to read:

```
<frame src="http://www.your_company_here.com" name="DisplayFrame"
scrolling="auto">
```

10.3.3.2 Launch pad frame

Use the launch pad to execute the various applications that appear on the user's webtop. The Tarantella administrator controls which applications are available to which user. These applications can be Unix applications (character or GUI), Windows applications, or 3270 applications. To launch an application, the user simply single clicks on the icon.

GuruNotes This frame and the Help/Logout frame do not support animated gifs (not well anyway) due to the earlier version of Java their respective applets use.

The launch pad frame is implemented in the default webtops by the file */inst_dir/webtops/en_US/theme/left.html*, where *theme* is the name of the webtop theme being used.

Aspects you may wish to modify:

- The color scheme used
- The icons used

AV 10-7: The Tarantella "asad" Applet

Use this slide to illustrate the **asad** applet, the tag used to invoke the **asad** applet, the parameters which should not be touched, the parameters which can be configured but not deleted, and the parameters which can be configured or omitted entirely.

Unlike the main frame, the launch pad frame consists of more than simple HTML code. The launch pad frame invokes the Tarantella **asad** applet. This applet is highly configurable. Modifying the following **asad** applet parameters can produce a dramatic effect on the appearance of the launch pad:

Table 9: asad Applet Parameters

Labels	Colors	Icons
ShowLabel	LabelColor	ShowIcon
AttachLabelTo	ObjectBackgroundColor	
LabelFontFamily	ObjectTopShadow	
LabelFontSize	ObjectBottomShadow	
LabelFontStyle	HostBackground Color	
LabelColor		

These parameters are extensively documented in the online documentation. In **Admin Guide**, see **Advanced Customization** ⇒ **Applet parameters and methods** ⇒ **Webtop tray applet** ⇒ **Applet parameters**.

Exercise: Modifying asad Applet Parameters

A bit of experimentation with these parameters can be highly enlightening.

- Step 1. Modify one or two of these parameters at a time in *left.html*.
- Step 2. Click on your browser's refresh/refresh button.
- Step 3. Examine the results.
- Step 4. Repeat steps 1 through 3 changing new parameters each time.

10.3.3.3 Print status frame

The print status frame informs the user which printer Tarantella is configured to use and the status of print jobs. Furthermore, the print status frame allows users to pause or cancel print jobs.

The print status frame is implemented in the default webtops by the file `/inst_dir/webtops/en_US/theme/print.html`, where *theme* is the name of the webtop theme being used.

Aspects you can modify include:

- The color scheme used
- The graphics files used

Like the launch pad, the print status frame uses the `asad` applet.

The parameters used by the print status frame are documented in the online documentation. In the Admin Guide, see Advanced Customization ⇒ Applet parameters and methods ⇒ Print applet ⇒ Applet parameters.

Hopefully by now the students have realized the wealth of information which resides in the **Applet parameter and methods** section of the **Admin Guide**. Make sure the students understand its usefulness.

GuruNotes Unlike the launch pad and the Help/Logout frame, this frame does support animated gifs.

10.3.3.4 Help/Logout frame

This frame serves a dual role. The question mark icon takes the user to the extensive online documentation for Tarantella. The **X** icon allows the user to log out of Tarantella.

The Help/Logout frame is implemented in the default webtops by these files:

- */inst_dir/webtops/en_US/theme/optframe.html*,
- */inst_dir/webtops/en_US/theme/confirmlogout.html*, and
- */inst_dir/webtops/en_US/theme/dologout.html*,

where *theme* is the name of the webtop theme being used.

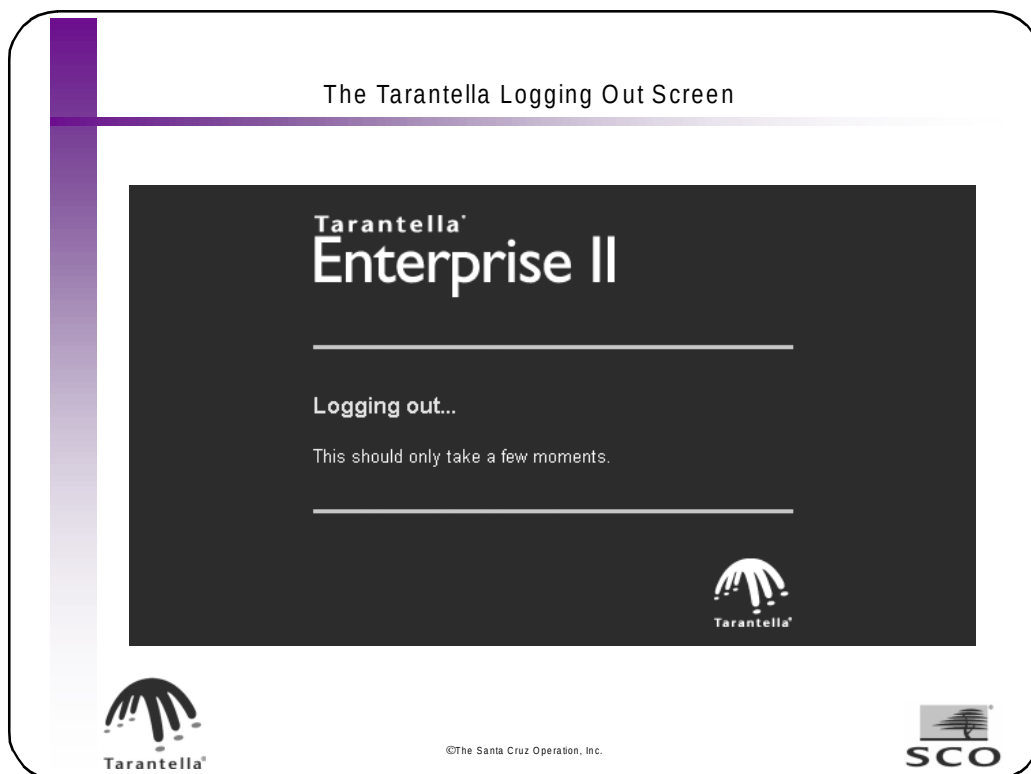
Aspects you may wish to modify:

- The color scheme used
- The graphics files used

Make sure the students are aware of the wealth of information provided in the **Admin Guide** and the **Release Notes**.

GuruNotes While this frame supports animation, it does not do so very well.

AV 10-8



AV 10-9



10.3.3.5 Logout confirmation frame

This frame, implemented by `/inst_dir/webtops/en_US/theme/confirmlogout.html`, is used to confirm the user's logout request.

Aspects you can modify include:

- The color scheme used
- The **yes** button (`optbar_yes.gif`)
- The **no** button (`optbar_no.gif`)

10.3.4 Logging out screen

AV 10-8: The Tarantella Logging Out Screen

Use this screen to show students the first of the two logout screens.

This is the first of two screens displayed when the user logs out. This screen is implemented by `/inst_dir/webtops/en_US/theme/dologout.html` and announces that Tarantella is logging out the user.

Aspects you can modify include:

- The color scheme used
- The graphics files used

10.3.5 Logged out screen

AV 10-9: The Tarantella Logged Out Screen

Use this screen to show students the second of the two logout screens.

This is the second of two screens displayed when the user logs out. This screen is implemented by `/inst_dir/webtops/en_US/theme/wt_shutdown.html` and announces that Tarantella has logged out the user.

Aspects you can modify include:

- The color scheme used
- The graphics files used

10.4 The Tarantella Solution Zone

The Tarantella Solution Zone contains extensive information on how to customize Tarantella Enterprise II. You can enter the Tarantella Solution Zone via your web browser at the following URL:

<http://tarantella.sco.com/tsz>

10.5 Lesson Summary

This lesson described the basic Web technologies used to configure the appearance of Tarantella. These included HTML, frames, cgi-bin scripts, and RGB colors. Also discussed were the various *.html* files that control the layout and appearance of Tarantella's login screen, webtop, and logout screens.

10.6 Review questions

1. What are the basic web technologies that are used to configure the appearance of Tarantella?

The basic web technologies used to configure the appearance of Tarantella are HTML, frames, cgi-bin, and RGB colors.

2. Tarantella uses “themes” to make customization easier. What types of themes does Tarantella provide?

Tarantella provides login, webtop, and icon themes.

3. What are the four webtop themes that Tarantella provides?

The four webtop themes provided by Tarantella are **standard**, **horizontal**, **maximum**, and **noicon**.

4. What are the names of the files that implement the **standard** login theme’s graphics?

Assuming that you are not logging in anonymously and not logging into a Tarantella array, the files that implement the standard login theme’s graphics are *top.gif*, *left.gif*, *main.gif*, *butup.gif*, and *butdown.gif*.

5. In which directory are webtop themes stored?

Webtop themes are stored in */inst_dir/webtops/en_US/theme*, where *theme* is the name of the webtop theme.

6. What utility do you use to change webtop themes?

Webtop themes are changed by using the Control Center.

7. How do you change the icon theme?

You change icon themes by editing `/inst_dir/webtops/en_US/standard/AdminTools.html` and `/inst_dir/webtops/en_US/standard/left.html`. In these files you must change the **IconTheme** parameter.

8. What is the purpose of the files *butup.gif* and *butdown.gif*?

These files are the graphic files for the **OK** button on the login screen.

9. What is the purpose of the file `/inst_dir/webtops/en_US/theme/left.html`?

left.html is the file that contains the HTML code and applet parameter definitions that control the appearance of the launch pad.

10. What are `ObjectTopShadow` and `ObjectBottomShadow` and what do they do?

`ObjectTopShadow` and `ObjectBottomShadow` are parameters to Tarantella's asad applet. They are used to set the color of the shadows on the top and bottom of the launch pad icons when the cursor is on top of an icon.

11. What is the file `/inst_dir/webtops/en_US/theme/wt_shutdown.html`?

`/inst_dir/webtops/en_US/theme/wt_shutdown.html` is the file which controls the second of the two logout screens. Specifically, this file controls the logged out screen (*dologout.html* controls the logging out screen).

10.7 Lab: Modifying the Login Theme

In this lab, you will customize Tarantella with a new login theme suitable for our hypothetical company, “Example Company, Inc.”

10.7.1 Overview

Create your own login theme by copying the **standard** login theme. Call the new login theme **exco**. Do the same for the webtop theme.

The instructor will provide you with a file called *excologin.ta*. This file contains the new graphics to be used by Example Company’s Tarantella login screen. Extract the contents of this file and place them in the appropriate directory on your Tarantella server.

Replace the standard login theme’s graphics files with those provided in the tar archive. Change the server’s login theme for the entire organization and test your modifications.

Note: If you really want to understand where each file appears on the login screen, replace these files one at a time and force your browser to reload the login screen. Notice as each new graphic appears where it is positioned.

To do this... Control Center ⇒ Server ⇒ Access ⇒ Login Theme

10.7.2 Procedure

To create a new login theme:

Step 1. Change directories to the Tarantella login theme directory:

```
# cd /inst_dir/login/en_US
```

where */inst_dir* is the Tarantella installation directory (usually */opt/tarantella*).

Step 2. Copy the **standard** login theme directory:

```
# copy -rom standard exco
```

The directory that you just created, *exco*, is a duplicate of the **standard** login theme.

Step 3. Log into Tarantella as the administrator and run the Control Center.

Step 4. In Control Center, pull down the Hierarchy view list menu and select **serve** .

Step 5. Click **Appl** .

Step 6. Change the **Login Theme** attribute to “exco”. Recall that this is the name of the login theme you created in Step 2.

Step 7. Click **Appl** . Make sure that the **Apply** button goes from solid black to greyed out before proceeding. The greying of this button is a visual indication that the change has been applied.

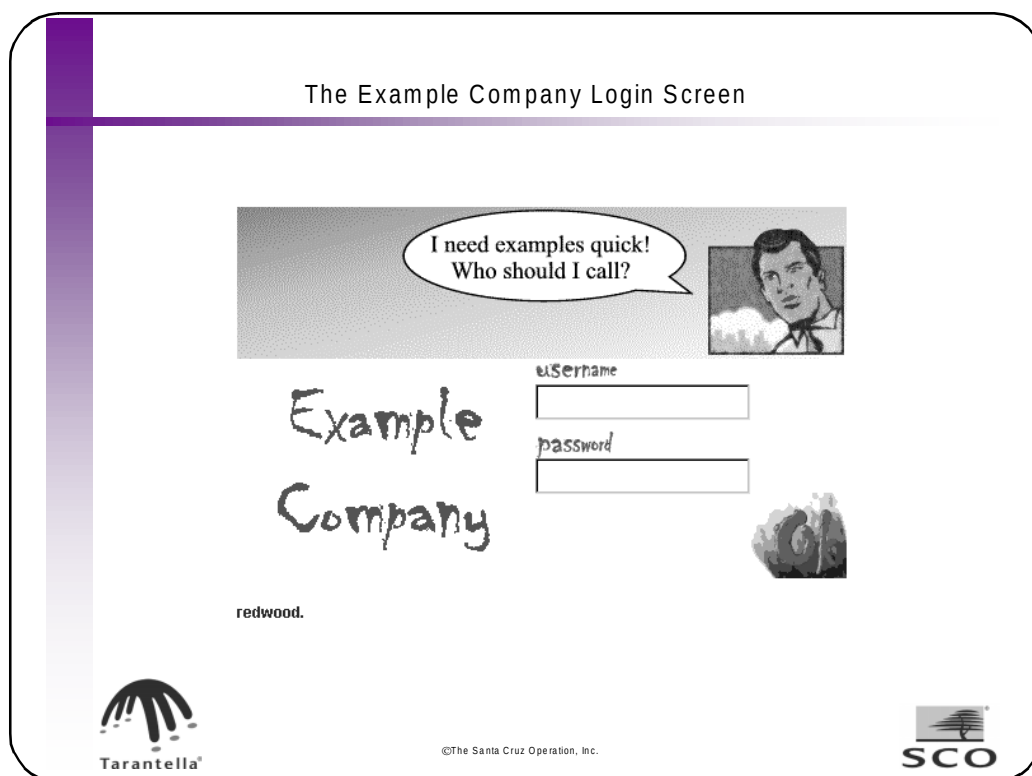
On occasions the “Apply” button doesn’t get greyed out (and correspondingly, the changes are not applied). On those occasions, exiting out of Control Center, invoking it again, making the same changes, and clicking “Apply” again works properly.

Step 8. Log out of Tarantella.

It is assumed that the students know at this point how to log out and log back in. Assist students as necessary

Step 9. Return to the login screen. While we have changed the login theme to **exco**, **exco** is still identical to the **standard** login theme. Consequently the login screen should still look exactly as it has previously. Do not login in yet.

AV 10-10



- Step 10. The instructor will provide you with a file called *excologin.ta* . This file contain the new graphics to be used by Example Company's Tarantella login screen.

Extract the graphics files in this tar archive:

```
# mv excologin.tar /opt/tarantella
# cd /opt/tarantella
# tar xvf excologin.tar
```

Note: The first two commands assume that the Tarantella installation directory is */opt/tarantella*. If Tarantella is installed in another directory, modify the first two commands accordingly.

- Step 11. Refresh/reload your web browser.

The login screen will change partially. While the top portion and the left portion of the login screen will have changed, the right hand side will not.

This is because the files for the top and the left portions of the login screen are loaded in as images in the HTML code. On the other hand, the right portion of the login screen is drawn by Tarantella's **asad** applet.

- Step 12. To get the entire login screen redrawn, restart your browser.

- Step 13. Return to the Tarantella login screen. At this point, the screen should appear like the login screen shown in slide AV 10-10 on page 10-38.

- Step 14. Return to the Tarantella login screen. At this point, the screen should appear like the login screen shown in slide AV 10-10 on page 10-40.

10.8 Lab: Modifying the Webtop Theme

In this lab, you will customize Tarantella with a new webtop theme suitable for our hypothetical company, “Example Company, Inc.”

GuruNotes Ways to pick RGB colors:

- `/opt/tarantella/data/rgb.txt`
Gives RGB definitions for many common colors
- In Windows: Start ⇒ Run ⇒ `mspaint` ⇒ `colors` ⇒ `Edit Colors` ⇒ `Define Custom Colors`
Gives RGB values in decimal in lower right corner

10.8.1 Overview

In Section 10.7 you created your own login theme by copying the **standard** login theme and modifying the new copy. Do the same for the webtop them and call the new webtop theme **exco**.

Change all backgrounds used on the various components of the new webtop to use blue (RGB: 0000FF) and the text to use white (RGB: FFFFFFFF). Change the server’s webtop theme for the entire organization and test your modifications.

To do this... Control Center ⇒ Organization ⇒ Right click Organization icon ⇒ Attributes ⇒ Webtop Theme

When you place the cursor on an icon in the standard webtop’s launch pad, Tarantella draws shadows around it in such a way that the icon appears to have popped up. Change the shadows so that the icon appears to have been pushed down. The colors you should use are RGB: 000080 and RGB: 8080FF.

000080 should be used on top (it’s the darker of the two colors) and 8080FF should be used on the bottom. This will give the icon the appearance of being pressed down when the cursor crosses over it.

10.8.2 Procedure

Step 1. Change directories to the Tarantella webtop theme directory:

```
# cd /inst_dir/webtops/en_US
```

where */inst_dir* is the Tarantella installation directory (usually */opt/tarantella*).

Step 2. Copy the **standard** login theme directory :

```
# copy -rom standard exco
```

The directory that you just created, *exco*, is a duplicate of the **standard** login theme.

Step 3. Log into Tarantella as the administrator and run the Control Center.

Step 4. In Control Center, pull down the Hierarchy view list menu and select **organization**.

Step 5. Right click the **Organization** icon.

Be prepared for students to make mistakes on Step 5. Make sure the students *right click* the “Organization” icon.

Step 6. Choose **Attributes**.

Step 7. Change the **Webtop Theme** attribute to “exco”. Recall that this is the name of the login theme you created in Step 2. Be aware that “exco” will not appear in the pull down list. This is normal. Instead of using the pull down menu, type “exco” in the **Webtop Theme** attribute box.

Step 8. Click **Apply** Make sure that the **Apply** button goes from solid black to greyed out before proceeding. The greying of this button is a visual indication that the change has been applied.

There is no need to logout of Tarantella at this point.

- Step 9. One of the quickest and easiest ways to make Tarantella appear to be an integral part of your corporate network is to point the webtop's main frame at your company's home page instead of *right.html*. In the file */inst_dir/webtops/en_US/exco/index.html*, change the line which reads:

```
<frame src="right.html" name="DisplayFrame"
scrolling="auto">
```

to read:

```
<frame src="http://www.sco.com" name="DisplayFrame"
scrolling="auto">
```

You can change "www.sco.com" to your own company's web page if you desire.

- Step 10. Change directories to the *exco* directory. In this directory, you will find a file called *optframe.html*. This file contains the HTML code responsible for drawing the Help/Logout frame. In this file you will find a line which reads:

```
</head><body bgcolor="#660099" text="#FFFFFF"
link="#FFFF00" vlink="#CCCC00" alink="#FFFFFF">
```

Change the background color to blue by changing the value of **bgcolor** to "#0000FF".

- Step 11. Refresh your web browser and notice the difference in the appearance of the webtop. The Help/Logout frame should now be blue.
- Step 12. Click on the "X" icon to logout. Notice that the frame returns to the **standard** webtop's purple. This is because clicking on the "X" icon causes the Help/Logout frame to be reloaded with the HTML code in */inst_dir/webtops/en_US/exco/confirmlogout.html*.
- Step 13. Change the background color to "#0000FF" in *confirmlogout.html*.
- Step 14. Refresh/reload your web browser.

- Step 15. Refreshing your web browser may cancel the logout. Simply click on the “X” icon again. Notice that the background is now blue.

The icons which appear in the Help/Logout frame are stored in the directory `/inst_dir/webtops/en_US/_art`. The file names for the four icons are:

- `optbar_help.gif`
- `optbar_logout.gif`
- `optbar_yes.gif`
- `optbar_no.gif`

Modifying these files is left as an exercise for the student.

- Step 16. The Tarantella logo in the Help/Logout is located in another directory. It is located in the directory `/inst_dir/webtops/art`. The name of the graphics file itself is `optbar_ttalogo.gif`.

Modifying this file is left as an exercise for the student.

- Step 17. The file `/inst_dir/webtops/en_US/exco/print.html` contains the HTML code responsible for drawing the printer status frame. Change the background color to blue by changing the value of **bgcolor** to “#0000FF”.

- Step 18. Refresh your web browser. Notice that only a portion of the background color changed as the result of the modification in Step 17.

- Step 19. In `print.html`, you will find another line which reads:

```
<param name="HostBackgroundColor" value="#9966cc">
```

Change the value to “#0000FF”.

- Step 20. Refresh/reload your web browser. Notice that **HostBackgroundColor** affected the background color appearing between the icons.

The remaining portions of this frame which are still the **standard** webtop’s purple are not part of the background. Rather, the purple is part of the icon’s graphic file itself. To modify this, you must modify the icons’ graphics files themselves, not the background.

The graphics files associated with these icons are stored in `/inst_dir/webtop/en_US/_art`.

- Step 21. The file *left.html* contains the HTML code responsible for drawing the launch pad. Change the background color to blue by changing the value of **bgcolor** to “#0000FF”.
- Step 22. Refresh/reload your web browser. Notice that only a portion of the background color changed as the result of the modification in Step 21.
- Step 23. In *left.html*, there is a line which reads:
- ```
<param name="ObjectBackgroundColor" value="660099">
```
- This line passes a parameter, **ObjectBackgroundColor**, to Tarantella’s asad applet. Change the value of this parameter to “#0000FF”.
- Step 24. Refresh/reload your web browser. Notice which portion of the launch pad changes color to blue.
- Step 25. Now change **HostBackgroundColor** to “#0000FF” in *left.html*.
- Step 26. Refresh/reload your web browser. Notice which portion of the launch pad changes color to blue.
- The launch pad should now conform to our hypothetical company’s blue color scheme.
- Step 27. Change the labels on the launch bar from yellow to white by changing the parameter **LabelColor** to “#FFFFFF”.
- Step 28. Refresh/reload your web browser. The labels should now be white.
- Step 29. Position the cursor on top of one of the launch pad’s icons. Notice that the shading makes the icon appear to pop up.
- Step 30. Now you will change the appearance of the icon shading to make the icon appear to be pushed in.
- Create a dark shadow on the top by changing **ObjectTopShadow** in *left.html* to “#000080”.
- Next create a light shadow on the bottom by changing **ObjectBottomShadow** in *left.html* to “#8080FF”.
- Step 31. Refresh/reload your web browser.
- Step 32. Position the cursor on an icon in the launch pad. The icon should now appear pressed inward.



Students who finish this section early are encouraged to experiment with other Tarantella customizations. Be sure to visit the Tarantella Solution Zone at <http://tarantella.sco.com/tsz> for other customization information.

## 10.9 Answers to Exercise and Review Questions

---

This section contains the answers to exercises, review questions, and labs presented in this lesson.

### Exercise answers

---

#### “Changing Webtop Themes,” on page 10-14

---

Please consult your instructor if you have any questions about this exercise.

### Review Question Answers

---

This section contains the answers to the review questions on page 10-34.

1. The basic web technologies used to configure the appearance of Tarantella are HTML, frames, cgi-bin, and RGB colors.
2. Tarantella provides login, webtop, and icon themes.
3. The four webtop themes provided by Tarantella are **standard**, **horizontal**, **maximum**, and **noicon**.
4. Assuming that you are not logging in anonymously and not logging into a Tarantella array, the files that implement the standard login theme’s graphics are *top.gif*, *left.gif*, *main.gif*, *butup.gif*, and *butdown.gif*.
5. Webtop themes are stored in */inst\_dir/webtops/en\_US/theme*, where *theme* is the name of the webtop theme.
6. Webtop themes are changed by using the Control Center.
7. You change icon themes by editing */inst\_dir/webtops/en\_US/standard/AdminTools.html* and */inst\_dir/webtops/en\_US/standard/left.html*. In these files you must change the **IconTheme** parameter.
8. These files are the graphic files for the “ok” button on the login screen.
9. *left.html* is the file that contains the HTML code and applet parameter definitions that control the appearance of the launch pad.

10. **ObjectTopShadow** and **ObjectBottomShadow** are parameters to Tarantella's asad applet. They are used to set the color of the shadows on the top and bottom of the launch pad icons when the cursor is on top of an icon.
11. `/inst_dir/webtops/en_US/theme/wt_shutdown.html` is the file which controls the second of the two logout screens. Specifically, this file controls the logged out screen (`dologout.html` controls the logging out screen).



---

# ***11***

## ***The Tarantella 3270 Connectivity Pack***

*Instructor Guide*

***Instructor Guide***



**Lesson 11**

## **The Tarantella 3270 Connectivity Pack**

### **Suggested lesson duration**

---

This lesson should take approximately .5 hours to complete. There is no lab.

### **Pre-lesson classroom preparation**

---

The classroom network needs to be setup properly (clients installed, DNS updated, etc.). The classroom must provide connectivity to the Internet. Aside from this, make sure you have the Tarantella media to install from (whether by CD-ROM or via the web).

Verify that you can ping locis.loc.gov.

### **Instructor preparation**

---

Read the documentation that accompanies the Tarantella 3270 Connectivity Pack.

## **Introduction**

---

The Tarantella 3270 Connectivity Pack provides access to 3270 applications through Tarantella. This lesson describes how it is installed, configured, and accessed.

## **Objectives**

---

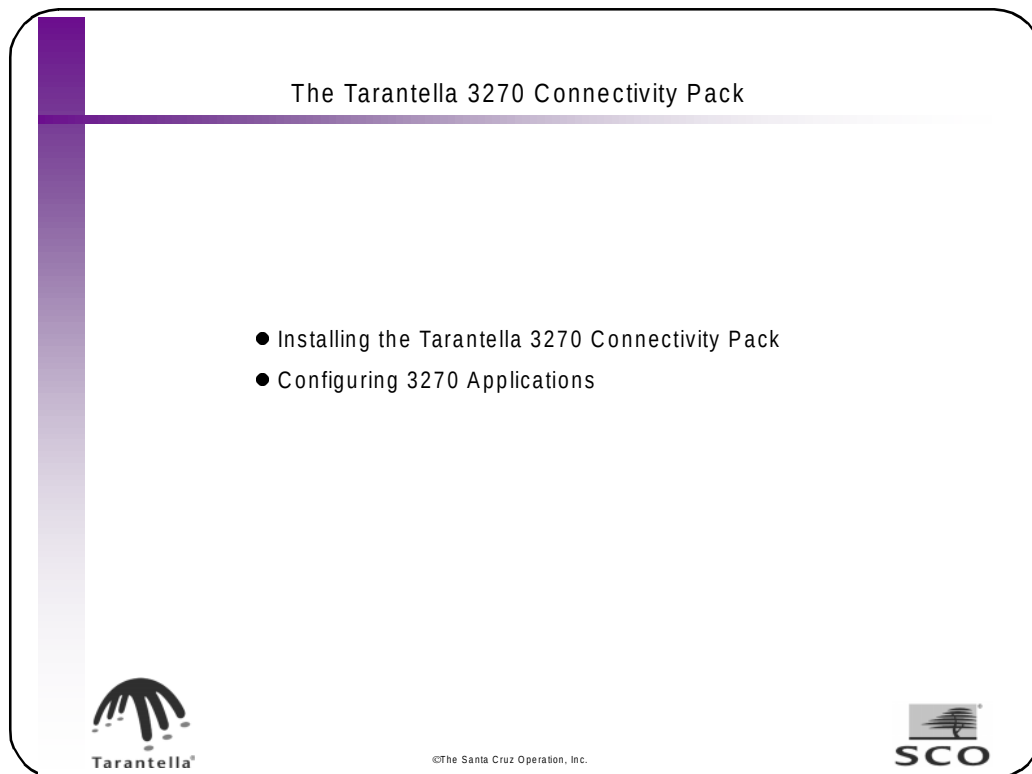
By the end of this lesson, you will be able to:

- Install the Tarantella 3270 Connectivity Pack
- Configure 3270 X applications and 3270 character applications





AV 11-1



Instructor Guide

---

## Topics

---

In order to meet these objectives, this lesson discusses:

- Installation — Discusses how to install the Tarantella 3270 Connectivity Pack from CD-ROM or via the web.
- Configuring 3270 Applications — Discusses how to configure the 3270 X applications and 3270 character applications.



### **AV 11-1: The Tarantella 3270 Connectivity Pack**

The first slide describes the overall topics covered in this lesson.

## 11.1 Installing the Tarantella 3270 Connectivity Pack

---

The Tarantella 3270 Connectivity Pack provides access to 3270 applications through Tarantella.

To install the Tarantella 3270 Connectivity Pack on a Tarantella server, the administrator should first install the Tarantella base software.

The Tarantella 3270 Connectivity Pack software itself installs exclusively on the second-tier.

### 11.1.1 Tarantella 3270 Connectivity Pack requirements

---

The Tarantella server software runs on the following platforms:

- UnixWare
- Solaris
- OpenServer
- AIX
- HP-UX

## 11.1.2 Distribution media

The Tarantella server software is distributed two ways:

Via the web	The Tarantella base product (along with the Windows Connectivity Pack, the Tarantella Security Pack, etc.) can be downloaded from <a href="http://tarantella.sco.com">http://tarantella.sco.com</a> . Web-distribution is the primary method of distribution.
On CD-ROM	In special instances, SCO distributes the software on CD-ROM. This is not the primary method of distribution.

**Table 10: Hints for Using CD-ROMs on SCO Platforms**

SCO OpenServer 5	<code>mount -f HS -o ro,lower /dev/cd0 /mnt</code>
SCO UnixWare 7 SCO UnixWare 2.1	<code>/usr/sbin/mount -rF cdfs /dev/cdrom/cdrom1 /mnt</code>

## 11.1.3 Installation procedure

To install the Tarantella 3270 Connectivity Pack, follow this procedure:

Step 1. Log in as root.

 There is no single-user mode requirement.

Step 2. Mount the CD-ROM.

Step 3. Run the following command:

**sh cleo\_file.shx**

where *cleo\_file.shx* is one of the following file names:

**Table 11: Tarantella 3270 Connectivity Pack SHX File Names**

Platform	SHX File name
SCO UnixWare® 7+	i3un0700.shx
SCO UnixWare 2.1.2+	i3un0212.shx
SCO OpenServer Release 5.0.2+	i3sc0325.shx
HP-UX 10.20+	pahp1020.shx
IBM AIX 4.2+	rsai0402.shx
SPARC Solaris 2.5.1+	spso0505.shx

Step 4. Follow the on-screen prompts.

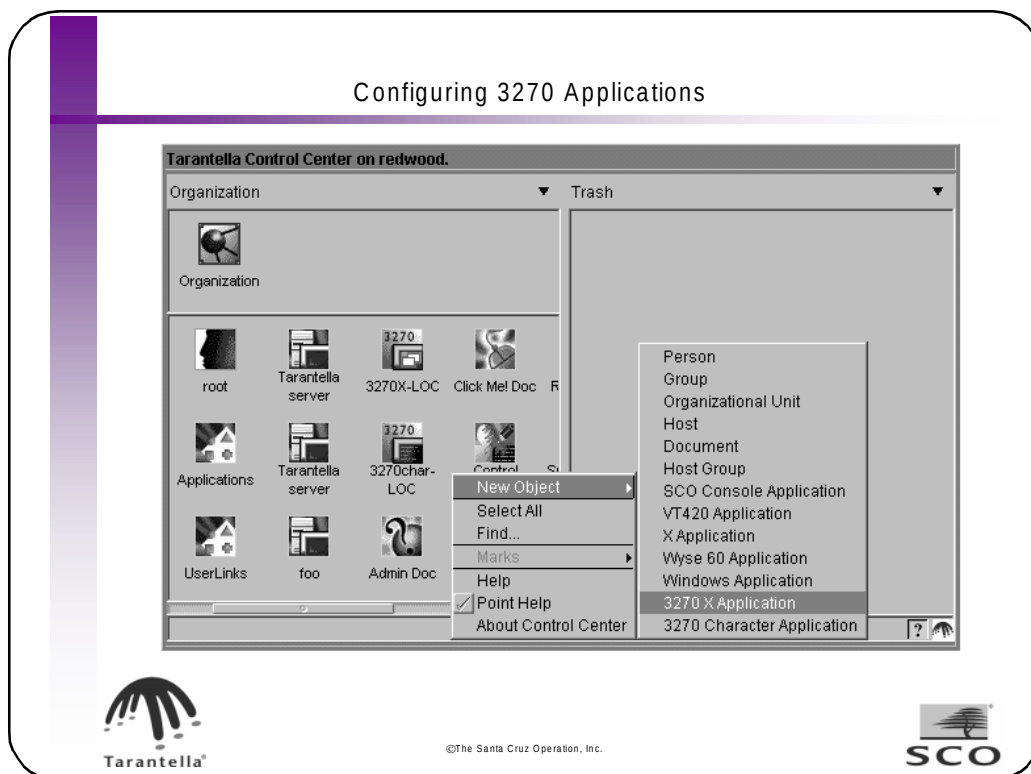
There is no need to restart Tarantella after the installation. It has already been started by the installation. Similarly, you needn't do anything to make the Tarantella 3270 Connectivity Pack restart upon reboot. The installation sets it up to automatically start upon reboot.

**Exercise: Installing the Tarantella 3270 Connectivity Pack**

---

Install the Tarantella 3270 Connectivity Pack on your Tarantella server.

AV 11-2





---

## 11.2 Using the Tarantella 3270 Connectivity Pack

---

### AV 11-2: Configuring 3270 Applications

Use this slide to illustrate configuring a 3270 application.

Configuring 3270 applications, whether X- or character-based, is much like installing any other application under Tarantella. Simply right click on the background of the **children box** in Control Center, select **New Object** ⇒ **3270 X Application** or **New Object** ⇒ **3270 Character Application**.

SlideAV 11-2 on page 11-12 shows Control Center after the installation of the Tarantella 3270 Connectivity Pack. Notice that the installation automatically created two 3270 application objects: **3270X-LOC** and **3270char-LOC**. These 3270 application objects are pre-configured to run a 3270 application at the Library of Congress. Use these 3270 application objects as examples when creating your own 3270 application objects.

#### **Exercise: Launching a 3270 Application**

---

In Control Center, deploy the 3270X-LOC application object to a Tarantella user. Log in as that user and launch 3270X-LOC.

## **11.3 Lesson Summary**

---

---

This lesson described how to install and use the Tarantella 3270 Connectivity Pack.

---

**A**

***Basic Networking  
and Tarantella***

*Instructor Guide*

***Instructor Guide***



**Appendix A**

## **Basic Networking and Tarantella**

### **Suggested lesson duration**

---

This lesson should take approximately six hours to complete including the lab.

### **Pre-lesson classroom preparation**

---

The machines must all be networked together and connected to the Internet. There must be *at least* one Tarantella server installed in the classroom. This shouldn't be a problem since by now the class should have multiple Tarantella servers up and running.

Using a network sniffer requires a NIC which supports promiscuous mode. Ideally, all the NICs in the classroom will support promiscuous mode. If this is not practical, there must be *at least* one NIC that supports promiscuous mode so that you can conduct a demo in place of the network sniffer lab.

### **Instructor preparation**

---

The instructor should be proficient in the materials covered in:

***TCP/IP Illustrated, Volume 1, The Protocols*** by W. Richard Stevens, ISBN 0-201-63346-9  
Chapters 1-5, 7-9, 11-12, 14, 17, 26-27

### **Introduction**

---

The vast majority of problems that Tarantella administrators face are related to networking, not Tarantella. This lesson prepares you with the networking related information needed for Tarantella administration.

This lesson discusses interfaces, IP addresses, IP packets, IP properties, IP protocols, port numbers, TCP packets, routing, subnetting, subnet classes, DNS, and various network protocols.

## Objectives

---

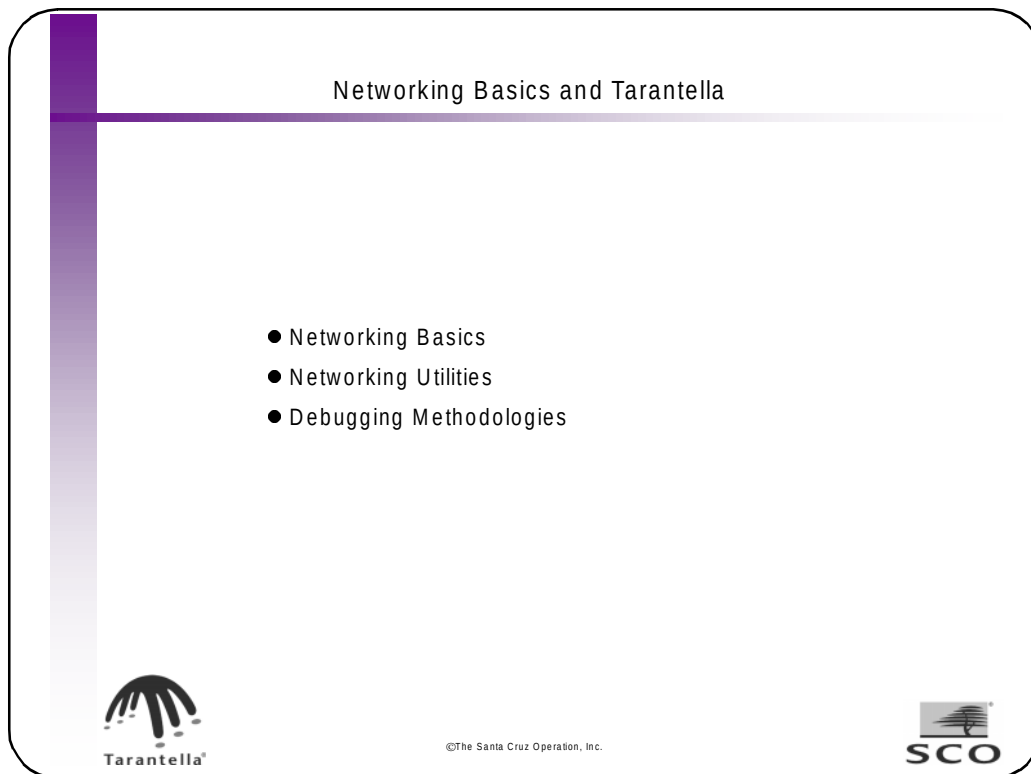
By the end of this lesson, you will be able to:

- Discuss the basic networking concepts that a Tarantella Administrator needs to know
- Interrogate web servers using the telnet command
- Analyze network traffic using a network sniffer
- Examine TCP segments, IP datagrams, and Ethernet frames



AV A-1

Instructor Guide





---

## Topics

---

In order to meet these objectives, this lesson discusses:

- Networking Basics — Discusses networking concepts including media types, interfaces, IP addresses, IP address classes, IP address types, IP datagrams, TCP, UDP, sequence numbers, acknowledgement numbers, encapsulation, port numbers, routing, subnetting, subnet masks, DNS, and various network protocols.
- Networking Utilities — Discusses utilities such as **ping**, **arp**, **ifconfig**, **netstat**, **tracert**, **nslookup**, **ipconfig**, and **winipcfg**.
- Debugging Methodologies — Discusses how to use tools such as telnet and network sniffers to troubleshoot network problems.



### AV A-1: Networking Basics and Tarantella

The first slide describes the overall topics covered in this lesson.



## A.1 Network Review

---

This section briefly discusses interfaces, IP addresses, IP packets, IP properties, IP protocols, port numbers, TCP packets, routing, subnetting, subnet classes, DNS, and various network protocols. This section is not intended as a exhaustive lesson on networking. Rather, this section is intended as a review of the network-related concepts that are relevant to Tarantella administrators.

Your instructor will provide you with a file called *net.hlp* that installs on Windows and provides a high-level overview of networking.

The *net.hlp* file is installed by the setup program on the courseware CD-ROM into the ftp server as *pub/labs/lab08/net.hlp*.

For an in depth discussion on the networking concepts and more, read the following books:

Stevens, W. Richard, ***TCP/IP Illustrated, Volume 1, The Protocols***, Addison Wesley, Reading, Massachusetts, Copyright 1994, ISBN 201-63346-9

Albitz, Paul & Liu, Cricket, ***DNS and Bind***, O'Reilly & Associates, Cambridge, Massachusetts, Copyright 1998, ISBN 1-56592-512-2

Comer, Douglas & Droms, Ralph, ***Computer Networks and Internets***, Prentice Hall, New York, New York, Copyright 1998, ISBN 0-13083-617-6

### A.1.1 Media types

---

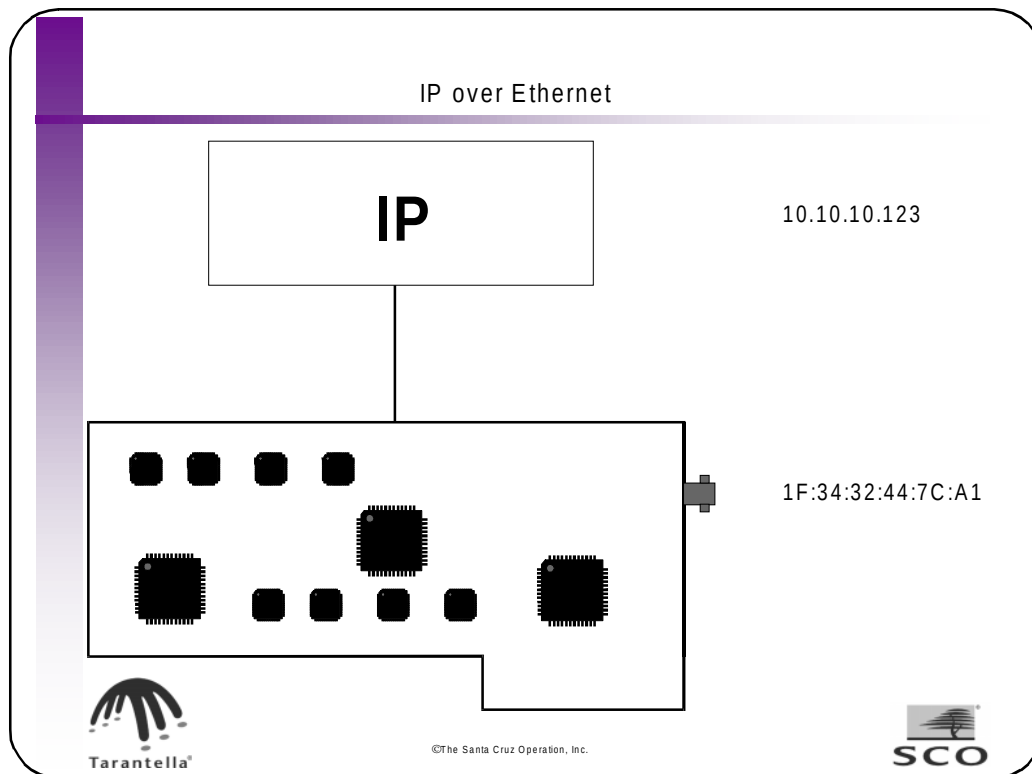
There are a multitude of media types. Some of the more common include:

- Ethernet
- Token Ring
- FDDI
- Serial / PPP

 This list is not comprehensive.



AV A-2



Instructor Guide

---

## A.1.2 Interfaces

---

Technically, it is inaccurate to say that a network consists of a number of *computers*. This is obvious when you consider the fact that on any given network you could find any combination of computers, printers, routers, terminal servers, etc.

It would be more accurate to speak of a network consisting of a number of *hosts* or *nodes*. But even these terms don't give the whole picture. In networking, we speak of *interfaces* rather than using the preceding terms.

Whether a device on the network is a computer, a printer, a router, a terminal server, a host, or a node, the device could have more than one connection to the network. For example, a computer could have more than one NIC installed. Each would have to be assigned a unique address. Each of these is called an *interface*.

Each media type (see Section A.1.1 on page A-10) has its own address scheme. For instance, Ethernet uses a six byte MAC address (eg. 00:00:1A:3B:5C:7D).

These addresses are proprietary to the media type.

### AV A-2: IP over Ethernet

Use this slide to show that the IP protocol runs atop of Ethernet.

The IP protocol was created to address issues such as the following:

Differing Network Types	An internet is a collection of networks. These networks may not use the same network types. For example, one of the networks may use Ethernet while another uses Token Ring. The IP protocol was designed to allow different types of networks to communicate with each other.
Hardware Addresses	Suppose you have a computer whose NIC's Ethernet MAC address is 12:34:56:78:9A:BC. Suppose you swap out the NIC. Since each Ethernet card has its own unique Ethernet address, the new NIC would necessarily have a new Ethernet address. After swapping out the NIC, other hosts on the network would no longer be able to communicate with the computer.

The IP protocol uses IP addresses, ARP, and RARP to resolve issues such as the preceding. IPv4 IP addresses are four bytes and are commonly written in "dotted decimal notation". For example: 10.25.230.82. In some circumstances, IP addresses are shown in hexadecimal. The preceding example would be 0A19E652 in hexadecimal.

### A.1.2.1 IP address classes

---

IPv4 addresses are divided into:

**Table 1: IPv4 Address Classes**

Class	Range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 247.255.255.255

### A.1.2.2 IP address types

---

There are different types of IP addresses:

- Unicast
- Broadcast
- Multicast

### A.1.3 IP datagrams

---

The IP protocol works in units called IP datagrams. Information included in IP datagrams includes:

Source IP address	The IP address of the sender.
Destination IP addresses	The IP address of the receiver.
Time To Live (TTL)	Sets an upper length on the number of hops this datagram can make. Each router is supposed to decrement this value by one before passing on the datagram.
Checksum	Used to detect data corruption.
Version	Identifies which version of IP is being used (eg. IPv4 versus IPv6).



---

Type of Service (TOS)	Enables applications to request the type of service they wish to receive. The five possible types of services are normal, minimize delay, maximize throughput, maximize reliability, and minimize monetary cost.
-----------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### A.1.4 IP properties

---

The IP protocol was designed with the following characteristics:

- Each packet is separate from all others
- Contents of packets could be corrupted
- Packets could be lost when transmitted
- Packets could be delivered more than once
- Packets can take differing amounts of time during delivery

### A.1.5 IP protocols

---

The IP portion of TCP/IP consists of multiple protocols:

TCP	“Transmission Control Protocol”
	• Connection oriented    • Ensures reliable receipt of data    • Automatically requests retransmission of missing pieces    • Automatically assembles data in order using sequence numbers    • Examples: http, smtp
UDP	“User Datagram Protocol”
	• Connectionless    • Low overhead    • Does not retransmit    • Does not order data in sequence

- Examples: RealAudio<sup>®</sup>, DNS

RealAudio uses UDP because if data from a live audio broadcast is lost, RealAudio should just continue onward. Latent data is useless in live audio.

### A.1.6 Port numbers

---

Port numbers are 16-bit numbers used to identify TCP and UDP programs. Both the TCP and the UDP protocols store the source and destination port numbers in their respective headers.

The port numbers are divided into three ranges:

**Table 2: Port Types and Ranges**

Type	Range
Well Known	0-1023
Registered	1024-49151
Dynamic and/or Private	49152-65535

Port numbers are listed in */etc/services*. Additionally, consult <http://www.iana.org> and <http://www.isi.edu/in-notes/iana/assignments/port-numbers> for official port number listings.

---

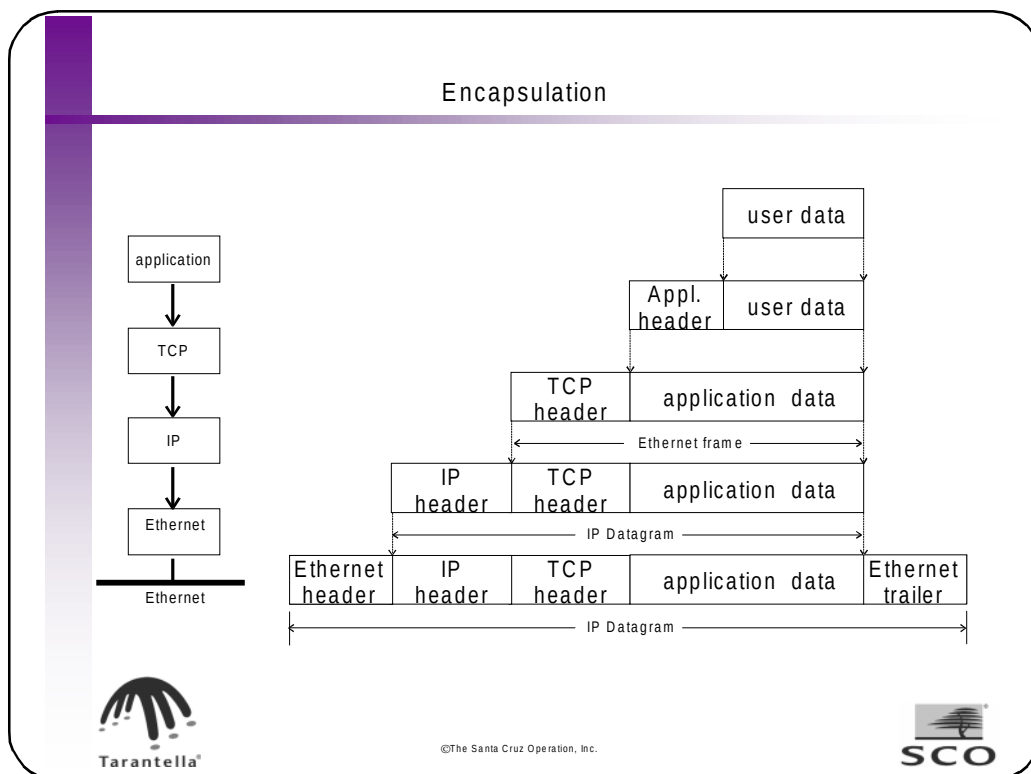
## A.1.7 Sequence numbers & acknowledgement numbers

---

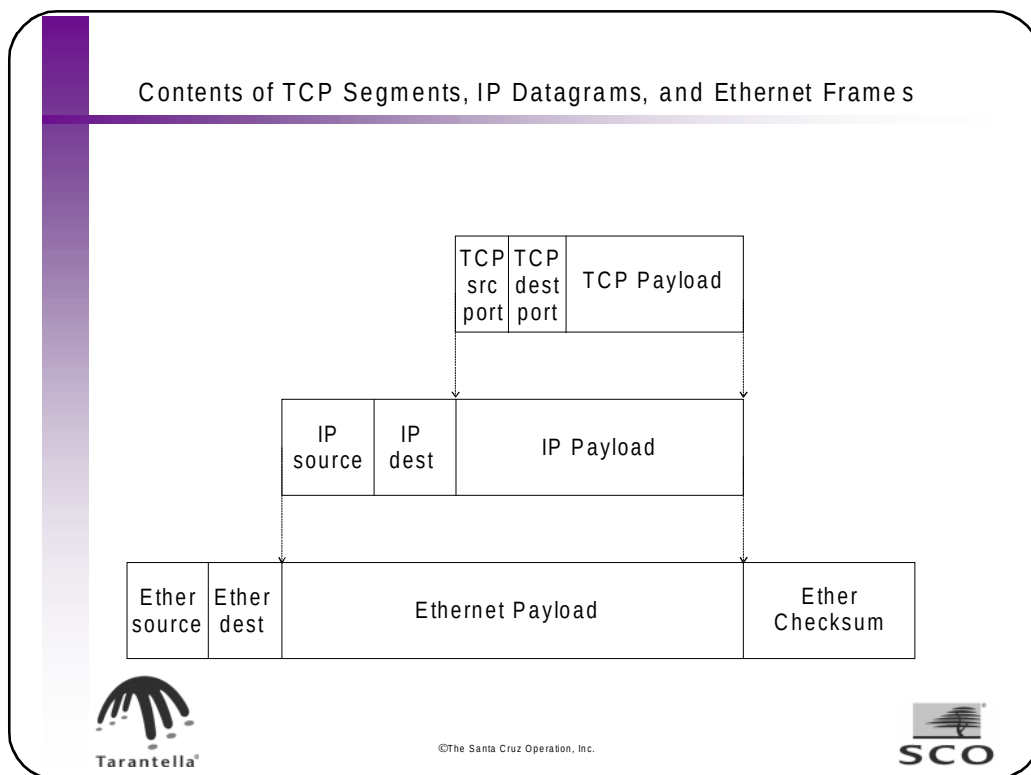
Each TCP header includes a *sequence number* . This number indicates which byte the first byte in the packet represents in the entire stream of data being sent from the source to the destination.

The *acknowledgement number* in the TCP header is used to acknowledge the receipt of data. It is the number of the next expected byte of data.

## AV A-3



## AV A-4



---

## A.1.8 Encapsulation

---

### AV A-3: Encapsulation

Use this slide to illustrate the concept of encapsulation.

### AV A-4: Contents of TCP Segments, IP Datagrams, and Ethernet Frames

Use this slide to illustrate the contents of TCP Segments, IP Datagrams, and Ethernet Frames. This diagram is a simplification. For more details, see the Stevens book.

When a TCP application sends data, the data is sent down the protocol stack (see AV A-3 on page A-18). As the packet travels down the protocol stack, each layer prepends a header (and possibly a trailer) to the data that it receives.

On the receiving machine, the packet travels up the protocol stack with each layer stripping off its header (and possibly its trailer). Consequently the data received by the destination is the same as what was sent.

The headers typically contain source and destination addresses plus additional information needed by the relevant layer of the protocol stack.

---

## A.1.9 Routing

---

An internet is a connected set of networks. Routing is the process by which packets are directed through the networks from their originating host to the destination.

Routing IP packets consists of each interface handing the packet to another interface which is “closer” to the destination. Typically the interface that the packet is handed to is a router. If the destination is the interface’s subnet, it gives the packet to the destination.

For routing to work properly, you must set your subnet mask correctly.

---

## A.1.10 Subnetting

---

Section A.1.2.1 on page A-14 discussed class A through class C IP addresses. By default, these classes are interpreted as follows:

**Table 3: IPv4 Class Interpretation**

Clas	Default Netmask	Number of Octets Indicating Network	Number of Octets Indicating Host
A	255.0.0.0	1	3
B	255.255.0.0	2	2
C	255.255.255.0	3	1

Notice that the table correctly points out that the values listed in the second column are *default* netmasks. Network administrators are free to modify the netmask to suit their own purposes.

For instance, a network administrator managing a class C network might choose to carve up the network into eight networks by using a netmask of 255.255.255.224. Netmasks that don't land on octet boundaries are called subnet netmasks.

Illustrate this example in binary if necessary for students unfamiliar with subnetting.

Subnet classes are being replaced by Classless Interdomain Routing (CIDR).

---

## A.1.11 DNS

---

Users typically don't want to, or are unable to, remember large numbers of IP addresses. Rather than use IP addresses only, names can be used (eg. `www.sco.com`). But for this convenience to work, name resolution must be performed. Something must map names to IP addresses (and vice versa).

Domain Name Service (DNS) provides name resolution. DNS was designed to be:

- Distributed
- Hierarchal
- Extensible
- Fast

DNS clients are told their DNS configuration through the following mechanisms:

- DHCP
- bootp
- `/etc/resolv.conf`

DNS performs both forward and reverse lookups. The latter are performed by lookups on `in-addr.arpa`.

DNS lookups can be performed using the **nslookup** command. This command will be discussed in Section A.3.6 on page A-31.

Modifications to DNS entries do *not* reconfigure the interface itself.

## A.1.12 Network protocols

---

There are many network protocols that run over TCP/IP. They include:

- Telnet
- Finger
- SMTP
- FTP
- HTTP
- SNMP
- POP3



## A.2 Before Embarking upon Tarantella

---

Before installing, configuring, or troubleshooting Tarantella, verify that your network infrastructure is configured and working properly. Minimally, you should verify the following areas:

- The hardware (eg. hubs, switches, routers, NICs, cables, etc.) must all be installed and correctly configured
- Routing must be working properly
- Machines involved must be able to ping each other
- Name resolution must be working properly for forward and reverse lookups
- The web server (presumably on port 80) must be installed, configured, and running
- **Telnet**, **rlogin**, and **rsh** (known as **rcmd** in SCO OpenServer) functionality must be working properly

## AV A-5

## The ifconfig Command

```
ifconfig net0 alias 10.10.10.2
ifconfig -a
lo0: flags=4049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
 inet 127.0.0.1 netmask ffffffff
 inet/perf: rcv size: 4096; send size: 8192; full-size frames: 1
 inet/options: rfc1323
net0: flags=4043<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet 10.10.10.1 netmask fffffff0 broadcast 10.10.10.255
 inet/perf: rcv size: 4096; send size: 8192; full-size frames: 1
 inet/options: rfc1323
 ether 00:00:b4:81:f7:b9
 (alias) inet 10.10.10.2 netmask fffffff0 broadcast 10.10.10.255
```



©The Santa Cruz Operation, Inc.



## AV A-6

## The ping Command

```
ping venezia.uss.sco.com
venezia.uss.sco.com is alive
#
#
ping -s venezia.uss.sco.co
PING venezia.uss.sco.com: 56 data bytes
64 bytes from venezia.uss.sco.com (10.10.10.59): icmp_seq=0. time=0. ms
64 bytes from venezia.uss.sco.com (10.10.10.59): icmp_seq=1. time=0. ms
64 bytes from venezia.uss.sco.com (10.10.10.59): icmp_seq=2. time=0. ms
64 bytes from venezia.uss.sco.com (10.10.10.59): icmp_seq=3. time=0. ms

----venezia.uss.sco.com PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```



©The Santa Cruz Operation, Inc.



## A.3 Network Utilities Used by Tarantella Administrators

---

Out of the scores of network related commands, a handful are particularly useful to Tarantella administrators. In this section, we discuss those utilities and why they are useful to Tarantella administrators.

### A.3.1 ifconfig

---

#### AV A-5: The ifconfig Command

Use this slide to illustrate **ifconfig -a** and **ifconfig interface alias**

Use the **ifconfig** command to:

- Display all interfaces configured
- Create aliases to enable one NIC to respond to multiple IP addresses

SlideAV A-5 on page A-24 illustrates the **ifconfig** command.

### A.3.2 ping

---

#### AV A-6: The ping Command

Use this slide to illustrate **ping** and **ping -s**

Use the **ping** command to test for connectivity between two hosts on the network. The **ping** is useful to Tarantella administrators because it gives them a quick way of ascertaining a) whether a host is present, and b) which hosts are on a particular network.

To test for the presence of all the hosts on a particular subnet, ping the broadcast address for that subnet.

**GuruNotes**      Windows 95/98 hosts do not respond to pings to the broadcast address.

SlideAV A-6 on page A-24 illustrates the **ping** command.

## AV A-7

## The netstat Command

```
netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp 0 0 venezia.uss.sco..ftp firenze.uss.sco..1038 FIN_WAIT_2
tcp 0 2 venezia.uss.sco..telne firenze.uss.sco..1037 ESTABLISHED
tcp 0 0 *.32782 *.* LISTEN
tcp 0 0 *.printer *.* LISTEN
tcp 0 0 *.listen *.* LISTEN
tcp 0 0 *.dtspc *.* LISTEN
tcp 0 0 *.i2odialo *.* LISTEN
tcp 0 0 *.chargen *.* LISTEN
tcp 0 0 *.daytime *.* LISTEN
tcp 0 0 *.discard *.* LISTEN
tcp 0 0 *.echo *.* LISTEN
tcp 0 0 *.time *.* LISTEN
tcp 0 0 *.netstat *.* LISTEN
tcp 0 0 *.systat *.* LISTEN
tcp 0 0 *.finger *.* LISTEN
tcp 0 0 *.imap-4 *.* LISTEN
tcp 0 0 *.pop-3 *.* LISTEN
tcp 0 0 *.exec *.* LISTEN
tcp 0 0 *.login *.* LISTEN
```



©The Santa Cruz Operation, Inc.



## AV A-8

## The netstat Command

```
netstat -r
Routing tables
Destination Gateway Flags Refs Use Interface
default xylan244.uss.sco.C UGS 0 111 net0
localhost localhost UH 5 77 lo0
10.10.10/24 venezia.uss.sco.co UC 0 0 net0
venezia.example. localhost UGHS 4 18 lo0
224/8 venezia.uss.sco.co UGS 1 9 net0
```



©The Santa Cruz Operation, Inc.



### A.3.3 netstat

---

#### AV A-7: The netstat Command

Use this slide to illustrate looking up available services using **netstat -a**

#### AV A-8: The netstat Command

Use this slide to illustrate lookup up routing information using **netstat -r**

Use the **netstat** command is useful to Tarantella administrators for two reasons. The **netstat** command can be used to:

- Look up which services are available on a machine
- Look up routing information

The **-n** option is used by Tarantella administrators to suppress IP address to name resolution. This is useful when you encounter name resolution problems.

The **-n** option is so very useful, many network administrators consider it a good habit to use **-n** by default.

Slides AV A-7 on page A-26 and AV A-8 on page A-26 illustrate the **netstat** command.

In addition to **netstat -a**, consult */etc/inetd.conf* to see what services are available and how they are launched.

Additionally consult */etc/inetd.conf* to see if TCP wrappers (also known as **tcpd**) is in use. See the **tcpd** manual page for more information on TCP wrappers.

## AV A-9

## The traceroute Command

```
traceroute standards.ietf.org
traceroute to standards.ietf.org (199.172.136.45), 30 hops max, 80 byte packets
 1 abovenet.wams.com (207.126.116.142) 0 ms 0 ms 0 ms
 2 209.133.3.3 (209.133.3.3) 50 ms 50 ms 40 ms
 3 216.200.0.205 (216.200.0.205) 40 ms 40 ms 40 ms
 4 216.200.0.21 (216.200.0.21) 130 ms 100 ms 120 ms
 5 209.133.31.106 (209.133.31.106) 140 ms 130 ms 80 ms
 6 iad3.ph100.verio.net (129.250.3.106) 110 ms 120 ms 130 ms
 7 fa-0-0-0.a00.phlapa01.us.ra.verio.net (129.250.31.36) 90 ms 110 ms 90 ms
 8 d3-1-0-0.a00.prtnnj01.us.ra.verio.net (130.94.40.102) 130 ms 120ms 130 ms
 9 d3-0-1-1.a01.jrcynj01.us.ra.verio.net (130.94.10.250) 140 ms 130 ms 90
10 fa-1-0-0.a00.jrcynj01.us.ra.verio.net (130.94.80.1) 140 ms 150ms 230 ms
11 130.94.83.2 (130.94.83.2) 110 ms 160 ms 110 ms
12 standards.ietf.org (199.172.136.45) 140 ms 120 ms 130ms
```



©The Santa Cruz Operation, Inc.



## AV A-10

## The arp Command

```
arp -a
bologna.example.COM (10.10.10.6) at 2:7:1:19:e3:5e (802.3)
firenze.example.COM (10.10.10.54) at 0:e0:98:72:d6:21 (802.3)
milano.example.COM (10.10.10.35) at 0:a0:c9:ec:68:f1 (802.3)
```



©The Santa Cruz Operation, Inc.



## A.3.4 traceroute

---

### AV A-9: The traceroute Command

Use this slide to illustrate **traceroute**

Use the **traceroute** command to trace the route from one host to another. In addition to showing the IP addresses, and possibly resolved names for those IP addresses, the **traceroute** command provides information about the relative speed of each hop along the route.

Under Windows, the **traceroute** command is called **tracert**.

Slides AV A-9 on page A-28 illustrates the **traceroute** command.

## A.3.5 arp

---

### AV A-10: The arp Command

Use this slide to illustrate **arp**

Use the **arp** command to:

- Look up Ethernet address to IP address mappings. When error messages report problems with a particular Ethernet address, **arp** can be used to track down the IP address of the offending host.
- Look up information about a particular NIC. The manufacturer is encoded into the Ethernet address of every NIC. The Ethernet address to manufacturer relationship can be looked up at the following URL:

<http://standards.ieee.org/regauth/oui/oui.txt>

Many manufacturers offer the ability to program the ethernet address.

Slides AV A-10 on page A-28 illustrates the **arp** command.

## AV A-11

## The nslookup Command

```
nslookup
Default Server: ns1.example.COM
Address: 10.10.10.1

> venezia.example.com
Server: ns1.sco.COM
Address: 10.10.10.1

Name: venezia.example.com
Address: 10.10.10.59
```



Tarantella®

©The Santa Cruz Operation, Inc.



## AV A-12

## The nslookup Command

```
nslookup
Default Server: ns1.example.COM
Address: 10.10.10.1

> set type=any
> www.sco.com
Server: ns1.example.COM
Address: 10.10.10.1

www.sco.com internet address = 209.1.8.14
example.COM nameserver = ns2.example.COM
example.COM nameserver = ns1.example.COM
ns2.example.COM internet address = 10.10.10.1
ns1.example.COM internet address = 10.10.10.2
```



Tarantella®

©The Santa Cruz Operation, Inc.





## A.3.6 nslookup

---

### AV A-11: The nslookup Command

Use this slide to illustrate **nslookup**

### AV A-12: The nslookup Command

Use this slide to illustrate the **set type=any** command in **nslookup**.

If you use DNS, use the **nslookup** command to:

- Look up mappings from host names to IP addresses (and vice versa)
- Identify name servers
- Identify name resolution problems

Slides AV A-11 on page A-30 and AV A-12 on page A-30 illustrate the **nslookup** command.

### GuruNotes

The **nslookup** command uses UDP by default. This is problematic in networks whose firewall let the DNS/UDP packet out but don't allow in the return packet. The **set vc** (set virtual connection) command in **nslookup** instructs **nslookup** to use TCP rather than UDP. Since TCP is connection oriented, the response will be allowed to return through the firewall.

## AV A-13

## The ipconfig Command

```
C:\WINDOWS\Desktop> ipconfig /all
Windows 98 IP Configuration

Host Name : firenze.example.com
DNS Servers : 10.10.10.1
 10.10.10.2
Node Type : Broadcast
NetBIOS Scope ID. :
IP Routing Enabled. : No
WINS Proxy Enabled. : No
NetBIOS Resolution Uses DNS : Yes

0 Ethernet adapter :

Description : ISA Ethernet Adapter.
Physical Address. : 00-E0-98-72-D6-21
DHCP Enabled. : No
IP Address. : 10.10.10.3
Subnet Mask : 255.255.255.0
Default Gateway : 10.10.10.1
Primary WINS Server :
Secondary WINS Server :
Lease Obtained. :
Lease Expires :
```



©The Santa Cruz Operation, Inc.



## A.3.7 ipconfig

---

### AV A-13: The ipconfig Command

Use this slide to illustrate **ipconfig**

Use the **ipconfig** command on Windows NT systems to look up basic network configuration information.

Slides AV A-13 on page A-32 illustrates the **ipconfig** command.

## A.3.8 winipcfg

---

The **winipcfg** command provides, in essence, the same information as **ipconfig**. The main differences between these commands are:

- **winipcfg** is graphical whereas **ipconfig** is not
- **ipconfig** is available on Windows 95/98/NT whereas **winipcfg** is available on Windows 95/98 only

AV A-14

### Telneting to an FTP Server

```
→ # telnet venezia 21
Trying 10.10.10.59
Connected to venezia.example.com.
Escape character is '^]'.
220 venezia.example.com FTP server (wu-2.4.2-academ-15) ready.
→ USER root
331 Password required for root.
→ PASS ClearText
230 User root logged in.
→ QUIT
221 Goodbye.
Connection closed by foreign host.
```

→ Commands typed



©The Santa Cruz Operation, Inc.



---

## A.4 Tarantella Administrator's Tools

---

While all the utilities discussed in Section A.3 on page A-25 are useful to Tarantella administrators, there are a few advanced techniques that, when properly understood, provide a tremendous amount of useful information.

### A.4.1 Telnetting to a port

---

#### AV A-14: Telnetting to an FTP Server

Use this slide to illustrate telnetting to the `ftpd` daemon.

Most network administrators know about the **telnet** command, but surprisingly few know that **telnet** can be used for more than remotely logging into a machine. A perusal of the **telnet** manual page reveals that the **telnet** command takes an optional argument specifying which port to attach to. If the option is not specified, **telnet** uses port 23, the port on which the **telnet** daemon listens.

When you telnet to a particular port, you are able to communicate directly with the daemon on the server. Each daemon (eg. `ftpd`, `telnetd`, etc.) uses its own network application protocol. If you know the protocol, you can communicate with the daemon directly.

Network application protocols are defined by Request For Comment (RFC) articles. You can look up RFCs at the following URL:

<http://www.rfc-editor.org>

SlideAV A-14 on page A-34 shows an example of telnetting to the `ftpd` daemon.

If necessary, explain to students the `^]` escape character and the `help` and `quit` commands in **telnet**'s interactive mode.

## A.4.2 Network sniffers

---

While most Tarantella troubleshooting issues don't require the use of a network sniffer, sniffers can provide a large amount of insightful information and in some situations sniffers are indispensable.

Network sniffers are utilities used to analyze network traffic. Sniffers work by setting a network card into promiscuous mode. Whereas NICs usually drop packets not addressed for the NIC (ie. the NICs address or the broadcast address), promiscuous mode instructs the NIC to pass all network traffic up the network stack.

Amongst other capabilities, typical sniffers provide the ability to:

- Analyze network performance
- Pinpoint the cause of congestion and bottlenecks
- Resolve address collision problems
- Track network traffic between specified machines
- Analyze network traffic for specified protocols

This list is by no means comprehensive.

There are numerous network sniffers available. In this course, we'll use Microsoft's Network Monitor.

---

## A.4.3 Using Network Monitor

---

Microsoft's Network Monitor provides many useful features. This section details how to make use of these features.

### A.4.3.1 Installing Network Monitor for Windows 95/98

---

If installing the NT version of Network Monitor, get the file *ntsetup.exe* from the courseware CD-ROM or the anonymous ftp directory. Run *ntsetup.exe*. If the NT cab files are not installed, you will need the NT CD-ROM. After running *ntsetup.exe*, reboot. Right click Network Neighborhood, select Properties, and select the Services tab. If Network Monitor shows up, double click it and it will run the configuration. If Network Monitor didn't show up, click on the Add button, install it, and run the configuration. Requires another reboot.

To install Microsoft's Network Monitor for Windows 95/98, follow these steps:

Step 1. The instructor will make a folder available to you called *netmon*. This folder contains a file (*ntsetup.exe*) and three directories (*disk1*, *disk2*, and *disk3*). The *ntsetup.exe* file, as its name suggests, installs Network Monitor for Windows NT.

This procedure explains how to install the Windows 95/98 version of Network Monitor

Step 2. Open the *netmon* directory with Windows Explorer.

Step 3. Open the *disk1* directory.

Step 4. Double click *setup.exe* to begin the installation.

Step 5. Next you will be prompted to specify where to install Network Monitor. Choose the default by clicking on the **Continue** button or select a different directory.

Step 6. If the installation directory doesn't exist, you will be asked whether to create it. Click the **OK** button.

Step 7. You are given the opportunity to set passwords for displaying and capturing network traffic. Click on the **No Password** button.

Step 8. Enter your name when prompted and click the **OK** button.

Step 9. You are asked to confirm the name. Click the **OK** button.

- Step 10. You are next prompted to install the Microsoft Network Monitor driver. Click the **OK** button.
- Step 11. You are informed that the Network Monitor was successfully installed. Click the **OK** button. Note: The installation is not complete.
- Step 12. Microsoft's network configuration utility is launched automatically by the installation. Click **Add** ⇒ **Service** ⇒ **Microsoft Network Monitor Agent**.
- Step 13. Click the **Cancel** button to return to Microsoft's network configuration utility. Note: While it is non-intuitive, clicking the **Cancel** button does result in the Network Monitor Agent being successfully installed.
- Step 14. Click the **OK** button to leave Microsoft's network configuration utility.

Here the students may have to coax Windows through its question(s) whether to save previous versions of relevant files.

### **Exercise: Installing Network Monitor**

---

The instructor will make the *netmon* folder (see Step 1. on page A-37) available to you. Install the appropriate version of Network Monitor.



### A.4.3.2 Launching Microsoft Network Monitor

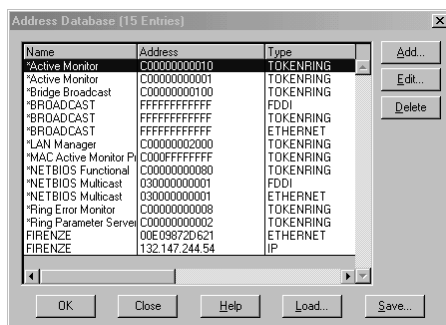
---

To launch the Windows 95/98 version of Network Monitor, click **Start** ⇒ **Programs** ⇒ **Network Analysis Tools** ⇒ **Network Monitor** .

To launch the Windows NT version of Network Monitor, click **Start** ⇒ **Programs** ⇒ **Administrative Tools** ⇒ **Network Analysis Tools** ⇒ **Network Monitor** .

## AV A-15

## Adding Ethernet and IP Addresses

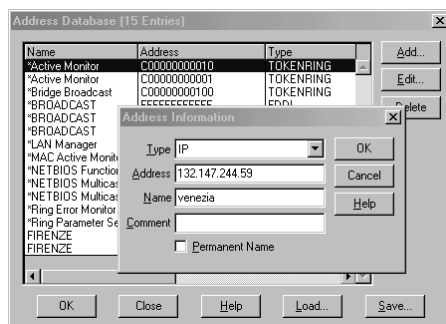


©The Santa Cruz Operation, Inc.



## AV A-16

## Adding Ethernet and IP Addresses



©The Santa Cruz Operation, Inc.



---

### A.4.3.3 Configuring addresses

---

#### AV A-15: Configuring Ethernet and IP Addresses

Use this slide to illustrate what **Capture ⇒ Address...** looks like *before* adding the new address configurations.

#### AV A-16: Configuring Ethernet and IP Addresses

Use this slide to illustrate what **Capture ⇒ Address...** looks like *while* adding the new address configurations.

#### AV A-17: Configuring Ethernet and IP Addresses

Use this slide to illustrate what **Capture ⇒ Address...** looks like *after* adding the new address configurations.

Initially, Network Monitor doesn't have any knowledge of the addresses in use other than those used by the machine on which Network Monitor is running. To make Network Monitor easier to use, teach Network Monitor about the Ethernet and IP addresses you will be analyzing.

Do this by selecting **Capture ⇒ Addresses...** on the menu bar.

Slide AV A-15 on page A-40 illustrates the addresses Network Monitor knows about before we add new address configurations.

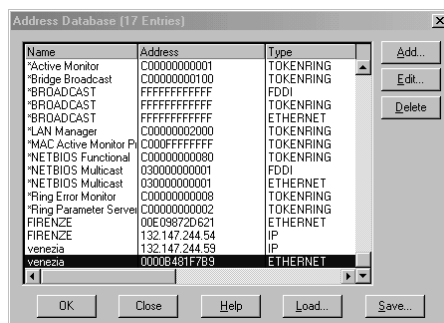
To add a new address configuration:

- Step 1. Click on the **Add...** button. Slide AV A-16 on page A-40 illustrates what you'll see.
- Step 2. Select which type of address (eg. ETHERNET, IP) you are configuring.
- Step 3. Type in the address and a name.
- Step 4. Click the **OK** button.
- Step 5. Click the **OK** button.

Slide AV A-17 on page A-42 illustrates Network Monitor after the addition of two new addresses (ie. the last two entries on the bottom of the window).

## AV A-17

## Adding Ethernet and IP Addresses

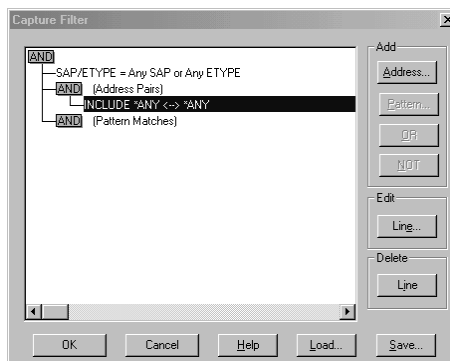


©The Santa Cruz Operation, Inc.



## AV A-18

## Filtering Capture Addresses



©The Santa Cruz Operation, Inc.



### A.4.3.4 Filtering addresses

---

#### AV A-18: Filtering Capture Addresses

Use this slide to illustrate what **Capture** ⇒ **Filter...** looks like *before* adding the capture address filter.

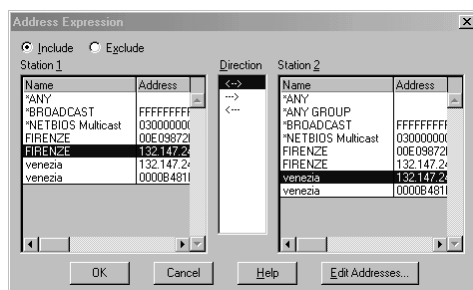
Capturing all the traffic on the network is generally impractical due to the abundance of data that would be logged to the hard drive. Now that you've configured into Network Monitor the addresses of the hosts that you will be analyzing, configure Network Monitor to filter out all traffic except that which matches the addresses you specify.

To inform Network Monitor which addresses' you want to capture, select **Capture** ⇒ **Filter...** on the menu.

Slide AV A-18 on page A-42 illustrates the capture address filter Network Monitor uses before we provide our specification of which addresses' traffic we want to analyze.

## AV A-19

## Filtering Capture Addresses



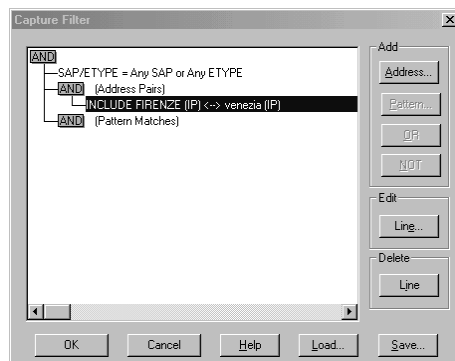
©The Santa Cruz Operation, Inc.



Instructor Guide

## AV A-20

## Filtering Capture Addresses



©The Santa Cruz Operation, Inc.



**AV A-19: Filtering Capture Addresses**

Use this slide to illustrate what **Capture** ⇒ **Filter...** looks like *while* adding the capture address filter.

**AV A-20: Filtering Capture Addresses**

Use this slide to illustrate what **Capture** ⇒ **Filter...** looks like *after* adding the capture address filter.

To specify the capture filter addresses:

- Step 1. Highlight **INCLUDE \*ANY <-->\*AN** .
- Step 2. Click on the **Line** button in the box labeled “Edit”. Slide AV A-19 on page A-44 illustrates what you’ll see:
- The two outer-most columns in this window correspond to the address pair that you want to capture.
  - The inner column allows you to specify whether the traffic to capture is one direction only or bi-directional.
- Step 3. In slide AV A-19 on page A-44 we’ve selected bi-directional traffic between the hosts *firenzia* and *venezia* (based on their IP addresses).
- Step 4. Click the **OK** button.
- Step 5. Click the **OK** button.

Slide AV A-20 on page A-44 illustrates Network Monitor after the addition of the capture address filter.

## AV A-21

## Generating Network Traffic with FTP

```

C:\WINDOWS\Desktop>ftp venezia,uss.sco.com
Connected to venezia,uss.sco.com.
220 venezia,uss.sco.com FTP server (wu-2.4.2-academ-15) ready.
User (132.147.244.59:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> dir /stand
220 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 17598
drwxr-xr-x 2 root sys 288 Dec 21 17:49 .
drwxr-xr-x 48 root sys 3072 Feb 9 10:16 ..
-rw-r--r-- 1 root sys 1036 Apr 7 1998 bfs.blm
-rw-r--r-- 1 root sys 151 Dec 20 03:14 boot
-rw-r--r-- 1 root sys 1211 Apr 7 1998 bootmsgs
-rw-r--r-- 1 root sys 9980 Apr 7 1998 dcmp.blm
-rw-r--r-- 1 root sys 1829 Mar 5 1999 hd.blm
-rw-r--r-- 1 root sys 3486 Apr 7 1998 help.txt
-rw-r--r-- 1 root sys 620 Feb 9 09:59 license
-rw-r--r-- 1 root sys 25359 Apr 7 1998 logo.img
-rw-r--r-- 1 root sys 5608 Mar 5 1999 platform.blm
-rw-r--r-- 1 root sys 13450 Feb 9 09:59 resmgr
-rw-r--r-- 1 root root 13450 Feb 9 09:41 resmgr.sav
-rw-r--r-- 1 root sys 891 Apr 7 1998 smallfs.blm
-rw-r--r-- 1 root sys 10848 Mar 5 1999 stage3.blm
-rwxr-xr-x 1 root root 2994836 Dec 21 17:49 unix
-rwxr-xr-x 1 root sys 2933688 Dec 21 17:37 unix.good
-rwxr-xr-x 1 root sys 2985916 Dec 21 17:46 unix.old
226 Transfer complete.
ftp: 1222 bytes received in 0.17Seconds 7.19Kbytes/sec.
ftp> bye
221 Goodbye.

C:\WINDOWS\Desktop>

```



©The Santa Cruz Operation, Inc.





### A.4.3.5 Beginning the capture

---

To begin capturing network traffic, select **Capture** ⇒ **Start** from the menu.

### A.4.3.6 Generating network traffic

---

#### AV A-21: Generating Network Traffic with FTP

Use this slide to show the students the FTP session whose data we're tracking.

Now that we have Network Monitor capturing data, we generate some data by running the FTP command. The actual FTP session that we're using to generate network traffic for this lesson is displayed in slide AV A-21 on page A-46.

## AV A-22

**Network Monitor Layout**

The screenshot displays the Network Monitor interface with the following components:

- Frame panel:** A table listing network frames. The selected frame (Frame 8) is highlighted.
- Details panel:** A pane showing the hierarchical structure of the selected frame, including Ethernet II, Internet Protocol, and FTP.
- Hex dump panel:** A pane showing the raw hexadecimal data of the selected frame, with corresponding ASCII text on the right.

Labels with arrows on the left side of the interface identify these panels:

- Frame panel
- Details panel
- Hex dump panel

The Tarantella logo is visible in the bottom left corner, and the SCO logo is in the bottom right corner. The text "©The Santa Cruz Operation, Inc." is centered at the bottom.

### A.4.3.7 Stopping the capture and viewing the results

---



#### AV A-22: Network Monitor Layout

Use this slide to illustrate the three panels present when displaying a capture in Network Monitor.

To stop capturing network traffic and view the results, select **Capture ⇒ Stop and View** from the menu.

SlideAV A-22 on page A-48 shows Network Monitor as it displays the data captured during the FTP session displayed in slideAV A-21 on page A-46.

The window in which Network Monitor displays the captured data is divided into three panels:

- Frame
- Details
- Hex Dump

**Frame** Network displays one line per packet of data captured. Each line contains the following information.

- **Frame** lists the frame number.
- **Time** shows the time stamp of the frame.
- **Src MAC Addr** shows the MAC (ETHERNET in our case) address of the host where the frame originated.
- **Dst MAC Addr** shows the MAC (ETHERNET in our case) address of the host to which the frame is addressed.
- **Protocol** lists the type of network protocol used in the frame.
- **Description** gives a description of the contents of the frame. For more information on the packet, consult the Details panel.
- **Src Other Addr** shows the address (IP address in our case) of the host where the frame originated.
- **Dst Other Addr** shows the address (IP address in our case) of the host to which the frame is addressed.
- **Type Other Addr** specifies the type of address displayed in the **Src Other Addr** and **Dst Other Addr** columns.

Slide AV A-22 on page A-48 is not wide enough to display the **Src Other Add** , **Dst Other Add** , and **Type Other Addr** columns.

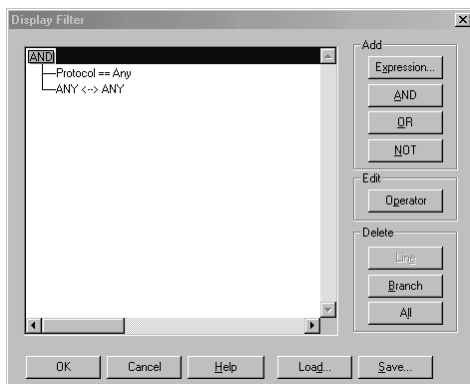
**Details** Network Monitor displays details about the packet selected in the Frame panel. This panel is discussed in more detail in Section A.4.3.10 on page A-59.

**Hex dump** Network Monitor displays a hexadecimal dump of the portion of the packet selected in the Details panel.

“Frame”, “Details”, and “Hex Dump” are not the names used by Microsoft.

## AV A-23

## Filtering Frames Displayed Based on Protocol Type

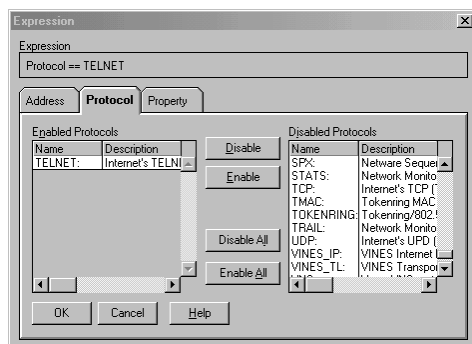


©The Santa Cruz Operation, Inc.



## AV A-24

## Filtering Frames Displayed Based on Protocol Type



©The Santa Cruz Operation, Inc.



---

## A.4.3.8 Filtering protocols

---

### AV A-23: Filtering Frames Displayed Based on Protocol Type

Use this slide to show the window displayed by Network monitor *before* setting a protocol filter.

### AV A-24: Filtering Frames Displayed Based on Protocol Type

Use this slide to show the window displayed by Network monitor *while* setting a protocol filter.

### AV A-25: Filtering Frames Displayed Based on Protocol Type

Use this slide to show the window displayed by Network monitor *after* setting a protocol filter.

In Section A.4.3.4 on page A-43, we set up a filter that captured particular addresses during the *capture*. When *displaying* the captured data, you can filter further based on addresses. Additionally, you can filter based on *protocol*.

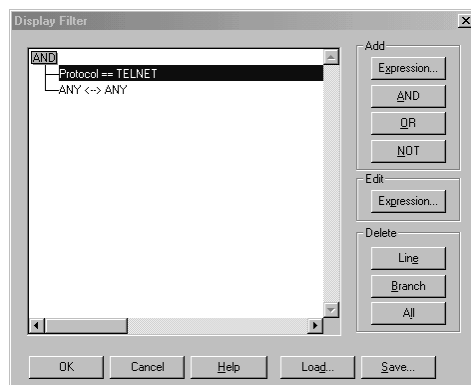
To filter based on protocol:

- Step 1.       Select **Display** ⇒ **Filter...** from the menu.  
  
Slide Section AV A-23 on page A-52 shows the window displayed by Network Monitor
- Step 2.       Select the line which reads **Protocol == Any** then click the **Operator** button in the “Edit” box.  
  
Slide Section AV A-24 on page A-52 shows the window in which Network Monitor allows you select which protocols are displayed.
- Step 3.       Click the **Disable All** button.
- Step 4.       Next highlight “FTP” in the “Disabled Protocols” column.
- Step 5.       Click the **Enable** button. Alternatively, you can double click “FTP” to move it to the “Enabled Protocols” column.
- Step 6.       Click the **OK** button.
- Step 7.       Click the next **OK** button.

Slide Section AV A-25 on page A-54 shows the window displayed by Network Monitor after setting up the protocol filter.

AV A-25

### Filtering Frames Displayed Based on Protocol Type



©The Santa Cruz Operation, Inc.





### **A.4.3.9 Analyzing the captured data**

---

In this section, we analyze the data captured in the FTP session.

**Exercise: Analyzing the FTP Session**

---

The instructor will provide you with a file called *ftp.cap*. This file is the captured data from the FTP session displayed in slideSection AV A-21 on page A-46.

Open this file by selecting **File ⇒ Open...** from the menu.

Set up a display filter which filters out everything but FTP protocol frames. Section A.4.3.8 on page A-53 outlines the procedure for doing so.

Double click on frame #4.

Instructor Guide

Explain to the students how to step through the frames in Network Monitor.

Step the students through the following table.

Point out:

- The commands from the client appear in bold in the table.
- FTP commands are sent in blocks (as opposed to telnet which sends a character at a time).
- FTP sends passwords in cleartext (the password for root in this example is "ClearText").
- Each line in the table indicates the direction in which the frame is travelling.

**Table 4: Analysis of the FTP Session**

Frame	Direction	Description
4	server ⇨ client	220 venezia.uss.sco.com FTP server (wu-2.4.2-academ-15) ready.
6	client ⇨ server	<b>USER root (ftp client authenticating as “root”)</b>
8	server ⇨ client	331 Password required for root.
10	client ⇨ server	<b>PASS ClearText (client supplies root password)</b>
12	server ⇨ client	230 User root logged in.
14	client ⇨ server	<b>PORT 132.147.244,54,4,33 (client sets port for data)</b>
16	server ⇨ client	200 PORT command successful.
17	client ⇨ server	<b>LIST /stand (client requests directory listing)</b>
22	server ⇨ client	150 Opening ASCII mode data connection for /bin/l
24	server ⇨ client	Directory listing
25	server ⇨ client	226 Transfer complete.
31	client ⇨ server	<b>QUIT (client quits)</b>
33	server ⇨ client	221 Goodbye.

## AV A-26

## The Application Data

```
ΦFRAME: Base frame properties
ΦETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
ΦIP: ID = 0x3C13; Proto = TCP; Len: 56
ΦTCP: .AP... len: 16, seq: 11343672-11343687, ack: 59878583, win: 8663, src: 1056 dst: 21 (FTP)
-FTP: Req. from Port 1056, 'PASS ClearText'
FTP: FTP Command = PASS
FTP: FTP Data: Number of data bytes remaining = 12 (0x000C)
```



©The Santa Cruz Operation, Inc.



### A.4.3.10 Encapsulation information

---



#### AV A-26: The Application Data

Use this slide to show Network Monitor displaying the application data (FTP in our example).

Section A.1.8 on page A-19 discussed the concept of encapsulation. The Details panel in Network Monitor allows you to look at each level of the encapsulation (ie. the application data, the TCP segment, the IP datagram, and the Ethernet frame). To look at a particular level, click the its “+” icon.

#### The application data

---

The Network Monitor displays information about network protocol specific packets. In slide AV A-26 on page A-58, Network Monitor is displaying the **PASS** command issued by the client to the server.

## AV A-27

## The TCP Segment

```

ΦFRAME: Base frame properties
ΦETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
ΦIP: ID = 0x3C13; Proto = TCP; Len: 56
 TCP: .AP..., len: 16, seq: 11343672-11343687, ack: 59878583, win: 8663, src: 1056 dst: 21 (RTP)
 TCP: Source Port = 0x0420
 TCP: Destination Port = FTP [control]
 TCP: Sequence Number = 11343672 (0xAD1738)
 TCP: Acknowledgement Number = 59878583 (0x391ACB7)
 TCP: Data Offset = 20 (0x14)
 TCP: Reserved = 0 (0x0000)
 TCP: Flags = 0x18 : .AP...
 TCP: ..0.... = No urgent data
 TCP: ...1.... = Acknowledgement field significant
 TCP: 1... = Push function
 TCP: 0.. = No Reset
 TCP: 0. = No Synchronize
 TCP: 0 = No Fin
 TCP: Window = 8663 (0x21D7)
 TCP: Checksum = 0x6456
 TCP: Urgent Pointer = 0 (0x0)
 TCP: Data: Number of data bytes remaining = 16 (0x0010)
ΦFTP: Req. from Port 1056, 'PASS ClearText'

```



©The Santa Cruz Operation, Inc.



## The TCP segment

---

### AV A-27: The TCP Segment

Use this slide to show Network Monitor displaying a TCP segment.

The Network Monitor displays information about a TCP segment in slide AV A-27 on page A-60. Included in this information is the following information:

- Source and destination port numbers
- Sequence and acknowledgement numbers
- Checksum
- Flags
  - ⦿ URG — The urgent pointer is valid
  - ⦿ ACK — The acknowledgement number is valid
  - ⦿ PSH — Instructs receiver to push all the data it has to the receiving process
  - ⦿ RST — Reset the connection
  - ⦿ SYN — Synchronize sequence numbers for initial connection
  - ⦿ FIN — The sender is finished sending data

See Section A.1.5 on page A-15 and Section A.1.8 on page A-19 for more information.

## AV A-28

## The IP Datagram

```

❖FRAME: Base frame properties
❖ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
❖IP: ID = 0x3C13; Proto = TCP; Len: 56
 IP: Version = 4 (0x4)
 IP: Header Length = 20 (0x14)
❖IP: Service Type = 0 (0x0)
 IP: Total Length = 56 (0x38)
 IP: Identification = 15379 (0x3C13)
❖IP: Flags Summary = 2 (0x2)
 IP: Fragment Offset = 0 (0x0) bytes
 IP: Time to Live = 128 (0x80)
 IP: Protocol = TCP - Transmission Control
 IP: Checksum = 0xCD13
 IP: Source Address = 132.147.244.54
 IP: Destination Address = 132.147.244.59
 IP: Data: Number of data bytes remaining = 36 (0x0024)
❖TCP: .AP..., len: 16, seq: 11343672-11343687, ack: 59878583, win: 8663, src: 1056 dst: 21 (FTP)
❖FTP: Req. from Port 1056, 'PASS ClearText'

```



©The Santa Cruz Operation, Inc.



## AV A-29

## The Ethernet Frame

```

❖FRAME: Base frame properties
❖ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
❖ETHERNET: Destination address : 0000B481F7B9
❖ETHERNET: Source address : 00E09872D621
 ETHERNET: Frame Length : 70 (0x0046)
 ETHERNET: Ethernet Type : 0x0800 (IP: DOD Internet Protocol)
 ETHERNET: Ethernet Data: Number of data bytes remaining = 56 (0x0038)
❖IP: ID = 0x3C13; Proto = TCP; Len: 56
❖TCP: .AP..., len: 16, seq: 11343672-11343687, ack: 59878583, win: 8663, src: 1056 dst: 21 (FTP)
❖FTP: Req. from Port 1056, 'PASS ClearText'

```



©The Santa Cruz Operation, Inc.





## The IP datagram

---

### **AV A-28: The IP Datagram**

Use this slide to show Network Monitor displaying an IP datagram.

The Network Monitor displays information about an IP datagram in slide AV A-28 on page A-62. Included in this information is the following information:

- The IP protocol version (IPv4 in our example)
- The Time To Live value
- The IP protocol type (TCP in our example)
- The checksum
- The source and destination IP addresses

See Section A.1.3 on page A-14 and Section A.1.5 on page A-15 for information.

## The Ethernet frame

---

### **AV A-29: The Ethernet Frame**

Use this slide to show Network Monitor displaying an Ethernet frame.

The Network Monitor displays information about an Ethernet frame in slide AV A-29 on page A-62. Included in this information is the following information:

- The source and destination Ethernet addresses (see Section A.1.3 on page A-14)

### **The Network Monitor Frame**

The “Frame” information in the Details panel contains information that Network Monitor needs (eg. time stamp, frame length, etc.). This data wasn’t actually transferred across the network.



## **A.5 Lesson Summary**

---

---

This lesson described the networking basics that Tarantella administrators need to know. Concepts discussed included media types, interfaces, IP addresses, IP address classes, IP address types, IP datagrams, TCP, UDP, sequence numbers, acknowledgement numbers, encapsulation, port numbers, routing, subnetting, subnet masks, DNS, and various network protocols. Additionally, this lesson discussed the various networking utilities that Tarantella administrators use. The chapter closed with a discussion on how to use tools such as telnet and network sniffers to troubleshoot networking problems.



---

## A.6 Review questions

---

1. Name three network media types.

■ The three network media types discussed by this lesson were Ethernet, Token Ring, and FDDI.

2. Name three types of IP addresses.

■ The three types of IP addresses are unicast, broadcast, and multicast.

3. What does TTL stand for? What is TTL?

■ TTL stands for TimeTo Live. TTL is a field set in IP packets that specifies the maximum number of hops that the packet should live. Each router that an IP packet travels through is supposed to decrement the TTL by one.

4. What do TCP and UDP stand for?

■ TCP stands for "Transmission Control Protocol." UDP stands for "User Datagram Protocol."

5. What are the minimum and maximum port numbers?

■ The minimum and maximum port numbers are 0 and 65535, respectively.

6. What are the port number ranges for well known and registered port numbers?

Well known ports are in the range of 0 - 1023. Registered ports are in the range 1024 - 49151.

7. Where on the web can you look up the official port numbers for well known and registered ports?

The official port numbers for well known and registered ports can be looked up at <http://www.iana.org> and <http://www.isi.edu/in-notes/iana/assignments/port-numbers>.

8. What utility can Tarantella administrators use to see what interfaces are configured on a server?

The ifconfig command can be used to determine what interfaces are configured on a server.

9. What command can Tarantella administrators use to create IP address aliases?

The ifconfig command can be used to create IP address aliases.

10. What command could a Tarantella administrator use to *easily* figure out which hop in a route was down?

The traceroute command can be used to determine which hop in a route is down.

11. What does the **arp** command do?

The **arp** command reports the Ethernet / IP address mappings known to the machine on which the command is run.

---

## A.7 Lab: Gathering Network Information

---

In this lab, you will gather information about your network.

### A.7.1 Overview

---

Your tasks in this lab are as follows:

- List all the network addresses of the interfaces on your computer.
- List all the Ethernet address  $\Rightarrow$  IP address mappings that your computer knows about.
- Print the routing table.
- List the services available on your computer.

### A.7.2 Procedure

---

Step 1. Log in as root on the Unix server.

Step 2. List the network addresses of the interfaces on your computer:

```
ifconfig -a
```

Alternatively:

```
netstat -i
```

On Windows machines you can find this same information using the following command:

```
C:\> ipconfig /all
```

 Alternatively, you can run **winipcfg** on Windows 95/98.

Step 3. List all the Ethernet address  $\Rightarrow$  IP address mappings that your computer knows about:

```
arp -a
```

Step 4.        Print the routing table:

```
netstat -rn
```

 Challenge the students to explain the routing table.

Step 5.        List the services available on your computer:

```
more /etc/inetd.conf
```

```
netstat -a
```



## A.8 Lab: Hypothetical Situations

---

---

In this lab, you will answer questions about a variety of hypothetical situations. While you may not encounter these exact questions in real life, you will face similar questions.

### A.8.1 Situation #1: Checksum Errors

---

You're receiving error messages that report checksum errors on the NIC at Ethernet address 00:00:b4:81:f7:b9. Furthermore, the error messages report the IP address of the machine.

While the IP address has helped you to track down the problematic machine, you remember that the machine has two NICs. How can you determine which NIC to repair/replace? (Hint: The NICs are from two different manufacturers.)

### A.8.2 Situation #2: 100MB File Transfer

---

You are given five minutes to transfer a 100MB file through a T1 connection. You calmly reply that this is an impossible task. Why do you say so? Approximately how long would it take to transfer the file?

### A.8.3 Situation #3: Webserver Configuration Exploration

You want to peek into another company's network infrastructure to see how they've set up their web server.

What web servers do the following web sites use? How many IP address do their web sites use?

**Table 5: Web Server Information**

Web Site	Web Server	Web Site IP Addresses
www.sco.com		
www.microsoft.com		
www.apache.org		
www.sun.com		
www.news.com		

The table has been left to the students to fill out. The information in the table above is subject to change without notice as the above companies rearrange their web sites to suit their own needs.

The **nslookup** command reports that www.sun.com uses only one IP address. What do you suspect is going on behind the scenes?

### A.8.4 Situation #4: Maximum Port Number

You are having a disagreement with a colleague who claims that port numbers can be as large as you want.

You know that your colleague is wrong. You know that the maximum port number is 65535. You would like to prove that you are correct, but you've misplaced your Stevens book (see Section A.1 on page A-9) and you don't recall where to look this up on the Internet.

You do, however, have Network Monitor. How can you show your colleague in Network Monitor that the maximum port number is 65535?

---

## A.9 Lab: Network Traffic Analysis

---

In this lab, you will analyze information about the traffic on your network.

### A.9.1 Overview

---

Your tasks in this lab are as follows:

- Capture the traffic resulting from a telnet between two machines
- Determine whether Tarantella sends cleartext passwords when users log in.
- Go to a web site that uses cookies (eg. [www.yahoo.com](http://www.yahoo.com)). Use Network Monitor to determine how cookies are handled by the client and the server.
- Go to [www.sco.com/about](http://www.sco.com/about) in your browser. Why does the URL change to [www.sco.com/about/](http://www.sco.com/about/) in the browser? Is it the web browser or the web server that is changing the URL? How can you use Network Monitor to tell?

### Part I: Telnet Traffic

---

To capture the data resulting from a telnet session, follow the directions in Section A.4.3 on page A-37.

Alternatively, the instructor will provide a file called *telnet.cap*. Open this file by selecting **File** ⇒ **Open...** from the menu.

Set a display filter which restricts Network Monitor to only showing TELNET protocol by selecting **Displa** ⇒ **Filter...** from the menu.

Display the captured information by double clicking the first frame (frame #4 in *telnet.cap*).

Click on the “+” on the TELNET line in the Details panel (see AV A-22 on page A-48).

**Table 6: Analysis of the Telnet Session**

Frame	Direction	Description
4-14	client ⇌ server server ⇌ client	Client and server communicate back and forth to negotiate exactly which features each side supports.
15	client ⇌ server	Client tells server that the terminal type is vt100.
16-18	client ⇌ server server ⇌ client	Client and server continue negotiating which features each side supports.
19	server ⇌ client	SCO UnixWare 7.1.0 (venezia) (pts/6)
20-23	client ⇌ server server ⇌ client	Client and server continue negotiating which features each side supports (eg. local echo).
25	server ⇌ client	login:
27	client ⇌ server	<b>r (client sends first character of the login name)</b>
28	server ⇌ client	<b>r (server echos back first character of the login name)</b>
30	client ⇌ server	<b>o</b>
31	server ⇌ client	o
33	client ⇌ server	<b>o</b>
34	server ⇌ client	o
35	client ⇌ server	<b>t</b>
36	server ⇌ client	t
40	server ⇌ client	Password:
43	client ⇌ server	<b>C (client sends first character of the password)</b>
45	client ⇌ server	<b>I (client sends second character of the password--no echo from server)</b>
47	client ⇌ server	<b>e</b>
49	client ⇌ server	<b>a</b>
51	client ⇌ server	<b>r</b>
53	client ⇌ server	<b>T</b>
55	client ⇌ server	<b>e</b>
57	client ⇌ server	<b>x</b>

**Table 6: Analysis of the Telnet Session**

Frame	Direction	Description
59	client ⇒ server	<b>t</b>
64	server ⇒ client	Copyright information
65	server ⇒ client	Last login information, registration notice, mail notification, and shell prompt (ie. "#").
68	client ⇒ server	<b>e (client sends first character of the "exit" command)</b>
69	server ⇒ client	<b>e (server echos first character of the command)</b>
71	client ⇒ server	<b>x</b>
72	server ⇒ client	x
74	client ⇒ server	<b>i</b>
75	server ⇒ client	i
76	client ⇒ server	<b>t</b>
77	server ⇒ client	t

Point out to students that **telnet** sends cleartext passwords.

Point out that **telnet**, unlike **ftp**, does not block its data. Rather, characters typed are sent one character at a time.

Instructor Guide

## Part II: Tarantella Passwords

Step 1. Start a Network Monitor session in which you capture traffic between the web browser machine and the web server machine. On request, the instructor will provide you with a file called *http.cap* which is a capture of the information gathered in the following steps.

Step 2. Start Tarantella by going to the following URL:

<http://server/tarantella>

where *server* is the name of your tarantella server.

Step 3. When the Tarantella *completes* drawing the login screen, ping the web server *once* from the client.

NOTE: In some versions of Unix (eg. OpenServer) you specify the number of pings with the **-c** option to **ping**. In other versions of Unix (eg. UnixWare) you specify the number of pings as the last argument to the **ping** command. In DOS you specify the number of pings with the **-n** option to **ping**.

Step 4. Enter the Tarantella user name.

Step 5. Enter the user's password.

Step 6. Click on the **OK** button.

Step 7. When the Tarantella login completes, stop the capture in Network Monitor by selecting **Capture** ⇒ **Stop and View** from the menu.

**Table 7: Analysis of a Tarantella Login Session**

Frame	Direction	Description
1-115	client ⇒ server server ⇒ client	These packets correspond to Tarantella drawing the login screen.
116	client ⇒ server	Client pings the server.
117	server ⇒ client	Server replies to client's ping.
118	client ⇒ server	Client sends user name and <i>encoded</i> password to server.
120	server ⇒ client	Server begins passing client information from the Tarantella datastore — starting with the object for the user called "root".

By "encoded" we mean that Tarantella *obfuscates* the password as opposed to *encrypting* the password.

As you can see, Tarantella encodes passwords even if the Tarantella Security Pack (TSP) isn't installed.

---

## Part III: Cookies

---

- Step 1. Start a Network Monitor session which captures data between your machine and [www.yahoo.com](http://www.yahoo.com). Alternately, the instructor will provide you a file called *http\_yahoo.cap*.
- Step 2. Point your browser to [www.yahoo.com](http://www.yahoo.com).
- Step 3. When Yahoo completes drawing your screen, stop the capture in Network Monitor by selecting **Capture** ⇒ **Stop and View** from the menu.
- Step 4. The first HTTP packet from the client to the server will contain an http GET request. Examine the entire packet and you will find that the *client* is passing the server a cookie.

---

## Part IV: URL Modification

---

- Step 1. Start a Network Monitor session which captures data between your machine and [www.sco.com](http://www.sco.com). Alternately, the instructor will provide you a file called *http\_sco.cap*.
- Step 2. Point your browser to the following URL:
- <http://www.sco.com/about>
- Step 3. When SCO completes drawing your screen, stop the capture in Network Monitor by selecting **Capture** ⇒ **Stop and View** from the menu.
- Step 4. The first HTTP packet from the client to the server will contain an http GET request. Examine the GET and you will see that the client is requesting the URL shown in Step 2 above.
- Step 5. The first HTTP response from the server to the client is a **302 Found**. This indicates that the server has located the requested document. Further into that same HTTP packet, the server tells the client:

Location: <http://www.sco.com/about/>

In so doing, the server has informed the client that the proper way to refer to the document is with this URL rather than the URL in Step 2.

This URL modification is performed *by the server* to support relative URLs.





---

## A.10 Answers to Exercise and Review Questions

---

This section contains the answers to exercises, review questions, and labs presented in this lesson.

### Exercise answers

---

Please consult your instructor if you have any questions about the exercises in this lesson.

### Answer to Lab Situation #1

---

Since you know that the two NICs are from different manufacturers, all you have to do is look up the Ethernet address 00:00:b4:81:f7:b9 at IEEE:

<http://standards.ieee.org/regauth/oui/out.txt>

### Answer to Lab Situation #2

---

NOTE: Pay close attention throughout this answer whether we're talking about kilobits (Kb), kilobytes (KB), megabits (Mb), or megabytes (MB).

It is impossible to transfer a 100MB file through a T1 in under five minutes. Click on the "The Speed of..." hypertext link at [www.whatis.com](http://www.whatis.com) and you will find that a T1 is 1.544Mb per second.

To make the math a little easier, we'll round that to 1.6Mb per second.

Divide 1.6Mb by 8 to convert the value to megabytes and you find that a T1's speed is approximately .2MB per second.

100MB divided by .2MB per second is approximately 500 seconds.

500 seconds is approximately 8 minutes.

Since this is more than the five minutes allotted, we can already safely say that the task was impossible. Factor in the overhead of TCP, IP, and Ethernet headers and you can clearly see that the task is, indeed, impossible.

## Answer to Lab Situation #3

---

Finding out which webserver a web site is running is easy. Simply telnet to the httpd port on the server:

```
telnet www.sco.com 80
```

and press  a few times. The resulting message from the httpd server will identify the web server. For sites that are a bit more reluctant to reveal this information (eg. www.apache.org), enter the following instead:

```
HEAD / HTTP/1.0
```





To find out how many IP addresses a particular web site uses, perform an **nslookup** on the web site name. For large web sites, you will see one of two things:

- The **nslookup** reports multiple addresses. In this configuration, the web site handles the heavy load by redirecting http requests to one out of many machines. The one name is redirected to many different machines — each with its own IP address. DNS is responsible for the redirection in this case.
- The **nslookup** reports a single address. For an example of this, see www.sun.com. While this appears to indicate that Sun Micro System's web site is handled by a single machine, the truth is that the web site is multiple machines. In this case, it is not DNS doing the redirection. Rather, Sun has a piece of hardware at the IP address reported by **nslookup** which does the redirection.

## Answer to Lab Situation #4

---

Any TCP packet captured by the Network Monitor will prove that 65535 is the upper limit on port numbers. Open a capture file by selecting **File** ⇒ **Open...** from the menu. The instructor will provide a capture file called *telnet.cap* upon request.

In the Detail panel (See AV A-22 on page A-48), click on the plus icon for TCP.

Click on the **TCP: Destination Port** line. Network Monitor informs you that the port is telnet. Notice how many bytes are highlighted in the Hexdump panel (See AV A-22 on page A-48). Two bytes are highlighted, meaning that the port number is two bytes (or sixteen bits).  $2^{16}=65536$ , therefore these two bytes can hold any number in the range 0-65535.

## Review Question Answers

---

This section contains the answers to the review questions on page A-67.

1. The three network media types discussed by this lesson were Ethernet, Token Ring, and FDDI.
2. The three types of IP addresses are unicast, broadcast, and multicast.
3. TTL stands for Time To Live. TTL is a field set in IP packets that specifies the maximum number of hops that the packet should live. Each router that an IP packet travels through is supposed to decrement the TTL by one.
4. TCP stands for “Transmission Control Protocol.” UDP stands for “User Datagram Protocol.”
5. The minimum and maximum port numbers are 0 and 65535, respectively.
6. Well known ports are in the range of 0 - 1023. Registered ports are in the range 1024 - 49151.
7. The official port numbers for well known and registered ports can be looked up at <http://www.iana.org> and <http://www.isi.edu/in-notes/iana/assignments/port-numbers>.
8. The ifconfig command can be used to determine what interfaces are configured on a server.
9. The ifconfig command can be used to create IP address aliases.
10. The traceroute command can be used to determine which hop in a route is down.
11. The **arp** command reports the Ethernet / IP address mappings known to the machine on which the command is run.

