Course Assignments by Week- CIS 125D

During week one, you must also post your SIA (Student Introductory Assignment) during one of the first three days of class to avoid being dropped. If you do not post your SIA by 9 PM on Wednesday of week 1, you may be dropped in week 1 by your instructor.

The SIA is the Student Introductory Assignment where you post something about yourself in Angel, in the Weekly Lessons -> Week 01 folder -> SIA Forum. I already posted something about myself there! Create a new post and tell us something about yourself.

**Homework** due dates: Please see the syllabus for details!

**Reading** consists of studying, taking notes, and performing all hands-on exercises found in each chapter assigned. Homework consists of the Lab Assignments (found at the end of each chapter in the book).

You will find Flash and PowerPoint presentations for each chapter in their respective folders. A Flash presentation is a voice over PowerPoint presentation that you can view using a Web browser. There is material contained in the Flash presentations that will be on your quizzes and exam. Flash presentations will be posted on Monday morning at the start of each week this term.

The **Final Exam** is made up of 85 multiple choice questions. You will take the final exam online after logging into Angel. The exam is open book, open notes, but it is timed at approx. 1 minute per question allocated. **Final Exam** instructions will be posted approximately one week before the exam and your instructor will answer any questions you have at that time. The final exam link will become visible under the Lessons link at the date and time you are to take the exam.

How to submit homework for grading:
1. Place all of your folders and files in a compressed (zipped) folder (one folder per week's worth of homework). You will only submit folders as part of your week 1 homework. Generally, you will submit Access database files as your homework. Do not put each file in a zipped folder. If you are only submitting one file, you do not need to zip it before uploading it into its drop box.
2. Name the zipped folder with your course number, your name and week number. For example, week one’s filename for me would be “CIS 125D, Week 1 – John Blackwood”.
3. Upload your zipped folder into that specific homework assignment's drop box. Drop boxes are located in the Homework section of each week's folder.

Week By Week Activities:

**Week 1: Jan 07 - Jan 13**

- SIA due by Wednesday at midnight during week one!
  - If you don’t complete your SIA on time you may be dropped from the course in week 1.
- Read and do hands-on work for Microsoft Office 2010 and Windows 7 chapter
  - This chapter does not have a number! It begins on p. OFF 1 of the text
- View the flash presentation for this chapter
- Do the Angel Quiz for the Microsoft Office 2010 and Windows 7 Chapter
- Homework due: Labs 2-3, starting on p. OFF 53 of the text
- Homework due: Case and Places Projects 1 and 3, starting on p. OFF 54
Week 2: Jan 14 – Jan 20

- Read and do hands-on work for Chapter 1: Databases and Database Objects: An Introduction
  - This chapter begins on p. AC 1 of the text
- View the flash presentation for Chapter 1
- Do the Angel quiz for Chapter 1
- Homework due for Chapter 1: Lab 2, starting on p. AC 68 of the text
- Homework due for Chapter 1: Case and Places Project 3, starting on p. AC 72

Week 3: Jan 21 – Jan 27

- Read and do hands-on work for Chapter 2: Querying a Database
- View the flash presentation for Chapter 2
- Do the Angel Quiz for Chapter 2
- Homework due for Chapter 2: Lab 3, starting on p. AC 134 of the text
- Homework due for Chapter 2: Case and Places Project 3, starting on p. AC 136 of the text

Week 4: Jan 28 – Feb 03

- Read and do hands-on work for Chapter 3: Maintaining a Database
- View the flash presentation for Chapter 3
- Do the Angel Quiz for Chapter 3
- Homework due for Chapter 3: Lab 2, starting on p. AC 202 of the text
- Homework due for Chapter 3: Case and Places Project 2, starting on p. AC 206 of the text

Week 5: Feb 04 - Feb 10

- Read and do hands-on work for Chapter 4: Creating Reports and Forms
- View the flash presentation for Chapter 4
- Do the Angel Quiz for Chapter 4
- Homework due for Chapter 4: Lab 2, starting on p. AC 268 of the text
- Homework due for Chapter 4: Case and Places Project 2, starting on p. AC 272 of the text

Week 6: Feb 11 - Feb 17

- Read and do hands-on work for Chapter 5: Multitable Forms
- View the flash presentation for Chapter 5
- Do the Angel Quiz for Chapter 5
- Homework due for Chapter 5: Lab 2, starting on p. AC 331 of the text
- Homework due for Chapter 5: Case and Places Project 2, starting on p. AC 334 of the text

Week 7: Feb 18 - Feb 24

- Read and do hands-on work for Chapter 6: Advanced Report Techniques
- View the flash presentation for Chapter 6
- Do the Angel Quiz for Chapter 6
- Homework due for Chapter 6: Lab 2, starting on p. AC 409 of the text
- Homework due for Chapter 6: Case and Places Project 2, starting on p. AC 415 of the text
Week 8: Feb 25 - Mar 03
  • Read and do hands-on work for Chapter 7: Using SQL
  • View the flash presentation for Chapter 7
  • Do the Angel Quiz for Chapter 7
  • Homework due for Chapter 7: Lab 2, starting on p. AC 461 of the text
  • Homework due for Chapter 7: Case and Places Project 2, starting on p. AC 463 of the text

Week 9: Mar 04 - Mar 10
  • Read and do hands-on work for Chapter 8: Advanced Form Techniques
  • View the flash presentation for Chapter 8
  • Do the Angel Quiz for Chapter 8
  • Homework due for Chapter 8: Lab 2, starting on p. AC 533 of the text
  • Homework due for Chapter 8: Case and Places Project 2, starting on p. AC 536 of the text

Week 10: Mar 11 - Mar 17
  • Read and do hands-on work for Chapter 11: Database Design
  • View the flash presentation for Chapter 11
  • Do the Angel Quiz for Chapter 11
  • Note: There are no student files for this week's homework. You will create new databases for each assignment!
  • Homework due for Chapter 11: Lab 1, starting on p. AC 717 of the text
  • Homework due for Chapter 11: Case and Places Project 2, starting on p. AC 719 of the text

Week 11: Mar 18 – Mar 22 (Finals Week)
  • Final Exam on Wednesday, March 20th
    • The final exam will be taken online
    • You can take the exam at your home and do not need to come to campus
    • The exam is open book, open notes, open Internet
    • Date / Time: Wednesday, March 20th, 2 PM – 11 PM exam available
    • Location: Online. You can take the exam anywhere you have Internet access

* Homework for Chapter 11 is due no later than Monday, March 18, 2013 by 1 PM. This is the Monday of finals week!
Syllabus

CIS 125D: Micro Apps - Databases

Winter 2013

Class Schedule:  Begin: January 7th          End: March 22nd
Class Hours:      Online (lecture via flash presentations)
Credits:          3 (2 lecture, 2 lab)
Instructor:       John Blackwood, MS (full-time CIS instructor)
Phone:            541-440-7686
Email:            john.blackwood@umpqua.edu

Course Description:
This course will serve as an introduction to the development and use of a modern database application using Microsoft Access 2010. Coursework will focus on proper design fundamentals used for database creation. Emphasis will be on using available database management system (DBMS) tools for data entry forms and report generation.

This syllabus is an initial plan for the term. Any changes and/or adjustments will be noted in Angel via an announcement and updated syllabus.

Course Outcomes:
Upon completion of this course the student should be able to:

- Use the basic features of a typical database management system (DBMS) application
- Understand and develop a simple, relational database
- Use database terminology as applied in modern business
- Use data entry tools and data manipulation techniques found in a typical DBMS
- Design and create reports with the report generator found in a typical DBMS
- Create queries to select and manipulate data subsets using Boolean logic and the query design grid

Course Prerequisite(s):
To take this course you should:

- Previously have completed CIS 120 and with a grade of C or better, or have prior instructor approval to take this course.
• To take any online class, you should already have proficiency in use of email, attachments, Windows operating systems, strong self study habits, a self-starter personal quality, and ability to take screenshots.
• Lastly, to take an online class at the UCC, you should be proficient in the use of Angel! Please arrange to complete an Angel orientation during week 1 of the term. Angel orientations are listed on the Angel logon Web page, on the right side of the window.

**Required Text:**

If you would prefer an electronic copy of the text, rather than a printed copy, you can purchase it directly from Cengage. Click [here](#) to open that link in your browser.

**Supplies:**
At least one (1) 32 GB USB portable hard disk drive and a computer with Microsoft Office 2010 with Access, Excel, PowerPoint, and Word applications installed.

**Hardware/Software:**
Students will use personally-owned computers in this online course. Your computer will need Internet access, a DVD player, and approximately 25% free hard disk space in which Microsoft Office 2010 will be installed (by you).

The UCC bookstore sells Microsoft Office 2010 for $17 to students enrolled half-time or more. If you do not have a copy of Office 2010, which includes Microsoft Access, please contact me immediately. You must have Access 2010 to take this course.

If you do not have access to a Windows 7 computer with Microsoft Office 2010 installed, you may be able to study and do your work at the UCC library. Please check the library's hours for availability. Please be aware that homework due dates and times are not adjusted when you are unable to locate a computer with the software you need to complete your work.

Important note: if you purchase Microsoft Office 2010 at a place other than the UCC bookstore, your copy most likely will NOT include Microsoft Access, which we will need to use in the course. Please talk to your instructor prior to purchasing any hardware or software for this class if you have any questions about what to purchase.

**Homework (AKA “Lab Work”):**
Students should plan to spend an average of 10-15 hours per week working in class lecture (delivered via flash presentations), assigned materials and reading. Homework, called "labs" in
this class, will be graded primarily on timely, complete, and accurate completion. Late assignments will be penalized up to 20% of that assignment’s grade. **Assignments turned in after graded work has been returned to the class will not be accepted for grading.**

Labs are due by 1 PM the Monday after they were assigned. For example, labs for Chapters 1 are assigned on Monday, January 7th. These labs are due on or before Monday, January 14th, before 1 PM.

You submit most of your homework by saving your work as Access database files, submitting them to your instructor by uploading them into their specified drop boxes. Please see the document link entitled **Course Assignments by Week** for details about how to submit your homework via a drop box.

One question that comes up early in week 1 is: "what should I turn in to get full credit for my work?" This is an excellent question! Open your book and let's make sure you know what to do to get off to a good start in this week's homework.

Lab 2 - Creating Folders for a Pet Supply Store, p. OFF 53 in your book, asks you to create a number of folders (directories) on your flash drive. You should place your folders in a zip folder and upload the zip folder to the week 1 drop box for that specific assignment when you are finished doing your work.

Lab 3 - Creating Access Databases in Appropriate Folders, p. OFF 54, starts off similar to what you did in Lab 2. However, here, you create Access database files and place them in specific folders. Just like you did in Lab 2, zip up all of your work and upload the zip folder to the week 1 drop box for that specific assignment when you are finished doing your work.

Please do not let the seemingly complexity of completing and submitting homework into drop boxes overwhelm you! If you make a 'good faith' effort to complete and submit your homework in week 1, you will earn full credit for that work. Then, when I grade that homework, I will provide you with specific feedback on how you might improve your work to earn full credit in upcoming weeks. In week 2, we will repeat this process, and in week 3, now fully 'trained' in what is expected of you, your homework will be graded on its merits.

Please contact me early in week 1 if you have any questions about how to complete and submit homework for grading. It is very important that you submit week 1 homework to get off to a good start in this class.

**Quizzes:**
There will be ten quizzes during the term. Quizzes are in the Assessments folder under Lessons and are also linked to each weekly folder. Quizzes must be taken weekly and have the same due date as homework. For example, quizzes for week 1 must be completed before 1 PM on Monday, January 14th, which is the same time your homework is to be completed and submitted for grading.
You can take each quiz two times and your highest score will be recorded in the gradebook.

**Grading & Points:**
Grades will be assigned based on the total points (pts) earned as follows; 90 to 100% = A, 80 to 89% = B, 70 to 79% = C, 60 to 69% = D, and less than 60% = F.
Points are distributed as follows:

<table>
<thead>
<tr>
<th>Description</th>
<th>Points</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 - Homework lab assignments (20 pts/each)</td>
<td>200</td>
<td>22.7%</td>
</tr>
<tr>
<td>11 - Homework project assignments (25 pts/each)</td>
<td>275</td>
<td>28.4%</td>
</tr>
<tr>
<td>10 - Quizzes (25 pts/each)</td>
<td>250</td>
<td>25.8%</td>
</tr>
<tr>
<td>1 - Final exam</td>
<td>225</td>
<td>25.8%</td>
</tr>
<tr>
<td><strong>Total possible points</strong></td>
<td><strong>970</strong></td>
<td><strong>100.0%</strong></td>
</tr>
</tbody>
</table>

**Course Outline:**
This outline is a plan for the term. It is subject to change should the need arise. It is your responsibility to note changes in the syllabus schedule as presented in lab or via Angel announcements during the term.
Please see the Homework section above for homework due dates.

The final exam will be comprehensive, will cover all (covered) chapters, and will be taken online as noted in the [Course Assignments by Week](#) page under Lessons in Angel.

Important note: All labs are due no later than Monday, March 18th, by 1 PM. This is the Monday of finals week.

**Lab Grading Rubric:**
Labs are to be completed in a professional manner. Business professionals must learn to write neatly and succinctly so that it can be understood by others. Some governing bodies require documentation for auditing purposes. Please review the lab rubric posted in Angel under Lessons for details about how your work will be graded.

**Use of Angel (online component):**
Angel will be used only to provide you access to class announcements, flash presentations, class files, weekly assessments, the final exam, and an online grade book.

Please be sure to log in daily to keep abreast of class announcements. This is very important!

**Communication:**
Please email me only at the address listed on this syllabus! I check this email address regularly and will promptly respond to email received. During the week, I will respond within one business day. For example, if you email me on Tuesday at 2pm, I will respond back to you by Wednesday at 2pm. If I don’t respond within that time frame, an error occurred, meaning that I did not get your email. So, please forward your original email to me (again).

On weekends, I may or may not respond depending on my personal schedule. Do not rely on a weekend response to get your work done! For example, if you email me on Friday at 9am, I will respond back to you by Monday at 9am. However, your homework due date is unchanged.

Further, if you need an answer to a question, please send the question via email rather than voice mail. Please only use the telephone to contact me for emergency situations. It may take me a few days to return phone calls.

**Course Policies:**

If you have problems completing an assignment, it is your responsibility to contact your instructor to resolve the situation. The college has a zero tolerance policy (721.1 Academic Integrity) regarding all forms of academic dishonesty. Students caught (and/or involved in) copying—or any of the other noted violations of academic dishonesty—will receive a zero (0) on that assignment, project, or test. Continued violations of this policy may result in student suspension from classes. Note that this policy specifically addresses plagiarism as it applies to students at UCC. The policy on academic integrity is posted throughout the campus; please take the time to read it!

Your instructor will generally grade your homework each week. For example, week 1 homework will be graded some time during week 2. When your homework is graded, your instructor will write comments on your work, when applicable, along with a grade for each assignment. Then, grades are posted in Angel later that same day.

You may work at your own pace throughout this course. For example, you can complete the whole course in less than ten weeks if you have the time to do so. However, your instructor will grade homework and answer course material questions weekly. Therefore, if you ask a week 6 question in week 2, your instructor may defer answering that question until that answer benefits the entire class.

Students are responsible for material presented in announcements (email or posted), flash presentations, YouTube videos, assigned reading, quizzes, and homework assignments. Any of these materials can and will be used by the instructor as the basis for test questions.

Make up tests will only be given in two circumstances:

1) The student contacts the instructor with a valid excuse prior to the scheduled test. (Examples of valid excuses are documented health problems, emergency medical appointments, “special” family events, etc.).
2) There was a personal, family, or medical emergency at the time of the test that prevented contact with instructor. (Examples of valid excuses are car accidents, death in the immediate family, or serious injury just prior to the test.)

The instructor retains the right to refuse non-health and/or family emergency excuses which appear to be avoidable or optional choices made by the student. The alternate test time will be set by the instructor. Make-up options for pop quizzes or class activities will be extremely limited and at the instructor’s discretion.

**Student Notice:**

Any student who feels he or she may need an accommodation for any type of disability, please make an appointment to see me during office hours or contact Disability Services in the Counseling Center."

http://www.umpqua.edu/disability-services

http://www.umpqua.edu/disability-services/329-disability-services-your-first-term

For more information, contact the Disabilities Services Coordinator:
Ms. Danielle Haskins
Phone (541)440-7655
Fax (541)440-4612, or
Oregon Relay (800)735-1232

Umpqua Community College Counseling Center provides comprehensive counseling services to assist you with career plans and academic advising as well as help to work out personal or social problems. Counselors are available to both current and prospective students in the Campus Center.

http://www.umpqua.edu/tutoring-center

The Counseling Center, Testing Center, Job Placement & the Transfer Opportunity Program are located in the Campus Center building across from UCC's Financial Aid Office. To contact our office you may stop by during business hours or call (541) 440-4610.

http://www.umpqua.edu/counseling-center

For assistance with homework assignments, students are encouraged to visit the Institutional Resources link in Angel, which is available via the Resources tab. Listed here you will find links to search local libraries, search newspapers and journals, You can also use one of the links to email a UCC librarian for assistance.
The ANGEL Learning Management System is compliant with ADA standards
Office 2010 & Windows 7

This chapter is not numbered in the textbook! It is the section immediately before chapter 1.

As you most likely are aware, Windows 7 is the newest version of Microsoft Windows, which is the most widely used desktop operating system on the planet.

An operating system is a computer program, or set of computer instructions, that coordinates all the activities of a computer’s hardware such as memory, storage devices, and printers. We will refer to an operating system using the acronym OS from now on.

Further, the OS provides the capability for you to communicate with the computer through the use of a graphical user interface, or GUI.

Windows 7 is used to run application software, which is software that you can purchase from a retailer. This software is usually in the form of games, reference material, and others. Some software comes as a suite, which is a number of applications bundled into one program. An example of an
application suite is Microsoft Office 2010, which we will discuss in this chapter.

Outcomes

- Perform basic mouse operations
- Start Windows and log on to the computer
- Identify the objects on the Windows 7 desktop
- Identify the programs in and versions of Microsoft Office
- Start a program
- Identify the components of the Microsoft Office Ribbon
- Create folders
- Save files
- Change screen resolution
- Perform basic tasks in Microsoft Access
- Manage files
- Use Microsoft Office Help and Windows Help

Readings

- Read and do hands-on work for Office 2010 & Windows 7
Click here to download this week's PowerPoint Presentation.

Homework

- Lab 2, p. OFF 53; Lab 2, p. OFF 54
- Click here to post something about yourself in the SIA (Student Introductory Assignment) forum.
  - You must post something about yourself by Wednesday at 9 PM. You may be dropped from this class in week 1 if you do not post your SIA to prove that you are participating in this class.
- Click here to open the Lab 2 drop box to upload this homework assignment
- Click here to open the Lab 3 drop box to upload this homework assignment
- Click here to open the Cases and Places Project 1 drop box to upload this homework assignment
- Click here to open the Cases and Places Project 3 drop box to upload this homework assignment
- Note: review the grading rubric for a reminder on what to do to earn full credit for homework!

Assessment
• Click [here](#) to begin this week's quiz

**Lecture Notes**

• Click [here](#) to view this week’s Flash presentation

• [Student Introductory Assignment](#)

• [Lab 2, p. OFF 53 drop box](#)

• [Lab 3, p. OFF 54 drop box](#)

• [Project 1, p. OFF 54 drop box](#)
• Project 3, p. OFF 55 drop box
Chapter 1 – Databases & Database Objects: An Introduction

In the chapter 1 hands-on activities, you will learn how to create a database, starting with an empty, blank Microsoft Access database file. A database contains one or more tables, as you will discover when you do the work in the chapter. A table is similar to an Excel worksheet, which, in turn, is similar to the green-bar paper an accountant uses to record transactions on. You will learn how to enter values and other things a table's fields, which, again, is similar to a worksheet's cell, and will be fully described in this week's work.

The database will contain customer data for the Camashaly Design Group, which I will refer to as CDG. CDG is a fictional entity that creates and maintains Web sites, and provides other online work for service, nonprofit, and retail businesses.

This chapter’s project is to create a database that contains data about its clients and its people.
Outcomes

- Design a database to satisfy a collection of requirements
- Describe the features of the Access window
- Create a new, blank database
- Create tables in Datasheet and Design views
- Add records to a table
- Close and open a database
- Print the contents of a table
- Create and use a query
- Create and use a form
- Create and print custom reports
- Modify a report in Layout view

Readings

- Read and do hands-on work for Chapter 1
- Click here to download the chapter 1 PowerPoint Presentation
Homework

- Chapter 1: Lab 2, p. AC 68; Cases and Places Project 3, p. AC 72
- Click here to open the Chapter 1: Lab 2 drop box to upload this homework assignment
- Click here to open the Chapter 1: Project 3 drop box to upload this homework assignment
- Note: review the grading rubric for a reminder on what to do to earn full credit for homework!

Assessment

- Click here to begin this week's quiz

Lecture Notes

- Click here to view this week’s Flash presentation
• Lab 2, p. AC 68 drop box

• Project 3, AC 72 drop box
CIS 125D_Week 1 Assessment: Office 2010 Windows 7 (Access)

1.

To display the Start menu, press ____.

- A) CTRL+ESC
- B) F5
- C) CTRL+F5
- D) ALT+F5

Correct answer(s): A

2.

If you are required to log on to the computer, the ____ screen is displayed, which shows the user names of users on the computer.

- A) Log-in
- B) Welcome
- C) Intro
- D) Entry

Correct answer(s): B

3.

The ____ command waits for Windows 7 to save your work and then turns off the computer fans and hard disk.
A) Shut down
B) Restart
C) Sleep
D) Snooze

Correct answer(s): C

4.

A(n) ____ is a named unit of storage.

A) index  
B) application  
C) operator  
D) file

Correct answer(s): D

5.

Which of the following applications is included with Microsoft Office Standard 2010?

A) SharePoint Workspace  
B) InfoPath  
C) Communicator  
D) OneNote
6. Which of the following applications is included with Microsoft Office Home and Student 2010?

- A) Excel
- B) Outlook
- C) Access
- D) Publisher

Correct answer(s): A

7. A(n) ____ is an area of a window that displays related content.

- A) taskbar
- B) integrated sidebar
- C) pane
- D) docking bar

Correct answer(s): C
A(n) ____ on a menu performs a specific action, such as saving a file.

Correct answer(s): B

A ____ consists of a drive letter and colon, to identify the storage device, and one or more folder names.

Correct answer(s): C
11.

Which of the following is a valid folder name?

- A) folder?
- B) folder!
- C) folder:
- D) "folder"

Correct answer(s): B

12.

A ____ is an icon on the desktop that provides a user with immediate access to a program or file.

- A) shortcut
- B) library
- C) command
- D) favorite

Correct answer(s): A

13.

A ____ helps you manage multiple folders and files stored in various locations on a computer.
As shown in the accompanying figure, the database file name appears on the ____ bar.

☐ A) title

Correct answer(s): D
15. ____ view can be used in Access (as well as Word and Excel) to close an open file.

- A) Backstage
- B) Navigation
- C) Web
- D) Options

Correct answer(s): A

16. As shown in the accompanying figure, each ____ contains a collection of groups, each of which
contains related functions.

A) cluster  
B) matrix  
C) tab  
D) base

**Correct answer(s): C**

17.

As shown in the accompanying figure, all Office programs have a ____ tab, which contains the more frequently used commands.

A) Gallery  
B) Navigation  
C) Home  
D) Quick Options

**Correct answer(s): C**
The tool tabs, as shown in the accompanying figure, are also called _____ tabs.

- A) contextual
- B) dialog
- C) shortcut
- D) navigation

**Correct answer(s):** A
You can press the ____ key on the keyboard to display KeyTips, like the kind in the accompanying figure.

A) CTRL  
B) F4  
C) ALT  
D) ESC

Correct answer(s): C
To remove KeyTips like the ones in the accompanying figure, you can press the ____ key until all KeyTips disappear.

A) ESC  
B) F1  
C) CTRL  
D) F4

Correct answer(s): A

21.
You can press the ____ keys to open an Office file.

A) ALT+O  
B) CTRL+O  
C) ALT+F  
D) CTRL+F

Correct answer(s): B

22.
Which of the following is NOT one of the main tabs displayed on the Ribbon when you start Access?

A) File  
B) Tools  
C) External Data  
D) Create
23. As shown in the accompanying figure, the External Data tab has three ____.

- A) groups
- B) placeholders
- C) layouts
- D) sliders

Correct answer(s): A

24.
To display more of a database or other item in the window in the accompanying figure, some users prefer to ____ the Ribbon.

- A) realign
- B) minimize
- C) replace
- D) append

**Correct answer(s): B**

25.

Which of the following buttons are contained on the Quick Access Toolbar by default?

- A) Save
- B) Redo
- C) Undo
- D) All of the above

**Correct answer(s): D**
CIS 125D Week 6 Assessment: Access Chapter 5

1. The _____ data type is used for a field that contains text that is variable in length and that can potentially be very lengthy.
   - A) Variable
   - B) Attachment
   - C) VarChar
   - D) Memo

2. To modify the design of a table, right-click the table in the Navigation Pane, and click _____ on the shortcut menu.
   - A) Modify Table
   - B) Change Table
   - C) Design View
   - D) Modify View

3. To use the Input Mask Wizard, select the Input Mask property in the field’s property sheet and then select the _____ button.
   - A) Wizard
   - B) Build
   - C) Input Mask
   - D) Expression
4. In the accompanying figure, the Comment field has been resized. To resize a field so that a larger portion of the text will appear, drag the right edge of the _____ to the desired size.

A) field selector
B) horizontal scroll bar
C) vertical scroll bar
D) datasheet
In the accompanying figure, the rows have been resized. To resize a row so that more data can appear, drag the lower edge of the _____ to the desired size.

- A) horizontal scroll bar
- B) vertical scroll bar
- C) datasheet
- D) record selector
6. In the accompanying figure, the Comment field has been resized. To resize a field so that a larger portion of the text will appear, right-click the field selector, and click _____ to change the column size.

☐ A) Field Width
☐ B) Field Size
☐ C) Width
☐ D) Size
In the accompanying figure, the rows have been resized. To resize a row so that more data can appear, right-click the record selector, and click _____ to change the row spacing.

- A) Height
- B) Row Spacing
- C) Row Height
- D) Size

8. To convert a picture from a Bitmap Image to Picture (Device Independent Bitmap), right-click the field, click _____, click Convert, and then select Picture (Device Independent Bitmap) in the Convert dialog box.

- A) Object
- B) Picture Object
- C) Convert Object
- D) Bitmap Image Object

9. To insert data into an Attachment field, use the _____ command on the Attachment’s field’s shortcut menu.

- A) Insert Attachments
- B) Insert Objects
10. To enter data into a Hyperlink field, right-click the Hyperlink field, click Hyperlink on the shortcut menu, and then click _____ on the Hyperlink submenu.
   - A) Insert Hyperlink
   - B) Insert Object
   - C) Edit Hyperlink
   - D) Attach Hyperlink

11. To create a form in Design view, select the table for the form, click Create on the Ribbon, and then click _____ on the Create tab.
   - A) Design View
   - B) Form Design
   - C) Blank Form
   - D) New Form

12. To display a field list in Design view, click the ____ button on the Design tab.
   - A) Show Table
   - B) Display Fields
   - C) Field List
   - D) Add Existing Fields

13. To save a form and assign it a name, click the Save button on the _____.
   - A) Design tab
   - B) Quick Access Toolbar
   - C) Home tab
   - D) Create tab

14. To change the background color of a form, you can use the _____ button on the Design tab.
   - A) Background
   - B) Back Color
   - C) Fill/Back Color
   - D) Format
15. To use the shortcut menu to change the background color of a form, right-click the form and select the _____ command on the shortcut menu.
   ☐ A) Background
   ☐ B) Format
   ☐ C) Back Color
   ☐ D) Fill/Back Color

16. To add a title to a form, click the _____ button on the Design tab.
   ☐ A) Form Title
   ☐ B) Name
   ☐ C) Title
   ☐ D) Text Box

17. To add a Form Header section to a form, right-click anywhere on the form background and click _____ on the shortcut menu.
   ☐ A) Add Section
   ☐ B) Form Header/Footer
   ☐ C) Insert Header
   ☐ D) Arrange

18. To switch from Design view to Form view to display the form, click the _____ button.
   ☐ A) Display
   ☐ B) Open
   ☐ C) Window
   ☐ D) View

19. To resize columns in a subform, right-click the subform in the Navigation Pane, and click ____ on the shortcut menu.
   ☐ A) Open
   ☐ B) Modify
   ☐ C) Change Columns
   ☐ D) Resize
20. To change the size mode for a picture, click the control, click the Property Sheet button on the Design tab, and then click the ______ property box.
   ○ A) Picture
   ○ B) Size Mode
   ○ C) Cropping
   ○ D) Alignment

21. To change the font color of a label, select the label, and click the ______ arrow on the Format tab to display a color palette.
   ○ A) Color
   ○ B) Label Color
   ○ C) Font Color
   ○ D) Text Color

22. To change the special effect of a label, select the label, click the ______ button on the Design tab, and then click the Special Effect property box arrow.
   ○ A) Property Sheet
   ○ B) Special Effect
   ○ C) Properties
   ○ D) Labels

23. The condition, ______, entered in the Criteria row of a memo field in a query window would retrieve all records where the memo field had any mention of Information.
   ○ A) *Information
   ○ B) ?Information
   ○ C) *Information*
   ○ D) ?Information?

24. To test for the current date in a query, type ______ in the Criteria row of the appropriate column.
   ○ A) Current()
   ○ B) CurrentDate()
   ○ C) Today()
   ○ D) Date()
25. To create a multitable form based on the “many” table, click the _____ button on the Create tab to create a form in Layout view.

○ A) Multitable Form
○ B) Blank Form
○ C) Many Form
○ D) Layout Form
Selecting a Project

- What are you interested in?
- What is your career field of choice?
- What do you want to do after graduation?
- Who do you currently work for?
- Who do you want to work for?
- Are you involved in a local non-profit?
- Are you involved in a local church?

- Meet with the manager, leader, pastor, etc.
  - Introduce yourself and ask if there is a project they want to do
  - Look for areas where things are not working properly
  - Look for a current challenge

- Project Process
  - Define the challenge
  - Interview, research, gather data, etc.
  - Develop a hypothesis or potential solution
  - Propose a solution
  - Design a solution
  - Test your design
  - Refine your proposal

- Write the Report
  - A – Impress me – solve a problem – demonstrate excellence
  - B – Good project – weak solution – poor report construction
  - C – Yep, you did a project – weak write-up, the world won’t be improved
  - D – Did a process not a project – poor report – no real change proposed
  - F – No report, no participation, gave up
Imagine This

Objective
Explain the operation of link aggregation in a switched LAN environment.

Scenario
It is the end of the work day. In your small- to medium-sized business, you are trying to explain to the network engineers about EtherChannel and how it looks when it is physically set up. The network engineers have difficulties envisioning how two switches could possibly be connected via several links that collectively act as one channel or connection. Your company is definitely considering implementing an EtherChannel network.

Therefore, you end the meeting with an assignment for the engineers. To prepare for the next day’s meeting, they are to perform some research and bring to the meeting one graphic representation of an EtherChannel network connection. They are tasked with explaining how an EtherChannel network operates to the other engineers.

When researching EtherChannel, a good question to search for is “What does EtherChannel look like?” Prepare a few slides to demonstrate your research that will be presented to the network engineering group. These slides should provide a solid grasp of how EtherChannels are physically created within a network topology. Your goal is to ensure that everyone leaving the next meeting will have a good idea as to why they would consider moving to a network topology using EtherChannel as an option.

Required Resources
- Internet connectivity for research
- Software program for presentation model

Step 1: Use the Internet to research graphics depicting EtherChannel.

Step 2: Prepare a three-slide presentation to share with the class.
   a. The first slide should show a very short, concise definition of a switch-to-switch EtherChannel.
   b. The second slide should show a graphic of how a switch-to-switch EtherChannel physical topology would look if used in a small- to medium-sized business.
   c. The third slide should list three advantages of using EtherChannel.
CIS 125E Course Outline
Assignments by Week

During week one, you must post something about yourself in the SIA (Student Introductory Assignment) forum (under the Week 1 Lesson link within Angel). Look at what I posted and post something similar about yourself. Please do this no later than Wednesday at midnight of week 1.

Homework due dates: All assignments are due on or before Sunday at midnight at the end of each semester week. For example, week 1 begins on Monday, September 26, 2011. Homework assigned for week 1 is due no later than midnight on Sunday, October 02, 2011.

Reading consists of studying, taking notes, viewing PowerPoint presentations, and performing all hands-on exercises found in each chapter assigned.

Homework consists of the work you do while reading/studying each chapter, projects found at the end of each chapter, and weekly quizzes. Whenever a homework assignment asks you to compose an e-mail please always send it to your instructor. An example is your homework assignment Chapter 1 Lab 1. Please remember to format your subject line as described below (two paragraphs down).

Online quizzes are available within Angel via the Weekly Assessments and Lessons Folder links (use either one). You will also find PowerPoint presentations for each tutorial in the Course Documents link. You may take these assessments up to two times. Your last score is the one that counts (which may not be your highest score).

How to turn in homework:
1. Be sure that all of your files are named as directed to do so in your homework. If files are misnamed, they will not be graded because I look for specific files to grade.
2. Do not print any work. Save it to your Flash drive and properly submit in your weekly assignments.
3. Send all e-mail messages directly to your instructor as noted in the assignments. Sometimes it will be in the To… box and other times it will be Cc…
4. The subject for the e-mail messages will be given to you in the assignment.
5. Place all of your files, properly named, for each chapter in one compressed folder.
6. Name the compressed folder with your course number, your name and week number. For example, week one’s filename would be "CIS125E_Week 1 – Jeff Spangenberg". Do not include the quotation marks.
7. Attach your compressed folder to an e-mail (one homework e-mail per week).
8. Complete your e-mail subject line with your course number, your name and week number. For example, week one’s filename would be "CIS125E_Week 1 – Jeff Spangenberg". Again, do not include the quotation marks.
9. Send the zipped file to my e-mail address: spangjucc@gmail.com. Do not send more than one homework e-mail per week.
10. Do NOT use any other e-mail address than the one listed above to submit your homework.

Week By Week Activities:

Week 1: September 26 – October 2
- SIA due by Wednesday at 5:00 pm during week one!
  - You must complete your SIA on time to not be dropped from the course in week 1.
- Read and do hands-on work for Chapter 1 and view PowerPoint presentation
- Homework due for Lesson 1:
Apply Your Knowledge
Extend Your Knowledge
Make It Right

Week 2: October 3 – October 9
- Review Chapter 1 Concepts
- Do the online Quiz this lesson
- Homework due for chapter 1: Lab 1, Lab 2, Lab 3, Cases & Places 1

Week 3: October 10 – October 16
- Read and do hands-on work for Chapter 2 and view PowerPoint presentation
- Homework due for Lesson 2:
  - Apply Your Knowledge
  - Extend Your Knowledge
  - Make It Right

Week 4: October 17 – October 23
- Review Chapter 2 Concepts
- Do the online Quiz this lesson
- Homework due for chapter 2: Lab 1, Lab 2, Lab 3, Cases & Places 1

Week 5: October 24 – October 30
- Read and do hands-on work for Chapter 3 and view PowerPoint presentation
- Homework due for Lesson 3:
  - Apply Your Knowledge
  - Extend Your Knowledge
  - Make It Right

Week 6: October 31 – November 6
- Review Chapter 3 Concepts
- Do the online Quiz this lesson
- Homework due for chapter 3: Lab 1, Lab 2, Lab 3, Cases & Places 1

Week 7: November 7 – November 13
- Read and do hands-on work for Chapter 4 and view PowerPoint presentation
- Homework due for Lesson 4:
  - Apply Your Knowledge
  - Extend Your Knowledge
  - Make It Right

Week 8: November 14 – November 20
- Review Chapter 3 Concepts
- Do the online Quiz this lesson
- Homework due for chapter 3: Lab 1, Lab 2, Lab 3, Cases & Places 1

Week 9: November 21 – November 27
- Read and do hands-on work for Chapter 3 and view PowerPoint presentation
- Homework due for Lesson 3:
Apply Your Knowledge
- Extend Your Knowledge
- Make It Right

Week 10: November 28 – December 4
- Review Chapter 3 Concepts
- Do the online Quiz this lesson
- *Homework due for chapter 3: Lab 1, Lab 2, Lab 3, Cases & Places 1

Week 11: December 5 – December 9
- Final Exam – Online (Opens December 5 at 8 am; Closes December 9 at 11:55 pm)

*Homework for Chapter 10 is due via e-mail to your instructor no later than Friday, December 4 at 11:55 pm.
Instructor: Jeff Spangenberg  
Class: Online  
Lab: Included with classes  
Course: CIS 125E  
Office: TC 102 (M 9-9:45; T 10-10:50; F 11-11:50)

Phone: 541.957.5850  
E-mail: spangjucc@gmail.com  
Credits: 2

Required Texts: 1) Microsoft Outlook 2010, Complete, Publisher: Shelly, Romanoski, Freund, Enger.

Book Web site: www.cengage.com/ct/studentdownload. To download the necessary files follow the directions on the web page. Be sure you save it in a location that is easy to access. I also suggest that you save the files in a backup location just in case something happens. **Having these files are critical to the success of this course.**

Course Description: This course will serve as an introduction to e-mail client software such as Microsoft Outlook 2010. This course is lab-oriented and will focus on using a modern e-mail software application to configure settings, work with rules, folders, contacts, calendars, and data files. Students will also work with advanced settings feature such as calendar, contact management, and security.

Course Prerequisite: Instructor enforced prerequisite of a minimum of 20 word per minute (WPM) is required. If you are unable to touch type at least 20 WPM contact your instructor before beginning the course.

Course Outcomes:

- Edit how the GUI looks and functions through use of on-screen tools
- Create and send messages
- Read and reply to messages
- Create, modify, or delete an out of office message
- Forward a message
- Attach a file to a message
- Save an attachment to a specific location
- Open an attachment
- Create, edit, format, or delete a signature
- Use advanced message options to set a sensitivity or importance level
- Use advanced message options to request delivery and read receipts
- Use advanced message options to receive replies at a specific address
- Use advanced message options to delay a message's delivery
- Create a standard or custom voting button
- Create a digital signature
- Send a message using encryption
- Restrict permissions to a message
• Search for messages
• Create, move, or delete a mail folder
• Remove deleted items from an e-mail data file
• Create and implement an archive plan
• Process messages with rules by using rule templates or by editing a rule
• Enable or delete an existing rule
• Create, edit, or delete a contact
• Send a contact as an attachment
• Save a contact received as a contact record
• Create a contact from a message header
• Edit, send, or create a contact from an electronic business card
• Search for a contact or for a specific attribute relating to a contact
• Create, schedule, mark, or delete an appointment
• Create a one-time or recurring appointment or meeting
• Determine when appointment or meeting attendees can meet
• Track responses to a meeting request
• Change, propose, accept, or update a meeting time
• Customize a calendar by defining a work week
• Customize a calendar by displaying multiple time zones, changing your time zone, or adding a holiday to the calendar
• Share your calendar
• Send calendar information via e-mail
• Publish calendar information to Microsoft Office Online
• View another network user’s calendar
• Subscribe to an Internet calendar
• Create, edit, or delete a one-time or recurring task
• Assign a task to someone else
• Respond to an assigned task
• Report the status of a task
• Create, modify, or sort a color category
• Assign or search for color categories
• Create an e-mail data file for multiple e-mail accounts

**Equipment:** It is intended that students will use their personally-owned PCs with *Microsoft® Office Outlook 2010*. Students will need to use their own computer and install this software. Please consult with your instructor prior to purchasing any software for this class.

The UCC bookstore sells Microsoft Office 2010 (includes Excel, PowerPoint, and Word) at student rates. If you wish to purchase these products, please visit the bookstore.
**Netiquette:**
The following are a few rules of Forum Netiquette compiled and adapted for UCC Online from Wikipedia, Google Groups, and the Netiquette book.

1. The most important rule of netiquette is, "Think before you post." If what you intend to post will not make a positive contribution to the discussion and be of interest to several readers, do not post it!

2. Never forget that the person on the other side is human. Always be courteous.

3. If you're new to the forum, lurk for a while before you post. "Lurking" is reading the forum discussions without actually participating. Despite the sinister tone of the word, lurking in cyberspace is not frowned upon -- in fact, it's encouraged. Lurking gives you an idea of who the participants are and what the tone of the discussion is. It helps you avoid mistaking a joke for a serious statement, or posting a comment only to find out that a virtually identical statement appeared in the forum yesterday.

4. Personal messages to one or two individuals should not be posted to the forums – send them an email instead.

5. Avoid double posting and crossposting.

6. Be brief.

7. Do not use inappropriate language (swearing, double meaning words/phrases, insults, etc.).

8. Write well. Follow standard grammar and spelling rules and try not to use slang. If needed, use the spell-check feature.


10. Be careful with humor and sarcasm. Without the voice inflections and body language of personal communications, it's easy for a remark meant to be funny to be misinterpreted.

11. Respond to topics started by others more often than starting topics of your own so that you don't appear arrogant and unlikable.

12. When quoting a previous post, include only the relevant portion of that post.

13. Avoid the use of all **CAPITAL LETTERS** in posts. (All CAPS is considered "shouting" and makes your posts harder to read.)

14. Do not resurrect a very old topic if you have nothing extremely significant to add.

15. Try to refrain from lashing back at a poorly behaving member or participating in a flame war; instead, notify your instructor of the event.

**Homework:** Students should plan to spend an average of 6-8 hours per week working in class lecture, assigned materials and reading. Knowledge assignments and lab work will be graded primarily on timely, completeness, and accuracy. Late assignments will be penalized 20% of that assignment’s grade for three days after it is due. Assignments turned in after the three day grace period will not be accepted for grading. All course work for week ten must be turned in and completed (including the quiz within Angel) no later than midnight, Wednesday, December 7, 2011. Work turned in after that date/time will not be accepted for grading.
Quizzes: There will be five quizzes during the term. Quizzes are available through our online component, Angel. Quizzes can be taken anytime during the week it is due, up to two times. The last score is the one that counts!

Final Exam: The final exam will be online and will be available through the online component, Angel. This exam can be taken anytime through the Finals week until Friday, December 9 until 5 pm. You will have one attempt at this exam.

Points: Grades will be assigned based on the total points (pts) earned as follows; 90 to 100% = A, 80 to 89.9% = B, 70 to 79.9% = C, 60 to 69.9% = D, and less than 60% = F. Points are distributed as follows:

<table>
<thead>
<tr>
<th>Description</th>
<th>Quantity</th>
<th>Points</th>
<th>Total</th>
<th>Category %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge Assignments</td>
<td>15</td>
<td>5</td>
<td>75</td>
<td>15.8%</td>
</tr>
<tr>
<td>Lab Assignments</td>
<td>20</td>
<td>10</td>
<td>200</td>
<td>42.1%</td>
</tr>
<tr>
<td>Quizzes</td>
<td>5</td>
<td>10</td>
<td>50</td>
<td>10.5%</td>
</tr>
<tr>
<td>Final exam - Online</td>
<td>1</td>
<td>150</td>
<td>150</td>
<td>31.6%</td>
</tr>
<tr>
<td><strong>Total Possible Pts</strong></td>
<td></td>
<td></td>
<td><strong>475</strong></td>
<td><strong>100.0%</strong></td>
</tr>
</tbody>
</table>

Course Outline: This outline is a plan for the term. It is subject to change should the need arise. Any such changes will be noted on Angel. It is your responsibility to note changes in the syllabus schedule as noted in Angel announcements during the term. Be sure you check the Angel announcements each week prior to starting your assignments.

Knowledge and lab assignments are due by midnight on the Sunday of each week’s assignment. For example, assignments for Week 1 are due on or before midnight on Sunday, October 2, 2011 (or thereabouts).

Your knowledge and lab homework is made up of homework assignments listed in your textbook. For each chapter you will manually perform many step-by-step exercises as you read and study. For example, in chapter 1, on p. OUT6 (and throughout the rest of the chapter) you set up Outlook and add the e-mail account you want to use for this course. You need to do this (and all exercises like it).

In Chapter 1, your other homework is listed at the very end of the lesson (starting on p. OUT40). Apply Your Knowledge (AYK), Extend Your Knowledge (EYK), and Make It Right (MIR) are all assigned. In fact, the first week of a chapter will always include the AYK, EYK, and MIR. The second week of each chapter will include all of the “In the Lab” and one “Cases and Places” assignment. Finally, in Angel, under the Lessons -> Week 1 link, click to take that week’s quiz. You will have one quiz for each lesson we cover during the term.

If you have ANY questions about what homework is assigned, please e-mail me immediately. If you wait until late in the week to ask homework questions, it will not extend your homework due date. Always ask questions as early in the week as possible.

Always keep a backup of your homework in your possession until I return your graded work back to you. This way if I don’t get your work, you can always send me your backup copy. Warning: your backup homework copy must have a date that is on or before the date it was due. This proves that you did the work before its due date.

You will e-mail your work to me each week. In some cases you will send me e-mail as a homework assignment. Please see the Angel announcement titled “How do I submit homework to my instructor?” for how to do this.

Please e-mail me only at the address listed on this syllabus! I check this e-mail address regularly and will promptly respond to e-mail received. During the week, I will respond within one business day. For example, if you e-mail me on Tuesday at 2 pm, I will respond back to you by Wednesday at 2 pm. When you have a question, please place a question mark in the subject box so I know to respond to that e-mail immediately.

On weekends, I may or may not respond depending on my personal schedule. Do not rely on a weekend response to get your work done! For example, if you e-mail me on Friday at 9am, I will respond back to you by Monday at 9am. Note that this does not change the due date of your homework. You will want to plan to ask questions so that you have all of the information you need to submit your homework on time.

All of our course documents will be kept on our UCC online component – Angel (http://angel.umpqua.edu). Download files to your USB drive and update these when you are informed of changes by your instructor.
**Course Policies:** If you have problems completing an assignment, it is your responsibility to contact your instructor to resolve the situation. The college has a zero tolerance policy (721.1 Academic Integrity) regarding all forms of academic dishonesty. Students caught (and/or involved in) copying—or any of the other noted violations of academic dishonesty—will receive a zero (0) on that assignment, project, or test. Continued violations of this policy may result in student suspension from classes. Note that this policy specifically addresses plagiarism as it applies to students at UCC. The policy on academic integrity is posted throughout the campus; please take the time to read it!

Students are responsible for material presented online, assigned reading, activities, handouts, videos, required presentations, and class assignments. Any of these materials can and will be used by the instructor as the basis for test questions.

_The instructor retains the right to refuse non-health and/or family emergency excuses which appear to be avoidable or represent optional choices made by the student._


**Counseling Center:** Any student who feels he or she may need an accommodation for any type of disability, should make an appointment to see me during office hours or contact Disability Services in the Counseling Center.

Umpqua Community College Counseling Center provides comprehensive counseling services to assist you with career plans and academic advising as well as help to work out personal or social problems. Counselors are available to both current and prospective students in the Campus Center.

The Counseling Center, Testing Center, Job Placement & the Transfer Opportunity Program are located in the Campus Center building across from UCC's Financial Aid Office. To contact our office you may stop by during business hours or call (541) 440-4610.

[http://www.umpqua.edu/Counsel/CCindex.htm](http://www.umpqua.edu/Counsel/CCindex.htm)

**Tutoring Services:**
Tutoring Services are available to UCC students. Contact information for UCC's tutoring center can be found at the following Web address: [http://www.umpqua.edu/BasicSkills/Tutor.htm](http://www.umpqua.edu/BasicSkills/Tutor.htm).
Student Introductory Activity (SIA)

Must be completed by Wednesday of the first week at 5:00 pm.

This is your introductory "check-in" activity. It is a graded activity (5 points) that must be completed by Wednesday at 5:00 pm to not be dropped from this course.

Please post some generic information about yourself and why you are taking this course.

Read other's postings as you may find you have some common thoughts. Respond to each other's postings if you would like, but it is not required.

I will respond to your post indicating I know you have checked in.
1. A ______ identifies the sender of an e-mail message and may contain additional information, such as a job title and phone number(s).

A) greeting line  
B) subject line  
C) signature line  
D) closing line  
Correct answer(s): C

2. In Outlook, an e-mail account is contained in an e-mail ______.

A) document  
B) profile  
C) message  
D) record  
Correct answer(s): B

3. As you type an e-mail message, Outlook automatically corrects some misspelled words.

A) True  
B) False  
Correct answer(s): True

4. A ______ folder is the location of a document to be moved or copied.

A) source  
B) start  
C) target  
D) personal  
Correct answer(s): A
5. A(n) ______ file is a data file that stores a user's Outlook items, including e-mail messages.

A) user
B) messages
C) e-mail
D) personal folders

Correct answer(s): D

6. Another name for a personal folders file is a(n) ______ file.

A) .pst
B) .doc
C) .pff
D) .fld

Correct answer(s): A

7. The ______ in a subject line indicates that a message is a reply to another message.

A) BCC:
B) HTTP:
C) RE:
D) CC:

Correct answer(s): C

8. The previewers in Office 2010 are designed to provide additional security against potentially harmful code.

A) True
B) False

Correct answer(s): True
9. The Outlook Junk E-mail Filter is turned on by default.
   A) True
   B) False
   Correct answer(s): False

10. The Trust Center allows you to configure the way Outlook handles attachments.
    A) True
    B) False
    Correct answer(s): True
1. A .pst file is a data file that stores all Outlook items in a specific location.
   A) True
   B) False
   Correct answer(s): True

2. When set to Day, the orange box in the appointment area indicates the time of the next appointment.
   A) True
   B) False
   Correct answer(s): False

3. Which view of your calendar cannot be printed?
   A) yearly
   B) daily
   C) weekly
   D) monthly
   Correct answer(s): A

4. An appointment entered into a calendar will be saved automatically when the user presses the ______ key.
   A) TAB
   B) CTRL
   C) ENTER
   D) HOME
   Correct answer(s): C
5. The _____ print style prints a daily appointment schedule for a specific date.

A) Calendar Details
B) Schedule
C) Daily
D) Tri-fold

Correct answer(s): C

6. The _____ calendar item status options shows time with a slashed bar in Day, Week, Work Week, or Month view.

A) Tentative
B) Out of Office
C) Free
D) Busy

Correct answer(s): A

7. Events appear in individual time slots in the appointment area.

A) True
B) False

Correct answer(s): False

8. When you change the appointment to an all-day event, the _____ identifies the item as an event.

A) navigation pane
B) ribbon
C) title bar
D) appointment area

Correct answer(s): C
9. The Standard folders include a shortcut to the _____ item.

A) Tasks
B) Mail
C) None of the choices
D) Calendar
E) Contacts
F) All possible choices

Correct answer(s): F

10. Meetings can only be scheduled on your main calendar.

A) True
B) False

Correct answer(s): False
CIS 125 E

How To Prepare Screen Shots

1. When the instructions indicate sending an e-mail be sure you send it from your Outlook to spangiucc@gmail.com. I do not check other UCC e-mail accounts, including Angel, for homework submissions.

2. Screen Shots
   a. Open a Word document
   b. Take the appropriate screen shot (note directions in Do This First PowerPoint presentation)
   c. Label the screen shot in your Word document before placing the screen shot. As an example; Ch 1 EYK 1 would be placed before taking the screen shot. See the sample below. Step 3 does not show all 3 screen shots that are necessary – one for each folder.

   ![Screen Shot Sample](image)

   ![2 rename folders](image)

   ![3 Move e-mail to folders](image)

   d. Submit your homework as indicated in the Course Assignments By Week document located on Angel.
Assignment Information

1. Students are expected to diligently work on lessons beginning the first day of each lesson. This allows you to ask necessary questions early in the week as the instructor has limited availability on the weekends.
2. I will generally check e-mail messages two times per day during the school week, once in the morning and once early evening during the week, except Friday evening. Times may vary depending on my schedule. Expect a response to questions within 24 hours. Keep in mind that an e-mail message sent on Friday afternoon may not be answered until Monday morning. This will not allow you time to complete assignments in time for the Sunday evening due time.
3. Your instructor will have approximately 90 students this term and I have other responsibilities. As much I will attempt to correct early in the week, it is quite possible that I will not complete correcting until Friday or Saturday. I will respond to all assignments turned in as I correct with that assignment's grade. This will allow you feedback on your progress.
4. I will post grades on Angel by the following Monday evening. This means that week 1 grades will be posted by evening on Monday, October 9.

Chapter 2 – Managing Calendars

Due October 16 by midnight

Chapter 2 focuses on managing, navigating, and editing calendars. You will be working with calendars displays, creating and editing appointments, and inviting others to appointments.

Outcomes

- Open a calendar folder
- Describe the components of the Outlook Calendar
- Navigate the Calendar using the Date Navigator
- Create a personal calendar
- Enter, save, move, edit, and delete appointments
- Set the status of and reminder for an appointment
- Create, edit, move, and delete events
- Create and edit meetings
- Respond to meeting requests
- Display the calendar in Day, Week, Work Week, Week, and Month views
- Print the Calendar in Daily Style

**Reading**

Read and do hands-on work for Chapter 2 (OUT 49-110)
Click [here](#) to view the Flash presentation.
Click [here](#) to download this chapter's PowerPoint Presentation

**Homework**

Projects: (OUT 111-115)

- Apply Your Knowledge
- Extend Your Knowledge
- Make It Right

If you need a reminder about how to submit your homework, click [here](#)

**Assessment**

- None this week.
Lecture Notes
Click here to view this week’s lecture notes
CIS 125E Week 7 Lesson 4

Chapter 4 – Creating and Managing Tasks

Due November 13 by midnight

This chapter focuses on creating and managing tasks which allows you to keep track of a project from start to finish. You will be able to categorize and monitor tasks so they are not neglected.

Outcomes

- Create, customize, and categorize tasks
- Create a recurring task
- Attach items to task
- Categorize and flag e-mail messages
- Configure quick click
- Assign a task
- Send a status report
- Print tasks
- Create a note
- Change the view of notes

Reading

Read and do hands-on work for Chapter 4 (OUT 169-222)
Click here to view the Flash presentation.
Click here to download this chapter's PowerPoint Presentation
Homework
Projects: (OUT 223-226)

- Apply Your Knowledge
- Extend Your Knowledge
- Make It Right

Assessment
- No Assessment this week.

Lecture Notes
Click [here](#) to view this week’s lecture notes
CIS 125E

Selecting a Project

• What are you interested in?

• What is your career field of choice?

• What do you want to do after graduation?

• Who do you currently work for?

• Who do you want to work for?

• Are you involved in a local non-profit?

• Are you involved in a local church?

• Meet with the manager, leader, pastor, etc.
  o Introduce yourself and ask if there is a project they want to do
  o Look for areas where things are not working properly
  o Look for a current challenge

• Project Process
  o Define the challenge
  o Interview, research, gather data, etc.
  o Develop a hypothesis or potential solution
  o Propose a solution
  o Design a solution
  o Test your design
  o Refine your proposal

• Write the Report
  o A – Impress me – solve a problem – demonstrate excellence
  o B – Good project – weak solution – poor report construction
  o C – Yep, you did a project – weak write-up, the world won’t be improved
  o D – Did a process not a project – poor report – no real change proposed
  o F – No report, no participation, gave up
Inside and Outside Control

Objective

Explain how wireless LAN components are deployed in a small- to medium-sized business.

Scenario

An assessment has been completed to validate the need for an upgrade to your small- to medium-sized wireless network. Approved for purchase are indoor and outdoor access points and one wireless controller. You must compare equipment models and their specifications before you purchase.

Therefore, you visit the Wireless Compare Products and Services web site and see a features chart for indoor and outdoor wireless access points and controller devices. After reviewing the chart, you note there is some terminology with which you are unfamiliar:

- Federal Information Processing Standard (FIPS)
- MIMO
- Cisco CleanAir Technology
- Cisco FlexConnect
- Band Select

Research the above terms. Prepare your own chart with your company’s most important requirements listed for purchasing the indoor and outdoor wireless access points and wireless controller. This chart will assist in validating your purchase order to your accounting manager and CEO.

Resources

Internet access to the World Wide Web

Part 1: Secure Background Knowledge of Wireless Terminology

Step 1: Define unfamiliar wireless terms.

a. FIPS
b. MIMO
c. Cisco CleanAir Technology
d. Cisco FlexConnect
e. Band Select

Step 2: Visit the Wireless Compare Products and Services web site.

a. Compare the devices in each category based on their feature sets.
b. Choose one model from each category: indoor, outdoor, and controller categories for the upgrades for your business.

Step 3: Create a chart for each device chosen in Step 2b to include:

a. The main type of selected device (indoor access point, outdoor access point, or controller).
b. A graphic of each selected device.
c. Five of the most beneficial features that the selected models would provide your business.
Inside and Outside Control

Step 4: After research is complete, explain, and justify your choices with another student, class group, or entire class.
CIS 125R – Microsoft PowerPoint 2010 – Presentation Software
Course Assignments by Week

During week one, you must post something about yourself in the SIA (Student Introductory Assignment) forum (under the Week 1 Lesson link within Angel). Look at what I posted and post something similar about yourself. Please do this no later than Wednesday at midnight of week 1.

Homework due dates: All assignments are due on or before Sunday at midnight at the end of each week. For example, week 1 begins on Monday, September 26, 2011. Homework assigned for week 1 is due no later than midnight on Sunday, October 02, 2011.

Reading consists of studying, taking notes, and performing all hands-on exercises found in each lesson (chapter) assigned.

Homework consists of the work you do while reading/studying each chapter, projects found at the end of each chapter, and weekly quizzes.

Online quizzes are available within Angel via the Weekly Lessons Folder links. You will also find PowerPoint presentations for each tutorial in the Course Documents link. You may take these tests up to two times and there is no time limit. Your highest score is the one that counts.

How to turn in homework:
1. Be sure that all of your files are named as directed to do so in your homework. If files are misnamed, they will not be graded because I look for specific files to grade.
2. Attach your homework files to an email (one homework email per week).
3. Complete your email subject line with your course number, week number, and your name. For example, week one’s filename for me would be “CIS125R, Week 1 – Micah Blackwood”.
4. Send your homework to my email address: micah.blackwood@umpqua.edu. Do not submit more than one homework email per week for the same assignment without discussing it with your instructor.
5. Do NOT use any other email address than the one listed above to submit your homework.

The schedule that follows is the same as the one listed on your syllabus. It is listed here so you can easily see all of your week’s activities in one location.

Week 1: Sept. 26 – Oct 02
- SIA due by Wednesday at midnight during week one!
  o If you don’t complete your SIA on time you may be dropped from the course in week 1.
- Read and do hands-on work for Chapter 1
- Do the online Quiz
- Homework due for Week 1: Projects Apply Your Knowledge (AYK)(PPT 57), Extend Your Knowledge (EYK)(PPT 58) & Make It Right (MIR)(PPT 59)

Week 2: Oct 03 – Oct 09
- Read and do hands-on work for Chapter 2
- Do the online Quiz
- Homework due for Week 2: Projects AYK(PPT 123), EYK(PPT 126) & MIR(PPT 129)
Week 3: Oct 10 – Oct 16
• Read and do hands-on work for Chapter 3
• Do the online Quiz
• Homework due for Week 3: Projects AYK(PPT 191), EYK(PPT 192) & MIR(PPT 194)

Week 4: Oct 17 – Oct 23
• Read and do hands-on work for Chapter 4
• Do the online Quiz
• Homework due for Week 4: Projects AYK(PPT 251), EYK(PPT 252) & MIR(PPT 253)

Week 5: Oct 24 – Oct 30
• Read and do hands-on work for Chapter 5
• Do the online Quiz
• Homework due for Week 5: Projects AYK(PPT 318), EYK(PPT 319) & MIR(PPT 321)

Week 6: Oct. 31 – Nov 06
• Read and do hands-on work for Chapter 6
• Do the online Quiz
• Homework due for Week 6: Projects AYK(PPT 387), EYK(PPT 387) & MIR(PPT 391)

Week 7: Nov 07 – Nov 13
• Read and do hands-on work for Chapter 7
• Do the online Quiz
• Homework due for Week 7: Projects AYK(PPT 452), EYK(PPT 454) & MIR(PPT 456)

Week 8: Nov 14 – Nov 20
• Read and do hands-on work for Chapter 8
• Do the online Quiz
• Homework due for Week 8: Projects AYK(PPT 515), EYK(PPT 517) & MIR(PPT 519)

Week 9: Nov 21 – Nov 27
• Read and do hands-on work for Chapter 9
• Do the online Quiz
• Homework due for Week 9: Projects AYK(PPT 581), EYK(PPT 583) & MIR(PPT 584)

Week 10: Nov. 28 – Dec 04
• Read and do hands-on work for Chapter 10
• Do the online Quiz
• *Homework due for Week 10: Projects AYK(PPT 639), EYK(PPT 641) & MIR(PPT 643)

Week 11: Dec 05 – Dec 07
• **Final Exam Projects: Cases & Places Projects 1,2 & 3 (PPT 592 & 656)
*Homework for Chapter 10 is due via email to your instructor no later than midnight on Sunday, December 4, **Skills Project is due via email to your instructor no later than midnight on Wednesday, December 7,
CIS 125R Syllabus Microsoft PowerPoint 2010 – Presentation Software

Instructor: Micah Blackwood, MBA  
Phone: 405.973.5319  
E-mail: micah.blackwood@umpqua.edu  
Course: CIS 125R, 2 credit hours  
CRN #

Class: Online


Book Resource Files: You will need certain data files to complete your weekly homework assignments. When your book directs you to open a file to do your homework, that file will be in your Student Data Files. You may download the Student Data Files by either downloading them from Angel or if they are too large I have provided a link to the book's website that you may download them from. Click [here](#) to go to your Student Data Files page. If you have any questions about how to download your data files, please contact your instructor immediately.

Course description: This course will serve as an introduction to presentation software. This course is lab-oriented and will focus on using a modern presentation software application to create, modify, customize and preview slide show presentations. Students will manage documents, work with text, visual elements, and program features that enhance slide shows. Import and export of files from Microsoft Word and Excel, and the use of sound or video clips are explored. Create hyperlinks to other slides, presentations, applications, or the Internet. Design principles are applied to create professional-looking presentations. Students are required to have access to a computer that is connected to the internet. High speed internet access is helpful but some students are able to get by with dialup. If you have dialup, try to get on campus and use the library or lab computers to view videos and PowerPoint slides as these involve large files that take a long time to download. To be successful in the online course students must have basic computer and internet skills and be comfortable with basic e-functions such as saving files, emailing, navigating the web, researching online sites, and uploading and attaching files.

Course outcomes:

- Use menus to create and modify a presentation.
- Copy, move, delete, format, and print presentation slides and notes.
- Insert, edit, format, or delete a background and theme.
- Insert, edit, format, or delete animations and transition affects.
- Insert, edit, format, or delete a basic table into or from a presentation.
- Insert, edit, format, or delete a table with special effects.
- Insert, edit, format, or delete a chart.
- Insert, edit, format, or delete art.
- Insert, edit, format, or delete pictures, video, or shapes.
- Finalize a presentation for sharing and security.
- Share a finalized presentation.
• Protect a shared presentation.
• Create and edit digital signatures.
• Insert, edit, format or delete comments.
• Prepare a presentation for delivery, including handouts, email, via slideshow, or CD/DVD.

**Equipment:** It is intended that students will use either their own home computer or the UCC lab computers. Your computer must have *Microsoft® Office PowerPoint 2010* installed on a computer to take this course.

The UCC bookstore sells Microsoft Office 2010 (includes Excel, PowerPoint, and Word) at student rates to students enrolled as half-time students or more. If you wish to purchase these products, please contact the bookstore.

**Homework:** Students should plan to spend an average of 6-8 hours per week working in class lecture, assigned materials and reading. Lab work will be graded primarily on timely, complete, and accurate completion. Late assignments will be penalized up to 20% of that assignment’s grade. **Assignments turned in after graded work has been returned to the class will not be accepted for grading.**

Please be aware that Week 10 homework is due via email to your instructor no later than midnight on Sunday, December 11, 2011.

Your Skills Project, which represents the final exam for this class, is due via email to your instructor no later than midnight, Wednesday, December 7, 2011.

All course work must be turned in and completed (within Angel) no later than midnight, Sunday, December 4, 2011. Work turned in after that date/time will not be accepted for grading.

**Quizzes:** There will be ten quizzes during the term. Quizzes are available through our online component, Angel. Quizzes can be taken anytime during their assigned week and have no time limit. You may take them up to two times. The last score is the one that counts!
Points: Grades will be assigned based on the total points (pts) earned as follows; 90 to 100% = A, 80 to 89% = B, 70 to 79% = C, 60 to 69% = D, and less than 60% = F.

Points are distributed as follows:

<table>
<thead>
<tr>
<th>Assignment Type</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 lab assignments @ 10 pts ea.</td>
<td>300</td>
</tr>
<tr>
<td>10 quizzes @ 30 pts ea.</td>
<td>300</td>
</tr>
<tr>
<td>Skills Projects (final exam) 6 @ 50</td>
<td>300</td>
</tr>
</tbody>
</table>

TOTAL POSSIBLE POINTS 900

Course outline: This outline is a plan for the term. It is subject to change should the need arise. Any such changes will be noted during assigned class or lab time. It is your responsibility to note changes in the syllabus schedule as presented in class or via Angel announcements during the term. Please note the rules of netiquette that will be used in this class. You can access this page by clicking here.

Lab assignments are due by midnight on the Sunday of each week’s assignment. For example, labs for Week 1 are due on or before midnight on Sunday, October 2, 2011.

Your homework is made up of homework assignments listed in your textbook. For each lesson (chapter) you will either create new or edit existing PowerPoint presentations. For example, in Lesson 1 you will create the Avoid the Flu presentation. This is part of your homework assignment for the week.

In Lesson 1, your other homework is listed at the very end of the lesson (starting on p. PPT56) under Apply Your Knowledge, Extend Your Knowledge & Make It Right. Finally, in Angel, under the Lessons -> Week 1 link, click to take that week’s quiz. You will have one quiz for each lesson we cover during the term. The quizzes are not timed and you can take the quiz 2 times. Your best score is the one that will count.

If you have ANY questions about what homework is assigned, please email me immediately. If you wait until late in the week to ask homework questions this will not extend your homework due date. Always ask questions as early in the week as possible.

Always keep a backup of your homework in your possession until I assign you a grade in the gradebook. This way if I don’t get your work, you can always send me your backup copy. Warning: your backup homework copy must have a date that is on or before the date it was due. This proves that you did the work before its due date.
You will email your work to me each week. Please see the Angel link titled “Course Assignments by Week” for how to do this.

<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
<th>Chapter Readings</th>
<th>Labs &amp; Exams</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Creating &amp; Editing a Presentation w/Clip Art</td>
<td>Chapter 1</td>
<td>Projects: Apply Your Knowledge, Extend Your Knowledge &amp; Make It Right</td>
</tr>
<tr>
<td>2</td>
<td>Enhancing a Presentation w/Pictures, Shapes &amp; WordArt</td>
<td>Chapter 2</td>
<td>Projects: Apply Your Knowledge, Extend Your Knowledge &amp; Make It Right</td>
</tr>
<tr>
<td>3</td>
<td>Reusing a Presentation &amp; Adding Media</td>
<td>Chapter 3</td>
<td>Projects: Apply Your Knowledge, Extend Your Knowledge &amp; Make It Right</td>
</tr>
<tr>
<td>4</td>
<td>Working with Information Graphics</td>
<td>Chapter 4</td>
<td>Projects: Apply Your Knowledge, Extend Your Knowledge &amp; Make It Right</td>
</tr>
<tr>
<td>5</td>
<td>Collaborating On &amp; Delivering a Presentation</td>
<td>Chapter 5</td>
<td>Projects: Apply Your Knowledge, Extend Your Knowledge &amp; Make It Right</td>
</tr>
<tr>
<td>6</td>
<td>Navigating Presentations Using Hyperlinks &amp; Action Links</td>
<td>Chapter 6</td>
<td>Projects: Apply Your Knowledge, Extend Your Knowledge &amp; Make It Right</td>
</tr>
<tr>
<td>7</td>
<td>Creating a Self-Running Presentation Using Animation</td>
<td>Chapter 7</td>
<td>Projects: Apply Your Knowledge, Extend Your Knowledge &amp; Make It Right</td>
</tr>
</tbody>
</table>
8  Customizing a Template & Handouts Using Masters  Chapter 8  Projects: Apply Your Knowledge, Extend Your Knowledge & Make It Right

9  Modifying a Presentation Using Graphical Elements  Chapter 9  Projects: Apply Your Knowledge, Extend Your Knowledge & Make It Right

10 Developing a Presentation w/Content from Outside Sources  Chapter 10  *Projects: Apply Your Knowledge, Extend Your Knowledge & Make It Right

11 Skills Project (this represents the final exam for this course)  N/A  **PPT 592 & PPT 656 Cases & Places 1,2 & 3

* Homework for Chapter 10 is due via email to your instructor no later than midnight on Sunday

**Skills Project is due via email to your instructor no later than midnight on Wednesday, Please email me only at the address listed on this syllabus! I check this email address regularly and will promptly respond to email received. During the week, I will respond within one business day. For example, if you email me on Tuesday at 2pm, I will respond back to you by Wednesday at 2pm.

On weekends, I may or may not respond depending on my personal schedule. Do not rely on a weekend response to get your work done! For example, if you email me on Friday at 9am, I will respond back to you by Monday at 9am.

All of our course documents will be kept on our UCC online component – Angel (http://angel.umpqua.edu). Download files to your USB drive and update these when you are informed of changes by your instructor.

Course policies: If you have problems completing an assignment, it is your responsibility to contact your instructor to resolve the situation. The college has a zero tolerance policy (721.1 Academic Integrity) regarding all forms of academic dishonesty. Students caught (and/or involved in) copying—or any of the other noted violations of academic dishonesty—will receive a zero (0) on that assignment, project, or test. Continued violations of this policy may result in student suspension from classes. Note that this policy specifically addresses plagiarism as it
applies to students at UCC. The policy on academic integrity is posted throughout the campus; please take the time to read it!

Students are responsible for material presented in lecture, assigned reading, activities, handouts, videos, required presentations, and class assignments. Any of these materials can and will be used by the instructor as the basis for test questions.

_The instructor retains the right to refuse non-health and/or family emergency excuses which appear to be avoidable or represent optional choices made by the student._


Counseling Center:
Any student, who feels he or she may need an accommodation for any type of disability, should make an appointment to see me during office hours or contact Disability Services in the Counseling Center.

Umpqua Community College Counseling Center provides comprehensive counseling services to assist you with career plans and academic advising as well as help to work out personal or social problems. Counselors are available to both current and prospective students in the Campus Center.

The Counseling Center, Testing Center, Job Placement & the Transfer Opportunity Program are located in the Campus Center building across from UCC’s Financial Aid Office. To contact our office you may stop by during business hours or call (541) 440-4610.

[http://www.umpqua.edu/Counsel/CCindex.htm](http://www.umpqua.edu/Counsel/CCindex.htm)

_Tutoring Services:_
Tutoring Services are available to UCC students. Contact information for UCC’s tutoring center can be found at the following Web address:

[http://www.umpqua.edu/BasicSkills/Tutor.htm](http://www.umpqua.edu/BasicSkills/Tutor.htm).

Any student who feels he or she may need an accommodation for any type of disability, please make an appointment to see me during office hours or contact Disability Services in the Counseling Center."

[http://www.umpqua.edu/disability-services](http://www.umpqua.edu/disability-services)


For more information, contact the Disabilities Services Department:

Phone (541) 440-7655

Fax (541) 440-4612, or Oregon Relay (800)735-1232
Tutoring services at UCC are FREE and available to all students on a drop in basis. Tutoring is offered in a variety of subject areas. The goal of tutoring is to promote your learning and to assist you in becoming a more capable and confident student. All peer tutors have successfully completed college classes and are anxious to share their knowledge with other students. The tutoring center is located in the Educational Skills Building (ESB) Room 15.

Tutoring Contact:
Ms. Vicki Formosa, Tutoring Coordinator
(541) 440-7733
Email: Vicki.Formosa@umpqua.edu

A tutoring schedule for the current college term is listed at the bottom of the Web page listed below.

http://www.umpqua.edu/tutoring-center

Umpqua Community College Counseling Center provides comprehensive counseling services to assist you with career plans and academic advising as well as help to work out personal or social problems. Counselors are available to both current and prospective students in the Campus Center.

http://www.umpqua.edu/tutoring-center

The Counseling Center, Testing Center, Job Placement & the Transfer Opportunity Program are located in the Campus Center building across from UCC's Financial Aid Office. To contact our office you may stop by during business hours or call (541) 440-4610.

http://www.umpqua.edu/Counsel/CCindex.htm

For assistance with homework assignments, students are encouraged to visit the Institutional Resources link in Angel, which is available via the Resources tab. Listed here you will find links to search local libraries, search newspapers and journals, You can also use one of the links to email a UCC librarian for assistance.

The ANGEL Learning Management System is compliant with ADA standards.
CIS 125R Student Introductory Activity

Post Your Introduction-
You must post something about yourself during week 1 (see Course Assignments by Week for the exact date/time details) to avoid being dropped! This is your Student Introduction Assignment. Click here to open the SIA discussion forum link.

Please post something about yourself so we can get to know you.
CIS 125R Week 1

**Chapter 1 – Creating & Editing a Presentation with Clip Art**

Microsoft PowerPoint is a great tool for you to use and one that has hundreds of different applications! In our first chapter you'll learn some introductory functions to PowerPoint, such as opening the application, adding slides, inserting clips & pictures and how to print your presentation!

A Powerpoint presentation can help you deliver a dynamic, professional-looking message to an audience. Powerpoint allows you to produce to use in an academic, business, or other environment. One of the more common uses of these slides is to enhance an oral presentation. The Powerpoint slides should reinforce the speakers message and help the audience retain the information being presented.

Have fun with this week's projects and please be sure to let me know if you have any questions! Good luck and have a great term.

**Outcomes**

- Select a document theme
- Create a title slide and a text slide with a multi-level bulleted list
- Add new slides and change slide layouts
- Insert clips and pictures into a slide with and without a content placeholder
- Move and size clip art
- Print a presentation

**Post Your Introduction-**

You must post something about yourself during week 1 (see [Course Assignments by Week](#) for the exact date/time details) to avoid being dropped! This is your Student Introduction Assignment. Click [here](#) to open the SIA discussion forum link.
Reading

• Read and do hands-on work for Chapter 1 in your book

• Click here to download this chapter's PowerPoint Presentation

Homework

• Projects: AYK(PPT 55), EYK(PPT 57) & MIR(PPT 58)

Assessment

• Click here to begin the assessment for Lesson 1

Student Introductory Assignment
Microsoft PowerPoint 2010

Chapter 1

Creating and Editing a Presentation with Clip Art
Objectives

• Select a document theme
• Create a title slide and a text slide with a multi-level bulleted list
• Add new slides and change slide layouts
• Insert clips and pictures into a slide with and without a content placeholder
• Move and size clip art
Objectives

- Change font size and color
- Bold and italicize text
- Duplicate a slide
- Arrange slides
- Select slide transitions
- View a presentation in Slide Show view
- Print a presentation
Project – Presentation with Bulleted Lists and Clip Art

(a) Slide 1 (Title Slide with Clip Art)

(b) Slide 2 (Multi-Level Bulleted List with Clip Art)

(c) Slide 3 (Title and Photograph)

(d) Slide 4 (Comparison Layout and Clip Art)

(e) Slide 5 (Closing Slide)
General Project Guidelines

• Find an appropriate theme
• Choose words for each slide
• Format specific elements of the text
• Determine where to save the presentation
• Determine the best method for distributing the presentation
Choosing a Document Theme

• Click Design on the Ribbon to display the Design tab
• Click the More button (Design tab | Themes group) to expand the gallery, which shows more Built-In theme gallery options
• Click the theme to apply
Choosing a Document Theme

Office Theme is default theme currently applied

Oriel theme
Entering the Presentation Title

• Click the label, Click to add title, located inside the title text placeholder to select the placeholder.
• Type the desired title in the title text placeholder. Do not press the ENTER key.
Entering the Presentation Subtitle Paragraph

- Click the label, Click to add subtitle, located inside the subtitle text placeholder to select the placeholder.
- Type the desired subtitle paragraph, but do not press the ENTER key.

[Image: IT IS EASY BEING GREEN Saving Energy at Home]

subtitle text entered in placeholder
Selecting a Paragraph

• Triple-click the paragraph to select
Italicizing Text

• With the text to italicize selected, click the Italic button on the Mini toolbar to italicize that text on the slide.
Increasing Font Size

• With the text selected, click the Increase Font Size button on the Mini toolbar the desired number of times to increase the font size of the selected text.
Selecting a Word

- Double-click the word to select it
Changing the Text Color

- Select the text, and click the Font Color arrow on the Mini toolbar to display the gallery of Theme Colors and Standard Colors.
- Click the desired color to change the font color.
- Click outside the selected text to deselect the word.
Adding a New Text Slide with a Bulleted List

• Click Home on the Ribbon to display the Home tab
• Click the New Slide button (Home tab | Slides group) to insert a new slide with the Title and Content layout
Adding a New Text Slide with a Bulleted List
Typing a Multi-Level Bulleted List

• Click the label, Click to add text, to select the text placeholder
• Type the first item in the bulleted list, and then press the ENTER key to type the second item
• To create a second-level paragraph, click the Increase List Level button (Home tab | Paragraph group)
• Click the Decrease List Level button (Home tab | Paragraph group) to promote a paragraph
Typing a Multi-Level Bulleted List

- Install low-flow faucets and shower heads
- Cut water consumption in half

Decrease List Level button not selected because paragraph level cannot be decreased
Selecting a Group of Words

- Position the mouse pointer immediately to the left of the first character of the text to be selected
- Drag the mouse pointer through the last character of the text to be selected
Bolding Text

• With the text to bold selected, click the Bold button on the Mini toolbar
Adding a Slide with the Title Only Layout

• Click the New Slide arrow (Home tab | Slides group) to display the Layout gallery
• Click Title Only to add a new slide and apply that layout
Adding a New Slide and Entering a Slide Title and Headings

• Click the New Slide arrow in the Slides group to display the Layout gallery
• Click Comparison
• Type the desired headings in the appropriate placeholders
Moving to Another Slide in Normal View

• Position the mouse pointer on the scroll box
• Press and hold down the mouse button and drag the scroll box up or down the vertical scroll bar to view the different slides
• When you are finished, release the mouse button
Inserting a Clip from the Clip Organizer into the Title Slide

• Click Insert on the Ribbon to display the Insert tab.
• Click the Clip Art button (Insert tab | Images group) to display the Clip Art task pane.
• Click the Search for text box in the Clip Art task pane. If necessary, delete any letters that are present and type desired search text for the clip art.
• If necessary, click the ‘Include Office.com content’ check box to select it.
Inserting a Clip from the Clip Organizer into the Title Slide

• Click the Go button so that the Microsoft Clip Organizer will search for and display all clips having the keyword(s)

• If necessary, click the Yes button if a Microsoft Clip Organizer dialog box appears asking if you want to include additional clip art images from Office.com

• Scroll the list to locate a clip you wish to insert

• Clip the clip to insert it into the slide
Inserting a Clip from the Clip Organizer into the Title Slide
Inserting a Clip from the Clip Organizer into a Content Placeholder

- Click the Clip Art icon in the content placeholder to select that placeholder and to open the Clip Art task pane
- Click the Search for text box in the Clip Art task pane, delete any letters that are present, type the desired search text in the Search for text box, and then click the Go button to search for and display all pictures having the keyword(s)
- Scroll the list to locate a clip you wish to insert
- Click the clip to insert it into the slide
Inserting a Clip from the Clip Organizer into a Content Placeholder

Adjust Your Thermostats

Furnace: 68 degrees  Water heater: 120 degrees

Click to add text

Clip keyword in Search for text box

desired clip inserted into slide

Creating and Editing a Presentation with Clip Art
Resizing Clip Art

- Click the clip to select it and display the selection rectangle
- Point to the lower-left corner sizing handle on the clip so that the mouse pointer changes to a two-headed arrow
- Drag the sizing handle diagonally until the clip is the desired size
- Release the mouse button
Resizing Clip Art
Moving Clips

- Click the object to select it
- Press and hold down the mouse button and then drag the photograph to the desired location
Duplicating a Slide

• With the slide to duplicate selected, click the New Slide arrow (Home tab | Slides group) to display the layout gallery

• Click Duplicate Selected Slides in the Oriel layout gallery to create a duplicate of the slide
Duplicating a Slide

- Clicking Duplicate Selected Slides creates a copy of Slide 1.
Arranging a Slide

- Drag the slide in the Slides pane to the desired location
Deleting Text in a Placeholder

• Position the mouse pointer immediately to the left of the first character of the text to be selected
• Drag the mouse pointer through the last character of the text to be selected
• Click the Cut button (Home tab | Clipboard group) to delete all the selected text
Deleting Text in a Placeholder
Adding a Transition between Slides

- Click the Transitions tab on the Ribbon and then point to the More button (Transitions tab | Transition to This Slide group)
- Click the More button to expand the Transitions gallery
- Click the desired transition in the Transitions gallery to apply the transition
- Click the Duration up arrow (Transitions tab | Timing group) three times to increase the transition speed
- Click the Preview Transitions button (Transitions tab | Preview area) to view the transition and the new transition time
Adding a Transition between Slides

- Click the Apply To All button (Transitions tab | Timing group) to apply the transition and the increased transition time to all slides in the presentation.
Changing Document Properties

- Click File on the Ribbon to open the Backstage view
- If necessary, click the Info tab in the Backstage view to display the Info gallery
- Click the Properties button in the right pane of the Info gallery to display the Properties menu
- Click Show Document Panel on the Properties menu to close the Backstage view and display the Document Information Panel in the PowerPoint document window
Changing Document Properties

- Type the document properties in the appropriate text boxes
- Click the Close the Document Information Panel button so that the Document Information Panel no longer is displayed
• Click the Slide 1 thumbnail in the Slides pane to select and display Slide 1
• Click the Slide Show button to display the title slide
Moving Manually through Slides in a Slide Show

- Click each slide to move through the slide show
- When the black slide appears with a message announcing the end of the slide show, click the mouse
Printing a Presentation

• Click File on the Ribbon to open the Backstage view
• Click the Print tab in the Backstage view to display the Print gallery
• Verify the printer name that appears on the Printer box Status button will print a hard copy of the document. If necessary, click the Printer Status button to display a list of available printer options and then click the desired printer to change the currently selected printer
• Click the Print button in the Print gallery to print the document on the currently selected printer
• When the printer stops, retrieve the hard copy
Printing a Presentation

(a) Slide 1

(b) Slide 2

(c) Slide 3

(d) Slide 4

(e) Slide 5
Chapter Summary

- Select a document theme
- Create a title slide and a text slide with a multi-level bulleted list
- Add new slides and change slide layouts
- Insert clips and pictures into a slide with and without a content placeholder
- Move and size clip art
Chapter Summary

- Change font size and color
- Bold and italicize text
- Duplicate a slide
- Arrange slides
- Select slide transitions
- View a presentation in Slide Show view
- Print a presentation
Chapter 1 Complete
1. **Multiple Choice**
The accompanying figure illustrates the _____ slide layout.

![Adjust Your Thermostats](image)

The accompanying figure illustrates the _____ slide layout.

2. **Multiple Choice**
The default document theme is the _____.
The default document theme is the _____.

3. **Multiple Choice**
The Themes gallery is located on the _____ Ribbon tab.
The Themes gallery is located on the _____ Ribbon tab.

4. **Multiple Choice**
The box on a slide that has a dotted or hatch-marked border and that contains the insertion point is a text _____.
The box on a slide that has a dotted or hatch-marked border and that contains the insertion point is a text _____.

5. **Multiple Choice**  
(1 points)  
When you open a new presentation, a slide with the default _____ layout appears.

6. **Multiple Choice**  
(1 points)  
By default, slides in a new presentation are in _____ orientation.

7. **Multiple Choice**  
(1 points)  
You can move the insertion point into the next text placeholder by pressing the _____ keyboard shortcut keys.

8. **Multiple Choice**  
(1 points)  
To change the font size of selected text, click the Decrease Font Size or Increase Font Size buttons located _____.

9. **Multiple Choice**  
(1 points)  
Using the_____, you can choose the arrangement of placeholders on a new slide.

10. **Multiple Choice**  
(1 points)  
You can type comments to yourself in the _____ for a specific slide while working in Normal view.
11. **True or False**  
(1 points)  
A slide show is another name for a PowerPoint presentation.  

A slide show is another name for a PowerPoint presentation.

12. **True or False**  
(1 points)  
The Mini toolbar contains the Bold, Italic, and Increase Font Size buttons.  

The Mini toolbar contains the Bold, Italic, and Increase Font Size buttons.

13. **True or False**  
(1 points)  
The Layout gallery displays 10 slide layouts with a variety of placeholders to define text and content positioning and formatting.  

The Layout gallery displays 10 slide layouts with a variety of placeholders to define text and content positioning and formatting.

14. **True or False**  
(1 points)  
Two popular electronic image formats are PDF and XPS.  

Two popular electronic image formats are PDF and XPS.

15. **True or False**  
(1 points)  
It is considered good practice to save a presentation before printing it.  

It is considered good practice to save a presentation before printing it.
16. Fill in the Blank(s)  
(1 points)

One of the more common uses of a presentation is to enhance a(n) ________________ presentation.

One of the more common uses of a presentation is to enhance a(n) ________________ presentation.

17. Fill in the Blank(s)  
(1 points)

PowerPoint initially uses the ________________ until you select a different theme, as shown in the accompanying figure.

PowerPoint initially uses the ________________ until you select a different theme, as shown in the accompanying figure.

18. Fill in the Blank(s)  
(1 points)

Some PowerPoint users create the ________________ as their last step in the design process so that it reflects the tone of the presentation.

Some PowerPoint users create the ________________ as their last step in the design process so that it reflects the tone of the presentation.
19. **Fill in the Blank(s)**
(1 points)
You can _________________________ a paragraph to select it, as shown in the accompanying figure.

20. **Fill in the Blank(s)**
(1 points)
Details about a presentation can be found in the presentation file’s _________________________.
Details about a presentation can be found in the presentation file’s _________________________.

21. **Matching**
(100 points)
Identify the letter of the choice that best matches the phrase or definition.
Identify the letter of the choice that best matches the phrase or definition.
CIS 125R

Selecting a Project

• What are you interested in?

• What is your career field of choice?

• What do you want to do after graduation?

• Who do you currently work for?

• Who do you want to work for?

• Are you involved in a local non-profit?

• Are you involved in a local church?

• Meet with the manager, leader, pastor, etc.
  o Introduce yourself and ask if there is a project they want to do
  o Look for areas where things are not working properly
  o Look for a current challenge

• Project Process
  o Define the challenge
  o Interview, research, gather data, etc.
  o Develop a hypothesis or potential solution
  o Propose a solution
  o Design a solution
  o Test your design
  o Refine your proposal

• Write the Report
  o A – Impress me – solve a problem – demonstrate excellence
  o B – Good project – weak solution – poor report construction
  o C – Yep, you did a project – weak write-up, the world won’t be improved
  o D – Did a process not a project – poor report – no real change proposed
  o F – No report, no participation, gave up
Layered Network Design Simulation

Objective
Explain the need to design a hierarchical network that is scalable.

Scenario
As the network administrator for a very small network, you want to prepare a simulated-network presentation for your branch manager to explain how the network currently operates.

The small network includes the following equipment:
- One Cisco 2911 series router
- One Cisco 3560 switch
- One Cisco 2960 switch
- Four user workstations (PCs or laptops)
- One printer

Resources
- Packet Tracer software

Directions
Step 1: Create a simple network topology using Packet Tracer software. Place the devices at the appropriate levels of the Cisco three-layer hierarchical model design, including:
  a. One Cisco 2911 series router
  b. One Cisco 3560 switch
  c. One Cisco 2960 switch
  d. Four user workstations (PCs or laptops)
  e. One printer

Step 2: Using Packet Tracer’s drawing tool and indicate the hierarchical layers with different color coding and labels:
  a. Access layer
  b. Distribution layer
  c. Core layer

Step 3: Configure the network and user devices. Check for end-to-end connectivity.

Step 4: Share your configuration and hierarchical network design Packet Tracer file with another student, group, the class, or the instructor.
Lesson 2 – Enhancing a Presentation

In our visually-oriented culture, audience members enjoy viewing effective graphics. Whether reading a document or viewing a Powerpoint presentation, people increasingly want to see photos, artwork, graphics and a variety of typefaces. Researchers have known for decades that documents with visual elements are far more effective than those that consist of only text because illustrations motivate audiences to study the material. People remember at least 1/3 more information when the document they are seeing or reading contains visual elements. These elements help clarify and emphasize details so that they can appeal to people with different backgrounds, reading levels, attention spans and motivations.

Outcomes

- Change theme colors
- Insert a picture to create a background
- Format slide backgrounds
- Insert and size a shape
- Add text to a shape
- Apply effects to a shape
- Change the font and add a shadow
- Format pictures
- Apply a WordArt style
- Format WordArt
- Format text using the Format Painter

Reading

- Read and do hands-on work for Chapter 2 in your book
- Click here to download this chapter's PowerPoint Presentation
**Homework**

- Projects: EYK(PPT 123), AYK(PPT126) & MIR(PPT129)

**Assessment**

- Click [here](#) to begin the assessment for Chapter 2
1. Studies show people remember at least _____ more information when the document they are seeing or reading contains visual elements.
   A) one-fourth
   B) one-half
   C) one-fifth
   D) one-third
   Correct answer(s): D

2. By default, PowerPoint capitalizes _____.
   A) coordinating conjunctions
   B) articles
   C) the first word of each paragraph
   D) all titles
   Correct answer(s): C

3. _____ colors are designed as colors for secondary features on a slide.
   A) Background
   B) Text
   C) Accent
   D) Hyperlink
   Correct answer(s): C

4. Which of the following contextual Ribbon tabs appears when you select a picture on a slide?
   A) Shape Tools Format
   B) Drawing Tools Format
   C) Picture Tools Format
   D) Clip Art Tools Format
   Correct answer(s): C
5. You can insert a picture saved in a file into a slide by clicking the Insert Picture from File button on the _____.
   A) (Home tab | Illustrations group)
   B) (Insert tab | Illustrations group)
   C) (Home tab | Images group)
   D) (Insert tab | Images group)
   Correct answer(s): D

6. Which of the following style elements are included in picture styles?
   A) edges
   B) shapes
   C) borders
   D) all of the above
   Correct answer(s): D

7. The Picture Effects button is located on the _____, as shown in the accompanying figure.
   A) (Picture Tools Format tab | Picture Styles group)
   B) (Drawing Tools Format tab | Picture Styles group)
   C) (Design Tools Format tab | Picture Styles group)
   D) (Formatting Tools tab | Picture Styles group)
   Correct answer(s): A

8. Which of the following PowerPoint features allows you to see what a picture border color change will look like before you apply it?
   A) Live preview
   B) Color preview
   C) Border preview
   D) Slide preview
   Correct answer(s): A
9. _____ is the content that makes up the interior of a shape, line, or character.
A) Fill
B) Color
C) Texture
D) Grain
Correct answer(s): A

10. You can _____ anywhere on a slide and then click Format Background to open the Format Background dialog box, shown in the accompanying figure.
A) click
B) triple-click
C) right-click
D) double-click
Correct answer(s): C

11. Researchers have known for decades that documents with visual elements are more effective than those that consist of only text.
A) True
B) False
Correct answer(s): True

12. WordArt text can enhance the visual appeal of any presentation, so you can use it freely.
A) True
B) False
Correct answer(s): False

13. Some document themes use the All Caps text effect which converts the uppercase text you type to lowercase.
A) True
B) False
Correct answer(s): False
14. Accent colors in a document theme are designed as colors for primary features on a slide.
A) True
B) False
Correct answer(s): False

15. Clips and photographs you see on Web pages are not covered by copyright law.
A) True
B) False
Correct answer(s): False

16. You can double-click a picture to display the Picture Tools and Format tabs.
A) True
B) False
Correct answer(s): True

17. When you change the height of a photo, PowerPoint automatically changes the width to maintain the photo’s proportions between height and width.
A) True
B) False
Correct answer(s): True

18. Once you resize a photograph, it cannot be returned to its original size.
A) True
B) False
Correct answer(s): False

19. To make a slide background appear on all slides in a presentation, click the Format All button in the Format Background dialog box.
A) True
B) False
Correct answer(s): False
20. If you have made many changes to a slide’s background, you can start over by clicking the Reset Background button in the Format Background dialog box.

A) True
B) False

Correct answer(s): True

21. Identify the letter of the choice that best matches the example.

A. modernist movement
B. Textures gallery
C. six accent colors
D. CTRL+SHIFT+F
E. Format Painter
F. ESC
G. picture effects
H. changed in predefined percentages
I. CTRL
J. view formatting changes before you apply them
CIS 125W Course Outline - Microcomputer Applications - Word Processing
Course Assignments by Week

Your first assignment in this class is to introduce yourself to your classmates and instructor. By Wednesday of week one, you must post something about yourself in the SIA (Student Introductions Assignment) forum. Look at what I posted and post something similar about yourself. This is a standard 25 point posting. To get full credit for this first exercise it must be posted by midnight, Wednesday, Sept. 26. Spend the remainder of the week looking over the other postings and hopefully finding someone in the class with interests similar to yours. Discussion questions (DQs) are a key online learning component. These help focus the week’s studies, provide you with an opportunity to show what you’ve learned in writing, learn from fellow students, and learn from your instructor.

Homework due dates: All assignments are due on or before midnight Sunday each week. For example, Week 1 begins on Monday, September 24, 2012. Homework assigned for Week 1 is due no later than midnight Sunday, Sept 30, 2012. No late work will be accepted! An exception may be made to this if PRIOR arrangements have been made with the instructor as described in the Course Expectations and Assignment Deadlines section of the Syllabus. Under no circumstances will homework be accepted after the week's work has been graded and grades posted.

Reading consists of studying, taking notes, and performing all Hands-on exercises found in each Tutorial (chapter) assigned. For example, in Tutorial 1, on page WD-4, find the section titled "To start Word". You need to manually perform all of the steps listed there. Do this for every reading assignment in this course! The homework that you will be assigned for each week may include the results from some of these Hands on Exercises or will come from the exercises found at the end of the Tutorials. Refer to the Syllabus for additional information. Review the chapter summary on page WD-53. You will also find links to PowerPoint presentations for each Tutorial in the Reading section of each week's folder.

Homework that will be submitted to your instructor for evaluation consists of any assigned Hands on Exercises, Review Assignments and Case Problems found in each Tutorial and your discussion question submissions. Refer to the detailed weekly assignments in each weekly folder to be sure you know which projects are assigned.

How to turn in homework:

1. Be sure that all of your files are named correctly as instructed in each assignment. If files are misnamed, they will not be graded because I look for specific files to grade.
2. Place all of your files for a given week in one compressed (Zipped) folder (only one folder for each week's work). If you are unsure how to create a zipped folder, review the YouTube Video Instruction under the "How To - Video instructions . . ." link under Lessons. Do not use a compression routine other than Windows Compression, which comes with your Windows system.
3. Name the Compressed folder with your course number, the week number and your name. For example, week one’s folder name would be 'CIS125W Week 1 – Your Name.zip'. (The folder must have the .zip extension.)
4. Upload your compressed Folder to your weekly Drop Box (one homework submission per week).
5. Complete your subject line with your course number, the week number and your name. For example, week one’s subject would be “CIS125W Week 1 – Your Name”.


6. **Only one zipped folder can be uploaded to the drop box per week.** Do NOT wait until the last minute to upload your work! The weekly folder and the drop box will close Sunday at midnight and you will be unable to submit your work.

7. **DO NOT send homework via email as it will not be accepted or graded.**

The schedule that follows represents a brief overview for the work that you will do this course during the term. But, be sure to open, read and follow the weekly assignment document for this gives you the detail information that you will need to complete the assignments. This Assignments by Week document is our plan for the term. If unexpected events occur that interfere with the completion of this plan, it will be changed. You will be notified of such change with an Announcement.

**Week 1: Sept. 24 - 30**
If you don’t complete your SIA and FM Tutorial homework by midnight Wednesday you may be dropped from the course on Thursday of week 1.

- **SIA due by Wednesday, April 4th at midnight during week one!**
- Office Tutorial - Office 2010 & Windows 7: Read and do hands-on work
- Chapter 1 - Creating, Formating, and Editing a Word Document with Pictures: Read and do hands-on work
- **SIA:** Introduce yourself to your instructor and your classmates.

**Week 2: Oct. 1 - 7**
WD Chapter 2 - Creating a Research Paper with Citations and References: Read and do hands-on work
- **DQ 1**

**Week 3: Oct. 8 - 14**
WD Chapter 3 - Creating a Business Letter with a Letterhead and Table: Read and do hands-on work
- **DQ 2**

**Week 4: Oct. 15 - 21**
WD Chapter 4 - Creating a Document with a Title Page, Lists, Tables, and a Watermark: Read and do hands-on work
- **DQ 3**

**Week 5: Oct. 22 - 28**
- WD Chapter 5 - Using a Template to Create a Resume and Sharing a Finished Document: Read and do hands-on work
- **DQ 4**
- **Mid Term Exam: Online, taken through Angel link** - May 2nd, 6pm-midnight
- Mid Term Assignments (two assignments in addition to the Mid Term exam)

**Week 6: Oct. 28 - Nov. 4**
WD Chapter 6 - Generating Form Letters, Mailing Labels, and a Directory: Read and do hands-on work
- **DQ 5**

**Week 7: Nov. 5 - 11**
WD Chapter 7 - Creating a Newsletter with a Pull-Quote and Graphics: Read and do hands-on work
DQ 6

Week 8: Nov. 12 - 18
WD Chapter 8 - Using Document Collaboration and Integration Tools: Read and do hands-on work
DQ 7

Week 9: Nov. 19 - 25
WD Chapter 9 - Creating a Reference Document with a Table of Contents and an Index: Read and do hands-on work
DQ 8

Week 10: Nov. 26 - Dec. 2
WD Chapter 10 - Creating a Template for an Online Form: Read and do hands-on work
DQ 9

ALL homework is due via the weekly drop box no later than midnight Friday, November 30, 2012

Friday, November 30, 2012
- Final Exam: Online, taken through Angel link
CIS 125W Syllabus: Microcomputer Applications -- Word Processing

Instructor: Jacinda Sullivan

Office: Off Campus

Phone: Please use e-mail, in an emergency leave a message for me at 541-440-4605

E-mail: Send all course e-mail to the instructor via the Angel Communicate facility (jacinda.sullivan@umpqua.edu)

Course: CIS 125W Online, 3 credits                  CRN: 41674

Online: http://angel.umpqua.edu/

Class time/date: Online

Required Text:


Your text has a companion Web site, which you are welcome to visit by clicking here.

You will find Student Data Files, PowerPoint Presentations and Internet Assignments for selected Tutorials on this Web site.

Supplies and Equipment:

1. Microsoft Office 2010 Full Version which may be purchased through the UCC book store for $17.00;
2. USB flash drive/jump drive -- 2 GB or better;
3. Fast Internet Access from your normal work site (you may use the computers on the campus);
4. A computer running a current version of Windows.

The text assumes Windows 7 but you may use Windows Vista or Windows XP Pro with SP2. A few of the illustrations in the book may not match what you see on your screen exactly. If you are running Windows XP Pro or Windows Vista, you assume responsibility for translating instructions provided for Windows 7 to your operating environment.

The book listed above is available in the UCC bookstore. If attempting to buy your books from an on-line vendor be sure that you get the correct version and format and that you receive it before the start of class. Please visit the bookstore for more information.
SKILLS YOU SHOULD ALREADY HAVE TO TAKE THIS ONLINE CLASS:

Prerequisite: The student should have well-developed keyboarding skills. These skills could be developed through hands on experience or by taking a formal keyboarding class such as OA121, Keyboarding.

In addition, you should already have basic computer skills before even considering taking an online class. If you cannot functionally use your computer ie.: send email with attachments, use the Internet and the World Wide Web, locate and manage files, create compressed (zipped) folders, load and use applications, you should **NOT** take this online class. Your instructor expects you to already know these things and will not be able to ‘bring you up to speed’ in time to be successful in a 10-week course. If after reviewing the Tutorials (chapters) in the text you have concerns about the above, please communicate with your advisor about taking this class at another time.

COURSE DESCRIPTION AND OUTCOMES: This course is designed as an introduction to computers, Microsoft word processing software, and their application in business. The course is lab-oriented and will focus on using a modern word processor, in this case Microsoft Office 2010 - Word. Reading material will be in support of the “practical use” assignments.

Upon completion of this course, you should be able to:

Describe what a computer is and give examples of its use in home, business, and the educational environments.
Describe the purpose and operation of the Windows Operating System.
Describe the components of the MS Office suite and discuss how to install it.
Start and stop a word processor, MS Office 2010 - Word in this case.
Use Word to create, edit and format a document.
Use the features of Word to save and print documents in a variety of formats.
Effectively use Word's online and built-in help program.
Use Word tools to produce correct, professional quality documents.
Plan and design effective personal or business documents.

COURSE WORK: You will complete and submit homework assignments and answer weekly Discussion Questions (DQs), check your grades and read announcements in Angel, which represents UCC’s online classroom environment. Be sure that you review the Weekly assignment document for more detailed information on each week's assignments. In some cases I will give you hints about how to complete a particular assignment or I may ask you to stop before the end of a particular assignment. No late work will be accepted after that homework has been graded. An exception may be made to this if PRIOR arrangements have been made with the instructor as described in the Course Expectations and Assignment Deadlines section of this document. **Under no circumstances will homework be accepted after the week's work has been graded and returned to the class.**

Discussion questions: (DQ's) are an important component of online learning. This is how you as a student establish a "Classroom Relationship" with the rest of your classmates. In order for this to work as a "Discussion" you must post your answer to the DQ - your original response, in your own words - no later than **WEDNESDAY** by midnight of each week. Then, you must post at least other two thoughts (comments) some time before Sunday night at midnight. Review other student’s responses and join in
the discussion. Look at responses to your original posting and feel free to reply to these also. (But be nice!)

Each DQ will be worth 25 points. A DQ may have more than one part. Your original post must address all parts of the Discussion Question. Your subsequent responses to your classmates may address only one part of their original post. So! To get full credit each week you must post a total of three times - one original response and two more responses for that DQ. If you post one time, you earn a maximum of 15 out of 25 points for that DQ. Then, each of your two subsequent posts is worth up to 5 more points per DQ. Refer to the DQ Grading Rubric for additional information. I expect that you answer the DQ in your own words (not copied from another classmate or anywhere else) and respond to at least two of your classmates (three posts per DQ). Address your responses to your classmate by name. Opinions should be respected and please use online etiquette (Netiquette) when posting. Grading will be based on substantive participation.

As your first DQ assignment, follow this link to the Forum Posting area and enter your Introductory Student information: Student Introductory Assignment (SIA). All of your posts should be substantive. Tell us something about your background, your goals and something special about you. If this initial post is not completed by Wednesday, June 27th, you may be dropped from the class!

Reading Assignments: When your assignment is to read, you are to read the Lesson and at the same time do all of the Hands-on-Exercises. For example, in your textbook, find the start of Chapter 1 on page WD-1. You are expected to read the objectives and the overview of the Case that will be used in the chapter. Then, on page WD-4 (open the book and check it out now), find the section titled "To start Word". You need to manually perform all of the steps listed there. Do this for every reading assignment in this course! The homework that you will be assigned for each week is found at the end of the chapters.

Course Expectations and Assignment Deadlines: Students should plan to spend approximately 12-16 hours per week working on assigned materials and reading. Each week some time will be spent working with Windows and Microsoft Word. Weekly assignments are due in the weekly Drop Box by midnight Sunday of the relevant week. All files submitted for evaluation must be in the Office 2010 format (.docx). Solutions created using other versions of Word or other word processors will not be graded. Please send all course email to the instructor's Angel e-mail address as directed above. Do not send email using any other email address unless you are specifically directed to do so. The course has an expectation that students are able to manage their time in such a way as to ensure timely submission of all assignments. The course uses a pace and process which builds knowledge and skills from week to week. Once an assignment closes there will be no late submissions accepted unless the reason for the late submission falls into one of the three allowed course absence areas. In order to apply for a time extension on an assignment you must fall into one of the following three scenarios and you must provide the required documentation. The request along with the supporting material must be submitted to the instructor’s Angel email. Supporting documentation should be scanned and attached to the email. If you are unable to scan and attach your documents please contact your instructor for other submission options. The following scenarios are the only categories which may be used in requesting permission for a late assignment submission:
1. Student is sufficiently ill or hospitalized for more than three days during any week of the term. Student must submit a copy of a doctor’s note or a copy of the hospital or emergency room admittance form. A copy of the note or form must accompany the request.

2. Student seeks and is granted assistance from either the UCC counseling center or the UCC disability services office. If you are feeling overwhelmed or lost in the school process you should seek support from these groups. In this case the UCC department will send notification to the instructor.

3. Student encounters a death in the immediate family. The student must submit a copy of the death notice and an explanation for the amount of time away from school.

All requests for assignment time extension will be reviewed by the instructor. The instructor reserves the right to modify or change the terms of the late assignment policy. All late assignment requests are reviewed and considered at the instructor’s sole discretion.

Failure to read and understand the course syllabus, failure to read and understand the course deadline, failure to plan and allow sufficient time for the assignments will not be considered for time extensions.

Technical issues and Angel platform issues will rarely be accepted as reasons for time extension. In almost all cases the assignments are open and available for one full week. Time restricted tests are always open for at least six hours. Students who wait until the last hours of the last day of an assignment and encounter technical difficulties will not be granted time extensions. For consideration of a technical time extension the student needs to demonstrate that they were attending class regularly and/or logged into the Angel system early and often during the assignment weeks. In general, technical problems encountered after 6:00 PM on Sunday will not be accepted as an excuse for not meeting the submission deadline.

I do not have an office on campus. I will be available to answer questions via email Monday - Friday. I may be available and check email on some Saturdays but I will not be available anytime on Sundays. If you have questions be sure to send me an email early in the week. DO NOT WAIT UNTIL SUNDAY! Please allow one business day for me to respond to email before sending another email about the same subject.

Homework Assignments:

Please carefully read the following instructions as you will be directed back to this information if you have questions about doing and submitting your homework.

All Hands-on Assignments will come from material in each Chapter. At the end of each chapter, you will find a number of assignments with increasing degrees of difficulty. These start with the Apply Your Knowledge section after the chapter's summary section. You will be assigned a selection of these problems to complete and submit for evaluation by your instructor. Each chapter also contains a number of Hands on Exercises (HE’s) as part of the unit's learning material. It is imperative that the students read and complete these HE’s if they are to be successful in completing the assigned problems. In some cases part of these hands on exercise solutions may be required for instructor evaluation. Refer to the individual week description to be sure that you know exactly what is required for each week’s submission.
You are required to use good grammar, capitalization, punctuation and good writing skill. This is part of your grade. You are not texting or tweeting. You are using the US version of the English language to communicate. That is the only way input will be accepted!

**Exams:**
There will be an online, timed, mid term exam that will be available during the 5th week of the term. There is also an online, timed, final exam for this class. Each of these will be similar in format and will have several multiple choice questions dealing with the basic concepts covered in the class and several hands on projects that will demonstrate the students grasp of the performance aspects of the class. The two exams will be timed and will be due by midnight the day assigned.

**Grading:**
Completed homework is due by midnight Sunday of the week assigned. Scores on this work will be accumulated throughout the term. Final grades are based on accumulated total points. You may follow your progress by accessing the online grade book from your Angel account. To view your current grade, log in to Angel, and click Report. Your grade book will display on the screen along with instructor comments on each assignment (to the far right side of the screen).  

Final grades will be assigned based on the total points earned as follows; 90 to 100% = “A”, 80 to 89% = “B”, 70 to 79% = “C”, 60 to 69% = “D”, and less than 60% = “F”. See the Homework Grading Rubric for more information regarding grading.

Graded components in CIS125W are:

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hands on Assignments</td>
<td>56.8%</td>
</tr>
<tr>
<td>Discussion Questions</td>
<td>20.5%</td>
</tr>
<tr>
<td>Mid Term Exam</td>
<td>13.6%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>9.1%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100.0%</strong></td>
</tr>
</tbody>
</table>

I attempt to grade homework weekly (I grade the previous week's work on Tuesday through Sunday of the following week) and provide you feedback about each individual assignment you submit for grading. I do this by replying to the homework that you have placed in the drop box with an e-mail containing my comments and your grade for that assignment.

**Getting Started:** Verify that you are running in a valid Windows environment (Vista, XP Pro or 7), that you have the Office 2010 software installed and that you have a functioning high speed Internet connection. Lacking any one of these means you will not be successful in this class.

Under the Lessons tab in Angel (at the top of this window), locate the link to **Week 1**. Click on this link. You will see displayed a detailed description of the material to be studied, the expected outcomes, the projects assigned and the points available for each project. You will also find a link to the discussion question for the week. In order to eliminate confusion in the assignments, always refer to this material for your current week. Before attempting to complete the assigned homework, read/study the assigned Tutorials. Week 1 will cover the Office 2010 & Windows 7 concepts and skills Tutorial and Tutorial 1 for Word. These are fairly short "Chapters" but don't put off getting started. Remember! You need to invest
12 to 16 hours per week of assigned reading and homework in this class and you can't do all of this starting on Sunday at noon!

**Student Data Files:** You will need to have your student data files copied to your flash drive. You will use the student data files to complete homework assignments from this book. **In other words, you can't study or do your homework without your student data files.** You can acquire these files by downloading them from the publisher's web site. Click [here](#) to open a new browser window so that you can download this file. All of your student data files are in one file, which is approx. 24 MB in size. This will open the web site for your text. Click the Data Files for Students link in the left navigation pane and then click the file named 1439079005_280965.exe. This is a self extracting zipped folder which contains all of the data that you need to complete the homework for a given chapter. Double click on the file to run it and extract its contents someplace on your computer where you can find it. (Your flash drive is a good choice!) Copy the entire set of data files to your flash drive so you have all of the files that you will need for the entire term.

**Course Policies:**
Students are expected to work independently on materials submitted for grading. If you have problems completing an assignment, it is your responsibility to contact your instructor immediately to resolve the situation. The college has a zero tolerance policy (721.1 Academic Integrity) regarding all forms of academic dishonesty. Students caught (and/or involved in) copying—or any of the other noted violations of academic dishonesty—will receive a zero (0) on that assignment, project, or test. Continued violations of this policy may result in student suspension from classes. Note that this policy specifically addresses plagiarism as it applies to students at the UCC. The policy on academic integrity is posted throughout the campus and on the UCC web site — please take the time to read it!

Assignments are due on **Sunday** at midnight of the current week specified in the assignment file. It is the student’s responsibility to be aware of these deadlines.

Students are responsible for material presented online, assigned readings, activities, handouts, videos, and class assignments. Any of these materials can and will be used by the instructor as the basis for test questions.

**If You Are Having Trouble with Angel:**
If you are having difficulties with Angel, please contact the UCC Help Desk at 440-7808 between 8am-5pm or email HelpDesk@umpqua.edu or the **Center for Innovative Learning (CIL)** 541-440-7685 or email us: jeanine.lum@umpqua.edu. If you are having difficulties with the course, please email your instructor using the Communicate tab at the top of the browser window.

**Student Notice:**
The UCC is committed to supporting all students. Any student who feels he or she may need an accommodation for any type of disability should make contact with the Disability Services Office in the Advising and Career Service Center of the Center Building. If you plan to use academic accommodations for this course, please contact your instructor as soon as possible to discuss your needs. Accommodations are not retroactive; they begin when the instructor receives the “Approved Academic Accommodations” letter.

To request academic accommodations for a disability, please contact Disability Services at:

[http://www.umpqua.edu/disability-services](http://www.umpqua.edu/disability-services)
For more information, contact the Disabilities Services Department:
Phone (541) 440-7655
Fax (541) 440-4612, or
Oregon Relay (800) 735-1232

Tutoring services at the UCC are FREE and available to all students on a drop in basis. Tutoring is offered in a variety of subject areas. The goal of tutoring is to promote your learning and to assist you in becoming a more capable and confident student. All peer tutors have successfully completed college classes and are anxious to share their knowledge with other students. The tutoring center is located in the Educational Skills Building (ESB) Room 15.

Tutoring Contact:
Ms. Vicki Formosa, Tutoring Coordinator
(541) 440-7733
Email: Vicki.Formosa@umpqua.edu

A tutoring schedule for the current college term is listed at the bottom of the Web page listed below.

http://www.umpqua.edu/tutoring-center

Umpqua Community College Counseling Center provides comprehensive counseling services to assist you with career plans and academic advising as well as help to work out personal or social problems. Counselors are available to both current and prospective students in the Campus Center.

http://www.umpqua.edu/counseling-center

The Counseling Center, Testing Center, Job Placement & the Transfer Opportunity Program are located in the Campus Center building across from UCC's Financial Aid Office. To contact our office you may stop by during business hours or call (541) 440-4610.

http://www.umpqua.edu/counseling-center

For assistance with homework assignments, students are encouraged to visit the Institutional Resources link in Angel, which is available via the Resources tab. Listed here you will find links to search local libraries, search newspapers and journals, You can also use one of the links to email a UCC librarian for assistance.

The ANGEL Learning Management System is compliant with ADA standards.
CIS 125W Week 1 Lesson

Week 1 Windows File Management, Getting Started with MS Office and Creating a Document with Word

This week's chapters - and there are two of them - review the concepts of using Windows File Management to save, name, and manage the files that you create on your computer system. They also give a quick overview of the MS Office 2010 Suite. This material is presented using graphic illustrations taken from a Windows 7 computer system so you may find some visual differences from what you see on your computer if you are running in a Windows XP or Windows Vista environment. You will also get started using Word to create some simple documents. Unless you have significant experience using Word or a similar word processor, it is very important that you read the chapters and do the hands on exercises in the chapters. MS Word 2010 has a totally new interface and many new functions, when compared to Word 2003. You need to begin learning how to use them in this week's exercises!

Upon completion of this week's material the student should be able to:

- Create, name, copy, move and delete folders
- Create, name and save files to folders
- Create and use Compressed (Zipped) folders
- Locate and start programs from the Microsoft Office Suite
- Use the ribbons, tabs and buttons of the new Office user interface
- Use the Office help menus and facilities
- Locate an attached printer and print a file
- Safely close a file
- Plan a simple document
- Create a new document
- Move around in a document
- Perform simple editing tasks using correct, undo and redo
- Use Autocomplete
- Change a documents line and paragraph spacing
- Save, preview and print a document

Reading:

- If you do not already have your Student Data Files for the Managing Your Files Tutorial, you may download them [here](#)
- Read and do hands on exercises in the Office Chapter (OFF 1 - OFF 51) "Office 2010 and Windows 7: Essential Concepts and Skills"
• Read and do hands on exercises in the Word 2010 Chapter (WD 1 - WD 53) "Creating, Formatting and Editing a Word Document with Pictures"
• View the Word 2010 Chapter 1 PowerPoint Presentation
• View the Word 2010 Chapter 1 Flash Presentation

Assignments:
You must post your SIA by midnight Wednesday or you may be dropped from the course!

• Post your Student Introductions Assignment (SIA) due as soon as possible after class begins but no later than midnight Wednesday of the first week! THIS IS REQUIRED OR YOU MAY BE DROPPED FROM THE COURSE ON THURSDAY!
• Homework due for Office Chapter:
  o OFF p. 53 "Make it Right" assignment. You do not need any data files to complete this assignment. Be sure that you save your completed work and that each folder is named as directed. Place your folders in your Week 1 homework zipped folder. Due by midnight Sunday.
• Homework due for Word Chapter 1:
  o WD 58 pp. 58-60 "Lab 1: Creating a Flyer with a Picture". Be sure that you save your completed document and that it is named as directed and include in your Week 1 homework folder. Due by midnight Sunday.
• Upload your Week 1 homework zipped folder with both homework assignments enclosed to the Week 1 Drop Box.

Reminder:

If you have not already done so you might wish to review the YouTube videos dealing with creating compressed folders.

You can access the YouTube videos by clicking here!

• Student Introductory Assignment
  o
  o
  o
  o
  o
• Week 1 Drop Box

Upload your week 1 zipped folder here
Angel Discussion Question 1:

It has been said that no matter what the document, ultimately the thing that it represents most is the individual or individuals who created it. What does this mean to you as a student? What will it mean to you as a professional after graduation? Post your responses in the Week 2 Discussion Forum.
CIS 125W Chapter 1 Assessment

1.
The default view in Word is ____.
   - A) Print Layout view
   - B) Headline view
   - C) Web Layout view
   - D) Outline view

2.
To enter a blank line into a document, press the ____ key without typing any text on the line.
   - A) CTRL
   - B) ALT
   - C) ENTER
   - D) ESC

3.

Adorable, loving, friendly, well-behaved dog found:
early Friday morning, June 1, wandering on the bike trail at Filcher Park in Hampton Township.

Tan color with patches of white on his chest.

Male, adult cocker spaniel.

Green and silver collar with the name, Bailey, on the tag.
The paragraph mark (¶) as shown in the accompanying figure is a formatting mark that indicates where the _____ was pressed.

☐ A) TAB key
☐ B) SPACEBAR
☐ C) ENTER key
☐ D) SHIFT key

4.
Press the ENTER key in all of the following circumstances EXCEPT _____.

☐ A) to insert a blank line into a document
☐ B) when the insertion point reaches the right margin
☐ C) to begin a new paragraph
☐ D) in response to prompts in Word dialog boxes

5.
When Word flags a possible spelling or grammar error, it also changes the Spelling and Grammar Check icon to a _____.

☐ A) green X
☐ B) green check mark
☐ C) red X
☐ D) red check mark

6.
If a flagged word is spelled correctly, right-click it and then click _____ on the shortcut menu to instruct Word not to flag future occurrences of the same word in this document.

☐ A) Not a Mistake
☐ B) Correct Spelling
☐ C) Do Not Correct
☐ D) Ignore All
7.
To move left one word with the keyboard, press the ____ key(s).

A) HOME  
B) CTRL+LEFT ARROW  
C) ALT+CTRL+LEFT ARROW  
D) ALT+LEFT ARROW

8.
To move to the beginning of a line with the keyboard, press the ____ key(s).

A) LEFT ARROW  
B) CTRL+HOME  
C) HOME  
D) PAGE UP

9.
To move to the end of the document, press the _____ key(s).

A) DOWN ARROW  
B) END  
C) CTRL+DOWN ARROW  
D) CTRL+END

10.
To move to the right one word, press the ____ key(s).

A) ALT+RIGHT ARROW  
B) F1  
C) CTRL+RIGHT ARROW  
D) RIGHT+ARROW

11.
To move up one paragraph, press the ____ key(s).

- A) F1
- B) ALT+UP ARROW
- C) UP ARROW
- D) CTRL+UP ARROW

12.
To move down one paragraph, press the ____ key(s).

- A) ALT+DOWN ARROW
- B) CTRL+DOWN ARROW
- C) DOWN ARROW
- D) F1

13.
To move to the bottom of a document window, press the ____ key(s).

- A) ALT+CTRL+PAGE DOWN
- B) CTRL+PAGE DOWN
- C) ALT+PAGE DOWN
- D) PAGE DOWN

14.
To move to the top of a document window, press the ____ key(s).

- A) CTRL+PAGE UP
- B) ALT+CTRL+PAGE UP
- C) PAGE UP
- D) ALT+PAGE UP

15.
When you use the keyboard to scroll to a different position in the document, the ____ automatically moves when you press the desired keys.
16. Word includes a variety of document _____ to assist you with coordinating these visual elements in a document.

- A) layouts
- B) formats
- C) themes
- D) graphs

17. _____ formatting is the process of changing the way letters, numbers, punctuation marks, and symbols appear on the screen and in print.

- A) Document
- B) Character
- C) Paragraph
- D) Object

18. The _____, or typeface, defines the appearance and shape of letters, numbers, and special characters.

- A) font
- B) font size
- C) point
- D) paragraph formatting

19. On most computers, the default font size in Word is _____.
20. A(n) ____ paragraph is a paragraph that begins with a dot or other symbol.
   - A) headline
   - B) centered
   - C) bulleted
   - D) indexed

21. The file type ____ is a Word 2010 document.
   - A) .doc
   - B) .docx
   - C) .dot
   - D) .doct

22. To select nonadjacent items, select the first item as usual, press and hold down the ____ key, and then while holding down the key, select the additional items.
   - A) HOME
   - B) F1
   - C) CTRL
   - D) ALT

23. Which of the following colors suggests neutrality?
24. With more than ____ predefined color schemes, Word provides a simple way to select colors that work well together.

A) 15  B) 20  C) 30  D) 40

25. You can select characters by using the ____ key(s).

A) SHIFT+RIGHT ARROW  B) CTRL+SHIFT+DOWN ARROW  C) SHIFT+END  D) SHIFT+UP ARROW

26. You can select a document by using the ____ key(s).

A) SHIFT+HOME  B) CTRL+A  C) SHIFT+END  D) CTRL+SHIFT+END

27. You can select a paragraph by using the ____ key(s).
28. You can select multiple paragraphs by using the ____ key(s) repeatedly.

A) CTRL+END
B) SHIFT+HOME
C) CTRL+SHIFT+DOWN ARROW
D) CTRL+SHIFT+END

29. You can select a word by using the ____ key(s).

A) CTRL+SHIFT+LEFT ARROW
B) CTRL+A
C) SHIFT+RIGHT ARROW
D) CTRL+W

30. You can select multiple words by using the ____ key(s) repeatedly.

A) CTRL+A
B) CTRL+SHIFT+RIGHT ARROW
C) SHIFT+RIGHT ARROW
D) CTRL+SHIFT+END

31.
The small squares and circles around a selected graphic, as shown in the accompanying figure, are called ___ handles.

- A) sizing
- B) shape
- C) base
- D) dimension

32.
To see the height and width of the currently graphic, as shown in the accompanying figure, look in the ____ group on the Picture Tools Format tab.

A) Measurements
B) Options
C) Size
D) Dimensions

33.

To center a page's contents vertically between the top and bottom margins, click the Page Setup Dialog Box Launcher, click the ____ tab, click the vertical alignment box arrow, click Center in the list, and then click the OK button.

A) Layout
B) Alignment
C) Position
34. _____ are types of changes that occur when text has been omitted from a document and must be inserted later.

A) Additions  
B) Deletions  
C) Modifications  
D) All of the above

35. To delete an incorrect character in a document, simply click next to the incorrect character and then press the ____ key(s) to erase to the left of the insertion point.

A) CTRL+HOME  
B) DELETE  
C) BACKSPACE  
D) END

36. To delete an incorrect character in a document, simply click next to the incorrect character and then press the ____ key(s) to erase to the right of the insertion point.

A) CTRL+HOME  
B) DELETE  
C) BACKSPACE  
D) END

37. _____ are words or phrases that describe a document.

A) Metakeys  
B) Enhanced ScreenTips
38. ___ is another term for document properties.

- A) Metadata
- B) Key terms
- C) Enhanced text
- D) Indices

39. To close the ____ view, click File on the Ribbon or click the preview of the document in the Info gallery to return to the document window.

- A) Outline
- B) Backstage
- C) Web Layout
- D) Both a and b

40. In Word, you can create electronic image files through the ____ tab in the Backstage view.

- A) PDF
- B) XPS
- C) Print
- D) Both a and b

41. **Modified Multiple Choice**

Using Word, you easily can change the ____ of text.

- A) shape
42.

**Modified Multiple Choice**

The text in a flyer is organized into the following areas: ____.

- A) footer
- B) headline
- C) signature
- D) body copy

43.

**Modified Multiple Choice**

In which of the following circumstances should you press the ENTER key?

- A) To insert a blank line in a document
- B) To terminate a short line of text and advance to the next line
- C) To begin a new paragraph
- D) To respond to questions or prompts in Word dialog boxes, task panes, and other on-screen objects

44.

**Modified Multiple Choice**

Word provides a means of canceling your recent ____.

- A) applications
- B) indices
- C) actions
- D) commands
45.

**Modified Multiple Choice**

The color orange denotes ____.

☐ A) success
☐ B) creativity
☐ C) victory
☐ D) harmony

46.

Word inserts text to the right of the insertion point.

☐ A) True
☐ B) False

47.

If Word finds a potential error in a document, a red, green, or blue wavy underline flags the problem.

☐ A) True
☐ B) False

48.

A raised dot (·) shows where the ENTER key was pressed.

☐ A) True
☐ B) False

49.

When typing, the insertion point moves to the left, and when the end of a line is reached, it moves downward to the next line.

☐ A) True
☐ B) False

50.
Each time the ENTER key is pressed, Word creates a new paragraph.

☐ A) True
☐ B) False

51.

Wordwrap forces you to stop typing words and press the ENTER key at the end of each line.

☐ A) True
☐ B) False

52.

As you enter text in the Word document window, you must press the ENTER key when the insertion point reaches the right margin.

☐ A) True
☐ B) False

53.

A document may wordwrap differently depending on the type of printer being used.

☐ A) True
☐ B) False

54.

A flagged word is one that is misspelled.

☐ A) True
☐ B) False

55.

Paragraph formatting requires the paragraph to be selected prior to formatting.

☐ A) True
☐ B) False
56.
A single point is about 1/12 of an inch in height.
- A) True
- B) False

57.
The mouse pointer becomes different shapes depending on the pointer’s location and locations you click on the screen.
- A) True
- B) False

58.
As shown in the accompanying figure, Word shades a shaded area from the left margin to the right margin of the current paragraph.
- A) True
- B) False

59.
Formatting marks, like those in the accompanying figure, may not display properly on the screen with some fonts.

A) True  
B) False

Word provides an Undo button that can be used to cancel the most recent command or action.

A) True  
B) False
If you do not use the transparent Mini toolbar, as shown in the accompanying figure, it disappears from the screen.

A) True
B) False

62.

To upload a picture taken with a digital camera is to copy the digital picture from the camera to your computer.

A) True
B) False

63.

A selected graphic can be resized using the Shape Height and Shape Width text boxes in the Size group on the Format tab on the Picture Tools tab.

A) True
B) False

64.
Five different types of document properties like those shown in the accompanying figure exist.

A) True
B) False
Using document properties, like those in the accompanying figure, is unlikely to save users time locating a particular file because they cannot view a document’s properties without opening the document.

A) True
B) False

66.
By creating consistent properties (like those in the accompanying figure) for files having similar content, users can better organize their documents.

☐ A) True

☐ B) False

67.
Some organizations require Word users to add document properties, like the ones in the accompanying figure, so that other employees can view details about these files.

- A) True
- B) False

68.

With electronic images of documents, such as PDF and XPS, users must have the software that created the original document in order to view the PDF or XPS file.

- A) True
- B) False

69.

If you want to print multiple copies of a document, display the Print dialog box by clicking the Print button on the Standard toolbar.

- A) True
70.
To quit Word, click the Restore button on the right side of the title bar.

B) False

71.
A green wavy underline indicates the text may contain a contextual spelling error such as the misuse of homophones.

A) True
B) False

72.
When the **Standard toolbar** appears, as shown in the accompanying figure, it initially is transparent.

A) True
B) False

73.
A color scheme in Word is a document theme that identifies 24 complementary colors for text, background, accents, and links in a document.

A) True
B) False
The content, size, shape, position, and format of a graphic on a flyer should capture the interest of passersby, enticing them to stop and read the flyer.

A) True  
B) False

Word provides more than 25 picture formats that enable you easily to change a picture's look to a more visually appealing one, including a variety of shapes, angles, borders, and reflections.

A) True  
B) False

The ________________ copy in a flyer consists of all text between the headline and the signature line.

______________

When you begin typing text, the ________________ appears on the status bar with an animated pencil writing on paper that indicates Word is checking for spelling and grammar errors.

______________
A(n) _________________________ is a character, like the ones in the accompanying figure, that Word displays on the screen but is not visible on a printed document.

79. Word automatically corrects misspelled words and displays the corrected word when you press the _________________________ or type a punctuation mark.

80. Many word processing documents use ____________________ character fonts, where some characters are wider than others.

81. As more lines of text are typed than Word can display in the document window, Word _______________________ the top or bottom portion of the document off the screen.

82.
83. **Formatting** is the process of changing the appearance of a paragraph.

84. **Character formatting** is the process of changing the way characters appear on the screen and in print.

85. In Word, the **Default** font usually is Calibri.

86. When a headline is **centered**, it is positioned horizontally between the left and right margins on the page.

87. When you **select** text, as shown in the accompanying figure, Word colors the rectangular area behind any text or graphics.
87. A(n) ____________________ list is a series of paragraphs, each beginning with a bullet character.

88. __________________ text prints with an underscore below each character.

89. A selected graphic, as shown in the accompanying figure, appears surrounded by a(n) ____________________, which has small squares and circles around its edges.

90.
includes both enlarging and reducing the size of a graphic, as shown in the accompanying figure.

91.

In ______________________, as a character is typed Word inserts the character and moves all the characters to the right of the typed character one position to the right.

92.

The default typing mode in Word is ______________________ mode.

93.

With ______________________ editing, you select the text to be moved and then drag the selected item to the new location and then insert it there.
94. A(n) _________________________ is information that exists on a physical medium such as paper.

95. ________________________ computing involves reducing the environmental waste generated when using a computer.

96. Identify the letter of the choice that best matches the phrase or definition.

| A. point                           | B. Calibri                        |
| C. character                      | D. font size                       |
| E. color scheme                   | F. headline                        |
| G. Normal                         | H. theme                           |
| I. font                           | J. style                           |

Defines the appearance and shape of the letters, numbers, and special characters.

A named group of formatting characteristics.

Type of formatting used to emphasize certain words and improve readability of a document.

The first line of text on a flyer.
The default font in Word.

Uses points as the units of measurement.

The default style in Word.

Identifies 12 complementary colors for text, background, accents, and links.

About 1/72 of one inch in height.

A set of unified formats for fonts, colors, and graphics.

97.

The text in a flyer is organized into three areas. List all three and briefly describe each.

98.

Under what circumstances should you press the ENTER key when typing in Word?

99.

By formatting the characters and paragraphs in a document, you can improve its overall appearance. List the formatting suggestions to consider when designing a flyer.
Critical Thinking Questions

Case 1-1

Your colleague Frank is editing a friend's novel in Word. To speed up the process, Frank would like to take advantage of the various techniques available for selecting text, and he asks you for help.

Which of the following techniques will allow Frank to select an entire sentence?

<table>
<thead>
<tr>
<th>a. click the sentence</th>
<th>c. press and hold down the CTRL key and then click the sentence</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. double-click the sentence</td>
<td>d. move the mouse to the left of the sentence and then triple-click</td>
</tr>
</tbody>
</table>

Critical Thinking Questions

Case 1-1

Frank would like to be able to select a full paragraph. Which of the following techniques will work?

<table>
<thead>
<tr>
<th>a. triple-click the paragraph</th>
<th>c. click the paragraph</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. double-click the paragraph</td>
<td>d. move the mouse to the left of the paragraph and then double-click</td>
</tr>
</tbody>
</table>
102.

Critical Thinking Questions
Case 1-2

You have written a novella on your new laptop and now, as you prepare to find a literary agent for your work, you would like to do some formatting of it to make it more appealing to prospective agents.

Which of the following changes you make to your text is an example of paragraph formatting?

| a. underlining the title on the title page | c. putting the title in boldface |
| b. italicizing the dedication section on the first page of the text | d. centering all of the paragraphs on the title page |

103.

Critical Thinking Questions
Case 1-2

You have written a novella on your new laptop and now, as you prepare to find a literary agent for your work, you would like to do some formatting of it to make it more appealing to prospective agents.

In your novella, you can change the formatting of all of the following EXCEPT ____.

<p>| a. a question mark | c. the asterisk symbol |</p>
<table>
<thead>
<tr>
<th>b. paragraph mark</th>
<th>d. the numeral 5</th>
</tr>
</thead>
</table>

**HTML Editor**
CIS 125W

Selecting a Project

- What are you interested in?
- What is your career field of choice?
- What do you want to do after graduation?
- Who do you currently work for?
- Who do you want to work for?
- Are you involved in a local non-profit?
- Are you involved in a local church?

- Meet with the manager, leader, pastor, etc.
  - Introduce yourself and ask if there is a project they want to do
  - Look for areas where things are not working properly
  - Look for a current challenge

- Project Process
  - Define the challenge
  - Interview, research, gather data, etc.
  - Develop a hypothesis or potential solution
  - Propose a solution
  - Design a solution
  - Test your design
  - Refine your proposal

- Write the Report
  - A – Impress me – solve a problem – demonstrate excellence
  - B – Good project – weak solution – poor report construction
  - C – Yep, you did a project – weak write-up, the world won’t be improved
  - D – Did a process not a project – poor report – no real change proposed
  - F – No report, no participation, gave up
CIS 125W Week 2 Outline of activities for the week

Week 2 Creating a Research Paper with Citations & References

This week we will move forward to Word Chapter 2. Since you will need to learn and master this skill for use in your life at college and at work, early in this course we have the opportunity to learn about how to cite sources we quote or materially use in our writings. Failure to do this properly means you might be charged with plagiarism, which is when we copy the work of another person or source without crediting them for their work. You will have a chance to apply the skills you have learned in this chapter by doing several of the exercises at the end of the lesson.

Upon completion of this week's material the student should be able to:

- Describe the MLA documentation style for research papers
- Change line and paragraph spacing in a document
- Modify a style
- Use a header to number pages of a document
- Apply formatting using shortcut keys
- Modify paragraph indentation
- Insert and edit citations and their sources
- Add a footnote to a document
- Insert a manual page break
- Create a bibliographical list of sources
- Cut, copy, and paste text
- Find test and replace text
- Find a synonym
- Use the Research task pane to look up information

Reading:

- Word Chapter 2 - Creating a Research Paper with Citations & References (If you do not already have your Student Data Files, you may download them here)
- Read and do hands on exercises in the Word 2010 Chapter 2 (WD 65 - WD 125) "Creating a Research Paper with Citations & References"
- View the Word 2010 Chapter 2 PowerPoint presentation
- View the Word 2010 Chapter 2 Flash presentation

Assignments:

- Homework due for Word Chapter 2:
  - WD pp. 132-134, In the Lab: Lab 2 "Preparing a Research Report with a Footnote". Be sure that you save your completed document and that it is named as directed. Include it in your zipped homework folder.
  - WD pp. 134-135, In the Lab: Lab 3 "Composing a Research Paper From Notes". Be sure that your completed document is saved and named as directed in the exercise. Include in your zipped folder.
  - Upload your Week 2 homework zipped folder with both homework assignments enclosed to the Week 2 Drop Box.
CIS 125W Week 1 Activity

Angel Discussion Question 1:

It has been said that no matter what the document, ultimately the thing that it represents most is the individual or individuals who created it. What does this mean to you as a student? What will it mean to you as a professional after graduation? Post your responses in the Week 2 Discussion Forum.
CIS 125W Week 5 Activity

Angel Discussion Question 4:

Why do you think Word ships with such a large number of templates? Examine templates that are available at Office.com, Microsoft’s website for Office. Find two other templates that interest you and explain their use. Post your responses in the Week 5 Discussion Forum.
1. The Office font set uses the ____ font for body text.

   A) Calibri  
   B) Times New Roman  
   C) Cambria  
   D) Arial

Correct answer(s): A

2. If you add text, delete text, or modify text on a page, Word recomputes the location of automatic page breaks and adjusts them accordingly.

   A) True  
   B) False

Correct answer(s): A

3. One way to add a correctly spelled word to the custom dictionary is to click the ____ button in the Spelling and Grammar dialog box.

   A) Add to Dictionary  
   B) New Entry  
   C) Add to Custom  
   D) Custom Entry

Correct answer(s): A
4. The rule is to press the SPACER BAR ____ time(s) after periods, colons, and other punctuation marks.

- A) one
- B) two
- C) three
- D) either A or B, in MLA style

Correct answer(s): A

5. To select nonadjacent text, select the first item, hold the ____ key, and then select the subsequent items.

- A) SHIFT
- B) CTRL
- C) ALT
- D) END

Correct answer(s): B
6. To display the Choose a SmartArt Graphic dialog box shown in the accompanying figure, click the ____ button on the Insert tab.

- A) New SmartArt
- B) Add Graphic
- C) Insert SmartArt Graphic
- D) Add Art

Correct answer(s): C

7. If you do not want to keep a change automatically made by Word and you immediately notice the automatic correction, you can undo the change by clicking the Undo button on the ____ toolbar.

- A) Office Button menu
- B) Quick Access Toolbar
- C) Ribbon
- D) any of the above
8. While plagiarism is unethical, it is not considered an academic crime.

- A) True
- B) False

Correct answer(s): B

9. The MLA style uses the term bibliographical references for works cited.

- A) True
- B) False

Correct answer(s): B

10. The _____ feature automatically corrects typing, spelling, capitalization, or grammar errors as you type them.

- A) AutoEntry
- B) AutoCorrect
- C) AutoAdd
- D) AutoSpell

Correct answer(s): B
11. Each time the _____ key is pressed, the paragraph formatting in the previous paragraph is carried forward to the next paragraph.

A) ENTER  
B) SHIFT  
C) CTRL  
D) ALT

Correct answer(s): A

12. Although many different styles of documentation exist for report preparation, each style requires the same basic information.

A) True  
B) False

Correct answer(s): A

13. A(n) ____ is a book of synonyms.

A) dictionary  
B) glossary  
C) index  
D) thesaurus

Correct answer(s): D

14. Which of the following is the first step in the process of resetting the default font settings?

A) Use Windows Explorer to locate the normal.dotm file.  
B) Start Word.  
C) Rename the normal.dotm file to another file name so that the normal.dotm file no longer exists.  
D) Quit Word.
Correct answer(s): D

15. If the top of a set of characters is chopped off, then line spacing may be set to ____.
   - A) Exactly
   - B) Cut
   - C) About
   - D) Near

Correct answer(s): A

16. To search for a special character, use the ____ button in the expanded Find dialog box.
   - A) Characters
   - B) Special
   - C) Options
   - D) Advanced

Correct answer(s): B

17. A(n) ____ paragraph is a paragraph that begins with a dot or other symbol.
   - A) headline
   - B) centered
   - C) bulleted
   - D) indexed

Correct answer(s): C
18. By default, the Normal style inserts a vertical space equal to ____ line(s) between each line of text.

- A) 1
- B) 1.15
- C) 2
- D) 2.15

**Correct answer(s):** B

19. The _____, or typeface, defines the appearance and shape of letters, numbers, and special characters.

- A) font
- B) font size
- C) point
- D) paragraph formatting

**Correct answer(s):** A
20. Font **___**, like those shown in the accompanying figure, define one font for headings and another for body text.

- A) rosters
- B) menus
- C) galleries
- D) sets

**Correct answer(s):** D

21. If you do not want the border style to carry forward each time the ENTER key is pressed, you need to ____.

- A) clear formatting
- B) return to the Standard style
- C) press the ESC key
- D) restore shading

**Correct answer(s):** A
22. To follow the MLA style, single-space text on all pages with one and a half-inch top and bottom margins, and one-inch left and right margins.

- A) True
- B) False

Correct answer(s): B

23. To create a text watermark, you use the ____.

- A) Clip Art menu
- B) Background command on the Format menu
- C) Watermark button on the Page Layout tab
- D) Style box

Correct answer(s): C

24. A(n) ____ is a placeholder for data whose contents can change.

- A) attribute
- B) element
- C) field
- D) value

Correct answer(s): C

25. To search for formatting or a special character, click the _____ button to expand the Find dialog box.

- A) Additional searching
- B) Find more
- C) More
- D) Search options

Correct answer(s): C
Make Mine Wireless

Objective
Explain how wireless LAN components are deployed in a small- to medium-sized business.

Scenario
As the network administrator for your small- to medium-sized business, you realize that your wireless network needs updating, both inside and outside of your building. Therefore, you decide to research how other businesses and educational and community groups set up their WLANs for better access to their employees and clients.

To research this topic, you visit the Customer Case Studies and Research website to see how other businesses use wireless technology. After viewing a few of the videos, or reading some of the case study PDFs, you decide to select two to show to your CEO to support upgrading to a more robust wireless solution for your company.

To complete this class modeling activity, open the accompanying PDF for further instructions on how to proceed.

Resources
Internet access to the WWW

Step 1:  Open your browser and the URL specified for this activity.

a. Choose two case studies about wireless LAN upgrades from the list to read, located on the Customer Case Studies and Research website.

b. As you view the media or read the PDFs, write notes for the following categories:
   1) The WLAN challenge that the company sought to mitigate
   2) The solution that was found to the challenge
   3) The results that were gained by WLAN updates

Step 2:  Share your findings.

a. Share your findings with the class or a classmate.

b. Play the media or show the PDF for one of the case studies you chose from the URL page.

c. In your own words, explain the challenge, solution, and results learned from the media or PDF.

d. Explain how the results you found could be applied to improve your company’s network.
Syllabus

CIS 152
Introduction to Basic Routers – Cisco 2

Class Hours: Lecture: M T W - 11:00 AM - 11:50 AM; Lab: TH – 10:00 AM - 11:50 AM
Class location: TC 106 for lecture and lab
Credits: 4
Instructor: John Blackwood
Office: Tower 3
Office Hours: Click here to open that link
Phone: 541.440.7686
Email: john.blackwood@umpqua.edu

Cisco Academy NetSpace: https://www.netacad.com/
Certification: http://www.vue.com/

Testing: The UCC is now a Vue testing center. To sit for a Cisco certification exam, please create your Vue profile and select to test at the UCC. The UCC is also a Prometric (Microsoft) testing center. Please talk to me before you register to take the 100-101 CCENT exam.

Course Description:
This course continues to provide students with classroom and laboratory experience in current and emerging networking technology that will empower them to enter employment or further education and training in the computer-networking field. A task analysis of current industry standards and occupational analysis was used to develop the content. Instruction includes, but is not limited to, the Open System Interconnection (OSI) Reference Model, local area networks (LANs), wide area networks (WANs), transmission control protocol/Internet protocol (TCP/IP) addressing, routers, router configuration, routing and routing protocols, internet work open system (IOS) images and network troubleshooting. Particular emphasis is given to understanding the nature of and component of networks that make up LANs, WANs and the Internet. Students will become familiar with the use of command protocols that are used when configuring networks and will learn how to troubleshoot a router-based topology.

Course Outcomes:
Upon completion of this course the student should be able to demonstrate (the):
- Working knowledge of router elements (RAM, ROM, CDP, Show commands).
- Working knowledge of RIP, EIGRP, and OSPF.
- Ability to apply basic subnetting & VLSM principles in an IP addressing scheme.
- Ability to distinguish between common router prompts.
- Ability to describe connection-oriented and connectionless network services.
- Ability to configure a router including interfaces, routing protocols, host tables, console, and virtual terminal sessions.
- Ability to edit router configuration and view command history.
- Ability to manage and troubleshoot router configuration using various show commands.
- Ability to prepare backup, upgrade, and load backup software image.

Required Text:
There is no required text for this course.

Lab Grading Rubric:
Labs are to be completed in a professional manner. Network administrators must learn to write neatly and succinctly so that steps can be repeated and/or understood by others. Some governing bodies require documentation for auditing purposes. Labs will be graded as follows:

**Poor** (0% – 60%): Lab is not completed at all or work is almost non-existent. Lab was turned in late.

**Marginally acceptable** (61% - 69%): Lab is somewhat completed but writing is difficult to read with illegible writing and/or incomplete thoughts/sentences. Lab manual work looks sloppy and lab was turned in late.

**Acceptable** (70% - 79%): Lab is mostly complete with incomplete sentences and/or mostly legible writing. Lab was turned in on time.

**Better than average** (80% - 89%): Lab is complete with legible, professional writing. Some sentences are incomplete. Lab manual is not scribbled in, but may have notes in margins. Lab was turned in on time.

**Excellent** (90% - 100%): Lab is complete with excellent writing, thoughts, and sentences. Lab manual has professional look and is a testament to a solid future network administrator. Lab was turned in on time.

Grading & Homework:
Traditional percentage grades (90% for an A, 80% for a B, etc) will be assigned based on the assignments listed in this document. The points and percentage of grade for each homework category is:

**Physical Labs**: 8 physical labs x 100 pts/each = 800 points (20.0%)

**Packet Tracer Labs**: 5 PT labs x 100 pts/each = 500 points (10.0%)
Packet Tracer Challenge Labs: 2 PTSIC labs x 100 pts/each = 200 points (7.5%)

Packet Tracer SBA Labs: 2 SBA labs x 100 pts/each = 200 points (7.5%)

Weekly online quizzes: 12 quizzes x 100 pts/each = 1,200 points (10.0%)

Notes Journals: 10 each x 100 pts/each = 1,000 points (10.0%)

Hands-on Skills SBA exam: 100 points (15.0%)

Final exam: 100 points 20.0%)

Homework labs are due the Monday after they were assigned by noon. For example, labs for Chapters 1 are assigned on Monday, September 30th. These labs are due on or before Monday October 6th, by noon.

Extra Credit: I will assigne extra credit sparingly. Please do not count on extra credit assignments to make up for assigned homework labs that you do not complete. However, if a quiz score or some other out-of-the-ordinary circumstance arises, I can be persuaded to assign extra credit. Warning: the extra credit will not represent easy points! You will earn them.

See the Weekly Course Assignments page under Lessons for the course schedule and assignments. Note that this schedule and its assignments may be changed at the instructor’s discretion due to class dynamics. You are expected to attend keep in regular contact with your instructor so that you are aware of any changes. Failure to do so will not extend homework due dates!

Important note: All labs are due no later than Monday, December 9th, by noon.

Student Notices
Assignments and projects are due on the dates indicated in the course outline above. Any assignment turned in late is assigned a 20% late fee deduction. Homework will NOT be accepted after grades have been posted to Angel and/or graded homework has been returned to the students.

Barring an unforeseen emergency, arrangements for making up tests must be made prior to missing a test. Specific instructions on assignments and projects will be revealed in class.

Each student is expected to complete each assignment independently unless assigned to group work. All students caught lacking in academic integrity will receive a zero (0) for the
assignment. Repeated violations of academic integrity may result in being dropped from the course and/or the UCC.

Cell phones are to be put into silent mode during regular lecture and lab class hours. In other words, cell phones should not make any noise during class, lab, or exam time. Further, during any proctored quiz or exam, cell phones must be turned off and placed in a location that cannot be accessed during the quiz or exam. Cell phones may not be used (voice, data, or camera) during any quiz or exam.

**Disability Policies & Services**

The UCC is committed to supporting all students. Any student who feels he or she may need an accommodation for any type of disability should make contact with the Disability Services Office in the Advising and Career Service Center of the Campus Center Building.

If you plan to use academic accommodations for this course, please contact your instructor and our office as soon as possible to discuss your needs. Accommodations are not retroactive; they begin when the instructor receives the “Approved Academic Accommodations” letter.

To request academic accommodations for a disability, please contact a Disability Service Coordinator at: Phone (541) 440-7655 or (541) 440-4610 or Oregon Relay 1-800-735-2900.

Veterans and active duty military personnel with special circumstances are welcome and encouraged to communicate these, in advance if possible, to Danielle Haskett in Disability Services.

Additional information may be found at the Disability Services web page at: [http://www.umpqua.edu/advising-a-career-services/993-disability-services](http://www.umpqua.edu/advising-a-career-services/993-disability-services)

New and returning students may access information at: [http://www.umpqua.edu/your-first-term](http://www.umpqua.edu/your-first-term)

Tutoring services at UCC are FREE and available to all students on a drop in basis. Tutoring is offered in a variety of subject areas. The goal of tutoring is to promote your learning and to assist you in becoming a more capable and confident student. All peer tutors have successfully completed college classes and are anxious to share their knowledge with other students. The tutoring center is located in the Educational Skills Building (ESB) Room 15.

**Tutoring Center:**

Educational Skills (ESB) Building
(541) 440-7733
A tutoring schedule for the current college term is listed at the bottom of the Web page listed below.

http://www.umpqua.edu/success-center

Umpqua Community College Counseling Center provides comprehensive counseling services to assist you with career plans and academic advising as well as help to work out personal or social problems. Counselors are available to both current and prospective students in the Campus Center.

The Counseling Center, Testing Center, Job Placement & the Transfer Opportunity Program are located in the Campus Center building across from UCC's Financial Aid Office. To contact our office you may stop by during business hours or call (541) 440-4610.

http://www.umpqua.edu/counseling-center

For assistance with homework assignments, students are encouraged to visit the Institutional Resources link in Angel, which is available via the Resources tab. Listed here you will find links to search local libraries, search newspapers and journals, You can also use one of the links to email a UCC librarian for assistance.

The ANGEL Learning Management System is compliant with ADA standards.
Course Assignments by Week

CIS 152C: Cisco 2

During week one, you must also post your SIA during one of the first three days of class to avoid being dropped. If you do not post your SIA, and there is a class waiting list, you may be dropped in week 1.

The SIA is the Student Introductory Assignment where you post something about yourself in Angel, in the Lessons -> Week 01 folder -> SIA Forum. Your instructor will have already posted something about himself there! Create a new post and tell your instructor and classmates something about yourself.

Homework due date details: Please see the Syllabus for details!

Reading consists of studying, taking notes, and performing all hands-on exercises found in each content area assigned. Homework consists of the Physical equipment and Packet Tracer lab assignments.

Online quizzes are available within Cisco’s NetSpace website. I placed the NetSpace website’s URL near the top of the syllabus. You may take these tests up to two times. Take them more than one time to get a perfect score! Your highest score is the one that counts. Quizzes are to be taken weekly! Once a quizzes open time expires, it will no longer be available. Quizzes become available each Monday morning at approximately 6:30 AM and expire the following Monday at 7:00 AM.

The Final Exam is made up of approximately 60 multiple choice scenario questions. You will take the exam online after logging into NetSpace. The exam is closed book and timed. You must be present, in class, to take the final exam. It is proctored by me. Final Exam instructions will be posted in Week 9 and I will answer any questions you have at that time. Although the final exam is closed book, you may use your weekly notes journal during the final exam. However, the Internet and other material are still off limits during the final exam.

How to turn in homework to an Angel drop box:

1. Place all of your files in a folder (one folder per week’s worth of homework). Files are Word or WordPad documents containing your screenshots.
   a. If you are uploading only one file, please do not place the one file in a folder.
2. **Place all of that week’s folders in one Windows Compressed folder.** Do not put each assignment in a compressed folder. Each email should only contain one compressed folder.

   a. **If you are uploading only one file, please do not place the one file in a compressed/zipped folder.**

3. **Name the Compressed folder with your course number, your name and week number.** For example, week one’s filename for me would be “CIS 152C, Week 1 – John Blackwood”.

4. **Upload the compressed folder into that specific homework assignment’s drop box.**

**Week By Week Activities:**

Please see the [Assignment Points Allocation](#) page for specific page numbers for each homework assignment!

---

**Week 1 (Sep 30 – Oct 06):**

- SIA due by Wednesday at midnight during week one!
- If you don’t complete your SIA on time you may be dropped from the course in week 01.
- View all flash material for: Unit 01 – Local Area Networks
- View all NetSpace material for: Chapter 01: Introduction to Switched Networks (including pretest)
- **Homework due:**
  - NetSpace Quiz for Chapter 01 (one quiz for all concepts and skills covered)
  - NetSpace Exam for Chapter 01
  - Physical lab: Initializing and Reloading a Router and Switch (0.0.0.1 Lab)

**Week 2 (Oct 07 – Oct 13):**

- View all flash material for: Unit 02 – Basic Switching
- View all NetSpace material for: Chapter 02: Basic Switching Concepts and Configuration (includes pretest)
- **Homework due:**
  - NetSpace Exam for Chapter 02
  - NetSpace PT SBA Exam for Chapter 02
  - Available via NetSpace after login
  - Physical lab: Configuring Switch Security Features (2.2.4.11 Lab)

**Week 3 (Oct 14 – Oct 20):**

- View all flash material for: Unit 03 – Virtual LANs
• View all NetSpace material for: Chapter 03: VLANs (including pretest)
• Homework due:
  o NetSpace Exam for Chapter 03
  o Physical lab: Troubleshooting VLAN Configurations (3.2.4.9 Lab)
  o PT lab: 3.2.1.7 Packet Tracer - Configuring VLANs

**Week 4 (Oct 21 – Oct 27):**
• View all flash material for: Unit 04 – Basic Routing
• View all NetSpace material for: Chapter 04: Routing Concepts (including pretest)
• Homework due:
  o NetSpace Exam for Chapter 04
  o Physical lab: Configuring Basic Router Settings with IOS CLI (4.1.4.6 Lab)
  o PT lab: 4.1.4.5 Packet Tracer - Configuring and Verifying a Small Network

**Week 5 (Oct 28 – Nov 03):**
• View all flash material for: Unit 05 – Inter-VLAN Routing
• View all flash material for: Unit 06 – Static Routing
• View all NetSpace material for: Chapter 05: Inter-VLAN Routing (including pretest)
• View all NetSpace material for: Chapter 06: Static Routing (including pretest)
• Homework due:
  o NetSpace Exam for Chapter 05
  o NetSpace Exam for Chapter 06
  o NetSpace PT SBA Exam for Chapter 06
  o Available via NetSpace after login
  o Physical lab: Configuring 802.1Q Trunk-Based Inter-VLAN Routing (5.1.3.7 Lab)

**Week 6 (Nov 04 – Nov 10):**
• View all flash material for: Unit 07 – Dynamic Routing
• View all NetSpace material for: Chapter 07: Routing Dynamically (including pretest)
• Homework due:
  o NetSpace Exam for Chapter 07
  o Physical lab: Class Activity - IPv6 (7.6.1.1 Lab)
  o PT lab: 7.3.2.3 Packet Tracer - Configuring RIPng
Week 7 (Nov 11 – Nov 17):
- View all flash material for: Unit 08 – Basic OSPF
- View all NetSpace material for: Chapter 08: Single-Area OSPF (including pretest)
- Homework due:
  o NetSpace Exam for Chapter 08
  o Physical lab: Configuring Basic Single-Area OSPFv3 (8.3.3.6 Lab)
  o PT lab: 8.4.1.2 Packet Tracer - Skills Integration Challenge

Week 8 (Nov 18 – Nov 24):
- View all flash material for: Unit 09 – Access Control
- View all NetSpace material for: Chapter 09: Access Control Lists (including pretest)
- Homework due:
  o NetSpace Exam for Chapter 09
  o PT lab: 9.1.1.6 Packet Tracer - ACL Demonstration
  o PT lab: 9.3.2.12 Packet Tracer - Scenario 3 (in Step #4, please enter the command in the ACL even though the lab does not ask you to do so. You will not earn 100% without it!)

Week 9 (Nov 25 – Dec 01):
- View all flash material for: Unit 10 – IP Address Assignment & Translation (continues on to next week)
- View all NetSpace material for: Chapter 10: DHCP (including pretest)
- Homework due:
  o NetSpace Exam for Chapter 10
  o PT lab: 10.3.1.2 Packet Tracer - Skills Integration Challenge

*Week 10 (Dec 02 – Dec 08):
- View all flash material for: Unit 10 – IP Address Assignment & Translation (continued from last week)
- View all NetSpace material for: Chapter 11: Network Address Translation for IPv4 (including pretest)
- Homework due:
  o NetSpace Exam for Chapter 11
  o PT lab: 11.3.1.4 Packet Tracer - Verifying and Troubleshooting NAT Configurations
  o Physical lab: Configuring NAT Pool Overload and PAT (11.2.3.7 Lab)
Week 11 – FINALS (Dec 09 – Dec 13):

- Final Exam – TC 106, online via NetSpace
- Location: TC 106
- Date: Wednesday, December 11, 2013
- Time: 10:00 - noon
- Instructions: the final exam is made up of approximately 60 multiple choice questions that cover all of the material covered in class via quizzes, projects, video, and Web research.
- Hands-on Skills final exam:
  - Assigned in Week 9
  - Due same day as final exam @ NOON

*Homework for Week 10 is due via email to your instructor no later than Monday, December 9th, 2013 by noon.*
It’s Network Access Time

Objectives
Describe features available for switches to support requirements of a small- to medium-sized business network.

Scenario
Use Packet Tracer for this activity. Work with a classmate to create two network designs to accommodate the following scenarios:

Scenario 1 – Classroom Design (LAN)
- 15 student end devices represented by 1 or 2 PCs.
- 1 instructor end device; a server is preferred.
- Device capability to stream video presentations over LAN connection. Internet connectivity is not required in this design.

Scenario 2 – Administrative Design (WAN)
- All requirements as listed in Scenario 1.
- Add access to and from a remote administrative server for video presentations and pushed updates for network application software.

Both the LAN and WAN designs should fit on one Packet Tracer file screen. All intermediary devices should be labeled with the switch model (or name) and the router model (or name).

Save your work and be ready to justify your device decisions and layout to your instructor and the class.

Reflection
1. What are some problems that may be encountered if you receive streaming video from your instructor’s server through a low-end switch?

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________

2. How would the traffic flow be determined: multicast or broadcast – in transmission?

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________

3. What would influence your decision on the type of switch to use for voice, streaming video and regular data these types of transmissions?

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________

4. As you learned in the first course of the Academy, video and voice use a special TCP/IP model, transport layer protocol. What protocol is used in this layer and why is it important to voice and video streaming?

_______________________________________________________________________________________
_______________________________________________________________________________________
Stand By Me

Objective
Describe the role of unicast, broadcast, and multicast in a switched network.

Scenario
When you arrived to class today, you were given a number by your instructor to use for this introductory class activity.

Once class begins, your instructor will ask certain students with specific numbers to stand. Your job is to record the standing students’ numbers for each scenario.

Scenario 1
Students with numbers starting with the number 5 should stand. Record the numbers of the standing students.

Scenario 2
Students with numbers ending in B should stand. Record the numbers of the standing students.

Scenario 3
Students with the number 504C should stand. Record the number of the standing student.

At the end of this activity, divide into small groups and record answers to the Reflection questions on the PDF for this activity.

Reflection
1. Why do you think you were asked to record the students’ numbers when and as requested?

2. What is the significance of the number 5 in this activity? How many people were identified with this number?

3. What is the significance of the letter C in this activity? How many people were identified with this number?

4. Why did only one person stand for 504C?

5. How do you think this activity represents data travelling on local area networks?

Save your work and be prepared to share it with another student or the entire class.
CCNA 1: An Introduction to Networking

Unit 3: IP Addressing
Welcome to CCNA 1, An Introduction to Networking, Unit 3, entitled IP Addressing. Plan to spend a good amount of time in this unit as you are introduced to the sometimes complex topic of IP version 4 addressing, subnetting, and variable-length subnet masking.

The objectives for this lecture, IP Addressing, are to gain the abilities to:

- Explain the purpose of IP addressing
- Differentiate and contrast between classful and classless IP addressing
- Convert between hexadecimal, binary, and decimal numbers
- Create a valid IP address scheme for a network
- Subnet a network address space
- Explain the concepts of CIDR and VLSM
- Use VLSM to best utilize IP address space
- Verify an IP address implementation using common network utilities
- Differentiate between IPv4 and IPv6 addressing
IPv4 Addressing Basics

- A basic IPv4 addressing pieces
  - Four groups of numbers
  - Each group represents 8 binary digits (bits)
  - Valid numbers are 0 – 255 for each group
  - IP address: 192.168.10.1
  - Subnet mask: 255.255.255.0
- Each group called an octet (8 bits)
  - 8 bits also called a byte

Notes:
An IP version 4 address is made up of four pieces, or groups of numbers, each of which is concatenated by a period, or dot. Each group of numbers represents eight bits, or binary digits. The 8-bit group is also referred to as an octet in IP addressing and alternatively as a byte. The terms are synonyms.

When an IP address is written in decimal, as you see it on the slide, its numbers must be in the range of zero through and including 255. The IP address on the slide is 192.168.10.1 and is accompanied by a subnet mask of 255.255.255.0.

Binary & Decimal

- IPv4 address = 32 bits
  - 4 groups x 8-bits/group = 32 total bits
- Dotted decimal address:
  - 192.168.10.1
- Dotted Binary equivalent:
  - 11000000.10101000.00001010.00000001
- Learn binary for subnetting
- Use decimal when writing IP addresses

Notes:
As I mentioned previously, an IP address is made up of four groups of numbers, with each 8-bit group combining to represent one decimal number. Therefore, 8-bits times 4 groups totals up to 32 total bits for one IP version 4 address.

Examine the dotted decimal and dotted binary numbers shown on the slide for a moment.

For example, the leftmost number of the IP address is 192 and its binary equivalent is 11000000. As you no doubt are now aware, we must learn binary to decimal and decimal to binary conversion techniques if we are to truly...
understand IP addressing. This is because much of the logic behind IP addressing is accomplished in binary, and we write IP addressing in its decimal equivalency format.

<table>
<thead>
<tr>
<th>Slide 5</th>
<th>Network &amp; Host Parts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration: 00:01:15</td>
<td>Advance mode: Auto</td>
</tr>
</tbody>
</table>

- IPv4 address broken into two portions
  - Break determined by subnet mask
- Network portion identifies specific network
- Host portion identifies specific host in specific network
- Example with IP address & subnet mask:
  - 192.168.10.1 & 255.255.255.0
  - Network & host portions of address in color

Notes:
A couple of slides back, we saw that an IP address is accompanied by a subnet mask. The subnet mask helps us to identify which portion of an IP address identifies the network the IP address belongs to. Once we identify the network portion of the IP address, starting from its left, whatever remains is known as the host portion of the IP address. The host portion of the IP address is used to actually assign IP addresses to hosts.

With these points in mind, examine the IP address and subnet mask shown near the bottom of the slide. The IP address is 192.168.10.1 and its subnet mask is 255.255.255.0. Using the subnet mask, we learn that the three leftmost octets of bits identify the network of 192.168.10.0 and we also learn that all of the bits in the rightmost octet are assigned and allocated as host bits.

Let's examine these concepts in more detail on the next slides by stepping outside of the networking world into the world of computers in general.
How Computers Work & Binary

- Computers understand only binary numbers.
- All input is translated into a binary value.
- Output is generally translated from a binary value to a code understood by users (people)
  - Output is sent from one computer to another in binary format.

Notes:
Computers understand only binary numbers. A binary number is represented as a burst of electricity (ON or 1) or a lack of electricity (OFF or 0). A string of ones and zeros represents binary values that the computer can understand. All data input into a computer is translated into a binary value. Output is generally translated from a binary value to a code understood by users, which are generally people or an output device. Output is then sent from one computer to another in binary format.

For example, when you press the letter A on your keyboard, a number of electronic signals are sent from the keyboard to the CPU. The software that runs your keyboard knows how to interpret that signal so that the CPU can understand it. Then after the CPU and operating system perform some operation, the keyboard letter that you pressed, in this case the A, is displayed on your screen as output.

Computer Binary Example

- Keyboard
  - Device whose key strokes are usually interpreted by software into some type of symbol or symbols.
  - For example, the capital letter "A," typed into a word processing document, is sent electronically in binary code to the motherboard (as "01000001") and output on the monitor in alphabetic format.
- Same logic governs IP addressing

Notes:
A keyboard is an input device - keystrokes are interpreted by software into some type of symbol or symbols. For example, the capital letter A typed into a Word processing document is sent electronically from the keyboard in binary code to the motherboard.

The capital letter A in binary is made up of eight distinct binary digits – or bits - viewed as one logical unit. The capital letter A, in binary, is 01000001. After the computer operates on the binary code received as input, the capital letter A is output on the monitor in an alphabetic format that we understand.
This same logic governs how computers understand IP addresses.

<table>
<thead>
<tr>
<th>Slide 8 🎨</th>
<th>Why Binary?</th>
<th>Notes:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Why Binary?</td>
<td>You may be wondering why you need to learn to convert decimal numbers to binary in the first place. Why not just stick with decimal numbers?</td>
</tr>
<tr>
<td></td>
<td>• Sometimes used to determine routes that routers advertise to other routers</td>
<td>As you will learn in subsequent courses, sometimes binary logic is used to determine routes that routers advertise to other routers. Further, binary math logic is also used in many implementations of network security, it determines which specific host or group of hosts can pass through a router’s interface using protocols such as HTTP, HTTPS, TCP, POP, SMTP, and so on.</td>
</tr>
<tr>
<td></td>
<td>• Used in many implementations of network security</td>
<td>At this stage of your learning, all of this information is just FYI. You will learn how to implement network security in subsequent CCNA courses.</td>
</tr>
</tbody>
</table>
With all of that background information in hand, let's move forward to using binary numbers in IP addressing. Let's begin with some basic knowledge about decimal, called base 10, and binary, called base 2, numbers.

Decimal is called a base 10 number system because its outcomes are based on the positional value of a given number. When we write the decimal number 214, we are really writing the outcome of logic we learned as children to create that number based on this concept of positional value. The number 214 is made up of \(2 \times 10^2\) + \(1 \times 10^1\) + \(4 \times 10^0\).

As you should recall from your math courses, any number with an exponent of zero is equal to 1. In this base 10 example, the number 4 is said to be in the "ones" position, the number 1 is said to be in the "tens" position, and the number 2 is said to be in the "hundreds" position.

If you need a review in these concepts, please visit with your instructor before moving ahead in this presentation.

To convert the decimal number 214 to binary, we employ the same logic, except this time we use the base 2 number system to do it. In the base 2 number system, only two numbers can be used to represent the outcome of math operations, and they are 0 and 1. And, the number 2 is the base number to which we add an exponent as you see on the slide. Before jumping into the logic, let's simply state that the binary equivalent to the decimal number 214 is 11010110. Next, let's figure out the logic.
Employing the same positional value logic we just discussed, we create the binary equivalent by breaking the decimal number into its binary positional values. Therefore, the decimal number 214, broken down into binary placeholders, is \( (1 \times 2^7) + (1 \times 2^6) + (0 \times 2^5) + (1 \times 2^4) + (0 \times 2^3) + (1 \times 2^2) + (1 \times 2^1) + (0 \times 2^0) \).

Pause the presentation and take a moment to look this over before moving on to the next slide in the presentation, where we will explain this in more detail.

Notes:
As we discussed on the previous slide, in the base 2 number system, only two numbers can be used to represent the outcome of math operations, and they are 0 and 1. And, the number 2 is the base number to which we add an exponent as you see on the slide.

When a position value is multiplied by a 1, its value is counted in the running tally of the decimal equivalent number we are creating. When a position value is multiplied by a 0, its value is not counted in the running tally of the decimal equivalent number we are creating. With that logic in mind, walk through the creation of the number 214, shown near the bottom of the slide and say the math out loud with me as I spell it out.

The decimal number 214, is broken down into: \( (1 \times 2^7) + (1 \times 2^6) + (0 \times 2^5) + (1 \times 2^4) + (0 \times 2^3) + (1 \times 2^2) + (1 \times 2^1) + (0 \times 2^0) \), which, reading off the ones and zeroes multiplied against the placeholder value, is 11010110.
Notes:
Since an IP address is made up of 4-octets, with an octet being a grouping of 8-bits, in this discussion, we only need to concern ourselves with the placeholders applicable to those 8-bits. Starting from the right with $2^0$, and moving left to the end to reach $2^7$, you should be able to manually compute the binary numbers you see on the slide beginning with its decimal equivalent, and vice-versa after we learn how to do this over the next few slides.

I will do one of the numbers with you and let you work out the rest. Let's tackle the third number in the list, the decimal number 168.

Steps To Convert Decimal to Binary

The steps to convert the decimal number 168 to binary are:

1. Start by determining the closest binary value that is less than or equal to the decimal number. This is $2^7$, which is 128. Take note that we will place a 1 in the $2^7$ placeholder position.
2. Subtract the binary value of 128 from the starting decimal number of 168 to obtain remaining decimal number, which is 40.
3. Next, return to Step #1 above until the remaining decimal number equals 0. To do that, we determine the closest binary value that is less than or equal to the remaining decimal number of 40, which is 32. This is $2^5$. Take note that we will place a 1 in the $2^5$ placeholder position.
4. Subtract the binary value of 32 from the
remaining decimal number of 40 to obtain new remaining decimal number, which is 8.

5. Next, determine the closest binary value that is less than or equal to the remaining decimal number of 8, which is 8. This is $2^3$. Take note that we will place a 1 in the $2^3$ placeholder position. Since our remainder is zero, the math is done. Our next step is to determine our binary equivalent to the decimal number 168.

6. Place zeroes in all of the other placeholders and construct the binary number. The decimal 168 is: $(2^7) + (2^6) + (2^5) + (2^4) + (2^3) + (2^2) + (2^1) + (2^0)$ in binary placeholder format, and is written as 10101000b. The lower-case "b" subscript indicates a binary number.

---

**Notes:**

Let's try one more! Using the decimal number 185, let's construct its binary equivalent.

The closest binary value that is less than or equal to 185 is 128. So, we recognize the placeholder value of $2^7$ and subtract 128 from 185, leaving a remainder of 57.

Using the remainder of 57, we next find the closest binary value that is less than or equal to 57 is 32. So, we recognize the placeholder value of $2^5$ and subtract 32 from 57, leaving a remainder of 25.
Notes:
Using the remainder of 25, we next find the closest binary value that is less than or equal to 25 is 16. So, we recognize the placeholder value of $2^4$ and subtract 16 from 25, leaving a remainder of 9.

Using the remainder of 9, we next find the closest binary value that is less than or equal to 9 is 8. So, we recognize the placeholder value of $2^3$ and subtract 8 from 9, leaving a remainder of 1.

Slide 15
Example To Convert
Decimal to Binary (cont’d)
Duration: 00:00:55
Advance mode: Auto

Notes:
Finally, using the remainder of 1, we next find the closest binary value that is less than or equal to 1, which is 1. So, we recognize the placeholder value of $2^0$ and subtract 1 from 1, leaving a remainder of 0. Since our remainder is zero, our math work is done and our next step is to construct our binary equivalent to the decimal number 185, which is 10111001.

If you feel like you’ve got this, return to slide 11 and manually create each of the decimal and binary numbers you see there. Convert decimal to binary and binary to decimal. If you need help, please talk to your instructor for this course as soon as possible so that you are able to finish the material in this unit.
So then, what does a complete 32-bit IP address look like in binary? Take a moment to review the information you see on the slide. Can you replicate the decimal to binary conversion shown here – and vice-versa?

Given the IP version 4 address of 192.168.10.1, we separate each dotted decimal number set so that it stands alone. This gives us the numbers 192, 168, 10, and 1.

The binary equivalent for 192 is 11000000, for 168 it is 10101000, for 10 it is 00001010 and for 1 it is 00000001. Again, if you cannot calculate the binary equivalents for this IP address, please talk to your instructor for this course as soon as possible so that you are able to finish the material in this unit.

For even more practice, open the Windows Calculator and select random numbers to convert them from binary to decimal and vice-versa.

To open the Windows Calculator, click the Windows key, type calc, and press the Enter key. When the Windows Calculator opens, click View and then click Programmer. Click between Dec & Bin on the left center side of the Windows Calculator screen to convert numbers from binary to decimal and vice-versa after typing them in using your keyboard.
Next, let’s begin to put all of this new knowledge to work by using it to understand IP addresses and subnet masks. We begin with the statement that a host with an assigned IP address of 192.168.10.1 and an accompanying subnet mask of 255.255.255.0 is in the 192.168.10.0 network.

Further, based on the host’s IP address and subnet mask, we know that the first usable address in the host’s network is 192.168.10.1, that the last usable address in the host’s subnet is 192.168.10.254, and that the subnet’s broadcast address is 192.168.10.255.

We will discuss the broadcast type of communication briefly later in this discussion. Suffice it to say, for now, that a broadcast is a one-to-all communication type. Your computer broadcasts communications quite often to learn about the other hosts in its network. You will learn about how this occurs later in this course.

The first question that should pop up in your mind is “how do we know all of this information based on a host’s assigned IP address and subnet mask?” Let’s begin to answer that...
Let's begin by stating that the subnet mask is used in conjunction with an IP address to determine a host's network.

The bits that are set to the value of 1 – said to be "on" – in the subnet mask identify the so-called network bits in the subnet mask’s partner host IP address.

For example, the decimal subnet mask of 255.255.255.0 is 11111111.11111111.11111111.00000000 in binary. This translates to a total of 24 network bits and 8 host bits in the host's 32-bit IP address.

The 24-bits in the subnet mask are sometimes written as /24, which is called a prefix.
Therefore, implementing our newly-learned logic about the subnet mask, and using our example IP address of 192.168.10.1 and its subnet mask of 255.255.255.0, we can say that the 24 leftmost bits of the host’s IP address are network bits and that the 8 rightmost bits of the host’s IP address are host bits.

Changing the prefix number changes both the network bit and host bit allocations, and creates a new network membership for its hosts. With 8 host bits, we have $2^8$ or 256 possible addresses for the one network, called a subnet. For this subnet, the range of valid numbers is 0, and 1 – 255, for a total of 256 possible number combinations.

The IP address of 192.168.10.0 is the network address for all of its hosts, the IP address range of 192.168.10.1 through and including 192.168.10.254 can be assigned to hosts, and the IP address of 192.168.10.255 is the broadcast address used to send communication to all of the hosts in this specific subnet.

As you will learn in a subsequent course, routers advertise network addresses and prefixes, called routes, to other routers they communicate with. This informs the other routers that they can send traffic to the router because the router has a direct connection to that specific network.
Manipulating Host Bits

- Address & prefix of 192.168.10.1 /28
  - 28 network bits & 4 host bits
  - Subnet mask is 255.255.255.240
  - Host is in 192.168.10.0 – 192.168.10.15 subnet
  - $2^4 = 16$ possible addresses in this subnet
- Address & prefix of 172.16.10.1 /16
  - 16 network bits & 16 host bits
  - Subnet mask is 255.255.0.0
  - Host is in 172.16.0.0 – 172.16.255.255 subnet
  - $2^{16} = 65,536$ possible addresses in this subnet

Notes:
Therefore, the subnet mask determines how many total IP addresses are assigned to a specific network.

For example, with a host IP address and prefix of 192.168.10.1 /28, we know that we have 28 network bits and 4 host bits for this subnet, and that the subnet mask for all of the hosts in this network is 255.255.255.240.

We also know that this host is in the 192.168.10.0 network, that valid host addresses are 192.168.10.1 through and including 192.168.10.14, that this subnet’s broadcast address is 192.168.10.15. And, lastly, with 4 host bits, or $2^4$, we know that there exist 16 total IP addresses in this subnet.

Using the host IP address and prefix of 172.16.10.1 /16, we know that we have 16 network bits and 16 host bits for this subnet, and that the subnet mask for all of the hosts in this network is 255.255.0.0.

We also know that this host is in the 172.16.0.0 network, that valid host addresses are 172.16.0.1 through and including 172.16.255.254, that this subnet’s broadcast address is 172.16.255.255. And, lastly, with 16 host bits, or $2^{16}$, we know that there exist 65,535 total IP addresses in this subnet.
Have you noticed how our subnet masks vary in our examples? To better understand subnet masks, we need to step back in time to the early 1980's where IP addresses were divided into classes, based on the value of the 8-bits in the leftmost octet of the IP address.

In a classful IP addressing system, IP addresses are assigned a static mask based on the class in which the address resides. The IP address range of numbers is 0.0.0.0 through and including 255.255.255.255. Not all IP addresses can be used by hosts, some are reserved and cannot be used at all, some IP addresses can only be used on private networks – not the Internet, and other IP addresses can be used both in private and on the Internet.

The original IP address classes are A, B, C, D, and E. You need to memorize the information shown on this and the next slide for each class of IP addresses.

A Class A address is assigned the 255.0.0.0 mask, or the /8 prefix. Class A addresses start at 1.0.0.0 and end at 126.255.255.255.

A Class B address is assigned the 255.255.0.0 mask, or the /16 prefix. Class B addresses start at 128.0.0.0 and end at 191.255.255.255.

A Class C address is assigned the
### IP Address Ranges & Classes

**Slide 24**

**IP Address Ranges & Classes**

<table>
<thead>
<tr>
<th>Class D</th>
<th>Class E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast &amp; no default mask</td>
<td>Reserved &amp; no default mask</td>
</tr>
<tr>
<td>Address range start: 224.0.0.0</td>
<td>Address range start: 240.0.0.0</td>
</tr>
<tr>
<td>Address range end: 239.255.255.255</td>
<td>Address range end: 255.255.255.255</td>
</tr>
<tr>
<td>Not discussed further in this course</td>
<td>Not discussed further in this course</td>
</tr>
</tbody>
</table>

Notes:
- A Class D address is not assigned any mask because it is assigned to be used for a special type of network communication called multicast. Class D addresses start at 224.0.0.0 and end at 239.255.255.255.
- A Class E address is reserved and also has no assigned mask. Class E addresses start at 240.0.0.0 and end at 255.255.255.255.
- Class D and E addresses are beyond the scope of this course and will not be discussed much in future CCNA courses. However, on occasion, we will discuss Class D addresses when we get to switching concepts in a subsequent course.

### Special IP Addresses

**Slide 25**

**Special IP Addresses**

- **The zero range is reserved & cannot be used:**
  - 0.0.0.0 through 0.255.255.255
  - More detail on 0.0.0.0 later in course

- **Private ranges can be used in private networks:**
  - 10.0.0.0 /8 through 10.255.255.255
  - 172.16.0.0 /12 through 172.31.255.255
  - 192.168.0.0 /16 through 192.168.255.255

- **TEST-NET:**
  - 192.0.2.0 / 24 through 192.0.2.255
  - Can be used in textbooks & in examples

Notes:
- As we mentioned earlier, some IP addresses have special uses assigned to them.
- For example, the zero range is reserved & cannot be used. The zero range is 0.0.0.0 through 0.255.255.255. You will learn more about the special IP address of 0.0.0.0 later in this course.
- Private ranges can be used in private networks. A private network is the network at your home, the library, an Internet café, or at your place of work. You need to memorize the ranges of IP addresses that are reserved for private IP addressing.
The private IP address ranges are:

- 10.0.0.0 /8 through 10.255.255.255
- 172.16.0.0 /12 through 172.31.255.255
- 192.168.0.0 /16 through 192.168.255.255

The 192.0.2.0 / 24 through 192.0.2.255 address range, called TEST-NET, can be used in textbooks & in examples, but should not be used on the Internet.

Lastly, the IP address range of 169.254.0.0 /16 through 169.254.255.255 is assigned by an OS when no other IP address is available. For example, in most home and work networks, hosts receive an IP address by automatic assignment when they boot up from a Dynamic Host Configuration Protocol, or DHCP server. Your home router most likely serves as the DHCP server for your network and at work, your desktop computer most likely receives its IP address from a Windows Server configured with the DHCP server role.

If the DHCP server is unable to assign an IP address to a host, then the OS implements Automatic Private IP Addressing, called APIPA, and randomly assigns an IP address from the APIPA range to the host.

You will learn more about APIPA in an operating system or server course.

Another special IP address range is 127.0.0.0 /8 through 127.255.255.255, which is called the Loopback address range. This entire range of IP addresses is reserved for loopback operations. For example, to test that your OS and NIC are
operating properly, you can open a command prompt and type the command `ping 127.0.0.1`. When the NIC receives a communication with this IP address as the destination, the NIC does not send the communication outside of the NIC onto the wires in the network cable. Instead, the NIC loops back, or redirects the communication back to the OS through its circuitry. We will use the ping command extensively in this course and again a few slides ahead in this unit.

**IPv4 Communication Types**

- **Unicast – 1:1**
  - One host communicates with one other host in its network
- **Broadcast – 1: All**
  - One host communicates with all of the other hosts in its network
- **Multicast – 1: Many**
  - One host communicates with many of the other hosts in its network – but not all of them!

**Notes:**

IP version 4 provides a number of communication types. The main types of communication are the Unicast which is where one host communicates with one other host in its network. An example of a unicast communication is when you ping another host.

The broadcast communication type occurs when one host communicates with all of the other hosts in its network. An example of a broadcast is when your computer sends a message to every listening computer in its network, asking for their MAC and IP address. Your computer actually does this every few seconds, by default.

Lastly, the multicast communication type is where one host communicates with many of the other hosts in its network – but not all of them!

You will learn a bit more about multicast when we discuss IP version 6 later in this course.
Creating an IP Addressed LAN

- Which devices need IP address?
  - Routers, switches, printers, servers, hosts, etc.
- Create block of addresses with prefix
- Plan for growth in network
- Manually assign address or use DHCP Server?
  - Hosts usually receive addresses via DHCP
  - Others configured manually with static address
- Subnetting might be needed to be successful

Notes:

When you are tasked with creating a LAN which will implement an IP addressing scheme, you need to plan before actually doing any of that work.

For example, you need to know which devices need IP addresses. Examples include routers, switches, printers, servers, hosts, and any other devices that will communicate on the network. You should also be aware of the network’s needs for the next 3-5 years so that you create networks that will provide enough IP addresses today and into the future.

You also need to determine whether you will assign addresses manually or implement a DHCP server in your router or in some server OS. If you are to create a small network, say approximately 10 hosts, then you might decide to manually configure each host’s IP address. However, if you implement a network much larger than that you will probably decide to implement DHCP. You will learn how to configure a Cisco router as a DHCP Server in a subsequent CCNA course.

Lastly, you need to determine whether you will create one large network, or segment the hosts into smaller, separate networks called subnets. A subnet is a large network that has been broken down into two or more smaller networks.
Creating a Basic Subnet

- A subnet is many networks created from one IP address range
- Subnets created by manipulating network/host bits from classful start point
- Example: start with 192.168.10.0 /24 network address space
  - Borrow 5 host bits so prefix is now /29
  - Leaves 3 host bits for addressing
  - Now can create $2^5 = 32$ subnets using 5 borrowed bits
  - Can create 8 addresses per subnet using 3 remaining host bits ($2^3 = 8$)

Notes:
As I just said, a subnet is a large network that has been broken down into two or more smaller networks. Here, we can add that the subnets are usually created based on one larger IP address range.

We create subnets by manipulating the network and host bits from some IP address start point. For example, if we start with the 192.168.10.0 /24 network address space and take, or borrow, as this is called, 5 host bits so that the prefix is now a /29, this leaves us 3 host bits for addressing.

Therefore, we can create $2^5 = 32$ subnets using the 5 borrowed bits with each of the 32 subnets assigned 8 addresses using the 3 remaining host bits.

Basic Subnet Example

- Example from previous slide
- Borrow (steal!!) 5 host bits
  - $2^5 = 32$ subnets
- Leaves 3 host bits for addressing in each subnet
  - $2^3 = 8$ addresses per subnet
- New prefix /29
  - New subnet mask: 255.255.255.248

Notes:
When we reallocate host bits as network bits, we say that we borrowed the bits. In reality, we are not borrowing them since we have no intention of returning them as host bits!

Continuing our example from the previous slide, when we borrow 5 host bits, this leaves us with 3 host bits, which we can use to create IP addresses for each of the 32 subnets we will create. Again, the three host bits permit us to have a total of 8 IP addresses for each subnet.

In this example, which is shown in all of its detail
in the graphic on the right side of the slide, all of
the hosts in all of the 32 subnets will be assigned
a prefix of /29, which translates into a subnet
mask of 255.255.255.248.

Please pause the presentation and take a few
minutes to review all of the information on this
slide. Before you move onto the next slide, be
sure you can create this subnet and that you
understand how we created each subnet and its
details shown in the graphic.

### Subnetting Practice

- **Starting IP address:** 192.168.10.0 /24
  - Need at least 25 addresses per subnet
  - Need 6 total subnets
  - Solution on next slide!

### Notes:

Since you are listening to the lecture for this
slide, I assume that you are now ready to
practice what you have learned.

Therefore, create a network with a starting IP
address and prefix of 192.168.10.0 /24 that
provides a total of 6 subnets, with each subnet
able to address 25 hosts.

Pause the presentation now and create the
subnet. It might take you 10 minutes or longer to
do this, but stay with it until you get it. Refer back
to the previous slides in this unit for help and talk
with your instructor if you need further
assistance.

Before moving on, be sure to write out all of the
subnet data for all of the subnets you create, just
as we did on the previous slide.
Subnetting Practice Solution

- Starting IP address: 192.168.10.0 /24
  - Need at least 25 addresses per subnet
  - Need 6 total subnets
- Solution:
  - Borrow 3 host bits
  - Prefix now /27 (255.255.255.224)
- TIP: continue practicing in class until you can do this correctly!

Our solution requires us to borrow 3 host bits, giving us 27 network bits and 5 host bits for addressing. The /27 prefix works out to a subnet mask of 255.255.255.224, which will be assigned to every host in every subnet we create based on our starting IP address range. Borrowing 3 host bits means that we can create 8 subnets. Our requirement was only for 6 subnets, but using binary logic, this is as close to the exact requirement as we can get. With 5 remaining host bits we can provide for 32 total IP addresses each of the 8 subnets.

Subnetting Practice Solution (cont’d)

- Borrow 3 bits & create $2^3 = 8$ subnets
- Still have 5 host bits for addressing
  - Allows for $2^5 = 32$ total addresses per subnet

This slide’s graphic shows the 8 subnets, along with the network address, the first and last usable IP address for each subnet, and the broadcast address for each subnet.

Again, if you are struggling with these concepts, please talk with your instructor as soon as possible. Binary math and subnetting are key components of the CCNA training curriculum and you will use it extensively throughout this and the remaining courses!
In our previous subnetting exercises, we created subnets where each and every subnet provided the same number of host bits and the same subnet mask to each and every subnet we created.

However, in the real world, we often need to create both large and small subnets, all based on the same starting IP address block. What do we do then?

Fortunately, back in the early 1990s, classful IP addressing was replaced by a classless system of addressing called Classless Inter-Domain Routing, or CIDR, which allows the implementation of something called Variable-Length Subnet Masking, or VLSM. CIDR is implemented in a device’s OS and VLSM is the work we do to create subnets with different subnet masks.

In classless IP addressing, any IP address can be assigned any valid mask. You should recall that in classful IP addressing, a Class A address, such as 10.1.1.1, was automatically assigned a mask of 255.0.0.0. Because of CIDR, the IP address of 10.1.1.1 can be assigned a mask of 255.255.255.0, 255.255.0.0, 255.255.255.252, or any other valid subnet mask.
To implement VLSM, we employ the same logic we learned in basic subnetting. The big change is that we can create each subnet based on that specific subnet’s needs, rather than creating one generic solution.

For example, examining the information on the slide, we see that we have a requirement to create 4 different subnets, all based on the starting IP address range of 10.0.0.0 /8. For Subnet A, 100 host addresses are needed. For Subnet B, 50 host addresses are needed. For Subnet C, 13 host addresses are needed. And, for Subnet D, only 2 host addresses are needed.

Using VLSM, we can create each subnet independently of the others, providing each subnet with a closer allocation of IP addresses to what is needed rather than creating four subnets satisfying the need of the largest subnet we need to create.

Let’s get to work on creating these networks on the next slide.

One rule of thumb is to implement VLSM first on the network with the largest host requirement. In this case, the network with the largest host address is Subnet A, which needs an address space large enough to accommodate 100 hosts. Now is a good time to point out that when we need 100 host addresses, we really need a total of 102 total addresses in the subnet since we need a subnet address and broadcast address for the subnet.

To create 102 IP addresses, we need to keep a minimum of 7 host bits since $2^7 = 128$ and fills our need, and $2^6 = 64$, which does not provide enough IP addresses to fill our need of 102 total addresses.
Keeping 7 host bits means that the remaining 25 bits can be classified as network bits and with this information set, we can now create our first VLSM subnet. Its starting IP address is 10.0.0.1; its ending IP address is 10.0.0.127; its new prefix and subnet mask are /25 and 255.255.255.128 respectively.

The next subnet, Subnet B, will begin with the first address following the last address for Subnet A, which is 10.0.0.128.

Let's next turn our attention to Subnet B, which, as we previously determined, will begin with the first address following the last address for Subnet A, which is 10.0.0.128.

To create 52 IP addresses, we need to keep a minimum of 6 host bits since $2^7 = 128$, which fills our need but provides too many IP addresses, and $2^6 = 64$, which does provide enough – and slightly more – IP addresses to fill our need of 52 total addresses, and $2^5 = 32$, which does not provide enough IP addresses to fill our need of 52 total addresses.

Keeping 6 host bits means that the remaining 26 bits can be classified as network bits and with this information set, we can now create our second VLSM subnet. It's starting IP address is 10.0.0.128; its ending IP address is 10.0.0.191; its new prefix and subnet mask are /26 and 255.255.255.192 respectively.

The next subnet, Subnet C, will begin with the first address following the last address for Subnet B, which is 10.0.0.128.
Let's next turn our attention to Subnet C, which, as we previously determined, will begin with the first address following the last address for Subnet B, which is 10.0.0.192.

To create 15 IP addresses, we need to keep a minimum of 4 host bits since $2^5 = 32$, which fills our need but provides too many IP addresses, and $2^4 = 16$, which does provide enough – and slightly more – IP addresses to fill our need of 15 total addresses, and $2^3 = 8$, which does not provide enough IP addresses to fill our need of 15 total addresses.

Keeping 4 host bits means that the remaining 28 bits can be classified as network bits and with this information set, we can now create our third VLSM subnet. It’s starting IP address is 10.0.0.192; its ending IP address is 10.0.0.207; its new prefix and subnet mask are /28 and 255.255.255.240 respectively.

The next subnet, Subnet D, will begin with the first address following the last address for Subnet C, which is 10.0.0.208.
VLSM Solution: Subnet D

<table>
<thead>
<tr>
<th>Notes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last up is Subnet D, which, as we previously determined, will begin with the first address following the last address for Subnet C, which is 10.0.0.208.</td>
</tr>
<tr>
<td>To create 4 IP addresses, we need to keep a minimum of 2 host bits since $2^2 = 4$, which exactly fills our need of 4 total addresses.</td>
</tr>
<tr>
<td>Keeping 2 host bits means that the remaining 30 bits can be classified as network bits and with this information set, we can now create our fourth and final VLSM subnet. It’s starting IP address is 10.0.0.208; its ending IP address is 10.0.0.211; its new prefix and subnet mask are /30 and 255.255.255.252 respectively.</td>
</tr>
<tr>
<td>The next subnet, will begin with the first address following the last address for Subnet D, which is 10.0.0.212. We do not have a need to create another network, so our work is complete!</td>
</tr>
<tr>
<td>Next, let’s take a look at the four subnets we created in graphical format.</td>
</tr>
</tbody>
</table>
Slide 40

VLSM Solution: Graphic
Duration: 00:00:18
Advance mode: Auto

Notes:
Take a moment to review the graphic shown on the slide. Did you come up with the same subnet data as you see in the graphic?
If you have any questions about basic subnetting, CIDR, or VLSM, please talk to your instructor as soon as possible!

<table>
<thead>
<tr>
<th>Subnet#</th>
<th>Subnet Address</th>
<th>First Usable</th>
<th>Last Usable</th>
<th>Broadcast</th>
<th>New Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>10.0.0.0</td>
<td>10.0.0.1</td>
<td>10.0.0.126</td>
<td>10.0.0.127</td>
<td>255.255.255.128</td>
</tr>
<tr>
<td>B</td>
<td>10.0.0.128</td>
<td>10.0.0.129</td>
<td>10.0.0.190</td>
<td>10.0.0.191</td>
<td>255.255.255.192</td>
</tr>
<tr>
<td>C</td>
<td>10.0.0.192</td>
<td>10.0.0.193</td>
<td>10.0.0.206</td>
<td>10.0.0.207</td>
<td>255.255.255.240</td>
</tr>
<tr>
<td>D</td>
<td>10.0.0.208</td>
<td>10.0.0.209</td>
<td>10.0.0.210</td>
<td>10.0.0.211</td>
<td>255.255.255.252</td>
</tr>
</tbody>
</table>

Slide 41

Testing Our IP Address Logic
Duration: 00:01:51
Advance mode: Auto

Notes:
With our IP addressing scheme in hand, we can manually assign IP addresses to our hosts or implement a DHCP solution. For our example, let’s assume that we used DHCP on the two large networks and manually assigned IP addressing for the two smaller networks.

When all of the hosts in a subnet have an IP address, you cannot assume that what you did worked without proving it. One way you can test your work — and logic — is to use the command line to look up your host’s IP address, subnet mask, and default gateway. To do this, click the Windows key on the keyboard, type the...
command cmd, and press Enter to open a Windows command prompt. Then, type the IPCONFIG command you see in the top right graphic and press Enter to display your NIC’s IP configuration data. This graphic shows the data for my wireless NIC. What you see here should match your work. We assigned this host an IP address of 192.168.1.13, a mask of 255.255.255.0, and a default gateway of 192.168.1.1.

Then, using this information, get started by pinging your host’s NIC by pinging its loopback address, which is shown in the graphic on the bottom right of the slide. Type the command ping 127.0.0.1 and press Enter. The output of four replies, all in the range of a few milliseconds, indicates that your host’s NIC is functioning properly.

**Notes:**
A host’s default gateway is the router through which its communications must pass to gain access to the Internet, which is outside of the local area network. In a home network, a cable modem router or some other device is usually the home network’s default gateway and the cable modem router also fills the role of the DHCP server in the network.

To test networking beyond your host’s NIC, ping the IP address of your default gateway based on the output you obtained when you ran IPCONFIG on your host. Again, the output of four replies, all in the range of a few
milliseconds, indicates that your host's NIC is functioning properly, as is the cable – or wireless antennae – connecting you to the default gateway. This test also indicates that this host is able to communicate with its default router and can, most likely, get to the Internet.

<table>
<thead>
<tr>
<th>Slide 43</th>
<th>More Testing Tools (cont’d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration: 00:01:07</td>
<td></td>
</tr>
<tr>
<td>Advance mode: Auto</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
<tr>
<td>The trace route command, shortened for use in the Windows command line as tracert, works similar to ping and is useful for testing in large networks or on the Internet.</td>
<td></td>
</tr>
<tr>
<td>For example, from your host’s command line, ping Google by its name – not by its IP address. The output, which based on my ping, is shown on the slide, displays a reply from each router in the path from my home router to Google’s actual Web server.</td>
<td></td>
</tr>
<tr>
<td>Looking through the lines of output, you should be able to gleam that my ping originated in Oregon and worked its way through to Seattle, Washington. However, the final line of output, line 16, does not make clear where on earth the Google Web server actually resides.</td>
<td></td>
</tr>
<tr>
<td>Notice that near the end of the trace route output, on line – or hop – 15, that the request timed out. This usually occurs because this router in the path does not reply to ping or trace route requests.</td>
<td></td>
</tr>
</tbody>
</table>
The ping and trace route commands are both based on the Internet Communication Messaging Protocol (ICMP), shortened to ICMP.

Trace route sends a message, requesting a reply from every router in route to destination – one at a time.

As we discussed on the previous slide, some devices are configured to ignore ICMP messages to enhance their security. Why reveal any information about an Internet device if it is not necessary? Attackers use tools like ping and trace route to perform reconnaissance, which is the very beginning operation of planning an attack against a target.

As you saw a few slides back, our trace route output did not reveal where on earth the Google website server actually is located. So, I used a search engine to determine its location based on the information revealed in the reply of the last line of the trace route output.

A small amount of research revealed that this Google Web server is located in California. You will learn more about ICMP, and the ping and trace route commands later in this course.
After all of our work in creating a VLSM network, it seemed a good idea to create a graphic to show what it might look like in the real world. Our four networks are joined by two routers, which are connected to each other using serial cables. Each router and all of the host devices in the network are connected to its switch through an Ethernet cable.

Since this is the end of this unit’s material, you should understand the VLSM implementation you see on the slide’s graphic. If you have any questions, please talk them over with your instructor.

We cannot close our discussion about IP addressing without a small tutorial on IP version 6, shortened to IPv6.

Please open this slide’s notes section now and read along with me as we discuss IPv6 and some of its underlying mathematics.

IP version 6 uses hexadecimal characters instead of decimal numbers. IPv6 addresses are made up of eight groups of four hexadecimal characters, with each hex character representing four bits. Therefore, performing basic math of 8x4x4, an IPv6 address is a 128-bit address.

Valid hexadecimal characters are zero through nine, and A through F. This allows us to represent numbers from ten to fifteen with one character. The characters A and F, in hexadecimal, represent the numbers ten and fifteen, respectively, in decimal.
Taking this discussion a bit further, each hex character initially stands alone when we need to convert it to a binary number. Then, all of the binary numbers are placed in order from left to right, to create a full binary word. For example, the leftmost four hex characters of fe80 are, in binary:

F, which is 15 in decimal, is 1111 in binary;
E, which is 14 in decimal, is 1110 in binary;
8, which is 8 in decimal, is 1000 in binary;
0, which is 0 in decimal, is 0000 in binary.

Therefore fe80 in hex expands to 1111111010000000 in binary. Performing binary math, the decimal equivalent for fe80 is 65,152. Test the math yourself by opening up the Windows calculator, viewing the Programmer calculator, clicking Hex, and typing in fe80. Next, click the Dec and Bin options to view fe80 in those two systems. They will match up with what is written in this slide's notes section.

While it is helpful to understand how hex, binary, and decimal numbers are related, we generally do not need to convert hex numbers into other formats.

An IPv6 address consists of an IP address and a prefix number, which we can relate to a subnet mask.

Assuming that IPv6 addressing now makes sense, if you look at the IP version 6 address as depicted on the screen, you can see that the device that possess this IPv6 address has a local or a private IP address. The prefix, which is a
/23, informs us that the first 23 bits of this address apply to the network and that the rest of the bits, 109 bits, can apply to host devices.

IPv6 offers enough address space to provide every person on the planet millions of IP addresses well into the future - even when the earth's population reaches 10 billion people!

IP addressing, in particular IPv6, represents a very complex topic. A deeper discussion of IPv6 is beyond the scope of this unit. You will learn about IPv6 in a subsequent course.

Notes:
Configuring IPv6 is the same as configuring IPv4, except that we need to use IPv6 addressing, which is different from IPv4 addressing, and a prefix rather than a subnet mask. This slide displays the IP version 6 Properties sheet from a Windows 7 desktop computer.

You will learn more about IPv6 later in a subsequent course.
This concludes Unit 3 of IP Addressing. In this lecture, we learned to:

- Explain the purpose of IP addressing
- Differentiate and contrast between classful and classless IP addressing
- Convert between hexadecimal, binary, and decimal numbers
- Create a valid IP address scheme for a network
- Subnet a network address space
- Use VLSM to best utilize IP address space
- Verify an IP address implementation using common network utilities
- Differentiate between IPv4 and IPv6 addressing

References

CCNA 2: Switching & Routing

Unit 2: Basic Switching
It seems wise to begin this unit with a caveat. If you are using simulation software to perform the switch commands and configurations you are learning here, be forewarned that a number of the commands you attempt here can only be used on physical equipment.

While simulation software is a great tool, currently, it does not provide the functionality to complete all of the commands in the CCNA curriculum.

The objectives for this lecture, Basic Switching, are to gain the abilities to:

- Differentiate between broadcast & collision domains
- Differentiate between half & full duplex modes
- Explain the concept of a network bottleneck & mitigation techniques
- Explain the switch boot sequence
- Explain basic switch forwarding operations & methods
- Explain why switch port security is necessary
- Configure a Cisco switch with basic settings
- Configure a Cisco switch with an IP address & default-gateway
- Configure a Cisco switch with basic port security settings
- Verify a switch configuration using SHOW commands
- Differentiate between MAC flood & DHCP snooping attacks
Notes:

One big limitation associated with hubs, is that hub ports can send or receive traffic simultaneously, but not both. This type of operation is referred to as half-duplex mode.

Switch ports, on the other hand, can send and receive traffic simultaneously. This type of operation is referred to as full-duplex mode.

Modern switch ports are set to autosense what the other end of the connection can handle. For example, if a switch port is connected to a hub, it senses that the hub’s port can only operate in half-duplex mode and acts accordingly.

Ports on a Cisco 2960 switch can be set to auto, full, or half duplex mode. The auto option is the default setting, but it can be changed in the CLI.
Notes:
Current PC NICs are set for Auto Negotiation. In the slide’s graphic, this PC’s Marvell Yukon NIC auto-negotiates its speed and duplex setting with the switch managing its switch port.

Notes:
Let’s take a moment to review and differentiate between broadcast and collision domains.

Each router interface creates a broadcast domain, and routers to not forward broadcast traffic unless you change its settings to allow broadcast traffic to pass from one router interface to another.

Switches, on the other hand, forward broadcasts out of every port on the switch, excepting the port through which the broadcast was received. Therefore, switch ports expand a broadcast domain, but do not define it as a router does.

Unfortunately, a larger broadcast domain adds latency to the network, slowing its communications because each physical interface in a packet’s path, from source to destination, must recreate the packet and forward it to the next switch or router in the path.

Obviously, inexpensive switches are quite a bit slower than more expensive Access layer switches.
Slide 6
Broadcast vs. Collision Domain
Duration: 00:00:19
Advance mode: Auto

Broadcast vs. Collision Domain
- How many broadcast & collision domains are in the graphic?

Notes:
How many broadcast & collision domains can you locate in the graphic? Pause the presentation and figure out the answer. Then, pause the presentation and look for the answer in this slide’s notes section.
Slide notes:
1. There are a total of four router interfaces in the graphic. Therefore, this network contains a total of four broadcast domains.
2. Router 1 and Router 2 have one collision domain contained in their serial connection.
3. Switch 1 has 10 PCs and 1 router connected to it. Therefore Switch 1 provides for 11 collision domains.
4. Switch 2 has 11 PCs and 1 router connected to it. Therefore Switch 2 provides for 12 collision domains.
5. This network contains a total of 24 (1 + 11 + 12) collision domains.

Slide 7
Local vs. Remote Frame
Duration: 00:01:30
Advance mode: Auto

Local vs. Remote Frame
- Switch reads port traffic to learn L2, L3, & port number mappings
- If frame destination MAC address not found in switch MAC address table, ARP to find it
- If MAC address still unknown, send to L2 address of default-gateway or send out all other ports
- PC maintains its own ARP table & will forward to its default-gateway if it can

Notes:
How does a switch forward traffic it receives on a switch port to its destination? A destination might be a port that is part of the switch’s motherboard, a port connected to another switch in the network, or a switch in some other network that must be reached via the Internet.

To get started, the switch reads port traffic to learn its Layer 2, Layer 3, and port number mappings. Then, when the switch receives traffic that it must forward, if the frame destination MAC address is not found in the switch’s MAC address table, the switch performs an ARP to find it, hoping that its own MAC address table is simply incomplete. If the switch learns of a path to the destination MAC address, the switch forwards the
traffic out the port associated with that path. However, if the destination MAC address is still unknown, the switch sends the traffic to the Layer 2 address of its default-gateway if it has one, or sends it out all of its other switch ports. Then, when the router receives the traffic, it looks up the Layer 3 address and routes it out the port associated with the port associated with that path.

As a side note, modern PCs maintain their own ARP tables and forward unknown traffic to their default-gateway on their own.

**Notes:**
Switches can add latency to the network's traffic, depending on the traffic forwarded. Consider too that switches are inter-connected via cables. Will the cables support the network's throughput needs? Or, will the switch create a bottleneck by being unable to forward traffic in a timely manner because the traffic received is too much to handle in a timely manner?

In addition, if a Layer 3 switch is configured to permit or deny certain network traffic via access control or other means, this too adds latency to the network.
Notes:
One thing that we can do as network administrators is to aggregate, or team switch ports together to prevent bottlenecks from occurring. Another thing we can do is install more than one NIC in our servers and team the server NICs together using the server’s OS and NIC drivers. With switch ports and server NICs each teamed, we are create an optimized communication channel between the switch and the server.

To do this, the server NICs must be compatible with switch channeling. For example, Intel server NICs are optimized to channel with Cisco switches. In this type of setup, the NIC driver communicates with the switch itself to best use the channel that directly connects the server NIC and switch ports together.

Obviously, inexpensive switches do not support port aggregation. As a reminder, Cisco’s term for port aggregation is EtherChanneling.

Notes:
When a switch receives a frame, the switch stores the packet for a brief period of time in a memory buffer. Memory buffering is built into the hardware of the switch and is generally not configurable.

There are two methods of memory buffering, which are port-based and shared memory. Think of a bank teller line to understand the concept of memory buffering.

In port-based memory buffering, frames are stored in queues that are linked to specific incoming ports. A frame is transmitted to the outgoing port only when all the frames ahead of it in the queue have been successfully transmitted. It is possible for a single frame to delay the transmission of all the frames in
memory because of a busy destination port. Port-based buffering can be likened to having one line for each bank teller in a bank lobby area. Shared memory buffering deposits all of the frames it receives into a common memory buffer that all the ports on the switch share. Therefore, the amount of buffer memory required by a port is dynamically allocated. The frames in the buffer are linked dynamically to the destination port. This allows the packet to be received on one port and then transmitted on another port, without moving it to a different queue. Shared buffering can be likened to having one line to all of the bank tellers in a bank lobby area.

<table>
<thead>
<tr>
<th>Slide 11</th>
<th>Switch Forwarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Forwarding</td>
<td>Notes:</td>
</tr>
<tr>
<td>Two default methods:</td>
<td>When switches receive frames, the frames are received and forwarded in one of two default methods, with one of the methods providing a couple of variants. A switch's switching mode is per switch and cannot be modified on a 'fixed configuration switch' – like a Cisco 2960. However, some Distribution and Core layer switches can have their switching mode changed to better fit the needs of the network.</td>
</tr>
<tr>
<td>a) Store &amp; forward (default for 2950/2960 series)</td>
<td>One switch forwarding mode is the store-and-forward method, which receives the entire frame, calculates the CRC on the frame, and then forwards the frame out of one of its switch ports. This is the default for a 2950/2960 switch.</td>
</tr>
<tr>
<td>b) Cut-through (Core switches)</td>
<td>The other main switch forwarding mode is the cut-through mode, which forwards a frame as soon as the switch learns the destination MAC address for the frame. There is no error checking with cut-through, so corrupt frames are forwarded onto the network by the switch.</td>
</tr>
<tr>
<td>1) Fast-forward</td>
<td>Cut-through is further broken down into one of two</td>
</tr>
<tr>
<td>1) Lowest level of latency</td>
<td></td>
</tr>
<tr>
<td>2) Forwards frame when MAC address is known</td>
<td></td>
</tr>
<tr>
<td>2) Fragment-free</td>
<td></td>
</tr>
<tr>
<td>1) Compromise between S&amp;F and CT</td>
<td></td>
</tr>
<tr>
<td>2) Reads first 64-bytes of frame to discover “runts” which are collision survivors</td>
<td></td>
</tr>
<tr>
<td>3) If first 64-bytes is okay, frame is forwarded</td>
<td></td>
</tr>
</tbody>
</table>

Notes:

- Two default methods:
  a) Store & forward (default for 2950/2960 series)
     - Receives entire frame before forwarding it
  b) Cut-through (Core switches)
     1) Fast-forward
        1) Lowest level of latency
        2) Forwards frame when MAC address is known
     2) Fragment-free
        1) Compromise between S&F and CT
        2) Reads first 64-bytes of frame to discover “runts” which are collision survivors
        3) If first 64-bytes is okay, frame is forwarded
variants. The first variant is fast-forward switching. Fast-forward switching offers the lowest level of latency because it immediately forwards a frame after reading its destination address.

The other variant is fragment-free switching. In fragment-free switching, the switch stores the first 64 bytes of a frame before forwarding it. Then, if the first 64 bytes contain the correct fields, the switch forwards the frame even as it is still receiving it.

Fragment-free switching can be viewed as a compromise between store-and-forward switching and cut-through switching. The reason fragment-free switching stores only the first 64 bytes of the frame is that most network errors and collisions occur within the first 64 frame bytes. Fragment-free switching tries to enhance cut-through switching by performing a small error check on the first 64 bytes of the frame to ensure that it is not the survivor of a collision before forwarding the frame back onto the network.

---

**Symmetric & Asymmetric Switching**

- Not all port speeds from all LANs the same
  - Symmetric – ports all same bandwidth
  - Asymmetric – ports of varying bandwidth

---

**Notes:**

All ports from all of the LANs in a network may not be of the same speed. Therefore, switches must account for these varying speeds and use memory buffering to place frames on the media in a speed that can be accepted by the device on the other end of the media. A switch can be set for symmetric or asymmetric operations and the setting applies to all of the ports on the switch.

When a switch is set for symmetric operation, all of its ports all support the same bandwidth; when a switch is set for asymmetric operation, its ports can handle varying bandwidths, as shown in the slide’s graphic.
Most switches today are asymmetric.

<table>
<thead>
<tr>
<th>Slide 13</th>
<th>Layer 2 vs. Layer 3 Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration: 00:01:24</td>
<td>Advance mode: Auto</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Layer 2 vs. Layer 3 Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Layer 2 switch forwarding based on MAC address only</td>
</tr>
<tr>
<td>✓ Layer 2 address is the MAC address</td>
</tr>
<tr>
<td>• Layer 3 routing based on IP address</td>
</tr>
<tr>
<td>• Layer 3 address is the IP address</td>
</tr>
<tr>
<td>• Layer 3 switch can perform most router functions:</td>
</tr>
<tr>
<td>• Not a good idea for Core implementations</td>
</tr>
<tr>
<td>• Can reduce cost by using in other layers though</td>
</tr>
<tr>
<td>• Can implement ACLs, QoS, etc.</td>
</tr>
</tbody>
</table>

**Notes:**
A Layer 2 switch performs switching and filtering based only on the OSI Data Link, or Layer 2 MAC address. A Layer 2 switch is completely invisible to network protocols and user applications. It simply receives and forwards frames.

A Layer 3 switch, such as a Cisco Catalyst 3500 series switch, functions similarly to a Layer 2 switch, such as the Cisco 2960, but instead of implementing only Layer 2 functionality, it also performs Layer 3 routing and access control functions.

Because Layer 3 switches are capable of performing Layer 3 routing functions, they reduce the need to purchase and place dedicated Layer 3 routers on a LAN. Because Layer 3 switches have specialized switching hardware, they can typically route data as quickly as they can switch it. A Layer 3 switch can also use IP address information to route packets.

I should point out that a Layer 3 switch isn't a good choice for connecting WANs because of protocol and WIC limitations. So, before you purchase a Layer 3 switch, ensure that you completely understand what functions the device will perform in the LAN.
Switch Boot Sequence
- Bootstrap loaded from motherboard ROM
- Begins the boot process
- Performs POST to discover hardware & interfaces
- During POST, switch LEDs blink & SYST LED rapidly blinks green when POST passes
- If POST fails, SYST LED flashes amber color
- Initiates flash memory so it can be read
- Bootstrap program locates default IOS image in flash memory & loads it into RAM
- Settings in Startup-Config file stored in NVRAM copied to RAM as Running-Config

Notes:
Next, let’s briefly review the switch boot process and sequence of bootup events. What follows is an overview of the process, not a detailed play-by-play call.

When the switch is plugged into an electrical outlet, the bootstrap program is loaded from the motherboard’s ROM to RAM, which begins the actual boot process. A switch, unlike a router, does not have an on/off switch. Plugging it into a receptacle powers it on. A bootstrap program allows a device to power itself up and perform POST to discover its hardware, including its interfaces. POST is an acronym for power on, self test.

During POST, the Cisco switch’s LED lights, located near its front, top left corner, blink and the SYST LED rapidly blinks green when POST passes its testing process. If POST fails, the SYST LED flashes an amber color. If POST fails, it is almost always the result of a hardware failure, meaning that you will, most likely, need to send the switch in for repairs or recycle it.

Next, the bootstrap program initiates the switch’s flash memory so that it can be read. After flash memory is ready for reading, the bootstrap program locates the default Cisco IOS image in flash memory and loads it into RAM. When viewing the boot process on the screen via a terminal emulation application, when the IOS is being unpacked into RAM, the screen fills with a flood of pound signs (#). Lastly, the settings in the startup-configuration file, which is stored in NVRAM, are copied to RAM as the running-configuration.
Slide 15
Initial Connection
Duration: 00:01:43
Advance mode: Auto

Notes:
To perform an initial connection and initial switch configuration, you follow the same process as you learned to perform for a router, using terminal emulation software with the same settings as you applied for a router.

The slide’s graphic on the left shows the settings for a serial connection to a Cisco switch or router. Note that in this example I used Putty to create a serial connection to the switch and that I configured these settings by clicking Serial in the left navigation pane.

The two bottom-right graphics display a console and USB-to-DB9 adapter respectively. The console and USB adapter cables are joined together via their female/male serial cable ends, the RJ-45 end of the console cable is connected to the router’s console port, and the USB adapter’s RJ-45 end is connected to a USB port on the switch or router.

Do not forget that the USB adapter cable will not function without first installing its driver. Notice too that the serial line was connected to a port labeled COM5. This is a virtual COM port created by the OS so that the USB adapter’s driver is able to have COM port traffic directed to it.

Lastly, the graphic at the top-right displays the rear left of a Cisco 2960 switch, with its console port in view.

Slide 16
Basic Configuration
Duration: 00:00:31
Advance mode: Auto

Notes:
A basic switch configuration involves renaming the switch, configuring its management VLAN interface, configuring other ports, or interfaces for PCs to connect to them, and to save the running-configuration data in RAM to the startup-configuration file in NVRAM.

In our example, on the next slide, we will only configure one interface for a PC to connect to, which is FastEthernet port 0/1.
Basic Configuration Commands

- Change switch name
- Configure management interface
- Configure port for general access

Switch Management Configuration

- Similar to configuring a router
  - Except when applying IP addresses!
  - Router interfaces operate at Layer 3 and are assigned IP addresses
  - Switch ports operate at Layer 2 and only use the burned-in MAC address
    - Only the switch management VLAN is configured with IP address to telnet and otherwise communicate with it

Notes:
This slide’s graphic displays the commands to move from User Exec mode to Privileged Exec mode, change the switch’s name to Switch1; configure its management VLAN, VLAN 99, with an IP address and change its status to up; configure port FastEthernet 0/1 for access by some end device, and lastly, to copy the running-configuration data in RAM to the startup-configuration file in NVRAM.

Let’s take a moment to learn more about the management VLAN on the next slide.

Notes:
Before we turn our attention to learning more about the switch’s virtual management interface, let’s first compare physical and virtual ports on a router, which do receive an IP address configuration, to physical and virtual ports on a switch.

Physical switch ports are not configured with an IP address. The host connecting to the switch port is configured with an IP address and the switch uses the host’s Layer 2 and Layer 3 data to forward traffic to and from the host via its connected port. Because a basic switch only operates at Layer 2 of the OSI model, switch ports mainly utilize a host’s Layer 2, or MAC address for their operations. Physical switch ports are also always in the “up” state, meaning that we do not need to configure them with the no shutdown command.

A switch is configured with one, and sometimes more, virtual interfaces, which are configured with an IP address and must be moved to the “up” status using the no shutdown command. In many of the examples you will see online and in this course, we will use VLAN 1 or 99 to configure a switch’s virtual interface, or VLAN interface. However, you can use any number you wish to use in the ‘real world.’

When a switch is configured with a management VLAN interface and is configured for telnet or SSH
access, we can use the IP address associated with the management VLAN interface to connect to the switch.

You should recall from your basic network training that just because Host 1 can communicate with Switch 2, this does not mean that Switch 2 can communicate with Host 1.

For example, using the graphic on the left as our example network, when Host 1 pings Switch 2, the ping request is forwarded by Switch 1 to Router 1. Router 1 examines its routing table for a route to Switch 2’s IP address, finds it, and forwards the ping request to Router 2. Router 2 performs the same routing table lookup as Router 1 did, and forwards the ping request to Switch 2.

When Switch 2 responds to the ping request, it sends its ping reply back to Host 1 via Router 2. As before, Router 2 examines its routing table for a route to Host 1’s IP address. However, this time, Router 2 does not locate a route back to Host 1’s network because Router 2 is not configured with a dynamic routing protocol and neither is it configured with a static route for that specific LAN.

To solve this dilemma, the network admins need to implement the same dynamic routing protocol on Routers 1 and 2, and configure each switch with a default gateway pointing to their respective routers, the
same as we configure a PC.

With these configurations in place, the ping reply from Switch 2 will be routed back to Host 1. The graphic on the right displays the command to configure a switch with a default gateway and save the setting to the startup-config file. Take note of the dash between the words default and gateway!

Notes:
Configuring telnet and SSH line configurations are the same for a switch as they are for a router.

As part of the configuration process, remember to configure the domain name and crypto keys, and to use the transport input ssh command as you see on the slide. Of course, don’t forget to copy the new settings to the startup-config file when you are finished.

Notes:
The slide’s top graphic provides you with a complete command set to enable SSH on a switch, and the bottom graphic shows you how to disable SSH.

To generate the RSA key pairs, use the crypto key generate rsa command in global configuration mode. Then, to configure Secure Shell, or SSH control parameters on the switch, use the ip ssh global configuration command to set the optional timeout interval, which is a time period that the switch waits for the SSH client to respond to an SSH connection negotiation request and the optional authentication-
The `retries` command, which is the number of login attempts that can be attempted before further connection attempts are refused. Next, we configure the `vty` line for SSH access only, requiring the password of `cisco` to login via SSH.

We disable SSH by zeroizing the RSA keys. In this example, we reverted back to permitting telnet sessions to the switch.

One other item we should mention, in the top configuration graphic, is the `service password-encryption` command, which is issued in global configuration mode. This command weakly encrypts all of the router’s existing unencrypted passwords using the Message Digest 7, or MD7 algorithm.

<table>
<thead>
<tr>
<th>Slide 22</th>
<th>MD7 Encryption</th>
</tr>
</thead>
</table>
| **Duration:** 00:01:06  
**Advance mode:** Auto | **Notes:**  
We way that this type of encryption is weak because it can be cracked using free online hacker tools. All you need is the output of the MD7 encryption process to input into the MD7 cracker tool.

In the slide’s output, we created an unencrypted enable password using the enable password rather than the enable secret command. Next, we issued the service password-encryption command to encrypt any existing, unencrypted passwords using the weak MD7 encryption algorithm. Then, we display the output of the MD7 encryption algorithm, which is called the password hash, via the `show run` command.

In the `show run` output, you can see that the enable password is encrypted using MD7 because the hash is preceded by the number 7.

Let’s see how easy it is to crack MD7 hashes on the next slide.
Notes:
This slide’s graphic illustrates how easy it is to crack an MD7 encrypted password.

After performing an online search using the term decrypt md7 password, I selected the link to the IFM Network Experts site, pasted in the password’s hash in the Type 7 Password field, and clicked Crack Password. The original, unencrypted password is immediately displayed in the field below the Crack Password button.

This website’s comment near the bottom of the page says it all, via the warning: “Don't use the old type 7 passwords anymore. Use the new "secret" keyword only.” This is good advice!

Slide notes:
http://www.ifm.net.nz/cookbooks/passwordcracker.html

Notes:
The Message Digest 5, or MD5 algorithm is a much better option than using the easily cracked MD7 option to encrypt passwords.

To encrypt a Cisco router or switch using MD5’s algorithm, when you configure its enable password, use the enable secret command, not the service password-encryption command.

Issuing the enable password command creates the enable password, but when the show run command is issued, the unencrypted enable password is displayed for anyone to see. We will never do that in the real world!

In the show run output, you can see that the enable password is encrypted using MD5 because the hash is preceded by the number 5.
For added fun, run these commands on your switch, copy the MD5 hash, and try to decrypt it using the tool we used on the previous slide. I pasted its URL in that slide’s notes section if you want to use it.

Notes:
Another good switch or router management practice is to configure the device with messages that inform users of upcoming device maintenance and/or to warn users that unless they are authorized to connect to the device, they should not attempt to do so.

The two main message types are the MOTD and LOGIN messages, each of which is called a banner. The Message of the Day, shortened to MOTD, displays itself before the login banner appears, if it is configured, just after the device finishes loading the settings in the startup-config file. The Login banner displays itself before the username and password prompt, if the device is configured to login via user accounts.

The slide’s graphic illustrates how to create each type of banner. For example, in global configuration mode, after issuing the banner motd command, we inform the router of the actual MOTD message by enclosing it within a pair of delimiter characters. I used the pound sign as the delimiter in my examples here. Everything placed between the delimiter pair represents the message and its formatting, which can include blank lines and punctuation.
Users & Passwords

- Good practice to create usernames with secret passwords
- Accounts stored in switch/router local security database
- Configure username & password
- Configure line access mode(s)
- Remember to save to startup-config file!

Notes:

Another good security practice is to create usernames and passwords for those who need to login to the switch or router, along with encrypted, or secret passwords. The user accounts you create can be stored in the device's local security database.

After configuring the usernames and passwords in global configuration mode, you next configure the applicable line access modes to require user accounts stored in the local security database. Lastly, remember to save the changes to the startup-config file when you are finished!

An advanced user account configuration can integrate itself with a server's active directory of user accounts and passwords. To accomplish this, you first configure the switch or router to send login authentication requests to what is called a RADIUS, or Remote Authentication Dial-In User Service server. Then, the RADIUS server is configured to securely communicate with the active directory server to receive login authentication permits or denials. The RADIUS server then sends the permit or denial back to the switch or router.

You will learn how to configure a Cisco device to communicate with a RADIUS server if you take the Cisco CCNA Security course.
Notes:

This slide’s graphic illustrates how to create a user account and password in global configuration mode. The top red arrow points to the creation of the user account with an MD5 encrypted password, and the bottom red arrow points to the line con 0 configuration, where the login local command is used to permit console port connections to users with user accounts in the switch’s local security database. After copying these changes to the startup-config file and reloading the router, the bottom output reveals a successful login using the student account and its password.

Notes:

An out-of-the-box switch is not configured with any port security. This means that any device can connect to any of its ports and communicate, whether you want them to or not. Unsecure switch ports are an easy target for attackers because, then, they can work to take over management of the switch to change its configuration, lock you out of its management tools, and/or to sniff all of the traffic that passes through the switch.

To enable port security on a port, we navigate to interface configuration mode and issue the switchport port-security command.

Enabling port security means that the switch can restrict port use by MAC address, that a violation of port security can shut the port down, and that we can set the number of MAC addresses permitted to use a port. The switch can learn MAC addresses by plugging devices into the switch port one at a time, or by the switch administrator manually entering each MAC addresses into the switch port’s configuration.
Switch Port Security Basic Example

- Enables default port security
  - Must be entered for each port
    - Can use range command to configure many ports simultaneously
  - Maximum MAC addresses = 1
  - Current address reset upon reload
  - Violation mode = shutdown

Notes:
This slide’s graphic illustrates how to enable a switch’s default port security. Remember, port security must be configured for each port; port security is not configured switch-wide using one set of commands.

In this example, we first configure Fast Ethernet ports 1-12 for access mode by issuing the switchport mode access command. The effect of this command is to set the ports so that any end device can connect to it.

We enable port security through the switchport port-security command. A switch’s default port security can be configured port-by-port or by configuring a range of ports all at once, as we did in this example by adding the range keyword to the interface configuration command.

A switch’s default port security provides for one MAC address to be associated with that port, with a MAC address violation resulting in the port being shut down. When a port is shut down it is unable to send or receive communication to or from the host device connected to the port and the port’s LED is set to a solid amber color.

Reloading the switch erases the one MAC address from its memory, permitting another host, with another
Switch Port Security Expanded

- A bit more complexity...
  - Configure ports 1-12 simultaneously
  - Set max. MAC addresses
  - Force switch to memorize MAC addresses & not forget them upon reboot
  - Set violation mode to shutdown

Notes:
This slide’s graphic displays a more robust security configuration for the same switch ports.

As before, we begin by placing the ports in access mode. Then, after enabling default port security settings using the switchport port-security command, we set the maximum MAC addresses to be learned for these ports to 3, make the MAC addresses sticky, and order the ports to shutdown if these settings are violated.

The term sticky in the configuration means that the first 10 MAC addresses the switch learns of on each of the ports in the range will be saved and remembered even when the switch is rebooted when we issue the copy run start command, which we will do when we are finished configuring the switch.
### Slide 31
#### Disable Unused Ports
Duration: 00:00:38
Advance mode: Auto

**Notes:**
Another good security practice is to disable unused switch ports by manually shutting them down using the `shutdown` command. This too can be done port-by-port or through the use of the range command.

Later, we can activate a port by issuing the `no shutdown` command if we need to use the port.

This slide’s graphic shows that ports FastEthernet 0/4 through 0/6 were disabled using the `shutdown` command and that port 18 is configured for end device use and is configured with default port security settings.

---

<table>
<thead>
<tr>
<th>Disable Unused Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Disable unused ports by shutting them down</td>
</tr>
<tr>
<td>- Done port-by-port or through range command</td>
</tr>
<tr>
<td>- Activate port by issuing <code>no shutdown</code> command</td>
</tr>
</tbody>
</table>

---

### Slide 32
#### Verify Configurations
Duration: 00:00:43
Advance mode: Auto

**Notes:**
When you are finished configuring a switch or router, it is a good practice to always verify the configurations using SHOW commands such as:

- Show version – shows IOS version
- Show flash: - shows what is stored in flash
- Show startup-config – startup file data
- Show running-config – what is in RAM
- Show mac-address-table – displays all known MAC addresses
- Show interfaces – status & config data

---

<table>
<thead>
<tr>
<th>Verify Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Always verify configurations using SHOW commands such as:</td>
</tr>
<tr>
<td>✓ Show version – shows IOS version</td>
</tr>
<tr>
<td>✓ Show flash: - shows what is stored in flash</td>
</tr>
<tr>
<td>✓ Show startup-config – startup file data</td>
</tr>
<tr>
<td>✓ Show running-config – what is in RAM</td>
</tr>
<tr>
<td>✓ Show mac-address-table – displays all known MAC addresses</td>
</tr>
<tr>
<td>✓ Show interfaces – status &amp; config data</td>
</tr>
</tbody>
</table>

---

| Version 1.0/Summer 2013 CCNA 2 – Switching and Routing
Published by Articulate® Presenter | www.articulate.com |
Starting Fresh!

- Beware: DO NOT erase flash
- Erase the startup-configuration file
- Resets switch to factory default settings

Notes:

Sometimes you will just need to erase the startup-configuration settings and reset the switch to its default settings.

When you decide to do this, please exercise caution so that you do not accidentally erase the switch’s flash memory. If you accidentally do this, you will erase the IOS image that is stored in flash and the switch will not be able to boot normally!

Issuing the erase startup-config command erases only that file from NVRAM. Then, when you reload the switch, it will boot itself without any of the startup-config file settings, since that file no longer exists in NVRAM.

Switch Flood Attack

- Switches able to remember ~ 8K MAC addresses in its MAC address table
- Attacker can use freeware to flood port with thousands of fake MAC addresses in a second
- When MAC address table is full, switch replaces oldest-learned addresses with newest-learned addresses
- Forces switch to act as a hub allowing attacker to sniff switch traffic for all ports
  - Sends traffic received on a port to all other ports since it currently knows no valid MAC addresses

Notes:

After spending a decent amount of time discussing switch port security, now is a good time to discuss just a couple of the attacks that can be directed at a switch by an attacker.

A switch is able to remember approximately 8,000 MAC addresses in its MAC address table. When the MAC address table is full, the switch replaces its oldest-learned addresses with its newest-learned addresses.

An attacker can use freeware to flood a switch port with thousands of fake MAC addresses in a second. When the MAC address table is full, the switch implements its replacement process to save the newly-learned, fake MAC addresses, which replace the older, valid MAC addresses.

This forces the switch to act as a hub, where the switch sends all of the traffic received on its ports to all of its other ports, because the switch currently knows of no valid MAC addresses! This, in turn, allows the attacker to sniff the switch’s traffic for all ports since all of the traffic from all of the other ports will now be sent to the port the attacker is connected to.

We can mitigate this type of attack by configuring a
Another type of attack is where an attacker connects to a switch port and tries to impersonate a DHCP server before a valid DHCP server can respond to a host's request to receive an IP address configuration. This type of attack is known as a “Man-in-the-middle” attack because the attacker stands between the host and its valid DHCP server.

We can protect the switch by untrusting the ports that are not connected to a DHCP server and trusting those that are connected to a DHCP server end device.

In the slide’s graphic, the attacker’s PC, manually configured with a valid IP address, is connected to port 12, which is configured so that the port cannot send DHCP communication out of that port. Port 18, which connects the DHCP server to the switch, is configured using the `ip dhcp snooping trust` command and is able to send DHCP communication out of its port.
Configure a Switch!

- Configure a Cisco 2950/2960 switch using commands in this unit
  - Change switch name
  - Configure line con & vty &/or telnet
  - Configure management interface (VLAN)
  - Configure ports for general device access
  - Configure port security with sticky MAC address
    - Use MAC address of a laptop & plug it into the port
  - Configure trusted & untrusted DHCP ports
- Copy running-config & show to instructor to review

Notes:
Well, you have learned a good amount of information in this unit. I hope you took the time to configure a switch with the commands as you learned the commands on each slide.

To further cement this knowledge in your mind, take the time to configure a Cisco 2950 or 2960 switch using all of the commands you learned in this unit.

Your task is to:
- Change the switch’s name;
- Configure line con and vty for telnet and/or SSH;
- Configure a management VLAN interface with a valid IP address and mask;
- Configure a range of ports for general device access;
- Configure port security with sticky MAC address learning;
  - Use the MAC address of a laptop and plug it into the port, then show the switch’s MAC address table;
- Configure trusted & untrusted DHCP ports;
- Copy the running-config to a text file and show it to your instructor to review what you learned.

Basic Switching Summary – Unit 2

- Differentiate between broadcast & collision domains
- Differentiate between half & full duplex modes
- Explain the concept of a network bottleneck & mitigation techniques
- Explain the switch boot sequence
- Explain basic switch forwarding operations & methods
- Explain why switch port security is necessary
- Configure a Cisco switch with basic settings
- Configure a Cisco switch with an IP address & default-gateway
- Configure a Cisco switch with basic port security settings
- Verify a switch configuration using SHOW commands
- Differentiate between MAC flood & DHCP snooping attacks

Notes:
This concludes Unit 2 of Basic Switching. In this lecture, we learned to:
- Differentiate between broadcast & collision domains
- Differentiate between half & full duplex modes
- Explain the concept of a network bottleneck & mitigation techniques
- Explain the switch boot sequence
- Explain basic switch forwarding operations & methods
- Explain why switch port security is necessary
- Configure a Cisco switch with basic settings
- Configure a Cisco switch with an IP address & default-gateway
• Configure a Cisco switch with basic port security settings
• Verify a switch configuration using SHOW commands
• Differentiate between MAC flood & DHCP snooping attacks
Do We Really Need a Map?

Objectives
Describe the primary functions and features of a router.

Scenario
Using the Internet and Google Maps, located at http://maps.google.com, find a route between the capital city of your country and some other distant town, or between two places within your own city. Pay close attention to the driving or walking directions Google Maps suggests.

Notice that in many cases, Google Maps suggests more than one route between the two locations you chose. It also allows you to put additional constraints on the route, such as avoiding highways or tolls.

- Copy at least two route instructions supplied by Google Maps for this activity. Place your copies into a word processing document or in the space below and save it to use with the next step.
- Open the .pdf accompanying this modeling activity and complete it with a fellow student. Discuss the reflection questions listed on the .pdf and record your answers.

Be prepared to present your answers to the class.

Resources
- Internet connection
- Web browser

Goggle Map Route
Space for first route instructions supplied by Google Maps.

Space for second route instructions supplied by Google Maps.

Reflection
1. What do the individual driving, or walking based on your criteria you input, and non-highway directions look like? What exact information do they contain? How do they relate to IP routing?

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.
2. If Google Maps offered a set of different routes, what makes this route different from the first? Why would you choose one route over another?

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________

3. What criteria can be used to evaluate the usefulness of a route?

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________

4. Is it sensible to expect that a single route can be “the best one”, i.e. meeting all various requirements? Justify your answer.

_______________________________________________________________________________________

5. As a network administrator or developer, how could you use a network map, or routing table, in your daily network activities?

_______________________________________________________________________________________

_______________________________________________________________________________________
VLAN Plan

Objective
Implement VLANs to segment a small- to medium-sized network.

Scenario
You are designing a VLAN switched network for your small- to medium- sized business.
Your business owns space on two floors of a high-rise building. The following elements need VLAN consideration and access for planning purposes:
• Management
• Finance
• Sales
• Human Resources
• Network administrator
• General visitors to your business location
You have two Cisco 3560-24PS switches.
Use a word processing software program to design your VLAN-switched network scheme.
Section 1 of your design should include the regular names of your departments, suggested VLAN names and numbers, and which switch ports would be assigned to each VLAN.
Section 2 of your design should list how security would be planned for this switched network.
Once your VLAN plan is finished, complete the reflection questions from this activity.
Save your work. Be able to explain and discuss your VLAN design with another group or with the class.

Required Resources
Word processing program

Reflection
1. What criteria did you use for assigning ports to the VLANs?

2. How could these users access your network if the switches were not physically available to general users via direct connection?

3. Could you reduce the number of switch ports assigned for general users if you used another device to connect them to the VLAN network switch? What would be affected?
The Inside Track

Objective

Explain how Layer 3 switches forward data in a small- to medium-sized business LAN.

Scenario

Your company has just purchased a three-level building. You are the network administrator and must design the company inter-VLAN routing network scheme to serve a few employees on each floor.

Floor 1 is occupied by the HR Department, Floor 2 is occupied by the IT Department, and Floor 3 is occupied by the Sales Department. All Departments must be able to communicate with each other, but at the same time have their own separate working networks.

You brought three Cisco 2960 switches and a Cisco 1941 series router from the old office location to serve network connectivity in the new building. New equipment is non-negotiable.

Refer to the PDF for this activity for further instructions.

Resources

- Software presentation program

Directions

Work with a partner to complete this activity.

Step 1: Design your topology.

a. Use one 2960 switch per floor of your new building.

b. Assign one department to each switch.

c. Pick one of the switches to connect to the 1941 series router.

Step 2: Plan the VLAN scheme.

a. Devise VLAN names and numbers for the HR, IT, and Sales Departments.

b. Include a management VLAN, possibly named Management or Native, numbered to your choosing.

c. Use either IPv4 or v6 as your addressing scheme for the LANs. If using IPv4, you must also use VLSM.

Step 3: Design a graphic to show your VLAN design and address scheme.

Step 4: Choose your inter-VLAN routing method.

a. Legacy (per interface)

b. Router-on-a-Stick

c. Multilayer switching

Step 5: Create a presentation justifying your inter-VLAN routing method of choice.

a. No more than eight slides can be created for the presentation.
b. Present your group’s design to the class or to your instructor.
   
   1) Be able to explain the method you chose. What makes it different or more desirable to your business than the other two methods?
   
   2) Be able to show how data moves throughout your network. Verbally explain how the networks are able to communicate using your inter-VLAN method of choice.
Packet Tracer – Skills Integration Challenge

Topology
### Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>G0/0.15</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>G0/0.30</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>G0/0.45</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>G0/0.60</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>S0/0/0</td>
<td></td>
<td>255.255.255.252</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>S0/0/1</td>
<td></td>
<td>255.255.255.252</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>S0/1/0</td>
<td></td>
<td>255.255.255.252</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>G0/0</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>S0/0/0</td>
<td></td>
<td>255.255.255.252</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>S0/0/1</td>
<td></td>
<td>255.255.255.252</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>G0/0</td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>S0/0/0</td>
<td></td>
<td>255.255.255.252</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>S0/0/1</td>
<td></td>
<td>255.255.255.252</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>VLAN 60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIC</td>
<td>DHCP Assigned</td>
<td>DHCP Assigned</td>
<td>DHCP Assigned</td>
<td></td>
</tr>
</tbody>
</table>

### VLANs and Port Assignments Table

<table>
<thead>
<tr>
<th>VLAN Number - Name</th>
<th>Port assignment</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 - Servers</td>
<td>F0/11 - F0/20</td>
<td></td>
</tr>
<tr>
<td>30 - PCs</td>
<td>F0/1 - F0/10</td>
<td></td>
</tr>
<tr>
<td>45 - Native</td>
<td>G1/1</td>
<td></td>
</tr>
<tr>
<td>60 - Management</td>
<td>VLAN 60</td>
<td></td>
</tr>
</tbody>
</table>

### Scenario

This culminating activity includes many of the skills that you have acquired during this course. First, you will complete the documentation for the network. So make sure you have a printed version of the instructions. During implementation, you will configure VLANs, trunking, port security and SSH remote access on a switch. Then, you will implement inter-VLAN routing and NAT on a router. Finally, you will use your documentation to verify your implementation by testing end-to-end connectivity.

### Documentation

You are required to fully document the network. You will need a print out of this instruction set, which will include an unlabeled topology diagram:

- Label all the device names, network addresses and other important information that Packet Tracer generated.
- Complete the Addressing Table and VLANs and Port Assignments Table.
- Fill in any blanks in the Implementation and Verification steps. The information is supplied when you launch the Packet Tracer activity.

Implementation

Note: All devices in the topology except ________________, ________________, and ________________ are fully configured. You do not have access to the other routers. You can access all the servers and PCs for testing purposes.

Implement to following requirements using your documentation:

- Configure remote management access including IP addressing and SSH:
  - Domain is cisco.com
  - User ________________ with ________________
  - Crypto key length of 1024
  - SSH version 2, limited to 2 authentication attempts and a 60 second timeout
  - Clear text passwords should be encrypted.

- Configure, name and assign VLANs. Ports should be manually configured as access ports.

- Configure trunking.

- Implement port security:
  - On Fa0/1, allow 2 MAC addresses that are automatically added to the configuration file when detected. The port should not be disabled, but a syslog message should be captured if a violation occurs.
  - Disable all other unused ports.

- Configure inter-VLAN routing.

- Configure DHCP services for VLAN 30. Use LAN as the case-sensitive name for the pool.

- Implement routing:
  - Use OSPF process ID 1 and router ID 1.1.1.1
  - Configure one network statement for the entire ________________ address space
  - Disable interfaces that should not send OSPF messages.
  - Configure a default route to the Internet.

- Implement NAT:
  - Configure a standard, one statement ACL number 1. All IP addresses belonging to the ________________ address space are allowed.
  - Refer to your documentation and configure static NAT for the File Server.
  - Configure dynamic NAT with PAT using a pool name of your choice and these two public addresses:
    ________________
    ________________

Verify ________________ has received full addressing information from ________________.
Packet Tracer – Skills Integration Challenge

Verification

All devices should now be able to ping all other devices. If not, troubleshoot your configurations to isolate and solve problems. A few tests include:

- Verify remote access to __________________ by using SSH from a PC.
- Verify VLANs are assigned to appropriate ports and port security is in force.
- Verify OSPF neighbors and a complete routing table.
- Verify NAT translations and statics.
  - Outside Host should be able to access File Server at the public address.
  - Inside PCs should be able to access Web Server.
- Document any problems you encountered and the solutions in the Troubleshooting Documentation table below.

Troubleshooting Documentation

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Suggested Scoring Rubric

Packet Tracer scores 70 points. Documentation is worth 30 points.
**Course Assignments by Week**

**CIS 151C: Network Essentials (Cisco 1)  
Campus Course**

During week one, **you must attend class during one of the first three days of class** to avoid being dropped. You **must also post your SIA during one of the first three days of class** to avoid being dropped. If you miss the first day of class and/or do not post your SIA, and there is a class waiting list, you may be dropped (immediately) by your instructor.

The SIA is the **Student Introductory Assignment** where you post something about yourself in Angel, in the **Lessons -> Week 01 folder -> SIA Forum**. Your instructor will have already posted something about himself there! Create a new post and tell your instructor and classmates something about yourself.

**Homework** due dates and **Quiz** information: Please see the syllabus for details!

You will find Flash and PowerPoint presentations for each tutorial in the **Course Documents** link. The Flash presentation is a voice over PowerPoint presentation that you can view using a Web browser. There is material contained in the Flash presentations that will be on your quizzes and final exam. Flash presentations will be posted each Monday morning for that week's material.

**How to turn in homework:**
1. Place all of your files in a folder (one folder per week's worth of homework).
2. Place all of that week's folders in **one** WinZip or compressed folder. Do not put each assignment in a compressed folder. Each submission into a drop box should only contain one compressed folder.
3. Name the compressed folder with your course number, your name and week number. For example, week one's filename would be “CIS 151C, Week 1 – John Blackwood”.
4. Upload your compressed folder into that week's drop box in Angel. Do not email your homework to me!

**Week By Week Activities:**

Note: Students should complete all Packet Tracer (PT) labs listed below using the latest version of Cisco's Packet Tracer network simulation tool. You download PT from the Cisco Networking Academy Web site, after logging in using your student credentials. Physical labs must be completed using actual (physical) hardware, which is available in TC 101.

**Week 1 (April 1st):**
- **SIA due by Wednesday at midnight during week one!**
  - If you don't complete your SIA on time you may be dropped from the course in week 1.
- View the flash presentation for Chapter 1
- Read and do textbook hands-on work for Chapter 1
- There is no Quiz for Chapter 1 (these start with Chapter 2)
• Notes Journal related to this week's material
• Homework due for Chapter 1: SLM Activity 1.1.1 (Google), Packet Tracer Lab 1.7.1 (Skills Integration Challenge)

**Week 2 (April 8th):**
• View the flash presentation for Chapter 2
• Read and do hands-on work for Chapter 2
• Complete the Cisco Quiz for Chapter 2
• Notes Journal related to this week's material
• Homework due for Chapter 2: SLM Lab 2.2.5 (NeoTrace), SLM Lab 2.6.2 (Wireshark)

**Week 3 (April 15th):**
• View the flash presentation for Chapter 3
• View the flash presentation for Chapter 4
• Read and do hands-on work for Chapter 3
• Read and do hands-on work for Chapter 4
• Complete the Cisco Quiz for Chapter 3
• Complete the Cisco Quiz for Chapter 4
• Notes Journal related to this week's material
• Homework due for Chapter 3: Packet Tracer Lab 3.5.1 (Skills Integration Challenge)
• Homework due for Chapter 4: Packet Tracer Lab 4.6.1 (Skills Integration Challenge)

**Week 4 (April 22nd):**
• View the flash presentation for Chapter 5
• Read and do hands-on work for Chapter 5
• Complete the Cisco Quiz for Chapter 5
• Notes Journal related to this week's material
• Homework due for Chapter 5: HW : Packet Tracer Lab 5.5.1 (Device Gateway), Packet Tracer Lab 5.5.2 (Route Examination), Packet Tracer Lab 5.6.1 (Skills Integration Challenge)

**Week 5 (April 29th):**
• View the flash presentation for Chapter 6
• Read and do hands-on work for Lesson 6
• Complete the Cisco Quiz for Chapters 6
• Notes Journal related to this week's material
• Homework due for Chapter 6: SLM Activity 6.7.3 (Subnetting, Part 1), SLM Activity 6.7.4 (Subnetting, Part 2), Packet Tracer Lab 6.8.1 (Skills Integration Challenge)

**Week 6 (May 6th):**
• View the flash presentation for Chapter 7
• Read and do hands-on work for Chapter 7
• Complete the Cisco Quiz for Chapter 7
• Notes Journal related to this week's material
• Homework due for Chapter 7: SLM Lab 7.5.2 (Frame Examination), Packet Tracer Lab 7.6.1 (Skills Integration Challenge)
Week 7 (May 13th):
- View the flash presentation for Chapter 8
- Read and do hands-on work for Chapter 8
- Complete the Cisco Quiz for Chapter 8
- Notes Journal related to this week's material
- Homework due for Chapter 8: SLM Lab 8.4.1 (Media Connectors), Packet Tracer Lab 8.5.1 (Skills Integration Challenge)

Week 8 (May 20th):
- View the flash presentation for Chapter 9
- Read and do hands-on work for Chapter 9
- Complete the Cisco Quiz for Chapter 9
- Notes Journal related to this week's material
- Homework due for Chapter 9: HW : SLM Lab 9.8.1 (ARP), SLM 9.8.2 (MAC Table), SLM Lab 9.8.3 (Intermediary Devices), Packet Tracer Lab 9.9.1 (Skills Integration Challenge)

Week 9 (May 27th):
- View the flash presentation for Chapter 10
- Read and do hands-on work for Chapter 10
- Complete the Cisco Quiz for Chapter 10
- Notes Journal related to this week's material
- Homework due for Chapter 10: SLM Lab 10.3.2 (How Many Networks?), SLM Lab 10.6.1 (Create Small Network), SLM Lab 10.6.2 (Console Session), Packet Tracer Lab 10.7.1 (Skills Integration Challenge)

Week 10 (June 3rd):
- View the flash presentation for Chapter 11
- Read and do hands-on work for Lesson 11
- Complete the Cisco Quiz for Chapter 11
- Notes Journal related to this week's material
- *Homework due for Chapter 11: SLM Lab 11.4.3.3 (Latency), SLM Lab 11.5.1 (Device Config.), SLM Lab 11.5.3 (Configure Hosts), SLM Lab 11.5.4 (Network Testing)

Week 10 (June 10th):
- **Final Exam (Comprehensive - covers all chapters)**
  - The final exam will be taken online through Cisco's Academy link
  - You must be physically present in class to take the final exam
  - A final exam study guide will be provided to you in week 10
  - Date / time: Friday, 10-noon, June 14th, TC 101
- **Skills Final Exam (taken immediately after online final exam or during week 10)**
  - A skills study guide will be provided to you in week 10

*Homework for Chapter 11 is due no later than Monday, June 10th, 2013 at 1:15 PM*
Syllabus

CIS 151C - Network Essentials (Cisco 1)
Spring 2013

Class Hours:        Lecture: M, T, W: 11-11:50 AM TC101 and
Lab: TH 1:00 - 2:50 PM, TC101
Credits:                4
Instructor:           John Blackwood
Office:                 Tower #3
Office Hours:       See schedule posted in Angel (under Lessons link)
Phone:                 541-440-7686
Email:                john.blackwood@umpqua.edu

Cisco Networking Academy Link:
http://cisco.netacad.net/staticcontentassets/choice/multilogin.html

Course Description:
This is the first in a four part series of courses that are mapped to the Cisco Networking Academy CCNA (Cisco Certified Network Administrator) certification.

This course is designed to provide students with classroom and laboratory experience in current and emerging networking technology that will empower them to enter employment or further education and training in the computer-networking field. A task analysis of current industry standards and occupational analysis was used to develop the content. Instruction includes, but is not limited to, networking, network terminology and protocols, network standards, local-area networks (LANs), wide-area networks (WANs), Open System Interconnection (OSI) models, cabling, cabling tools, routers, router programming, Ethernet, Internet Protocol (IP) addressing, and network standards.

Particular emphasis is given to the use of decision-making and problem-solving techniques in applying science, mathematics, communication, and social studies concepts to solve networking problems. In addition, instruction and training are provided in the proper care, maintenance, and use of networking software, tools, and equipment and all local, state, and federal safety, building, and environmental codes and regulations.

Course Outcomes:
Upon completion of this course the student should be able to:
• Ability to identify and describe the functions of each layer of the OSI reference model including devices and services used at each layer.
• Ability to describe data link and network addresses along with key differences between them.
• Ability to distinguish between classes of IP addresses and calculate subnets using classful and variable length subnet mask (VLSM) techniques.
• Ability to define and explain data encapsulation.
• Ability to identify functions of the TCP/IP network-layer protocols.
• Ability to make different types of networking cables.
• Apply a basic configuration to a router.
• Utilize command line tools to test and verify network connectivity.
• Use Packet Tracer to build and test a basic network containing routers, switches, and end devices.

Course Prerequisites:
To take this course you should:

• Previously have completed CIS 120 and passed with a grade of C or better.
• You should be able to use and have access to Windows XP Professional (or newer) on your computer.
• Send and receive email and use compressed folders.
• Be able to purchase the textbook, lab manual, and other equipment listed in this syllabus.

Required Text:
ISBN: 9781118217146
This bundle is available in the UCC bookstore. You will use this book bundle set throughout your four course sequence of Cisco courses.

Supplies:
At least one (1) 500 GB USB portable hard disk drive, and five (5) rewriteable CD\DVDs.

Equipment:
It is intended that students will use UCC lab computers, routers, switches, and the Packet Tracer simulation software provided by Cisco. Please talk to your instructor prior to purchasing any hardware or software for this class.
Students using their own computer will need to install this software. Please talk to your instructor prior to purchasing any hardware or software for this class.

To take this course you must also have:

- A computer running Windows 7. XP Pro with SP3 will suffice, but you are responsible for the differences between what you see on the screen and what is shown in any presentations you view.
- Microsoft Office viewers, which can be downloaded by clicking here.
- High-speed Internet access availability to view Cisco Academy presentations and take quizzes.

**Homework (AKA "Lab work"):**

Students should plan to spend an average of 12-15 hours per week working in class lecture, assigned materials, reading, and homework. Homework will be graded primarily on timely, complete, and accurate completion. Late assignments will be penalized up to 20% of that assignment’s grade. **Assignments turned in after graded work has been returned to class will not be accepted for grading.**

Some of your homework will be completed using **Cisco’s Packet Tracer (PT)** simulation program. Please view the “Do This First” flash presentation posted under Lessons for instructions on how to get and use PT. You will use PT throughout all of your Cisco Academy courses. PT provides you with a simulated networking environment in which you can configure computers, switches, routers, wireless routers, the Internet, and servers.

Other homework will be done by working through the material your lab manual. Lab manual work revolves around expressing what you’ve learned in written format. Therefore, in the lab manual you will answer written questions, answer questions in your own words, complete simple labs, and perform matching exercises.

Lab assignments are due by 1 PM on the Monday following each week’s assignment. For example, labs for Week 1 are assigned on April 1st and are due on or before 1:15 PM on Monday, April 8th.

You are to submit printed lab work for grading, and you must place your printed lab work in my mailbox as I won’t accept them in class (too many to carry!). I do not take responsibility for (real or imagined) lost labs! Always keep a backup of your homework in your possession until I return your graded work back to you.

Finally, some of the "Challenge" lab assignments contain work not covered in the text. You must use the Internet, Windows Help, and other tools to complete these assignments. The goal is to force you to take principles learned and apply them in new situations. **Important note: All labs are due no later than Monday, June 10th by 1:15 PM.**

**Lab time:** you may attend a campus lab offered Thursday of each week from 1:00-2:50 PM to get help installing and using Packet Tracer, and with general lab questions. If you attend this lab you can get personal assistance related to questions you have about class materials and/or
homework. Depending on student lab aid availability, students may be able to obtain tutoring assistance here as well. Lab attendance is optional, but strongly recommended. If you do not attend lab you will not receive extra time to complete that homework! Be wise. Attend lab each week.

**Quizzes:**

There will be ten quizzes during the term (Chapter 1 does not have a quiz – they begin with Chapter 2). Quizzes are available through Cisco’s Networking Academy link (the link is near the top of this document). Quizzes are taken weekly, up to two times. The last score recorded is the one that counts, so consider this important fact if you decide to retake a quiz (you might get a lower score). Please do not ask me to override your quiz score if your retake results in a lower score.

Quizzes must be completed during the week in which they are assigned. For example, the Chapter 2 quiz is assigned Monday, April 8th and will remain open for one week, closing the following Monday, April 15th, at 1:15 PM. Each week's quiz will follow this same schedule. Once the open time period for a quiz expires, I will not reopen it.

Please view the “Do This First” flash presentation posted under Lessons for instructions on how to access and complete your quizzes.

**Grading & Points:**

Grades will be assigned based on the total points (pts) earned as follows; 90 to 100% = A, 80 to 89% = B, 70 to 79% = C, 60 to 69% = D, and less than 60% = F.

Points are distributed as follows:

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Pts</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 lab assignments @ 8 pts ea.</td>
<td>216</td>
<td>32.0%</td>
</tr>
<tr>
<td>10 weeks of Notes Journal @ 10</td>
<td>100</td>
<td>15.0%</td>
</tr>
<tr>
<td>10 quizzes @ 10 pts ea.</td>
<td>100</td>
<td>15.0%</td>
</tr>
<tr>
<td>Skills final exam</td>
<td>100</td>
<td>15.0%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>150</td>
<td>23.0%</td>
</tr>
<tr>
<td>TOTAL POSSIBLE POINTS</td>
<td>666</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Course Outline:**

This outline is a plan for the term. It is subject to change should the need arise. Changes will be noted during assigned class or lab time. It is your responsibility to note changes in the syllabus schedule as presented in class or via Angel announcements during the term.
Since you are assigned a lot of homework, this class will not include a midterm exam. The final exam will be comprehensive and will cover all chapters. Please see the Course Assignments by Week document posted in Angel under Lessons for the final exam date.

**Lab Grading Rubric:**
Labs are to be completed in a professional manner. Network administrators must learn to write neatly and succinctly so that steps can be repeated and/or understood by others. Some governing bodies require documentation for auditing purposes. Please review the lab rubric posted in Angel under Lessons for details about how your work will be graded.

**Course Schedule:**
Please see the document entitled Course Assignments by Week for all weekly activities. This document is posted in Angel, under Lessons.

**Use of Online Components:**
Angel will be used only to provide you access to class files, chapter quizzes (assessments), the final exam, and an online grade book.

In addition, we will utilize Cisco's Networking Academy site to administer/download chapter quizzes, simulation tools, student review material, and your final exam. Please see the URL near the top of this document for the link to the Academy.

The Angel Learning Management System is compliant with ADA standards.

**Course Policies:**
If you have problems completing an assignment, it is your responsibility to contact me to resolve the issue at hand. You are strongly encouraged to begin homework assignments early in the week so that you can get assistance when help is available.

The college has a zero tolerance policy (721.1 Academic Integrity) regarding all forms of academic dishonesty. Students caught (and/or involved in) copying—or any of the other noted violations of academic dishonesty—will receive a zero (0) on that assignment, project, or test. Continued violations of this policy may result in student suspension from classes. Note that this policy specifically addresses plagiarism as it applies to students at UCC. The policy on academic integrity is posted throughout the campus; please take the time to read it!

Although it is not normal procedure—after corrected materials have been returned to the class, late assignments may be accepted at my discretion.

I will generally grade your homework each week. For example, week 1 homework will be graded some time during week 2. When your homework is graded, I will write comments on
your printed work, when applicable, along with a grade for each assignment. Then, grades are posted in Angel later that same day.

Students are responsible for running weekly grade reports to verify that what is in the gradebook is correct. Gradebook entries may be challenged within one week after homework is graded except for grades issued for week 10 homework, which must be challenged no later than Thursday at noon of week 11 (finals week).

You may work at your own pace throughout this course. For example, you can complete the whole course in less than ten weeks if you have the time to do so. However, I will grade homework and answer course material questions weekly. Therefore, if you ask a week 8 question in week 2, I may defer answering that question until that answer benefits the entire class.

Students are responsible for material presented in lectures, Cisco Networking Academy presentations, flash presentations, assigned readings, homework (labs, which are made up of Study Guide and Packet Tracer work), handouts, videos, and other assignments I deem appropriate during the course. Any of these materials may be used by as the basis for test questions.

Since quizzes are taken through Cisco's Networking Academy site, quiz scores will be copied to Angel within one week after the quiz is no longer available.

Make up tests will only be given in two circumstances:

1. You contact me with a valid excuse prior to the scheduled test. (Examples of valid excuses are documented health problems, emergency medical appointments, etc.).
2. There was a personal, family, or medical emergency at the time of the test that prevented contact with me in a timely manner. (Examples of valid excuses are car accidents, death in the immediate family, or serious injury just prior to the test.). I may ask you for written proof of the emergency if you request a make up test.

I retain the right to refuse non-health and/or family emergency excuses which appear to be avoidable or optional choices made by you. Alternate test times will be set by me, to occur at my convenience. Make-up options for class activities will be extremely limited.

**Student Notice:**

UCC is committed to supporting all students. Any student who feels he or she may need an accommodation for any type of disability should make contact with the Disability Services Office in the Advising and Career Service Center of the Campus Center Building.

If you plan to use academic accommodations for this course, please contact your instructor and the Disability Services Office as soon as possible to discuss your needs. Accommodations are not retroactive; they begin when the instructor receives the “Approved Academic Accommodations” letter.

To request academic accommodations for a disability, please contact a Disability Service
Coordinator.

Phone (541) 440-7655 or (541) 440-4610 or Oregon Relay 1-800-735-2900.

Additional information may be found at the Disability Services web page at: http://www.umpqua.edu/disability-services-home

New and returning students may access information at: http://www.umpqua.edu/your-first-term
Portfolio RIP and EIGRP

Objectives
Configure EIGRP for IPv4 in a small routed network (review).

Scenario
You are preparing a portfolio file for comparison of RIP and EIGRP routing protocols.

Think of a network with three interconnected routers with each router providing a LAN for PCs, printers, and other end devices. The graphic on this page depicts one example of a topology like this.

In this modeling activity scenario, you will be creating, addressing and configuring a topology, using verification commands, and comparing/contrast routing protocol outputs.

Complete the PDF reflection questions. Save your work and be prepared to share your answers with the class. Also save a copy of this activity for later use within this course or for portfolio reference.

Resources
Packet Tracer and word processing software programs

Directions
Step 1: WAN and LAN topology design
a. Use Packet Tracer to design a network with three routers (1941 model, suggested). If necessary, add NIC cards to the routers to provide connectivity to the routers to provide for at least one LAN to each router. Add at least one PC to each LAN.
b. Address the networks. You may use a flat addressing scheme or VLSM. Use only IPv4 networks for this entire activity.

Step 2: Copy the topology
a. Highlight the entire topology by using your cursor.
b. Use Ctrl+C to make a copy of the highlighted topology.
c. Use Ctrl+V to insert a full copy of the topology to the desktop of Packet Tracer. You will now have displayed two exact, IPv4-addressed topologies with which to work for routing protocols configurations.
d. While highlighted, move the copied topology to a different location on the Packet Tracer desktop to create room between the two for configuration purposes.

Step 3: Configure RIP and EIGRP on the separate topologies.
a. Configure the RIP routing protocol on the first topology and EIGRP on the second routing topology.
b. Once you have successfully configured RIP on one topology and EIGRP on the other, check to make sure your PCs can ping each other.
c. Save your work so no configuration information is lost.

Step 4: Use verification commands to check output for the routing protocols.
a. To compare/contrast routing protocol information from the two topologies, issue the show ip route command on R1 for topology 1 and 2.
b. Copy the output into a table in your word processing program file. Label each column with RIP or EIGRP and place the output you received from the `show ip route` command.

c. Issue the `show ip protocols` command on R1 for topology table 1 and 2. Create another table in your word processing software file and place the output information below RIP or EIGRP.

d. Issue the `show cdp neighbors` command on R1’s topology 1. Copy the output to a third table with RIP as the heading and issue the `show ip eigrp neighbors` command on R1’s topology 2. Copy the output from this command in column 2 of table 3 under the heading EIGRP.

Reflection

1. Compare and contrast the output for the `show ip route` verification command.

2. Compare and contrast the output for the `show ip protocol` verification command.

3. Compare and contrast the `show cdp neighbors` command for the RIP topology and the `show ip eigrp neighbors` command for the EIGRP topology.

4. After comparing and contrasting the RIP and EIGRP output, which do you find most informative? Support your answer.
Layered Network Design Simulation

Objective
Explain the need to design a hierarchical network that is scalable.

Scenario
As the network administrator for a very small network, you want to prepare a simulated-network presentation for your branch manager to explain how the network currently operates.

The small network includes the following equipment:

- One Cisco 2911 series router
- One Cisco 3560 switch
- One Cisco 2960 switch
- Four user workstations (PCs or laptops)
- One printer

Resources
- Packet Tracer software

Directions

Step 1: Create a simple network topology using Packet Tracer software. Place the devices at the appropriate levels of the Cisco three-layer hierarchical model design, including:

   a. One Cisco 2911 series router
   b. One Cisco 3560 switch
   c. One Cisco 2960 switch
   d. Four user workstations (PCs or laptops)
   e. One printer

Step 2: Using Packet Tracer’s drawing tool and indicate the hierarchical layers with different color coding and labels:

   a. Access layer
   b. Distribution layer
   c. Core layer

Step 3: Configure the network and user devices. Check for end-to-end connectivity.

Step 4: Share your configuration and hierarchical network design Packet Tracer file with another student, group, the class, or the instructor.
Stormy Traffic

Objective

Explain the purpose of the Spanning Tree Protocol (STP) in a switched LAN environment with redundant switch links.

Scenario

It is your first day on the job as a network administrator for a small- to medium-sized business. The previous network administrator left suddenly after a network upgrade took place for the business.

During the upgrade, a new switch was added. Since the upgrade, many employees complain that they are having trouble accessing the Internet and servers on your network. In fact, most of them cannot access the network at all. Your corporate manager asks you to immediately research what could be causing these connectivity problems and delays.

So you take a look at the equipment operating on your network at your main distribution facility in the building. You notice that the network topology seems to be visually correct and that cables have been connected correctly, routers and switches are powered on and operational, and switches are connected together to provide backup or redundancy.

However, one thing you do notice is that all of your switches’ status lights are constantly blinking at a very fast pace to the point that they almost appear solid. You think you have found the problem with the connectivity issues your employees are experiencing.

Use the Internet to research STP. As you research, take notes and describe:

- Broadcast storm
- Switching loops
- The purpose of STP
- Variations of STP

Complete the reflection questions that accompany the PDF file for this activity. Save your work and be prepared to share your answers with the class.

Resources

- Internet access to the World Wide Web

Reflection

1. What is a definition of a broadcast storm? How does a broadcast storm develop?

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________

2. What is a definition of a switching loop? What causes a switching loop?

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
3. How can you mitigate broadcast storms and switching loops caused by introducing redundant switches to your network?

_______________________________________________________________________________________

_______________________________________________________________________________________

_______________________________________________________________________________________

4. What is the IEEE standard for STP and some other STP variations, as mentioned in the hyperlinks provided?

_______________________________________________________________________________________

_______________________________________________________________________________________

_______________________________________________________________________________________

5. In answer to this scenario, what would be your first step (after visually checking your network) to correcting the described network problem?

_______________________________________________________________________________________

_______________________________________________________________________________________

_______________________________________________________________________________________
Documentation Tree

Objective
Identify common STP configuration issues.

Scenario
The employees in your building are having difficulty accessing a web server on the network. You look for the network documentation that the previous network engineer used before he transitioned to a new job; however, you cannot find any network documentation whatsoever. Therefore, you decide create your own network recordkeeping system. You decide to start at the access layer of your network hierarchy. This is where redundant switches are located, as well as the company servers, printers, and local hosts.
You create a matrix to record your documentation and include access layer switches on the list. You also decide to document switch names, ports in use, cabling connections, and root ports, designated ports, and alternate ports.
For more detailed instructions on how to design your model, use the student PDF that accompanies this activity.

Resources
- Packet Tracer software
- Word processing software

Directions
Step 1: Create the topology diagram with three redundant switches.
Step 2: Connect host devices to the switches.
Step 3: Create the switch documentation matrix.
   a. Name and switch location
   b. General switch description
   c. Model, IOS version, and image name
   d. Switch serial number
   e. MAC address
   f. Ports currently in use
   g. Cable connections
   h. Root ports
   i. Designated ports, status, and cost
   j. Alternate ports, status, and cost
Step 4: Use show commands to locate Layer 2 switch information.

a. show version
b. show cdp neighbors detail
c. show spanning-tree
1.7.1: Skills Integration Challenge-Introduction to Packet Tracer

Topology Diagram
Addressing Table

Fa0/0 192.168.254.253 255.255.255.0 N/A
R1-ISP
S0/0/0 10.10.10.6 255.255.255.252 N/A
Fa0/0 172.16.255.254 R2- 255.255.0.0 N/A
Central S0/0/0 10.10.10.5 255.255.255.252 N/A
S1-
Central VLAN 1 172.16.254.1 255.255.0.0 172.16.255.254
PC 1A NIC 172.16.1.1 255.255.0.0 172.16.255.254
PC 1B NIC 172.16.1.2 255.255.0.0 172.16.255.254
Eagle
Server NIC 192.168.254.254 255.255.255.0 192.168.254.253

Learning Objectives
• Explore Packet Tracer Real-time mode
• Explore the Logical Workspace
• Explore Packet Tracer operation
• Connect devices
• Examine a device configuration
• Review the standard lab setup
• Overview of the devices

Background
Throughout the course you will be using a standard lab setup created from actual PCs, servers, routers, and switches to learn networking concepts. This method provides widest range of features and the most realistic experience. Since equipment and time are limited, this experience can be supplemented by a simulated environment. The simulator that is used in this course is Packet Tracer. Packet Tracer provides a rich set of protocols, equipment, and features but only a fraction of what is possible with real equipment. Packet Tracer is a supplement to not a replacement for experience with real equipment. You are encouraged to compare the results obtained from Packet Tracer network models with the behavior of real equipment. You are also encouraged to examine the Help files built into Packet Tracer, which include an extensive "My First PT Lab", tutorials, and information on the strengths and limitations of using Packet Tracer to model networks.

This activity will provide an opportunity to explore the standard lab setup using Packet Tracer simulator. Packet Tracer has two file formats it can create: .pkt files (network simulation model files) and .pka files (activity files for practice). When you create your own networks in Packet Tracer, or modify existing files from your instructor or your peers, you will often use the .pkt file format. When you launched this activity from the curriculum, these instructions appeared. They are the result of the .pka, Packet Tracer activity file format. At the bottom of these instructions are two buttons: Check Results (which gives you feedback on how much of the activity you have completed) and Reset Activity (which starts the activity over, if you want to clear your work or gain more practice).

Task 1: Explore the PT Interface.
Step 1: Examine the Logical Workplace.
When Packet Tracer starts it presents a logical view of the network in real-time mode. The main part of the PT interface is the Logical Workplace. This is the large area where devices are placed and connected.

Step 2: Symbols Navigation.
The lower left portion of the PT interface, below the yellow bar, is the portion of the interface that you use to select and place devices into the logical workplace. The first box in the lower left contains symbols that represent groups of devices. As you move the mouse pointer over these symbols the name of the group appears in the text box in the center. When you click on one of these symbols the specific devices in the group appear in the box to the right. As you point to the specific devices, a description of the device appears in the text box below the specific devices. Click on each of the groups and study the various devices that are available and their symbols.

Task 2: Explore PT operations

Step 1: Connect the devices using auto connect.
Click on the connections group symbol. The specific connection symbols provide different cable types that can be used to connect devices. The first specific type, the gold lightning bolt, will automatically select the connection type based on the interfaces available on the devices. When you click on this symbol the pointer resembles a cable connector.
To connect two devices click the auto connection symbol, click the first device, and then click the second device. Using the auto connection symbol, make the following connection:
• Connect the Eagle Server to the R1-ISP router.
• Connect PC-PT 1A to the S1-Central switch.

Step 2: Examine device configuration with a mouse over.
Move your mouse over the devices found in the logical workplace. As you move the mouse pointer over these symbols the device configurations appears in a text box.
• A router will display port configuration information including IP address, port status, and MAC address.
• A server will display IP address, MAC address, and Gateway information
• A switch will display port configuration information including IP address, MAC address, port status, and VLAN membership.
• A PC will display IP address, MAC address, and Gateway information.

Step 3: Examine device configuration.
Left mouse click on each device type found in the logical workplace to view the device configuration.
• Router and Switch devices contain three tabs. These tabs are Physical, Config, and CLI (Command Line Interface).
  o The Physical tab displays the physical components of the device such as modules. New modules can also be added using this tab.
  o The Config tab displays the general configuration information such as device name.
  o The CLI tab allows the user to configure the device using the command line interface.
• Server and Hub devices contain two tabs. These tabs are Physical and Config.
  o The Physical tab displays components of the device such as ports. New modules can also be added using this tab.
• PC devices contain three tabs. These tabs are Physical, Config, and Desktop.
  o The Physical tab displays the general information such as device name.
  o The Config tab displays components of the device. New modules can also be added using this tab.
  o The Config tab displays the device name, IP address, subnet mask, DNS, and gateway information.
  o The Desktop tab allows the user to configure, IP address, subnet mask, default gateway, DNS server, dial-up, and wireless. A terminal emulator, the command prompt and a simulated web browser can also be accessed using the Desktop tab.
Task 3: Review the Standard Lab Setup.

Step 1: Overview of the devices.
The standard lab setup will consist of two routers, one switch, one server, and two PCs. Each of these devices will be pre-configured with such information as device names, IP addresses, gateways, and connections.

Reflection:
You are encouraged to obtain Packet Tracer from your instructor and complete My First PT Lab. 1.7.1: Skills Integration Challenge-Introduction to Packet Tracer

Topology Diagram

Addressing Table

<table>
<thead>
<tr>
<th>Device Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/0</td>
<td>192.168.254.253</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td>R1-ISP</td>
<td>10.10.10.6</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>172.16.255.254</td>
<td>255.255.0.0</td>
<td>N/A</td>
</tr>
<tr>
<td>Central S0/0/0</td>
<td>10.10.10.5</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td>S1-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central VLAN 1</td>
<td>172.16.254.1</td>
<td>255.255.0.0</td>
<td>172.16.255.254</td>
</tr>
<tr>
<td>PC 1A NIC</td>
<td>172.16.1.1</td>
<td>255.255.0.0</td>
<td>172.16.255.254</td>
</tr>
<tr>
<td>PC 1B NIC</td>
<td>172.16.1.2</td>
<td>255.255.0.0</td>
<td>172.16.255.254</td>
</tr>
<tr>
<td>Eagle</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server NIC</td>
<td>192.168.254.254</td>
<td>255.255.255.0</td>
<td>192.168.254.253</td>
</tr>
</tbody>
</table>

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information. Page 1 of 4

Learning Objectives
• Explore Packet Tracer Real-time mode
• Explore the Logical Workspace
• Explore Packet Tracer operation
• Connect devices
• Examine a device configuration
• Review the standard lab setup
• Overview of the devices

Background
Throughout the course you will be using a standard lab setup created from actual PCs, servers, routers, and switches to learn networking concepts. This method provides widest range of features and the most realistic experience. Since equipment and time are limited, this experience can be supplemented by a simulated environment. The simulator that is used in this course is Packet Tracer. Packet Tracer provides a rich set of protocols, equipment, and features but only a fraction of what is possible with real equipment. Packet Tracer is a supplement to not a replacement for experience with real equipment. You are encouraged to compare the results obtained from Packet Tracer network models with the behavior of real equipment. You are also encouraged to examine the Help files built into Packet Tracer, which include an extensive "My First PT Lab", tutorials, and information on the strengths and limitations of using Packet Tracer to model networks.

This activity will provide an opportunity to explore the standard lab setup using Packet Tracer simulator. Packet Tracer has two file formats it can create: .pkt files (network simulation model files) and .pka files (activity files for practice). When you create your own networks in Packet Tracer, or modify existing files from your instructor or your peers, you will often use the .pkt file format. When you launched this activity from the curriculum, these instructions appeared. They are the result of the .pka, Packet Tracer activity file format. At the bottom of these instructions are
two buttons: **Check Results** (which gives you feedback on how much of the activity you have completed) and **Reset Activity** (which starts the activity over, if you want to clear your work or gain more practice).

**Task 1: Explore the PT Interface.**

**Step 1: Examine the Logical Workplace.**

When Packet Tracer starts it presents a logical view of the network in real-time mode. The main part of the PT interface is the **Logical Workplace**. This is the large area where devices are placed and connected.

**Step 2: Symbols Navigation.**

The lower left portion of the PT interface, below the yellow bar, is the portion of the interface that you use to select and place devices into the logical workplace. The first box in the lower left contains symbols that represent groups of devices. As you move the mouse pointer over these symbols the name of the group appears in the text box in the center. When you click on one of these symbols the specific devices in the group appear in the box to the right. As you point to the specific devices, a description of the device appears in the text box below the specific devices. Click on each of the groups and study the various devices that are available and their symbols.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information. Page 2 of 4

CCNA Exploration

Network Fundamentals:

Living in a Network-Centric World 1.7.1: Skills Integration Challenge-Introduction to Packet Tracer

**Task 2: Explore PT operations**

**Step 1: Connect the devices using auto connect.**

Click on the connections group symbol. The specific connection symbols provide different cable types that can be used to connect devices. The first specific type, the gold lightning bolt, will automatically select the connection type based on the interfaces available on the devices. When
you click on this symbol the pointer resembles a cable connector.

To connect two devices click the auto connection symbol, click the first device, and then click the second device. Using the auto connection symbol, make the following connection:

- Connect the Eagle Server to the R1-ISP router.
- Connect PC-PT 1A to the S1-Central switch.

**Step 2: Examine device configuration with a mouse over.**

Move your mouse over the devices found in the logical workplace. As you move the mouse pointer over these symbols the device configurations appears in a text box.

- A **router** will display port configuration information including IP address, port status, and MAC address.
- A **server** will display IP address, MAC address, and Gateway information
- A **switch** will display port configuration information including IP address, MAC address, port status, and VLAN membership.
- A **PC** will display IP address, MAC address, and Gateway information.

**Step 3: Examine device configuration.**

Left mouse click on each device type found in the logical workplace to view the device configuration.

- **Router and Switch devices** contain three tabs. These tabs are Physical, Config, and CLI (Command Line Interface).
  - The Physical tab displays the physical components of the device such as modules. New modules can also be added using this tab.
  - The Config tab displays the general configuration information such as device name.
  - The CLI tab allows the user to configure the device using the command line interface.
• **Server and Hub devices** contain two tabs. These tabs are Physical and Config.
  - The Physical tab displays components of the device such as ports. New modules can also be added using this tab.
  - The Config tab displays the general information such as device name.

• **PC devices** contain three tabs. These tabs are Physical, Config, and Desktop.
  - The Physical tab displays components of the device. New modules can also be added using this tab.
  - The Config tab displays the device name, IP address, subnet mask, DNS, and gateway information.
  - The Desktop tab allows the user to configure, IP address, subnet mask, default gateway, DNS server, dial-up, and wireless. A terminal emulator, the command prompt and a simulated web browser can also be accessed using the Desktop tab.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information. Page 3 of 4

CCNA Exploration

Network Fundamentals:

Living in a Network-Centric World 1.7.1: Skills Integration Challenge-Introduction to Packet Tracer

**Task 3: Review the Standard Lab Setup.**

**Step 1: Overview of the devices.**

The standard lab setup will consist of two routers, one switch, one server, and two PCs. Each of these devices will be pre-configured with such information as device names, IP addresses, gateways, and connections.

**Reflection:**

You are encouraged to obtain Packet Tracer from your instructor and complete My First PT Lab.
Lab 2.6.2: Using Wireshark™ to View Protocol Data Units

Learning Objectives

☐ Be able to explain the purpose of a protocol analyzer (Wireshark).
☐ Be able to perform basic PDU capture using Wireshark.
☐ Be able to perform basic PDU analysis on straightforward network data traffic.
☐ Experiment with Wireshark features and options such as PDU capture and display filtering.

Background

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. Before June 2006, Wireshark was known as Ethereal.

A packet sniffer (also known as a network analyzer or protocol analyzer) is computer software that can intercept and log data traffic passing over a data network. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is programmed to recognize the structure of different network protocols. This enables it to display the encapsulation and individual fields of a PDU and interpret their meaning.

It is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting.

For information and to download the program go to - http://www.Wireshark.org

Scenario

To capture PDUs the computer on which Wireshark is installed must have a working connection to the network and Wireshark must be running before any data can be captured.

To start data capture it is first necessary to go to the Capture menu and select the Options choice.

The Options dialog provides a range of settings and filters which determines which and how much data traffic is captured.

First, it is necessary to ensure that Wireshark is set to monitor the correct interface. From the Interface drop down list, select the network adapter in use. Typically, for a computer this will be the connected Ethernet Adapter.

Then other Options can be set. Among those available in Capture Options, the two highlighted below are worth examination.

Setting Wireshark to capture packets in promiscuous mode

If this feature is NOT checked, only PDUs destined for this computer will be captured.

If this feature is checked, all PDUs destined for this computer AND all those detected by the computer NIC on the same network segment (i.e., those that "pass by" the NIC but are not destined for the computer) are captured.

Note: The capturing of these other PDUs depends on the intermediary device connecting the end device computers on this network. As you use different intermediary devices (hubs, switches, routers) throughout these courses, you will experience the different Wireshark results.

Setting Wireshark for network name resolution

This option allows you to control whether or not Wireshark translates network addresses found in PDUs into names. Although this is a useful feature, the name resolution process may add extra PDUs to your captured data perhaps distorting the analysis.

There are also a number of other capture filtering and process settings available.

Clicking on the Start button starts the data capture process and a message box displays the progress of this process.
As data PDUs are captured, the types and number are indicated in the message box. The examples above show the capture of a ping process and then accessing a web page. When the Stop button is clicked, the capture process is terminated and the main screen is displayed. This main display window of Wireshark has three panes.

The PDU (or Packet) List Pane at the top of the diagram displays a summary of each packet captured. By clicking on packets in this pane, you control what is displayed in the other two panes. The PDU (or Packet) Details Pane in the middle of the diagram displays the packet selected in the Packet List Pane in more detail. The PDU (or Packet) Bytes Pane at the bottom of the diagram displays the actual data (in hexadecimal form representing the actual binary) from the packet selected in the Packet List Pane, and highlights the field selected in the Packet Details Pane.

Each line in the Packet List corresponds to one PDU or packet of the captured data. If you select a line in this pane, more details will be displayed in the "Packet Details" and "Packet Bytes" panes. The example above shows the PDUs captured when the ping utility was used and http://www.Wireshark.org was accessed. Packet number 1 is selected in this pane. The Packet Details pane shows the current packet (selected in the "Packet List" pane) in a more detailed form. This pane shows the protocols and protocol fields of the selected packet. The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed. The Packet Bytes pane shows the data of the current packet (selected in the "Packet List" pane) in what is known as "hexdump" style. In this lab, this pane will not be examined in detail. However, when a more in-depth analysis is required this displayed information is useful for examining the binary values and content of PDUs.

**Packet List Pane**

**Packet Details Pane**

**Packets Bytes Pane**

---

**Task 1: Ping PDU Capture**

**Step 1:** After ensuring that the standard lab topology and configuration is correct, launch Wireshark on a computer in a lab pod.

Set the Capture Options as described above in the overview and start the capture process. From the command line of the computer, ping the IP address of another network connected and powered on end device on in the lab topology. In this case, ping the Eagle Server at using the command ping 192.168.254.254.

After receiving the successful replies to the ping in the command line window, stop the packet capture.

**Step 2:** Examine the Packet List pane.

The Packet List pane on Wireshark should now look something like this:

Look at the packets listed above; we are interested in packet numbers 6, 7, 8, 9, 11, 12, 14 and 15. Locate the equivalent packets on the packet list on your computer.
From the Wireshark Packet List answer the following:
What protocol is used by ping? ______________________________
What is the full protocol name? ______________________________
What are the names of the two ping messages? ______________________________

Are the listed source and destination IP addresses what you expected? Yes / No
Why? ___________________________________

Step 3: Select (highlight) the first echo request packet on the list with the mouse.
The Packet Detail pane will now display something similar to:
Click on each of the four "*" to expand the information.
The packet Detail Pane will now be similar to:

As you can see, the details for each section and protocol can be expanded further. Spend some time
scrolling through this information. At this stage of the course, you may not fully understand the
information displayed but make a note of the information you do recognize.
Locate the two different types of "Source" and "Destination". Why are there two types?

What protocols are in the Ethernet frame?

As you select a line in the Packets Detail pane all or part of the information in the Packet Bytes pane also
becomes highlighted.
For example, if the second line (+ Ethernet II) is highlighted in the Details pane the Bytes pane now
highlights the corresponding values.
This shows the particular binary values that represent that information in the PDU. At this stage of the
course, it is not necessary to understand this information in detail.

Step 4: Go to the File menu and select Close.
Click on Continue without Saving when this message box appears.

Task 2: FTP PDU Capture
Step 1: Start packet capture.
Assuming Wireshark is still running from the previous steps, start packet capture by clicking on the Start
option on the Capture menu of Wireshark.
At the command line on your computer running Wireshark, enter **ftp 192.168.254.254**
When the connection is established, enter **anonymous** as the user without a password.

When successfully logged in enter **get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe**
and press the enter key <ENTER>. This will start downloading the file from the ftp server. The output will
look similar to:

```
C:\Documents and Settings\ccnal>ftp eagle-server.example.com
Connected to eagle-server.example.com.
220 Welcome to the eagle-server FTP service.
User (eagle-server.example.com:(none)): anonymous
331 Please specify the password.
Password:<ENTER>
230 Login successful.
ftp> get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for
pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes).
226 File send OK.
```
When the file download is complete enter \texttt{quit}.
\texttt{ftp> quit}
221 Goodbye.

Step 2: Increase the size of the Wireshark Packet List pane and scroll through the PDUs listed.
Locate and note those PDUs associated with the file download.
These will be the PDUs from the Layer 4 protocol TCP and the Layer 7 protocol FTP.
Identify the three groups of PDUs associated with the file transfer.
If you performed the step above, match the packets with the messages and prompts in the FTP command line window.
The first group is associated with the "connection" phase and logging into the server.
List examples of messages exchanged in this phase.

The third group of PDUs relate to logging out and "breaking the connection".
List examples of messages exchanged during this process.

Step 3: Examine Packet Details.
Select (highlight) a packet on the list associated with the first phase of the FTP process.
View the packet details in the Details pane.
What are the protocols encapsulated in the frame?
Highlight the packets containing the user name and password.
Examine the highlighted portion in the Packet Byte pane.
What does this say about the security of this FTP login process?

Highlight a packet associated with the second phase.
From any pane, locate the packet containing the file name.
The filename is: ______________________________
Highlight a packet containing the actual file content - note the plain text visible in the Byte pane.
Highlight and examine, in the Details and Byte panes, some packets exchanged in the third phase of the file download.
What features distinguish the content of these packets?

When finished, close the Wireshark file and continue without saving.

Task 3: HTTP PDU Capture
Step 1: Start packet capture.
Assuming Wireshark is still running from the previous steps, start packet capture by clicking on the \texttt{Start} option on the \texttt{Capture} menu of Wireshark.
\textbf{Note:} Capture Options do not have to be set if continuing from previous steps of this lab.
Launch a web browser on the computer that is running Wireshark.
Enter the URL of the Eagle Server of \texttt{example.com} or enter the IP address-192.168.254.254. When the webpage has fully downloaded, stop the Wireshark packet capture.
Step 2: Increase the size of the Wireshark Packet List pane and scroll through the PDUs listed.
Locate and identify the TCP and HTTP packets associated with the webpage download.
Ethernet

Network Fundamentals – Chapter 9
Objectives

- **Learning Objectives**
  - Upon completion of this chapter, you will be able to:
  - Describe the evolution of Ethernet
  - Explain the fields of the Ethernet Frame
  - Describe the function and characteristics of the media access control method used by Ethernet protocol
  - Describe the Physical and Data Link layer features of Ethernet
  - Compare and contrast Ethernet hubs and switches
  - Explain the Address Resolution Protocol (ARP)
Historic Ethernet

- The foundation for Ethernet technology was first established in 1970 with a program called Alohanet.
  - Alohanet was a digital radio network designed to transmit information over a shared radio frequency between the Hawaiian Islands.
  - Alohanet required all stations to follow a protocol in which an unacknowledged transmission required re-transmitting after a short period of waiting.

- The techniques for using a shared medium in this way were later applied to wired technology in the form of Ethernet.
  - Ethernet was designed to accommodate multiple computers that were interconnected on a shared bus topology.

- The first version of Ethernet incorporated a media access method known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
  - CSMA/CD managed the problems that result when multiple devices attempt to communicate over a shared physical medium.
Ethernet

- The term "ether" in "Ethernet" is said to have come from "luminiferous aether," the medium that 19th century physicists thought responsible for the propagation of light.
Ethernet – Standard and Implementation

- Ethernet operates in the lower two layers of the OSI model: the Data Link layer and the Physical layer.

- Robert Metcalfe and his coworkers at Xerox designed the 1st Ethernet LAN more than thirty years ago.
  - The first Ethernet standard was published in 1980 by a consortium of Digital Equipment Corporation, Intel, and Xerox (DIX).

- In 1985, the Institute of Electrical and Electronics Engineers (IEEE) standards committee for Local and Metropolitan Networks published standards for LANs.
  - These standards start with the number 802.
  - The standard for Ethernet is 802.3.
  - The IEEE wanted to make sure that its standards were compatible with those of the International Standards Organization (ISO) and OSI model.
  - The IEEE 802.3 standards address the needs of Layer 1 and the lower portion of Layer 2 of the OSI model.
Ethernet – Layer 1 and Layer 2

- Ethernet operates across 2 layers of the OSI model.
  - The Physical layer.
    - Ethernet at Layer 1 involves signals, bit streams that travel on the media, physical components that put signals on media, and various topologies.
    - Ethernet Layer 1 performs a key role in the communication that takes place between devices.
  - Ethernet is actually implemented in the lower half of the Data Link layer, which is known as the Media Access Control (MAC) sublayer,
    - Ethernet at Layer 2 addresses the limitations in layer 1.
    - The MAC sublayer is concerned with the physical components that will be used to communicate the information and prepares the data for transmission over the media.

- The Logical Link Control (LLC) sublayer remains relatively independent of the physical equipment that will be used for the communication process.
Logical Link Control – Connecting to the Upper Layer

- Ethernet separates the functions of the Data Link layer into two distinct sublayers:
  - the Logical Link Control (LLC) sublayer
    - IEEE 802.2 standard describes the LLC sublayer
    - LLC handles the communication between the upper layers and the networking software,
    - The LLC takes the network protocol data, and adds control information to help deliver the packet to the destination node.
    - LLC is implemented in software, and it is independent of the physical equipment.
    - In a computer, the LLC can be considered the driver software for the NIC.
  - the Media Access Control (MAC) sublayer.
    - IEEE 802.3 standard describes the MAC sublayer and the Physical layer functions.
    - MAC is implemented in hardware, typically in the NIC.
    - MAC handles the communication to the lower layers, typically the hardware.
Logical Link Control – Connecting to the Upper Layer

- The ability to migrate the original implementation of Ethernet to current and future Ethernet implementations is based on the practically unchanged structure of the Layer 2 frame.

- Physical media, media access, and media control have all evolved and continue to do so.

- But the Ethernet frame header and trailer have essentially remained constant.

<table>
<thead>
<tr>
<th>Logical Link Control Sublayer</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.3 Media Access Control</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical Signaling Sublayer</th>
<th>Physical Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>10BASE5 (500m)</td>
<td>50 Ohm Coax N-Style</td>
</tr>
<tr>
<td>10BASE2 (100m)</td>
<td>50 Ohm Cat 5e BNC</td>
</tr>
<tr>
<td>10BASE-T (100m)</td>
<td>100 Ohm UTP RJ-45</td>
</tr>
<tr>
<td>10BASE-TX (100m)</td>
<td>100 Ohm STP mini-DB-9</td>
</tr>
<tr>
<td>100BASE-TX (100m)</td>
<td>100 Ohm UTP RJ-45</td>
</tr>
<tr>
<td>100BASE-CX (25m)</td>
<td>150 Ohm Fiber SC</td>
</tr>
<tr>
<td>100BASE-SX (220m)</td>
<td>150 Ohm Fiber LC</td>
</tr>
<tr>
<td>100BASE-EX (650m)</td>
<td>150 Ohm Fiber SC</td>
</tr>
<tr>
<td>100BASE-LX (550m)</td>
<td>150 Ohm Fiber SC</td>
</tr>
</tbody>
</table>

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Public
MAC – Getting Data to the Media

The Ethernet MAC sublayer has two responsibilities:

- Data Encapsulation
  - Frame delimiting
    - The MAC layer adds a header and trailer to the Layer 3 PDU.
    - It aids the grouping of bits at the receiving node.
    - It provides synchronization between the transmitting and receiving nodes.
  - Addressing
    - Each header contains the physical address (MAC address) that enables a frame to be delivered to a destination node.
  - Error detection
    - Each trailer contains a CRC. After reception of a frame, the receiving node creates a CRC to compare to the one in the frame. If these two CRC calculations match, the frame can be trusted to have been received without error.

- Media Access Control
  - The MAC sublayer controls the placement of frames on the media and the removal of frames from the media.
    - This includes the initiation of frame transmission and recovery from transmission failure due to collisions.
  - The media access control method for Ethernet is CSMA/CD.
    - All the nodes in that network segment share the medium.
    - All the nodes in that segment receive all the frames transmitted by any node on that segment.
**Physical Implementations of Ethernet**

- Ethernet has evolved to meet the increased demand for high-speed LANs. The success of Ethernet is due to the following factors:
  - Simplicity and ease of maintenance
  - Ability to incorporate new technologies
  - Reliability
  - Low cost of installation and upgrade

- The introduction of Gigabit Ethernet has extended the original LAN technology to distances that make Ethernet a Metropolitan Area Network (MAN) and WAN standard.
  - As a technology associated with the Physical layer, Ethernet specifies and implements encoding and decoding schemes that enable frame bits to be carried as signals across the media.

- When optical fiber media was introduced, Ethernet adapted to this technology to take advantage of the superior bandwidth and low error rate that fiber offers.
  - Today, the same protocol that transported data at 3 Mbps can carry data at 10 Gbps.
  - Ethernet uses UTP copper cables and optical fiber to interconnect network devices via intermediary devices such as hubs and switches.

<table>
<thead>
<tr>
<th>Physical Devices Implementing Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTP patch panels in a rack</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ethernet fiber connectors</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Logical Link Control Sublayer</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>802.3 Media Access Control</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Physical Signaling Sublayer</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Physical Medium</th>
</tr>
</thead>
</table>

| 100BASE-T (1000Base-T) | 100BASE-T (1000Base-T) | 100BASE-T (1000Base-T) | 100BASE-T (1000Base-T) | 100BASE-T (1000Base-T) | 100BASE-T (1000Base-T) | 100BASE-T (1000Base-T) | 100BASE-T (1000Base-T) | 100BASE-T (1000Base-T) | 100BASE-T (1000Base-T) | 100BASE-T (1000Base-T) | 100BASE-T (1000Base-T) |
|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|
| 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) | 1000BASE-CX (1Gbps) |
Early Ethernet Media

- The first versions of Ethernet used coaxial cable to connect computers in a bus topology.
  - Each computer was directly connected to the backbone.
  - This topology became problematic as LANs grew larger.
  - This versions of Ethernet were known as Thicknet, (10BASE5) and Thinnet (10BASE2).
    - 10BASE5, used a thick coaxial that allowed for distances up to 500 meters before the signal required a repeater.
    - 10BASE2, used a thin coaxial cable and more flexible than Thicknet and allowed for cabling distances of 185 meters.

- The original thick coaxial and thin coaxial physical media were replaced by early categories of UTP cables.
  - Compared to the coaxial cables, the UTP cables were easier to work with, lightweight, and less expensive.

- The physical topology was also changed to a star topology using hubs.
  - Hubs concentrate connections.
  - When a frame arrives at one port, it is copied to the other ports so that all the segments on the LAN receive the frame.
  - Using the hub in this bus topology increased network reliability by allowing any single cable to fail without disrupting the entire network.
Ethernet Collision Management

- **Legacy Ethernet (Hub and half-duplex)**
  - In 10BASE-T networks, typically the central point of the network segment was a **hub**. This created a shared media.
  - Because the media is shared, only one station could successfully transmit at a time.
  - This type of connection is described as a **half-duplex**.
  - As more devices were added to an Ethernet network, the amount of frame collisions increased significantly.

- **Current Ethernet (switch and full-duplex)**
  - To enhanced LAN performance, **switch** was introduced to replace hubs in Ethernet-based networks.
  - This corresponded with the development of **100BASE-TX**.
  - Switches can isolate each port and sending a frame only to its proper destination (if the destination is known), rather than send frame to every device.
  - This, and the later introduction of **full-duplex** communications (having a connection that can carry both transmitted and received signals at the same time), has enabled the development of 1Gbps Ethernet and beyond.
Switch operation

- Full Duplex
  - Another capability emerges when only two nodes are connected.
  - In a network that uses twisted-pair cabling, one pair is used to carry the transmitted signal. A separate pair is used for the return or received signal. It is possible for signals to pass through both pairs simultaneously.
  - The capability of communication in both directions at once is known as full duplex.
  - Most switches are capable of supporting full duplex, as are most network interface cards (NICs).
  - In full duplex mode, there is no contention for the media. Thus, a collision domain no longer exists.
  - Theoretically, the bandwidth is doubled when using full duplex.

A switch uses full-duplex mode to provide full bandwidth between two nodes on a network.
Switch operation

- **Microsegments**
  - When only one node is connected to a switch port, the collision domain on the shared media contains only two nodes.
  - These small physical segments are called microsegments.

A bridge or switch increase the number of collision domains but have no impact on broadcast domains.
Moving to 1Gbps and Beyond

- The applications that cross network links on a daily basis tax even the most robust networks.
  - For example, the increasing use of Voice over IP (VoIP) and multimedia services requires connections that are faster than 100 Mbps Ethernet.

- The increase in network performance is significant when throughput increases from 100 Mbps to 1 Gbps and above.
  - Gigabit Ethernet is used to describe bandwidth of 1000 Mbps (1 Gbps) or greater.
  - This capacity has been built on the full-duplex capability and the UTP and fiber-optic media technologies of earlier Ethernet.

- Upgrading to 1 Gbps Ethernet does not always mean that the existing network infrastructure of cables and switches has to be completely replaced.
  - Some of the equipment and cabling in modern, well-designed and installed networks may be capable of working at the higher speeds with only minimal upgrading.
Ethernet Beyond the LAN

- Ethernet was initially limited to LAN cable systems within single buildings, and then extended to between buildings. It can now be applied across a city in what is known as a Metropolitan Area Network (MAN).
  - The increased cabling distances enabled by the use of fiber-optic cable in Ethernet-based networks has resulted in a blurring of the distinction between LANs and WANs.
The Frame – Encapsulating the Packet

- The Ethernet frame structure adds **headers** and **trailers** around the Layer 3 PDU.

- There are 2 Ethernet framing: **Ethernet** and **IEEE 802.3**.
  - The most significant difference between the Ethernet and IEEE 802.3 is the addition of a Start Frame Delimiter (SFD) and a small change to the Type field to include the Length.

- **Ethernet Frame Size**
  - The original Ethernet standard defined the minimum frame size as 64 bytes and the maximum as 1518 bytes.
  - This includes all bytes from the Destination MAC Address field through the Frame Check Sequence (FCS) field.
  - The Preamble and Start Frame Delimiter fields are not included when describing the size of a frame.
  - The IEEE 802.3ac standard, released in 1998, extended the maximum allowable frame size to 1522 bytes.
    - The frame size was increased to accommodate a technology called Virtual Local Area Network (VLAN).
  - If the size of a frame is less than the minimum or greater than the maximum, the receiving device drops the frame.
The Frame – Encapsulating the Packet

- **Preamble (7 bytes) and Start Frame Delimiter (1 byte)**
  - They are used for synchronization between the sending and receiving devices.
  - Essentially, the first few bytes tell the receivers to get ready to receive a new frame.

- **Destination MAC Address Field (6 bytes)**
  - It is the identifier for the intended recipient.
  - The address in the frame is compared to the MAC address in the device. If there is a match, the device accepts the frame.

- **Source MAC Address Field (6 bytes)**
  - It identifies the frame's originating NIC or interface.
  - Switches also use this address to add to their lookup tables.

- **Length/Type Field (2 bytes)**
  - The field labeled Length/Type was only listed as Length in the early IEEE versions and only as Type in the DIX version.
  - If the two-octet value is equal to or greater than 0x0600 hexadecimal or 1536 decimal, then the contents of the Data Field are decoded according to the protocol indicated.

- **Data and Pad Fields (46 - 1500 bytes)**
  - It contains the encapsulated data from a higher layer, which is a generic Layer 3 PDU, or more commonly, an IPv4 packet.
The Frame – Encapsulating the Packet

- **Frame Check Sequence Field (4 bytes)**
  - It is used to detect errors in a frame.
  - It uses a cyclic redundancy check (CRC).
  - The sending device includes the results of a CRC in the FCS field of the frame.
  - The receiving device receives the frame and generates a CRC to look for errors.
  - If the calculations match, no error occurred.
  - Calculations that do not match are an indication that the data has changed; therefore, the frame is dropped.
The Ethernet MAC Address

- A unique identifier called a Media Access Control (MAC) address was created to assist in determining the source and destination address within an Ethernet network.
  - It provided a method for device identification at a lower level of the OSI model.
  - As you will recall, MAC addressing is added as part of a Layer 2 PDU.
  - An Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits.
MAC Address Structure

IEEE require any vendor that sells Ethernet devices to register with IEEE and to follow two simple rules:

- All MAC addresses assigned to a NIC must use that vendor's assigned OUI as the first 3 bytes.
- All MAC addresses with the same OUI must be assigned a unique value in the last 3 bytes.

The MAC address is often referred to as a burned-in address (BIA) because it is burned into ROM (Read-Only Memory) on the NIC.

- However, when the computer starts up, the NIC copies the address into RAM. When examining frames, it is the address in RAM that is used as the source address to compare with the destination address.

When the device forwarding the message to an Ethernet network, each NIC in the network see if the MAC address matches its address.

- If there is no match, the device discards the frame.
- If there is a match, the NIC passes the frame up the OSI layers, where the decapsulation process take place.

http://standards.ieee.org/regauth/oui/oui.txt
Hexadecimal Numbering and Addressing

- Hexadecimal is used to represent Ethernet MAC addresses and IP Version 6 addresses.
- Hexadecimal ("Hex") is a way to represent binary values.
  - Decimal is a base ten numbering system
  - Binary is base two,
  - Hexadecimal is a base sixteen system.
    • It uses the numbers 0 to 9 and the letters A to F.
- Given that 8 bits (a byte) is a common binary grouping,
  - Binary 00000000 to 11111111 can be represented in hexadecimal as the range 00 to FF.
  - Leading zeroes are always displayed to complete the 8-bit representation. For example, the binary value 0000 1010 is shown in hexadecimal as 0A.
- Hexadecimal is usually represented in text by the value preceded by 0x (for example 0x73) or a subscript 16. Less commonly, it may be followed by an H, for example 73H.
Viewing the MAC

- A tool to examine the MAC address of our computer is the `ipconfig /all` or `ifconfig`.

- You may want to research the OUI of the MAC address to determine the manufacturer of your NIC.
Another Layer of Addressing

- **Data Link Layer**
  - OSI Data Link layer (Layer 2) physical addressing, implemented as an Ethernet MAC address, is used to transport the frame across the local media.
  - They are non-hierarchical. They are associated with a particular device regardless of its location or to which network it is connected.

- **Network Layer**
  - Network layer (Layer 3) addresses, such as IPv4 addresses, provide the ubiquitous, logical addressing that is understood at both source and destination.
  - To arrive at its eventual destination, a packet carries the destination Layer 3 address from its source.

- **In short:**
  - The Network layer address enables the packet to be forwarded toward its destination.
  - The Data Link layer address enables the packet to be carried by the local media across each segment.
Another Layer of Addressing

The data frames are then transmitted on the Ethernet segment. All stations pick up the packet and check to see if the packet is for them. All devices except for the Router discard the packet.
Ethernet Unicast, Multicast & Broadcast

- A unicast MAC address is the unique address used when a frame is sent from a single transmitting device to single destination device.

- In the example shown in the figure, a host with IP address 192.168.1.5 (source) requests a web page from the server at IP address 192.168.1.200.
  - For a unicast packet to be sent and received, a destination IP address must be in the IP packet header.
  - A corresponding destination MAC address must also be present in the Ethernet frame header.
  - The IP address and MAC address combine to deliver data to one specific destination host.
Ethernet Unicast, Multicast & Broadcast

- With a broadcast, the packet contains a destination IP address that has all ones (1s) in the host portion.
  - Direct broadcast
    - This numbering in the address means that all hosts on that local network (broadcast domain) will receive and process the packet.
  - Limited broadcast
    - All 32 bits address are all 1s

- Many network protocols, such as Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP), use broadcasts.

- As shown in the figure, a broadcast IP address for a network needs a corresponding broadcast MAC address in the Ethernet frame.

- On Ethernet networks, the broadcast MAC address is 48 ones displayed as Hexadecimal FF-FF-FF-FF-FF-FF.
Ethernet Unicast, Multicast & Broadcast

- Multicast addresses allow a source device to send a packet to a group of devices.
  - Devices that belong to a multicast group are assigned a multicast group IP address.
  - The range of multicast addresses is from 224.0.0.0 to 239.255.255.255.
  - Multicast addresses represent a group of addresses, they can only be used as the destination of a packet.
  - The source will always have a unicast address.

- As with the unicast and broadcast addresses, the multicast IP address requires a corresponding multicast MAC address to actually deliver frames on a local network.
  - The multicast MAC address is a special value that begins with 01-00-5E in hexadecimal.
  - The value ends by converting the lower 23 bits of the IP multicast group address into the remaining 6 hexadecimal characters of the Ethernet address.
  - The remaining bit in the MAC address is always a "0".
Media Access Control in Ethernet

- In a shared media environment, all devices have guaranteed access to the medium, but they have no prioritized claim on it.
  - If more than one device transmits simultaneously, the physical signals collide and the network must recover in order for communication to continue.
  - Collisions are the cost that Ethernet pays to get the low overhead associated with each transmission.

- Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to detect and handle collisions and manage the resumption of communications.
  - Because all computers using Ethernet send their messages on the same media, a distributed coordination scheme (CSMA) is used to detect the electrical activity on the cable.
  - When a device detects that no other computer is sending a frame, or carrier signal, the device will transmit, if it has something to send.
CSMA/CD – The Process

- **Carrier Sense**
  - In the CSMA/CD access method, all network devices that have messages to send must listen before transmitting.
  - If a device detects a signal from another device, it will wait for a specified amount of time before attempting to transmit.
  - When there is no traffic detected, a device will transmit its message.
  - While this transmission is occurring, the device continues to listen for traffic or collisions on the LAN.
  - After the message is sent, the device returns to its default listening mode.

- **Multi-access**
  - If the distance between devices is such that the one device's signals are not detected by a second device, the second device may start to transmit, too.
  - The media now has two devices transmitting their signals at the same time.
  - Their messages will propagate across the media until they encounter each other.
  - At that point, the signals mix and the message is destroyed.
  - Although the messages are corrupted, the jumble of remaining signals continues to propagate across the media.
CSMA/CD – The Process

- **Collision Detection**
  - The detection of a collision is made possible because all devices can detect an increase in the amplitude of the signal above the normal level.
  - Once a collision occurs, the other devices in listening mode - as well as all the transmitting devices - will detect the increase in the signal amplitude.
  - Once detected, every device transmitting will continue to transmit to ensure that all devices on the network detect the collision.

- **Jam Signal and Random Backoff**
  - Once the collision is detected by the transmitting devices, they send out a jamming signal.
  - This jamming signal is used to notify the other devices of a collision, so that they will invoke a backoff algorithm.
  - This backoff algorithm causes all devices to stop transmitting for a random amount of time, which allows the collision signals to subside.
  - A random backoff period ensures that the devices that were involved in the collision do not try to send their traffic again at the same time, which would cause the whole process to repeat.
  - But, this also means that a third device may transmit before either of the two involved in the original collision have a chance to retransmit.
CSMA/CD – Hubs and Collision Domains

- Collisions will occur in any shared media topology.

- Hubs were created as intermediary network devices that enable more nodes to connect to the shared media.
  - Because hubs operate at the Physical layer, collisions can occur between the devices they connect.
  - Using hubs to provide network access to more users reduces the performance because the fixed capacity of the media has to be shared between more devices.

- The connected devices that access a common media via a hub or series of directly connected hubs make up what is known as a collision domain.
  - A collision domain is also referred to as a network segment.
  - Hubs and repeaters therefore have the effect of increasing the size of the collision domain.

- As shown in the figure, the interconnection of hubs form a physical topology called an extended star.
  - The extended star can create a greatly expanded collision domain.
Collision domains

- Collision domains are the connected physical network segments where collisions can occur.
  - Every time a collision happens on a network, all transmission stops for a period of time.
  - The length of this period of time without transmissions varies and is determined by a backoff algorithm for each network device.

- The types of devices that interconnect the media segments define collision domains.
  - Layer 1 devices do not break up collision domains,
    - Layer 1 devices, such as repeaters and hubs, can only extend the collision domain.
  - Layer 2 and Layer 3 devices do break up collision domains.
    - Breaking up, or increasing the number of collision domains with Layer 2 and 3 devices is also known as segmentation.
Segmentation with switch

How many collision domain?

- A switch eliminates the impact of collisions through microsegmentation
- Low latency and high frame-forwarding rates at each interface port
- Works with existing 802.3(CSMA/CD) compliant network interface cards and cabling
Segmentation with router

- More manageable, greater functionality, multiple active paths
- Broadcast Domain
- Smaller Broadcast
- Operates at Layer 3 and 4
Ethernet Timing: Latency

- Each device that wants to transmit must first "listen" to the media to check for traffic. If no traffic exists, the station will begin to transmit immediately.
  - The electrical signal that is transmitted takes a certain amount of time (latency) to propagate (travel) down the cable.
  - Each hub or repeater in the signal's path adds latency as it forwards the bits from one port to the next.

- This accumulated delay increases the likelihood that collisions will occur because a listening node may transition into transmitting signals while the hub or repeater is processing the message.
  - Because the signal had not reached this node while it was listening, it thought that the media was available.
  - This condition often results in collisions.
Ethernet Timing: Timing and Synchronization

- In half-duplex mode, if a collision has not occurred, the sending device will transmit 64 bits of timing synchronization information, which is known as the Preamble.
  - The sending device will then transmit the complete frame.

- Ethernet with throughput speeds of 10 Mbps and slower are asynchronous.
  - An asynchronous communication in this context means that each receiving device will use the 8 bytes of timing information to synchronize the receive circuit to the incoming data and then discard the 8 bytes.

- Ethernet implementations with throughput of 100 Mbps and higher are synchronous.
  - Synchronous communication in this context means that the timing information is not required.
  - However, for compatibility reasons, the Preamble and Start Frame Delimiter (SFD) fields are still present.
Ethernet Timing: Bit Time

- For each different media speed, a period of time is required for a bit to be placed and sensed on the media. This period of time is referred to as the bit time.
  - On 10-Mbps Ethernet, one bit at the MAC layer requires 100 nanoseconds (nS) to transmit.
  - At 100 Mbps, that same bit requires 10 nS to transmit.
  - And at 1000 Mbps, it only takes 1 nS to transmit a bit.
  - As a rough estimate, 20.3 centimeters (8 inches) per nanosecond is often used for calculating the propagation delay on a UTP cable.
  - The result is that for 100 meters of UTP cable, it takes just under 5 bit times for a 10BASE-T signal to travel the length the cable.

- For CSMA/CD Ethernet to operate, the sending device must become aware of a collision before it has completed transmission of a minimum-sized frame.
  - At 1000 Mbps, special adjustments are required because nearly an entire minimum-sized frame would be transmitted before the first bit reached the end of the first 100 meters of UTP cable. For this reason, half-duplex mode is not permitted in 10-Gigabit Ethernet.
Ethernet Timing: Slot Time

- In half-duplex Ethernet, where data can only travel in one direction at once, slot time becomes an important parameter in determining how many devices can share a network.
  - Determining slot time is a trade-off between the need to reduce the impact of collision recovery (backoff and retransmission times) and the need for network distances to be large enough to accommodate reasonable network sizes.
  - Slot time for 10- and 100-Mbps Ethernet is 512 bit times, or 64 octets.
  - Slot time for 1000-Mbps Ethernet is 4096 bit times, or 512 octets.

- The slot time ensures that if a collision is going to occur, it will be detected within the first 512 bits (4096 for Gigabit Ethernet) of the frame transmission.

- Slot time is an important parameter for the following reasons:
  - The 512-bit slot time establishes the minimum size of an Ethernet frame as 64 bytes. Any frame less than 64 bytes in length is considered a "collision fragment" or "runt frame" and is automatically discarded by receiving stations.
  - The slot time establishes a limit on the maximum size of a network's segments. If the network grows too big, late collisions can occur. Late collisions are considered a failure in the network.

- Slot time is calculated assuming maximum cable lengths on the largest legal network architecture.
### Interframe Spacing

- The Ethernet standards require a minimum spacing between two non-colliding frames.
  - This gives the media time to stabilize after the transmission of the previous frame and time for the devices to process the frame.
  - Referred to as the interframe spacing, this time is measured from the last bit of the FCS field of one frame to the first bit of the Preamble of the next frame.

- A 10 Mbps Ethernet network are required to wait a minimum of 96 bit times (9.6 microseconds) before any device can transmit its next frame.
- On faster versions of Ethernet, the spacing remains the same - 96 bit times - but the interframe spacing time period grows correspondingly shorter.
The Truth About Interframe Spacing

Introduction

– The IEEE 802.3 specification states that before a station can attempt to transmit on the wire, it must first wait until it has heard 9.6 microseconds of silence. Many popular myths have arisen surrounding the reasons for the 9.6 microsecond interframe gap. The purpose of this section is to clarify the true reason for the 9.6 microsecond interframe gap.

The Truth

– The sole reason for the 9.6 microsecond interframe gap is to allow the station that last transmitted to cycle its circuitry from transmit mode to receive mode. Without the interframe gap, it is possible that a station would miss a frame that was destined for it because it had not yet cycled back into receive mode.

– There is, however, an interesting sidebar to this discussion and that is that most Ethernet cards in today's market are capable of switching from transmit to receive in much less time than 9.6 microseconds. This is an example of what can happen when 1970's specifications are applied to 1990's technology. In fact, some adapter manufacturers are designing their cards with a smaller interframe spacing, thereby achieving higher data transfer rates than their competitors.

– The problem arises when cards with a smaller interframe spacing are mixed on a network with cards that meet the specifications. In this case, there is a potential for lost data.

– The moral of the story is that a network administrator needs to know what is going on in his or her network and be aware that not all vendors will stick to the specs. Contact your vendors and find out what they're doing differently -- it'll pay off!
Interframe Spacing and Backoff: Jam Signal

- In the event that two devices transmit simultaneously, the network CSMA/CD attempts to resolve the issue.
  - As soon as a collision is detected, the sending devices transmit a 32-bit "jam" signal that will enforce the collision. This ensures all devices in the LAN to detect the collision.
  - It is important that the jam signal not be detected as a valid frame; otherwise the collision would not be identified.
  - The most commonly observed data pattern for a jam signal is simply a repeating 1, 0, 1, 0 pattern, the same as the Preamble.
- The corrupted, partially transmitted messages are often referred to as collision fragments or runts.
  - Normal collisions are less than 64 octets in length and therefore fail both the minimum length and the FCS tests, making them easy to identify.
Backoff Timing

- After a collision occurs and all devices allow the cable to become idle (each waits the full interframe spacing), the devices whose transmissions collided must wait an additional - and potentially progressively longer - period of time before attempting to retransmit the collided frame.
  - The waiting period is intentionally designed to be random so that two stations do not delay for the same amount of time, which would result in more collisions.

- If media congestion results in the MAC layer unable to send the frame after 16 attempts, it gives up and generates an error to the Network layer.
  - Such an occurrence is rare in a properly operating network and would happen only under extremely heavy network loads or when a physical problem exists.

- The methods described in this section allowed Ethernet to provide greater service in a shared media topology based on the use of hubs.
  - With the use of switches, the need for CSMA/CD starts to diminish or, in some cases, is removed altogether.
Overview of Ethernet Physical Layer

- The differences between standard Ethernet, Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet occur at the Physical layer, often referred to as the Ethernet PHY.

- Ethernet is covered by the IEEE 802.3 standards. Four data rates are currently defined for operation over optical fiber and twisted-pair cables:
  - 10 Mbps - 10Base-T Ethernet
  - 100 Mbps - Fast Ethernet
  - 1000 Mbps - Gigabit Ethernet
  - 10 Gbps - 10 Gigabit Ethernet

- While there are many different implementations of Ethernet at these various data rates, only the more common ones will be presented here.
10 Mbps Ethernet

- The principal 10 Mbps implementations of Ethernet include:
  - 10BASE5 using Thicknet coaxial cable (bus topology)
  - 10BASE2 using Thinnet coaxial cable (bus topology)
  - 10BASE-T using Cat3/Cat5 unshielded twisted-pair cable (start topology)

10 Mbps Ethernet - 10BASE-T

- The early implementations of 10BASE-T used Cat3 cabling.
- 10BASE-T uses two pairs of a four-pair cable and is terminated at each end with an 8-pin RJ-45 connector.
  - It uses Manchester-encoding over two unshielded twisted-pair cables.
  - The pair connected to pins 1 and 2 are used for transmitting and the pair connected to pins 3 and 6 are used for receiving.
- However, Cat5 or later cabling is typically used today.
- It uses a physical star topology.
- It could be up to 100 meters in length before requiring a hub or repeater.
- The 10BASE-T links connected to a switch can support either half-duplex or full-duplex operation.
100 Mbps Fast Ethernet

- 100 Mbps - Fast Ethernet
  - 100 Mbps Ethernet, also known as Fast Ethernet, can be implemented using twisted-pair copper wire or fiber media.

- The most popular 100 Mbps Ethernet are:
  - 100BASE-TX (Cat5 or later UTP)
    - 100BASE-TX was designed to support transmission over either two pairs of Category 5 UTP copper wire or two strands of optical fiber.
    - 100BASE-TX implementation uses the same two pairs and pinouts of UTP as 10BASE-T.
    - 100BASE-TX requires Category 5 or later UTP. The 4B/5B encoding is used for 100BASE-T Ethernet.
    - As with 10BASE-TX, 100Base-TX is connected as a physical star.
  - 100BASE-FX (fiber-optic cable)
    - 100BASE-FX standard uses the same signaling procedure as 100BASE-TX, but over optical fiber media rather than UTP copper.
    - Although the encoding, decoding, and clock recovery procedures are the same for both media, the signal transmission is different - electrical pulses in copper and light pulses in optical fiber.
    - 100BASE-FX uses Low Cost Fiber Interface Connectors (commonly called the duplex SC connector).
1000 Mbps Ethernet: 1000BASE-T Ethernet

- 1000BASE-T Ethernet provides full-duplex transmission using all four pairs in Category 5 or later UTP cable.
  - Gigabit Ethernet over copper wire enables an increase from 100 Mbps per wire pair to 125 Mbps per wire pair, or 500 Mbps for the four pairs.
  - Each wire pair signals in full duplex, doubling the 500 Mbps to 1000 Mbps.
  - 1000BASE-T uses 4D-PAM5 line encoding to obtain 1 Gbps data throughput.
  - It translates an 8-bit byte of data into a simultaneous transmission of four code symbols (4D), which are sent over the media, one on each pair, as 5-level Pulse Amplitude Modulated (PAM5) signals.

- Unlike most digital signals where there are usually a couple of discrete voltage levels,
  - 1000BASE-T uses many voltage levels. In idle periods, nine voltage levels are found on the cable.
  - During data transmission periods, up to 17 voltage levels are found on the cable.
1000 Mbps Ethernet: 1000BASE-SX and 1000BASE-LX

- The fiber versions of Gigabit Ethernet - 1000BASE-SX and 1000BASE-LX - offer the following advantages over UTP:
  - noise immunity,
  - small physical size,
  - increased unrepeated distances
  - bandwidth.

- All 1000BASE-SX and 1000BASE-LX versions
  - support full-duplex binary transmission at 1250 Mbps over two strands of optical fiber.
  - The transmission coding is based on the 8B/10B encoding scheme.
  - The principal differences among the 1000BASE-SX and 1000BASE-LX fiber versions are the link media, connectors, and wavelength of the optical signal.

<table>
<thead>
<tr>
<th>Link Configuration</th>
<th>1000Base-SX (850 nm Wavelength)</th>
<th>1000Base-LX (1300 nm Wavelength)</th>
</tr>
</thead>
<tbody>
<tr>
<td>125/82.5 µm multimode optical fiber</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>125/50 µm multimode optical fiber</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>125/10 µm single mode optical fiber</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>
Ethernet - Future Options

- The IEEE 802.3ae standard was adapted to include 10 Gbps, full-duplex transmission over fiber-optic cable.
  - 10-Gigabit Ethernet (10GbE) is evolving for use not only in LANs, but also for use in WANs and MANs.

- 10Gbps can be compared to other varieties of Ethernet in these ways:
  - Frame format is the same, allowing interoperability between all varieties of legacy, fast, gigabit, and 10 gigabit Ethernet.
  - Bit time is now 0.1 ns. All other time variables scale accordingly.
  - Because only full-duplex fiber connections are used, CSMA/CD is not necessary.
  - The IEEE 802.3 sublayers within OSI Layers 1 and 2 are mostly preserved, with a few additions to accommodate 40 km fiber links and interoperability with other fiber technologies.

- Future Ethernet Speeds
  - The IEEE and the 10-Gigabit Ethernet Alliance are working on 40-, 100-, or even 160-Gbps standards.
Legacy Ethernet – Using Hubs

- Classic Ethernet uses hubs to interconnect nodes on the LAN segment.
  - Hubs do not perform any type of traffic filtering.
  - Hub forwards all the bits to every device connected to the hub.
  - This forces all the devices in the LAN to share the bandwidth.
  - It often results in high levels of collisions on the LAN.
  - This type of Ethernet LAN has limited use in today's networks.

- Sharing media creates issues as the network grows.
  - Scalability
    - With each device added to the shared media, the average bandwidth available to each device decreases.
  - Latency
    - Increasing the length of media or the number of hubs connected to a segment results in increased latency.
    - With greater latency, it is more likely that nodes will not receive initial signals, thereby increasing the collisions present in the network.
  - Network Failure
    - If any device connected to the hub generates detrimental traffic, the communication for all devices on the media could be impeded.
  - Collisions
    - A network with a larger number of nodes on the same segment has a larger collision domain and typically has more traffic.
Ethernet – Using Switches

- In the last few years, switches have quickly become a fundamental part of most networks.
  - Switches allow the segmentation of the LAN into separate collision domains.
  - Each port of the switch represents a separate collision domain and provides the full media bandwidth to the node or nodes connected on that port.
  - With fewer nodes in each collision domain, there is an increase in the average bandwidth available to each node, and collisions are reduced.

- In a LAN where a hub is connected to a switch port, there is still shared bandwidth, which may result in collisions within the shared environment of the hub.
  - However, the switch will isolate the segment and limit collisions to traffic between the hub’s ports.
Ethernet – Using Switches

- In a LAN where all nodes are connected directly to the switch, the throughput of the network increases dramatically. These physical star topologies are essentially point to point links.

  - Dedicated bandwidth to each port
    - With switches, each device effectively has a dedicated point-to-point connection between the device and the switch, without media contention.

  - Collision-free environment
    - A dedicated point-to-point connection to a switch also removes any media contention between devices, allowing a node to operate with few or no collisions.
      - In a moderately-sized classic Ethernet network using hubs, approximately 40% to 50% of the bandwidth is consumed by collision recovery.

  - Full-duplex operation
    - With full-duplex enabled in a switched Ethernet network, the devices connected directly to the switch ports can transmit and receive simultaneously, at the full media bandwidth.
Ethernet – Using Switches

- There are three reasons why hubs are still being used:
  - Availability - LAN switches were not developed until the early 1990s and were not readily available until the mid 1990s. Early Ethernet networks used UTP hubs and many of them remain in operation to this day.
  - Economics - Initially, switches were rather expensive. As the price of switches has dropped, the use of hubs has decreased and cost is becoming less of a factor in deployment decisions.
  - Requirements - The early LAN networks were simple networks designed to exchange files and share printers. For many locations, the early networks have evolved into the converged networks of today, resulting in a substantial need for increased bandwidth available to individual users. In some circumstances, however, a shared media hub will still suffice and these products remain on the market.
Switches – Selective Forwarding

- Switch forwarding is based on the **Destination MAC**
  - The switch maintains a table, called a MAC table, that matches a destination MAC address with the port used to connect to a node.
  - For each incoming frame, the destination MAC address in the frame header is compared to the list of addresses in the MAC table.
  - If a match is found, the port number in the table that is paired with the MAC address is used as the exit port for the frame.

- The **MAC table** can be referred to by many different names.
  - It is often called the **switch table**.
  - Because switching was derived from transparent bridging, the table is sometimes called the **bridge table**.
Switches – store and forward

- Any node operating in full-duplex mode can transmit anytime it has a frame, without regard to the availability of the receiving node.
  - This is because a LAN switch will buffer an incoming frame and then forward it to the proper port when that port is idle.
  - This process is referred to as store and forward.

- With store and forward switching, the switch receives the entire frame, checks the FSC for errors, and forwards the frame to the appropriate port for the destination node.
  - Because the nodes do not have to wait for the media to be idle, the nodes can send and receive at full media speed without losses due to collisions or the overhead associated with managing collisions.
Switch Operation

- Ethernet LAN switches use 5 basic operations:

1. Learning
   - The MAC table must be populated with MAC addresses and their corresponding ports.
   - The Learning process allows these mappings to be dynamically acquired during normal operation.
   - As each frame enters the switch, the switch examines the source MAC address.
     - If no entry exists, the switch creates a new entry in the MAC table using the source MAC address and pairs the address with the port on which the entry arrived.
   - The switch now can use this mapping to forward frames to this node.

2. Aging
   - The entries in the MAC table are time stamped.
   - After entry made in MAC table, a countdown begins.
   - After the value reaches 0, the entry in the table will be removed.
Switch Operation

- **Flooding**
  - If the switch does not know to which port to send a frame because the destination MAC address is not in the MAC table, the switch sends the frame to all ports except the port on which the frame arrived.
  - Flooding is also used for frames sent to the broadcast MAC address.

- **Selective Forwarding**
  - Selective forwarding is the process of examining a frame's destination MAC address and forwarding it out the appropriate port.

- **Filtering**
  - One use of filtering has already been described: a switch does not forward a frame to the same port on which it arrived.
  - A switch will also drop a corrupt frame. If a frame fails a CRC check, the frame is dropped.
  - An additional reason for filtering a frame is security.
  - A switch has security settings for blocking frames to and/or from selective MAC addresses.
Switches – Activity: page 9.6.4

Activity

Determine how the switch forwards a frame based on the Source MAC and Destination MAC addresses and information in the switch MAC table.

1. Where will the switch forward the frame?
   - Fa1
   - Fa2
   - Fa3
   - Fa4
   -Fa5
   - Fa6
   - Fa7
   - Fa8
   - Fa9
   - Fa10
   - Fa11
   - Fa12

2. When the switch forwards the frame, which statement(s) are true?
   - Switch adds the source MAC address to the MAC table.
   - Frame is a broadcast frame and will be forwarded to all ports.
   - Frame is a unicast frame and will be sent to specific port 0.
   - Frame is a unicast frame and will be flooded to all ports.
   - Frame is a unicast frame but it will be dropped at the switch.

Please go to the page and do more exercise, until you competently understand the topics.
The ARP Process – Mapping IP to MAC Address

- The ARP protocol provides two basic functions:
  - Resolving IPv4 Addresses to MAC Addresses
    - For a frame to be placed on the LAN media, it must have a destination MAC address.
    - When a packet is sent to the Data Link layer to be encapsulated into a frame, the node refers to a table in its memory to find the Data Link layer address that is mapped to the destination IPv4 address.
    - This table is called the ARP table or the ARP cache.
    - The ARP table is stored in the RAM of the device.
  - Maintaining the ARP Table
    - There are 2 ways that a device can gather MAC addresses.
      - One way is to monitor the traffic occurs on the local segment.
      - Another way is to broadcast an ARP request.
    - ARP sends a Layer 2 broadcast to all devices on the Ethernet LAN. The frame contains an ARP request packet with the IP address of the destination host.
      - The node receiving the frame that identifies the IP address as its own responds by sending an ARP reply packet back to the sender as a unicast frame. This response is then used to make a new entry in the ARP table.
    - These dynamic entries in the MAC table are timestamped.
ARP Process – Destinations not on the local Network

- If the destination IPv4 host is not on the local network, the source node needs to deliver the frame to the router interface that is the gateway or next hop used to reach that destination.
  - The source node will use the MAC address of the gateway as the destination address for frames containing an IPv4 packet addressed to hosts on other networks.
  - In the event that the gateway entry is not in the table, the normal ARP process will send an ARP request to retrieve the MAC address associated with the IP address of the router interface.
Proxy ARP—Destinations not on the local Network

- There are circumstances under which a host might send an ARP request seeking to map an IPv4 address outside of the range of the local network.
  - In these cases, the device sends ARP requests for IPv4 addresses not on the local network instead of requesting the MAC address with the IPv4 address of the gateway.
  - To provide a MAC address for these hosts, a router uses proxy ARP to respond on behalf of remote hosts.
  - This means that the ARP cache of the requesting device will contain the MAC address of the gateway mapped to any IP addresses not on the local network.
  - If proxy ARP is disabled on the router interface, these hosts cannot communicate out of the local network.

- One such use of this process is
  - IPv4 cannot determine whether the destination host is on the same network as the source.
  - When a host believes that it is directly connected to the same network as the destination host. This generally occurs when a host is configured with an improper mask.
  - When a host is not configured with a default gateway. Proxy ARP can help devices on a network reach remote subnets.
ARP Process – Removing Address Mapping

- For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time.
  - The times differ depending on the device and its operating system.
  - For example, some Windows operating systems store ARP cache entries for 2 minutes. If the entry is used again during that time, the ARP timer for that entry is extended to 10 minutes.

- Commands may also be used to manually remove all or some of the entries in the ARP table.

- After an entry has been removed, the process for sending an ARP request and receiving an ARP reply must occur again to enter the map in the ARP table.
ARP Broadcasts Issues

- **Overhead on the Media**
  - As a broadcast frame, an ARP request is received and processed by every device on the local network.
  - On a typical business network, these broadcasts would probably have minimal impact on network performance.

- **Security**
  - In some cases, the use of ARP can lead to a potential security risk. ARP spoofing, or ARP poisoning, is a technique used by an attacker to inject the wrong MAC address association into a network by issuing fake ARP requests.
    - An attacker forges the MAC address of a device and then frames can be sent to the wrong destination.
  - Manually configuring static ARP associations is one way to prevent ARP spoofing.
  - Authorized MAC addresses can be configured on some network devices to restrict network access to only those devices listed.
Summary

In this chapter, you learned to:

- Identify the basic characteristics of network media used in Ethernet.
- Describe the Physical and Data Link layer features of Ethernet.
- Describe the function and characteristics of the media access control method used by Ethernet protocol.
- Explain the importance of Layer 2 addressing used for data transmission and determine how the different types of addressing impacts network operation and performance.
- Compare and contrast the application and benefits of using Ethernet switches in a LAN as opposed to using hubs.
- Explain the ARP process.
Planning and Cabling Networks

Network Fundamentals – Chapter 10
Objectives

Upon completion of this chapter, you will be able to:

- Identify the basic network media required to make a LAN connection.
- Identify the types of connections for intermediate and end device connections in a LAN.
- Identify the pinout configurations for straight-through and crossover cables.
- Identify the different cabling types, standards, and ports used for WAN connections.
- Define the role of device management connections when using Cisco equipment.
- Design an addressing scheme for an internetwork and assign ranges for hosts, network devices, and the router interface.
- Compare and contrast the importance of network designs.
LAN Device: Router

- Routers are the primary devices used to interconnect networks.
  - Each port on a router connects to a different network and routes packets between the networks.
  - Routers have the ability to break up broadcast domains and collision domains.
  - Routers are also used to interconnect networks that use different technologies.
  - They can have both LAN and WAN interfaces.

- The router's LAN interfaces allow routers to connect to the LAN media. This is usually UTP cabling, but modules can be added for using fiber-optics.
  - Depending on the model of router, there can be multiple interface types for connection of LAN and WAN cabling.
  - Each LAN will have a router as its gateway connecting the LAN to other networks. Inside the LAN will be one or more hubs or switches to connect the end devices to the LAN.
  - For this course, the choice of which router to deploy is determined by the Ethernet interfaces that match the technology of the switches at the center of the LAN.
Intranetwork Devices LAN Device: Hub and switch

- **Hub**
  - A hub receives a signal, regenerates it, and sends the signal over all ports.
  - The use of hubs creates a logical bus.
  - This means that the LAN uses multiaccess media.
  - The ports use a shared bandwidth approach and often have reduced performance in the LAN due to collisions and recovery.
  - Multiple hubs can be interconnected, they remain a single collision domain.
  - A hub is typically chosen as an intermediary device within a small LAN, in a LAN that has low throughput requirements, or when finances are limited.

- **Switch**
  - A switch receives a frame and regenerates each bit of the frame on to the appropriate destination port.
  - Switch is used to segment a network into multiple collision domains.
  - Switch reduces the collisions on a LAN. Each port on the switch creates a separate collision domain. This creates a point-to-point logical topology to the device on each port.
  - Switch provides dedicated bandwidth on each port.
  - Switch can also be used to interconnect segments of different speeds.
  - There is a range of switches available with a variety of features that enable the interconnection of multiple computers in a typical enterprise LAN setting.
Switch Selection Factors

- To meet user requirements, a LAN needs to be planned and designed.
  - Planning ensures that all requirements, cost factors and deployment options are given due consideration.

- These factors include, but are not limited to:
  - Cost
  - Speed and Types of Ports/Interfaces
  - Expandability
  - Manageability
  - Additional Features and Services

- The two topics will be explored further:
  - cost
  - interface characteristics.
Switch Selection Factors: Cost

- The cost of a switch is determined by its capacity and features.
  - The switch capacity includes the number and types of ports available and the switching speed.
  - Other factors that impact the cost are its network management capabilities, embedded security technologies, and optional advanced switching technologies.

- Using a simple "cost per port" calculation, it may appear initially that the best option is to deploy one large switch at a central location.
  - However, this apparent cost savings may be offset by the expense from the longer cable lengths required to connect every device on the LAN to one switch.
  - This option should be compared with the cost of deploying a number of smaller switches connected by a few long cables to a central switch.

- Another cost consideration is how much to invest in redundancy.
  - We can provide a secondary central switch to operate concurrently with the primary central switch.
  - We can also provide additional cabling to provide multiple interconnections between the switches.
  - The goal of redundant systems is to allow the physical network to continue its operation even if one device fails.
Switch Selection: Speed and Types of Ports/Interfaces

- Newer computers with built-in 10/100/1000 Mbps NICs are available. Choosing Layer 2 devices that can accommodate increased speeds allows the network to evolve without replacing the central devices.

- When selecting a switch, choosing the number and type of ports is a critical decision. Ask yourself these questions: Would you purchase a switch with:
  - Just enough ports for today's needs?
  - A mixture of UTP speeds?
  - Both UTP and fiber ports?

  • Consider carefully how many UTP ports will be needed and how many fiber ports will be needed.
  • Consider how many ports will need 1 Gbps capability and how many ports only require 10/100 Mbps bandwidths.
  • Consider how soon more ports will be needed.
Router Selection Factors

- When selecting a router, we need to match:
  - Cost
    - Routers can be expensive based on interfaces and features.
  - Interface types
    - Additional module, such as fiber-optics, can increase the costs.
  - Expandability
    - Routers come in both fixed and modular configurations.
      - Fixed configurations have a specific number and type of ports.
      - Modular devices have expansion slots that provide the flexibility to add new modules as requirements evolve. Most modular devices come with a basic number of fixed ports as well as expansion slots.
  - Media
    - The media used to connect to the router should be supported without needing to purchase additional modules.
  - Operating System Features
    - Depending on the version of the operating system, the router can support certain features and services such as:
      - Security
      - Quality of Service (QoS)
      - Voice over IP (VoIP)
      - Routing multiple Layer 3 protocols
      - Services such as NAT and DHCP
LAN cabling

- When planning the LAN cabling, there are 4 areas:
  - **Work area**
    - It is the locations for the end devices and individual users.
    - It uses patch cables to connect individual devices to wall jacks.
    - It has a maximum length of 5 meters.
    - Straight-through cable is the most common patch cable used.
    - When a hub or switch is placed in the work area, a crossover cable is typically used to connect the device to the wall jack.
  - **Distribution cabling, also known as horizontal cabling**
    - Horizontal cabling refers to the cables connecting the telecommunication rooms with the work areas.
    - The maximum length for a cable from a termination point in the telecommunication room to the termination at the work area outlet must not exceed 90 meters.
    - This 90 meter maximum cabling distance is the permanent link because it is installed in the building structure.
LAN cabling

- When planning the LAN cabling, there are 4 areas:
  - Telecommunications room (distribution facility)
    - The rooms contain - hubs, switches, routers, and data service units (DSUs) - that tie the network together.
    - These devices provide the transitions between the backbone cabling and the horizontal cabling.
    - The patch cord, with a length of up to 5 meters, is used to connect equipment and patch panels in the telecommunications room.
    - These rooms often serve dual purposes. In many organizations, the telecommunications room also contains the servers.
  - Backbone cabling (vertical cabling)
    - Backbone cabling refers to the cabling used to connect telecommunication rooms to the equipment rooms, where the servers are often located.
    - Backbone cabling also interconnects multiple telecommunications rooms throughout the facility.
    - These cables are sometimes routed outside the building to the WAN connection or ISP.
    - Backbones cabling are used for aggregated traffic, such as traffic to and from the Internet and access to corporate resources.
    - Therefore, backbones typically require high bandwidth media such as fiber-optic cabling.
Total Cable Length: 100 meters

- For UTP installations, the ANSI/TIA/EIA-568-B standard specifies that the total combined length of cable spanning the 3 areas listed above is limited to a maximum distance of 100 meters per channel.

  - This standard specifies there can be up to 5 meters of patch cable for interconnecting patch panels.
  - There can be up to 5 meters of cable from the cable termination point on the wall to the telephone or computer.
  - 90 meters for the horizontal cable.
LAN and WAN – Types of Media

- Choosing the cables necessary to make a successful LAN or WAN connection requires consideration of the different media types.
  - UTP (Category 5, 5e, 6, and 7)
  - Fiber-optics
  - Wireless

- Each media type has its advantages and disadvantages:
  - Cable length - Does the cable need to span across a room or from building to building?
  - Cost - Does the budget allow for using a more expensive media type?
  - Bandwidth - Does the technology used with the media provide adequate bandwidth?
  - Ease of installation - Does the implementation team have the ability to install the cable or is a vendor required?
  - Susceptible to EMI/RFI - Is the local environment going to interfere with the signal?
LAN and WAN – Types of Media

- **Cable Length**
  - The total length of cable required to connect a device includes all cables from the end devices to the intermediary device in the telecommunication room (usually a switch).
    - For example, when using UTP cabling for Ethernet, it has the recommended maximum distance of 90 (100) meters.
    - Fiber-optic cables may provide a greater cabling distance—up to 500 meters to a few kilometers depending on the technology.
  - Attenuation is reduction of the strength of a signal as it moves down a media.
    - The longer the media, the more attenuation will affect the signal.
    - Cabling distance is a significant factor in data signal performance.

- **Cost**
  - Although fiber provides greater bandwidth than UTP, the material and installation costs are significantly higher.
    - Network designers must match the performance needs of the users with the cost of the equipment and cabling to achieve the best cost/performance ratio.

- **Bandwidth**
  - A fiber cable may be a logical choice for a server connection.
    - For example, a server generally has a need for more bandwidth than a computer dedicated to a single user.
  - Wireless is also supporting huge increases in bandwidth, but it has limitations in distance and power consumption.
LAN and WAN – Getting Connected

- **Ease of Installation**
  - UTP cable is relatively lightweight and flexible and has a small diameter, which allows it to fit into small spaces.
    - The connectors, RJ-45 plugs, are easy to install and are a standard.
    - A raceway is an enclosure or tube that encloses and protects the cable.
  - Many fiber-optic cables contain a thin glass fiber. This creates issues for the bend radius of the cable.
    - Crimps or sharp bends can break the fiber. The termination of the cable connectors (ST, SC, MT-RJ) are significantly more difficult to install.
  - Wireless networks require cabling, at some point, to connect devices, such as access points, to the wired LAN.
    - However, a wireless LAN requires more careful planning and testing.
    - There are many external factors, such as other radio frequency devices and building construction, that can affect its operation.

- **Electromagnetic Interference/Radio Frequency Interference**
  - Interference can be produced by electrical machines, lightning, and other communications devices, including radio equipment.
  - Interconnected devices in two separate buildings.
    - Fiber cable is the best choice.
  - Wireless is the medium most susceptible to RFI.
    - Before using wireless technology, potential sources of interference must be identified and, if possible, minimized.
Making LAN Connections: RJ-45 connector

- UTP cabling connections are specified by the Electronics Industry Alliance / Telecommunications Industry Association (EIA/TIA).

- The RJ-45 connector is the male component crimped on the end of the cable.
  - When viewed from the front, the pins are numbered from 8 to 1.
  - When viewed from above with the opening gate facing you, the pins are numbered 1 through 8, from left to right.
Making LAN Connections: Straight-through UTP Cables

- A straight-through cable has connectors on each end that are terminated the same in accordance with either the T568A or T568B standards.
  - Identifying the cable standard used allows you to determine if you have the right cable for the job.
  - More importantly, it is a common practice to use the same color codes throughout the LAN for consistency in documentation.

- Use straight-through cables for the following connections:
  - Switch to a router Ethernet port
  - Computer to switch
  - Computer to hub
Making LAN Connections: Crossover UTP Cables

For two devices to communicate through a cable that is directly connected between the two, the transmit terminal of one device needs to be connected to the receive terminal of the other device.

– The cable must be terminated so the transmit pin, Tx, taking the signal from device A at one end, is wired to the receive pin, Rx, on device B.
– Similarly, device B’s Tx pin must be connected to device A’s Rx pin.

To achieve this type of connection with a UTP cable, one end must be terminated as EIA/TIA T568A pinout, and the other end terminated with T568B pinout.

Crossover cables directly connect the following devices on a LAN:

– Switch to switch
– Switch to hub
– Hub to hub
– Router to router Ethernet port connection
– Computer to computer
– Computer to a router Ethernet port
Making LAN Connections: Console (rollover) Cables

- To initially configure the Cisco device, a management connection must be directly connected to the device. (For Cisco equipment this management attachment is called a console port).

- The cable used between a terminal and a console port is a rollover cable, with RJ-45 connectors. The rollover cable, also known as a console cable. It has a different pinout than the straight-through or crossover RJ-45 cables. The pinout for a rollover is as follows:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

- PCs require an RJ-45 to DB-9 or RJ-45 to DB-25 adapter.
- COM port settings are 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control.
- This provides out-of-band console access.
- AUX switch port may be used for a modem-connected console.
Making LAN Connections

- On the figure, identify the cable type used based on the devices being connected.

- Use straight-through cables for connecting:
  - Switch to router
  - Computer to switch
  - Computer to hub

- Use crossover cables for connecting:
  - Switch to switch
  - Switch to hub
  - Hub to hub
  - Router to router
  - Computer to computer
  - Computer to router
Making LAN Connections: MDI or MDIX

- Typically, when connecting different types of devices, use a straight-through cable.
- And when connecting the same type of device, use a crossover cable.
- In an Ethernet LAN, devices use one of two types of UTP interfaces - MDI or MDIX.
  - The MDI (media-dependent interface) uses the normal Ethernet pinout.
    - Pins 1 and 2 are used for transmitting and Pins 3 and 6 are used for receiving.
    - Devices such as computers, servers, or routers will have MDI connections.
  - The MDIX (media-dependent interface, crossover) swap the transmit pairs internally.
    - This swapping allows the end devices to be connected to the hub or switch using a straight-through cable.

www.answers.com/topic/mdi-port
Many devices allow the UTP Ethernet port to be set to MDI or MDIX. This can be done in one of three ways, depending on the features of the device:

1. On some devices, ports may have a mechanism that electrically swaps the transmit and receive pairs.
   - The port can be changed from MDI to MDIX by engaging the mechanism.

2. As part of the configuration, some devices allow for selecting whether a port functions as MDI or as MDIX.

3. Many newer devices have an automatic crossover feature.
   - On some devices, this auto-detection is performed by default. Other devices require an interface configuration command for enabling MDIX auto-detection.
Making WAN Connections

- By definition, WAN links can span extremely long distances.
  - These distances can range across the globe as they provide the communication links.

- Wide area connections between networks take a number of forms, including:
  - Telephone line RJ11 connectors for dialup or Digital Subscriber Line (DSL) connections
  - 60 pin Serial connections

- In the course labs, you may be using Cisco routers with one of two types of physical serial cables.
  - The first cable type has a male DB-60 connector on the Cisco end.
  - The second type is a more compact version and has a Smart Serial connector on the Cisco device end.
    - Both cables use a large Winchester 15 Pin connector on the network end.
    - This end of the cable is used as a V.35 connection to a Physical layer device such as a CSU/DSU.
Making WAN Connections: DCE and DTE

The following terms describe the types of devices that maintain the link:

- **Data Communications Equipment (DCE)** –
  - It supplies the clocking services to another device.
  - It is at the WAN access provider end of the link.
  - In most cases, the telco or ISP provides the clocking service that synchronizes the transmitted signal.
  - For example, if a device running at 1.544 Mbps, each receiving device must use a clock, sending out a sample signal every 1/1,544,000th of a second.

- **Data Terminal Equipment (DTE)** –
  - It receives clocking services from another device and adjusts accordingly.
  - It is at the WAN customer or user end of the link.
  - If a serial connection is made directly to a service provider or to a device that provides signal clocking such as a channel service unit/data service unit (CSU/DSU), the router is DTE and will use a DTE serial cable.

Be aware that there will be occasions, especially in our labs, when the local router is required to provide the clock rate and will therefore use a DCE cable.
Making WAN Connections

- When making WAN connections between two routers in a lab environment, connect two routers with a serial cable to simulate a point-to-point WAN link.
  - In this case, decide which router is going to be the one in control of clocking.
  - Routers are DTE devices by default, but they can be configured to act as DCE devices.

- The V35 compliant cables are available in DTE and DCE versions. To create a point-to-point serial connection between two routers, join together a DTE and DCE cable.
  - Each cable comes with a connector that mates with its complementary type.
  - These connectors are configured so that you cannot join two DCE or two DTE cables together by mistake.
How Many Hosts in the Network?

- To develop an addressing scheme for a network, start with determining the total number of hosts. (current and future)
  - The end devices requiring an IP address include:
    - User computers
    - Administrator computers
    - Servers
    - Other end devices such as printers, IP phones, and IP cameras
  - Network devices requiring an IP address include:
    - Router LAN interfaces
    - Router WAN (serial) interfaces
  - Network devices requiring an IP address for management include:
    - Switches
    - Wireless Access Points

- Next, determine if all hosts will be part of the same network, or whether the network as a whole will be divided into separate subnets.
  - Recall that the number of hosts on one network or subnet is calculated using the formula $2^n - 2$, where $n$ is the number of bits available as host bits.
  - Recall also that we subtract two addresses - the network address and the network broadcast address - cannot be assigned to hosts.
How Many Network?

- There are many reasons to divide a network into subnets:
  - Manage Broadcast Traffic - Broadcasts can be controlled because it is divided into a number of smaller domains.
  - Different Network Requirements - If different groups of users require specific network, it is easier to manage these requirements if those users are all together on one subnet.
  - Security - Different levels of network security can be implemented based on network addresses.

- Counting the Subnets
  - Each subnet, as a physical network segment, requires a router interface as the gateway for that subnet.
  - Each connection between routers is a separate subnet.
  - The number of subnets on one network is also calculated using the formula $2^n$, where $n$ is the number of bits "borrowed" from the given IP network address.

- Subnet Masks
  - The next step is to apply one subnet mask:
    - A unique subnet and subnet mask for each physical segment
    - A range of usable host addresses for each subnet
Determining the Address Standard for our Internetwork

- For example, when allocating an IP address to a router interface that is the gateway for a LAN, it is common practice to use the first (lowest) or last (highest) address within the subnet range. This consistent approach aids in configuration and troubleshooting.

- Similarly, when assigning addresses to devices that manage other devices, using a consistent pattern within a subnet makes these addresses easily recognizable. For example, in the figure, addresses with 64 - 127 in the octets always represent the general users.

- In addition, remember to document your IP addressing scheme on paper.

- Some of the different categories for hosts are:
  - General users
  - Special users
  - Network resources
  - Router LAN interfaces
  - Router WAN links
  - Management access
Calculating Addresses: Case 1

- The figure shows the network topology for this example:

  - **Student LAN**
    - Student Computers: 460
    - Router (LAN Gateway): 1
    - Switches (management): 20
    - Total for student subnetwork: 481

  - **Instructor LAN**
    - Instructor Computers: 64
    - Router (LAN Gateway): 1
    - Switches (management): 4
    - Total for instructor subnetwork: 69

  - **Administrator LAN**
    - Administrator Computers: 20
    - Server: 1
    - Router (LAN Gateway): 1
    - Switch (management): 1
    - Total for administration subnetwork: 23

  - **WAN**
    - Router - Router WAN: 2
    - Total for WAN: 2

- There are two methods available for allocating addresses to an internetwork.
  - We can use Variable Length Subnet Masking (VLSM), where we assign the prefix and host bits to each network based on the number of hosts in that network.
  - Or, we can use a non-VLSM approach, where all subnets use the same prefix length and the same number of host bits.
Calculating Addresses: Case 1: Addresses-without VLSM

- When using the non-VLSM method of assigning addresses, all subnets have the same number of addresses.
  - We base the number of addresses for all networks on the addressing requirements for the largest network.

- In Case 1, the Student LAN is the largest network, requiring 481 addresses.

- We use 9 as the value for n because 9 is the first power of 2 that is over 481.
  - Borrowing 9 bits for the host portion yields this calculation:
    - \(2^9 = 512\)
    - \(512 - 2 = 510\) usable host addresses
  - This meets the current requirement for at least 481 addresses, with a small allowance for growth. This also leaves 23 network bits (32 total bits - 9 host bits).

- Because there are four networks in our internetwork, we will need four blocks of 512 addresses each, for a total of 2048 addresses.
  - We will use the address block 172.16.0.0 /23. This provides addresses in the range from 172.16.0.0 to 172.16.7.255.
Calculating Addresses: Case 1: Addresses-without VLSM

- For the Student network block, the values would be:
  - The student network required 481 address
  - The address block is 172.16.0.1 to 172.16.1.254.
  - Only 29 address will go unused

- Instructor LAN
  - The instructor network requires a total of 69 addresses.
  - The address block is 172.16.2.1 to 172.16.3.254.
  - The 441 addresses will go unused.

- Administrator LAN
  - The administrator network requires a total of 23 addresses.
  - The address block is 172.16.4.1 to 172.16.5.254.
  - The 487 addresses will go unused.

- WAN
  - The WAN network requires a total of 2 addresses.
  - The address block is 172.16.6.1 to 172.16.7.254.
  - The 508 addresses will go unused.

- We can use VLSM in this internetwork to save addressing, but using VLSM requires more planning.
Calculating Addresses: Case 1: Addresses-with VLSM

- For the VLSM assignment, we can allocate a much smaller block of addresses to each network, as appropriate.

- The address block 172.16.0.0/22 (subnet mask 255.255.252.0) has been assigned to this internetwork.
  - Ten bits will be used to define host and sub networks.
  - It has a total of 1024 addresses from 172.16.0.0 to 172.16.3.0.

- Student LAN
  - The largest subnet is the Student LAN requires 481 addresses.
  - Using the formula usable hosts = 2^n - 2, borrowing 9 bits for the host portion gives 512 - 2 = 510 usable host addresses.
  - Using the lowest available address gives us of 172.16.0.0 /23.
  - The IP host range would be 172.16.0.1 through 172.16.1.254.

- Instructor LAN
  - The next largest network is the Instructor LAN. It requires at least 69 addresses.
  - Using 6 in the power of 2 formula, 2^6 - 2, only provides 62 usable addresses.
  - We must use an address block using 7 host bits. The calculation 2^7 -2 will yield a block of 126 addresses.
  - The next available block is the 172.16.2.0 /25 network.
  - This provides an IP host range of 172.16.2.1 to 172.16.2.126.
Calculating Addresses: Case 1: Addresses-with VLSM

- **Administrator LAN**
  - For the Administrator LAN, we need to accommodate 23 hosts.
  - This will require the use of 6 host bits: $2^6 - 2$.
  - The next available block of addresses that can accommodate these hosts is the 172.16.2.128 /26 block.
  - This provides IP host range of 172.16.2.129 to 172.16.2.190.

- **WAN**
  - The last segment is the WAN, requiring 2 host addresses.
  - Only 2 host bits will accommodate the WAN links. $2^2 - 2 = 2$.
  - The next available address block is 172.16.2.192 /30.
  - This gives an IP host range of 172.16.2.193 to 172.16.2.194.

This completes the allocation of addresses using VLSM for Case 1. If an adjustment is necessary to accommodate future growth, addresses in the range of 172.16.2.196 to 172.16.3.255 are still available.
Calculating Addresses: Case 2

- In Case 2, the challenge is to subnet this internetwork while limiting the number of wasted hosts and subnets.

- The figure shows 5 different subnets, each with different host requirements. The given IP address is 192.168.1.0/24.

- The host requirements are:
  - NetworkA - 14 hosts
  - NetworkB - 28 hosts
  - NetworkC - 2 hosts
  - NetworkD - 7 hosts
  - NetworkE - 28 hosts
Calculating Addresses: Case 2

- As we did with Case 1, we begin the process by subnetting for the largest host requirement first.

- In this case, the largest requirements are for NetworkB and NetworkE, each with 28 hosts.
  - For networks B and E, 5 bits are borrowed from the host portion and the calculation is \(2^5 = 32 - 2\).
  - This allows 8 subnets with 30 hosts each.
  - Network B will use Subnet 0: 192.168.1.0/27
    - host address range 1 to 30
  - Network E will use Subnet 1: 192.168.1.32/27
    - host address range 33 to 62

- The next largest host is NetworkA, followed by NetworkD.
  - Network A will use Subnet 0: 192.168.1.64/28
    - host address range 65 to 78
  - Network D will use Subnet 1: 192.168.1.80/28
    - host address range 81 to 94

- NetworkC has only two hosts.
  - Network C will use Subnet 1: 192.168.1.96/30
    - host address range 97 to 98

- The host requirements are:
  - NetworkA - 14 hosts
  - NetworkB - 28 hosts
  - NetworkC - 2 hosts
  - NetworkD - 7 hosts
  - NetworkE - 28 hosts
Device Interfaces

- It is important to understand that Cisco devices, routers, and switches have several types of interfaces.

- **LAN Interfaces - Ethernet**
  - The Ethernet interface is used for connecting cables that terminate with LAN devices such as computers and switches.
  - Several conventions for naming Ethernet interfaces, including AUI (older Cisco devices), Ethernet, FastEthernet and Fa 0/0.
  - The name used depends on the type and model of the device.

- **WAN Interfaces - Serial**
  - Serial interfaces are used for connecting WAN devices to the CSU/DSU.
  - For lab, we will make a back-to-back connection between two routers, and set a clock rate on one of the interfaces.
  - To establish communication with a router via a console on a remote WAN, a WAN interface is assigned an IPv4 address.

- **Console Interface**
  - The console interface is the interface for initial configuration.
  - Physical security of network devices is extremely important.

- **Auxiliary (AUX) Interface**
  - This interface is used for remote management of the router.
  - Typically, a modem is connected to the AUX interface for dial-in access.
Making the Device Management Connection

- Typically, networking devices do not have their own displays, keyboards, or input devices such as trackballs and mice. Accessing a network device for configuration, verification, or troubleshooting is made via a connection between the device and a computer.

- To enable this connection, the computer runs a program called a terminal emulator.
  
  - A terminal emulator is a software program that allows one computer to access the functions on another device. It allows a person to use the display and keyboard on one computer to operate another device, as if the keyboard and display were directly connected to the other device.

  - The cable connection between the computer running the terminal emulation program and the device is often made via the serial interface.
Making the Device Management Connection

To connect to a router or switch for device management using terminal emulation, follow these steps:

Step 1:
- Connect a computer to the console port using console cable.
- The console cable has a DB-9 connector on one end and an RJ-45 connector on the other end.
- Many newer computers do not have a serial interface. You can use a USB-to-serial cable to access the console port.

Step 2:
- For the purpose of this course, we will usually use HyperTerminal. This program can be found under All Programs > Accessories > Communications. Select HyperTerminal.
- Open HyperTerminal, configure the port with these settings:
  - Bits per second: 9600 bps
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None

Step 3:
- Log in to the router using the terminal emulator software.
- You can access the router by pressing the Enter key.
Summary

In this chapter, you learned to:

- Identify the basic network media required to make a LAN connection.
- Identify the types of connections for intermediate and end device connections in a LAN.
- Identify the pinout configurations for straight-through and crossover cables.
- Identify the different cabling types, standards, and ports used for WAN connections.
- Define the role of device management connections when using Cisco equipment.
- Design an addressing scheme for an internetwork and assign ranges for hosts, network devices, and the router interface.
- Compare and contrast the importance of network designs.
Course Assignments by Week
CIS 153C: LAN Switching & Wireless

During week one, you must post something about yourself in the SIA (Student Introductory Assignment) forum (under the Week 1 Lesson link within Angel). Look at what I posted and post something similar about yourself. Please do this no later than Wednesday at midnight of week 1 so that I can accurately report week 1 attendance to financial aid.

Homework due dates: Please see your syllabus for details!

Quizzes are available through Cisco’s Networking Academy Web site. You should be familiar with this since this is the exact same procedure used in CIS 152C.

Submit Packet Tracer homework via the assignment's drop box. Submit physical lab paperwork by printing out that specific lab and placing it in my inbox, which is outside of my office. Homework is submitted the same as we did during fall term in CIS 152C.

Week By Week Activities:

Week 1 (January 06, 2014):
- SIA due by Wednesday at midnight during week one!
  - If you don’t complete your SIA on time you may be dropped from the course in week 1
- Read and do hands-on work for Chapter 1
- Do the online Quiz for Chapter 1
- Homework due for Chapter 1 - PT lab
  - PT lab: 1.3.1.3 PTSIC

Week 2:
- Read and do hands-on work for Chapter 2
- Do the online Quiz for Chapter 2
- Homework due for Chapter 2: Physical lab
  - Physical lab: Lab 2.3.2.3 - Configuring Rapid PVST+, PortFast, and BPDU Guard

Week 3:
- No school on Monday, January 20th, in observance of Martin Luther King's Birthday
- Read and do hands-on work for Chapter 3
- Do the online Quiz for Chapter 3
- Homework due for Chapter 3: PT lab
  - PT lab: 3.3.1.2 PTSIC

Week 4:
- Read and do hands-on work for Chapter 4
- Do the online Quiz for Chapter 4
- Homework due for Chapter 4: Physical lab
  - Physical lab: Labs 4.4.2.3 - Configuring a Wireless Router and Client AND 4.5.1.1 - Inside and Outside Control
Week 5:
- Read and do hands-on work for Chapter 5
- Do the online Quiz for Chapter 5
- Homework due for Chapter 5: Physical or PT lab
  - Physical lab: Lab 5.1.2.13 - Configuring OSPFv2 on a Multiaccess Network
  - PT lab: 5.3.1.2 PTSIC

Week 6:
- Read and do hands-on work for Chapter 6
- Do the online Quiz for Chapter 6
- Homework due for Chapter 6: PT lab
  - PT lab: Lab 6.2.3.7 - Configuring Multi-area OSPFv3

Week 7:
- **No school on Monday, February 17th in observance of President's Day**
- Read and do hands-on work for Chapter 7
- Do the online Quiz for Chapter 7
- Homework due for Chapter 7: PT lab
  - PT lab: 7.2.2.4 - Configuring Basic EIGRP with IPv4

Week 8:
- Read and do hands-on work for Chapter 8
- Do the online Quiz for Chapter 8
- Homework due for Chapter 8: Physical lab
  - Physical lab: Lab 8.0.1.2 - EIGRP – Back to the Future

Week 9:
- Read and do hands-on work for Chapter 9
- Do the online Quiz for Chapter 9
- Homework due for Chapter 9: PT lab
  - PT lab: Lab 9.1.1.9 - Decoding IOS Image Names
  - Note: please print out the PT lab file, write your answers in it, and submit them in your instructor's office mailbox

Week 10:
- Review for final exam (study guide posted this week)
- Complete the Skills Final Exam:
  - PT lab: 9.3.1.4 PTSIC
  - Due by Monday, March 17, 2014 @ 1 PM

Week 11: Mar 17 – Mar 21
- Final Exam
  - **The final exam will be taken through Cisco's Networking Academy link**
  - You must physically present in class to take the final exam
  - Date / time: Monday, March 17, 2014 @ 1000 - NOON in TC 106
Syllabus: CIS 153C - Intermediate Routing & Switching (Cisco 3)

Instructor: John Blackwood, MS, CCNA/CCAI
Phone: 541-440-7686
E-mail: john.blackwood@umpqua.edu
Course: CIS 153C, 4 credit hours
Class: Lecture: MTW 1100 - 1150 in TC 101 and Lab: TH 1300 - 1450 in TC 101
Cisco Networking Academy Link: https://www.netacad.com/

Prerequisites: Students should have previously completed CIS 152C with a grade of C or better, or have obtained instructor approval.

Course Requirements: Students must have the following components and equipment to take this online class:

- High-speed Internet availability
- A PC running Windows 7 Professional or better, 2 GB of RAM, at least 1 GB free disk space, and all Windows critical updates applied
- Office 2010 or its Viewers installed. Click here for more information
- IE 8.0 or better browser installed
- Professional (not freeware) virus protection with up-to-date virus patterns

Required Texts: This course does not have any required textbook. All of the course material is within the Cisco Academy website.

Course Description: This course is the third of four Cisco Networking Academy courses, mapped to the Cisco Certified Network Administrator industry credential. The focus of this course is on the architecture, components, and operations of routers and switches in a larger and more complex network. You will learn how to configure routers and switches for advanced functionality.

Course Outcomes: Upon completion of this course, students should have the ability to:

- Configure and troubleshoot DHCP and DNS operations for IPv4 and IPv6
- Describe the operations and benefits of the Spanning Tree Protocol (STP)
- Configure and troubleshoot STP operations
- Describe the operations and benefits of link aggregation and Cisco VLAN Trunk Protocol (VTP)
- Configure and troubleshoot VTP, STP, and RSTP
- Configure and troubleshoot basic operations of routers in a complex routed network for IPv4 and IPv6
- Configure and troubleshoot advanced operations of routers and implement RIP, OSPF, and EIGRP routing protocols for IPv4 and IPv6
- Manage Cisco IOS Software licensing and configuration files

**Instruction:** This course will utilize class lecture and lab time, along with material available online via the Cisco Networking Academy (NetSpace) website.

**Equipment:** Students will use UCC-owned computers, routers, and switches to complete study and lab work. Students wishing to use their own resources may need to download and install Packet Tracer software and/or purchase their own hardware. Please consult with your instructor prior to purchasing any hardware or software for this class.

**Expected student commitment:** Students should plan to spend an average of 12 - 15 hours per week working in class lecture, assigned homework, and reading.

Students are strongly encouraged to work together to complete lab assignments since each assignment typically entails configuring three switches and routers. In addition, working in teams means that students will be able to share personal equipment and learn from each other.

**Quizzes:** There will be nine quizzes during the term. Quizzes are available through the online Cisco Networking Academy connection. Quizzes can be taken anytime during the week, up to two times. The highest score is the one that is recorded in the gradebook. Quizzes are automatically graded and feedback is provided after you complete each quiz. Quizzes must be taken during the week in which the chapter is under discussion. The quiz will be accessible for one week after it is enabled. For example, the Chapter 1 quiz must be completed no later than 1 PM on Monday, January 13th, 2014. I will enable each quiz on Monday of each week. No exceptions.

**Points:** Grades will be assigned based on the total points (pts) earned as follows; 90 to 100% = A, 80 to 89% = B, 70 to 79% = C, 60 to 69% = D, and less than 60% = F. Points are distributed as follows:

<table>
<thead>
<tr>
<th>Description</th>
<th>Category %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter quizzes</td>
<td>15%</td>
</tr>
<tr>
<td>Lab assignments (homework)</td>
<td>45%</td>
</tr>
<tr>
<td>Skills final exam</td>
<td>20%</td>
</tr>
<tr>
<td>Final exam</td>
<td>20%</td>
</tr>
<tr>
<td><strong>Total Possible Points</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

**Course Outline & homework:** This outline is a plan for the term. It is subject to change should the need arise. Any such changes will be noted during assigned class or lab time. It is your responsibility to note changes in the syllabus schedule as presented in class or via Angel announcements during the term.
All of the assignments for this term are listed by week in the Course Assignments by Week document, which is posted under Lessons.

Lab (homework) assignments are due by noon of the Tuesday after each week’s assignment. For example, labs for Week 1 are due on or before noon on Tuesday, January 14, 2014. Homework is due on Tuesday to provide you with extra time due to equipment conflicts, etc.

Your homework is made up of assignments listed in your physical and Packet Tracer lab manuals. For each chapter, you will manually perform many step-by-step exercises as you read and study each lesson. For example, in chapter 1, on p. 39 you should complete the Packet Tracer Activity shown there using the file on your book's CD.

- Click here to download the Physical lab manual.
- Click here to download the PT lab manual.
- Click here to download the PT source files.

Lab work will be graded primarily on timely, complete, and accurate submission. Late assignments will be penalized up to 20% of that assignment’s grade. Assignments turned in after graded work has been returned to the class will not be accepted for grading.

If you have ANY questions about what homework is assigned, please contact me immediately. If you wait until late in the week to ask homework questions this will not extend your homework due date. Always ask questions as early in the week as possible.

You must physically submit your physical lab work to me each week. Always keep a backup of your homework in your possession until I return your graded work back to you. This way if I don’t get your work, you can always resubmit your backup copy.

You must upload each completed Packet Tracer assignment into its specific drop box. The same due date/time applies to all homework assignments, except quizzes, which were described previously.

Please email me only at the address listed on this syllabus! I check this email address regularly and will promptly respond to email received. During the week, I will respond within one business day. For example, if you email me on Tuesday at 2pm, I will respond back to you by Wednesday at 2pm. If I don't respond within that time frame, an error occurred, meaning that I did not get your email. So, please forward your original email to me (again).

On weekends, I may or may not respond depending on my personal schedule. Do not rely on a weekend response to get your work done! For example, if you email me on Friday at 9am, I will respond back to you by Monday at 9am.
All of our course documents will be maintained on Angel. Download files to your USB drive and update these when you are informed of changes by your instructor.

**Course Policies:** If you have problems completing an assignment, it is your responsibility to contact your instructor to resolve the situation. The college has a zero tolerance policy (721.1 Academic Integrity) regarding all forms of academic dishonesty. Students caught (and/or involved in) copying—or any of the other noted violations of academic dishonesty—will receive a zero (0) on that assignment, project, or test. Continued violations of this policy may result in student suspension from classes. Note that this policy specifically addresses plagiarism as it applies to students at UCC. The policy on academic integrity is posted throughout the campus; please take the time to read it!

Students are responsible for material presented in lecture, assigned reading, activities, handouts, videos, required presentations, and class assignments. Any of these materials can and will be used by the instructor as the basis for test questions.

*The instructor retains the right to refuse non-health and/or family emergency excuses which appear to be avoidable or represent optional choices made by the student.*

UCC’s Student Services Web site URL is: [http://www.umpqua.edu/DisSvc/DisSvc1.htm](http://www.umpqua.edu/DisSvc/DisSvc1.htm)

**Communication:** Please keep the following guidelines in mind when you need help or otherwise want to talk with me:

- Only send me an e-mail if you have a quick question AND if that question is of a personal nature. You might want me to “unlock” your quiz or you might want me to make an appointment to visit me during my office hours or speak with me on the telephone. I do not want to handle ANY problems via e-mail.
- Voice mail - be clear and concise, speak slowly. Include the course reference number, your FULL name, and your telephone number.
- I will make it my duty to respond to any e-mail or voice mail questions or comments within 24 hours. However, I usually respond much faster.
- You can visit me during my office hours. I strongly recommend that you call me first to make a personal appointment since I have many students vying for my time. This way, you are guaranteed an appointment and that I haven’t stepped out for a meeting or other matter.

**Counseling Center:** Any student who feels he or she may need an accommodation for any type of disability, should make an appointment to see me during office hours or contact Disability Services in the Counseling Center.

Umpqua Community College Counseling Center provides comprehensive counseling services to assist you with career plans and academic advising as well as help to work out personal or social
problems. Counselors are available to both current and prospective students in the Campus Center.

The Counseling Center, Testing Center, Job Placement & the Transfer Opportunity Program are located in the Campus Center building across from UCC's Financial Aid Office. To contact our office you may stop by during business hours or call (541) 440-4610.

http://www.umpqua.edu/advising-and-career-service/992-counseling

**Tutoring Services:** Tutoring Services are available to UCC students. Contact information for UCC's tutoring center can be found at the following Web address:

http://www.umpqua.edu/current-students/tutoring-center
EIGRP – Back to the Future

Objectives
Implement advanced EIGRP features to enhance operation in a small- to medium-sized business network.

Scenario
Many of these bulleted concepts were mentioned in the previous chapter’s curriculum content and will be the focus of this chapter:

- Auto-summarization
- Load balancing
- Default routes
- Hold-down timers
- Authentication

With a partner, write 10 EIGRP review questions based on the previous chapter’s curriculum content. Three of the questions must focus on the bulleted items above. Ideally, Multiple Choice, True/False, or Fill in the Blank question types will be designed. As you design your questions, make sure you record the curriculum section and page numbers of the supporting content in case you need to refer back for answer verification.

Save your work and then meet with another group, or the entire class, and quiz them using the questions you developed.

Resources

- Word processing software program
- Curriculum content from the previous chapter
Tweaking EIGRP

Objectives
Implement advanced EIGRP features to enhance operation in a small- to medium-sized business network.

Scenario
The purpose of this activity is to review EIGRP routing protocol fine-tuning concepts.
You will work with a partner to design one EIGRP topology. This topology will be the basis for two parts of the activity. The first will use default settings for all configurations and the second will incorporate, at least, three of the following fine-tuning EIGRP options:

- Manual summary route
- Default routes
- Default routes propagation
- Hello interval timer settings

Refer to the labs, Packet Tracer activities, and interactive activities to help you as you progress through this modeling activity.

Directions are listed on the PDF file for this activity. Share your completed work with another group. You may wish to save a copy of this activity to a portfolio.

Resources
- Packet Tracer software or real network lab equipment
- Word processing program

Directions

Step 1: Design a WAN and LAN topology.

a. Use Packet Tracer to design a network with two routers (1941 model, suggested). If necessary, add NICs to the routers to provide connectivity to the routers to provide for, at least, two LANs for each router. Add, at least, one PC to each LAN.

b. Address the networks using either an IPv4 or IPv6 addressing scheme. VLSM may or may not be used per group discretion. If you use a full VLSM-addressed network, you will need to turn off auto-summarization from the beginning of your configuration design.

c. Configure the topology using basic EIGRP default settings.

d. Make sure all PCs can ping each other to prove connectivity. If not, work to make this so.

e. Save your work.

Step 2: Copy the topology.

a. Using your cursor, highlight the entire EIGRP-configured topology.

b. Press Ctrl+C to copy the highlighted topology.

c. Use Ctrl+V to paste a full copy of the topology to the Packet Tracer desktop. You will now have displayed two exact EIGRP-configured topologies. You will use the topology copy to tweak the network.

d. While highlighted, move the copied topology to a different location on the Packet Tracer desktop to create room between the two for configuration purposes.
Step 3: Configure fine-tuning features on the copied topology.

a. Choose three of the bulleted items from the Scenario section of this activity. Configure your changes on the copied topology. **Note:** By changing the Hello interval times, network instability may occur. You should be able to configure it; however, notice adjacencies status changing if you do choose this configuration option.

b. Save your work to avoid losing your configuration.

Step 4: Use verification commands to compare and contrast your default and fine-tuned configurations.

a. Use, at least, three output commands to compare and contrast the two topologies, and copy them to a word processing software program. For example, some useful commands include:

- `show ip route`
- `show running-configuration`
- `show ip protocols, show ip eigrp neighbors`

b. Share your work with another group. Explain how you changed the second topology from the first configured example. Justify what happened when you configured the three EIGRP fine-tuning options.
OSPF Troubleshooting Mastery

Objective
Explain the process and tools used to troubleshoot a single-area OSPF network.

Scenario
You have decided to change your routing protocol from RIPv2 to OSPFv2. Your small- to medium-sized business network topology will not change from its original physical settings. Use the diagram on the PDF for this activity as your company’s small- to medium- business network design.

Your addressing design is complete and you then configure your routers with IPv4 and VLSM. OSPF has been applied as the routing protocol. However, some routers are sharing routing information with each other and some are not.

Open the PDF file that accompanies this modeling activity and follow the directions to complete the activity. When the steps in the directions are complete, regroup as a class and compare recorded activity correction times. The group taking the shortest time to find and fix the configuration error will be declared the winner only after successfully explaining how they found the error, fixed it, and proved that the topology is now working.

Required Resources
- Topology diagram
- Packet Tracer software
- Timer
Choose a partner from the class with whom to work on this activity. Use Packet Tracer to create the topology diagram shown for this activity.

**Step 1:** Build the topology based on the modeling activity page for this scenario.

**Step 2:** Configure the routers.
   a. Use IPv4 for all interfaces.
   b. Incorporate VLSM into the addressing scheme.
   c. Make one intentional configuration error.
   d. Verify that the network does not work based upon the intentional error.
   e. Save your file to be used with Step 3.

**Step 3:** Exchange your Packet Tracer file with another group.
   a. Find the configuration error on the Packet Tracer network file you received from another group.
   b. Fix the OSPF configuration error so that the network operates fully.
   c. Record the time it took to find and fix the OSPF network error. _____________________
   d. When complete, meet with your class to determine the Master Troubleshooter for the day.
Portfolio RIP and EIGRP

Objectives
Configure EIGRP for IPv4 in a small routed network (review).

Scenario
You are preparing a portfolio file for comparison of RIP and EIGRP routing protocols.
Think of a network with three interconnected routers with each router providing a LAN for PCs, printers, and other end devices. The graphic on this page depicts one example of a topology like this.
In this modeling activity scenario, you will be creating, addressing and configuring a topology, using verification commands, and comparing/contrasting RIP and EIGRP routing protocol outputs.
Complete the PDF reflection questions. Save your work and be prepared to share your answers with the class. Also save a copy of this activity for later use within this course or for portfolio reference.

Resources
Packet Tracer and word processing software programs

Directions

Step 1: WAN and LAN topology design
a. Use Packet Tracer to design a network with three routers (1941 model, suggested). If necessary, add NIC cards to the routers to provide connectivity to the routers to provide for at least one LAN to each router. Add at least one PC to each LAN.
b. Address the networks. You may use a flat addressing scheme or VLSM. Use only IPv4 networks for this entire activity.

Step 2: Copy the topology
a. Highlight the entire topology by using your cursor.
b. Use Ctrl+C to make a copy of the highlighted topology.
c. Use Ctrl+V to insert a full copy of the topology to the desktop of Packet Tracer. You will now have displayed two exact, IPv4-addressed topologies with which to work for routing protocols configurations.
d. While highlighted, move the copied topology to a different location on the Packet Tracer desktop to create room between the two for configuration purposes.

Step 3: Configure RIP and EIGRP on the separate topologies.
  a. Configure the RIP routing protocol on the first topology and EIGRP on the second routing topology.
  b. Once you have successfully configured RIP on one topology and EIGRP on the other, check to make sure your PCs can ping each other.
  c. Save your work so no configuration information is lost.

Step 4: Use verification commands to check output for the routing protocols.
  a. To compare/contrast routing protocol information from the two topologies, issue the `show ip route` command on R1 for topology 1 and 2.
b. Copy the output into a table in your word processing program file. Label each column with RIP or EIGRP and place the output you received from the `show ip route` command.

c. Issue the `show ip protocols` command on R1 for topology table 1 and 2. Create another table in your word processing software file and place the output information below RIP or EIGRP.

d. Issue the `show cdp neighbors` command on R1’s topology 1. Copy the output to a third table with RIP as the heading and issue the `show ip eigrp neighbors` command on R1’s topology 2. Copy the output from this command in column 2 of table 3 under the heading EIGRP.

Reflection

1. Compare and contrast the output for the `show ip route` verification command.

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________

2. Compare and contrast the output for the `show ip protocol` verification command.

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________

3. Compare and contrast the `show cdp neighbors` command for the RIP topology and the `show ip eigrp neighbors` command for the EIGRP topology.

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________

4. After comparing and contrasting the RIP and EIGRP output, which do you find most informative? Support your answer.

_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________
Documentation Tree

Objective
Identify common STP configuration issues.

Scenario
The employees in your building are having difficulty accessing a web server on the network. You look for the network documentation that the previous network engineer used before he transitioned to a new job; however, you cannot find any network documentation whatsoever. Therefore, you decide to create your own network recordkeeping system. You decide to start at the access layer of your network hierarchy. This is where redundant switches are located, as well as the company servers, printers, and local hosts.

You create a matrix to record your documentation and include access layer switches on the list. You also decide to document switch names, ports in use, cabling connections, and root ports, designated ports, and alternate ports.

For more detailed instructions on how to design your model, use the student PDF that accompanies this activity.

Resources
- Packet Tracer software
- Word processing software

Directions

Step 1: Create the topology diagram with three redundant switches.

Step 2: Connect host devices to the switches.

Step 3: Create the switch documentation matrix.
  a. Name and switch location
  b. General switch description
  c. Model, IOS version, and image name
  d. Switch serial number
  e. MAC address
  f. Ports currently in use
  g. Cable connections
  h. Root ports
  i. Designated ports, status, and cost
  j. Alternate ports, status, and cost
Step 4: Use show commands to locate Layer 2 switch information.

a. show version
b. show cdp neighbors detail
c. show spanning-tree
Powerful Protocols

Objective
A review of EIGRP and OSPF routing protocol configuration and verification commands.

Scenario
At the end of this course, you are asked to complete two Capstone Projects where you will create, configure, and verify two network topologies using the two main routing protocols taught in this course, EIGRP and OSPF.

To make things easier, you decide to create a chart of configuration and verification commands to use for these two design projects. To help devise the protocol charts, ask another student in the class to help you.

Refer to the PDF for this chapter for directions on how to create a design for this modeling project. When complete, share your work with another group or with the class. You may also want to save the files created for this project in a network portfolio for future reference.

Resources
- Previous curriculum chapter content for EIGRP and OSPF
- Word processing software

Directions

Step 1: Create a matrix for each routing protocol (EIGRP and OSPF).

a. Within each routing protocol matrix, design two sections.
   1) one section for configuration commands
   2) one section for verification or show commands

b. Use a word processing program to save your matrix designs, or in the space provided below, one for EIGRP and one for OSPF.

Step 2: Review the chapters in this curriculum.

a. Refer to the different sections and activities presented in the curriculum.
   1) Content
   2) Labs
   3) Packet Tracer Activities

b. Record configuration commands for each protocol on their respective matrix. Note: Some commands are universal, and some are used only for IPv4 or IPv6.

c. Record verification commands used for each protocol on their respective matrix. Note: Some of these commands are universal, and some are used only with IPv4 or IPv6.

d. Leave extra, blank rows for the group or classroom portion of this activity.

Step 3: Meet as a class or with another group.

a. Compare configuration commands.

b. Compare verification commands.
Powerful Protocols

c. Add any commands to each matrix mentioned in the full- or group-setting that you did not record in your own group.

d. Save your work for use with the two Capstone projects which summarize this entire course.
CCNA 3: Intermediate LANs & Routing

Unit 01: Troubleshooting Basic LANs & Routing
Troubleshooting Basic LANs & Routing
Learning Objectives

• Explain the ICMP and identify its role as a messaging protocol
• Differentiate between the ping and trace route utilities
• Use OS utilities to identify L2 & L3 issues
• Use OS and IOS utilities to reveal host configurations
• Use basic subnetting & VLSM techniques to identify a host’s network
• Explain how DHCP & DNS work together and separately to facilitate locating network resources
What is a Message Protocol?

• TCP a transmission protocol
  • Transmit Control Protocol transmits data between hosts
• UDP also a transmission protocol
  • Just not as reliable as TCP
• Internet Control Message Protocol
  • Not a transmit (TCP/UDP) protocol
  • Part of IP protocol suite
  • Used to query for data and reply to IP/ICMP events
Base ICMP Utilities

• Ping – sends packet to remote host requesting a reply
• Pathping – traces path from source of ping to remote destination
• Trace route – same as Pathping, but with many more details
Generic ICMP Info

- Utilities ask one or more hosts to reply
- “Ask” means echo request
  - “Echo” means to visibly place reply as output on display
- “Reply” means echo reply
- Timing always in milliseconds
  - 1 Millisecond = 1/1,000 second
- Many ICMP reply types
- ICMP header contains ICMP data
ICMP Header Fields

- **Type**
  - ICMP type
- **Code**
  - Sub-type to ICMP Type
- **Checksum**
  - Error checking data
- **Rest of Header**
  - Varies based on the ICMP type and code
Well-Known ICMP Types

- **Type 0:**
  - Echo reply response from remote host in reply to echo request

- **Type 3:**
  - Destination unreachable response from last host able to process ICMP request

- **Type 8:**
  - Echo request sent to remote host

- **Type 11:**
  - Time exceeded
ICMP Sub-Types

• Type 3: Destination Unreachable ICMP Type
• 15 Sub-types to Type 3 reply:
  • Code 0: destination network unreachable
  • Code 1: destination host unreachable
  • Code 2: destination protocol unreachable
  • Code 3: destination port unreachable
  • Code 6: destination network unknown
  • Code 7: destination host unknown
  • Many others!
ICMP Sub-Types (cont’d)

- Type 11: Time Exceeded ICMP Type
- 2 Sub-types to Type 3 reply:
  - Code 0: TTL expired in transit
  - Code 1: fragment reassembly time exceeded
What is TTL (Time To Live)?

- IP packet field
  - Value varies by OS &/or technology
- TTL in format of allowable hops or maximum lifetime timestamp
  - If either exceeded, packet or frame dropped
  - Ensures packet or frame not forwarded forever
  - Defines infinity
- Each L3 host in path reduces (decrements) hop or checks timestamp
  - If hops = 0 or timestamp older than now – DROPPED!
Wireshark: TTL In Action

Ping www.yahoo.com

DNS query to resolve name to IP address

MAC address

TTL of 128 ms

DNS query from host uses UDP

Source/Destination IP addresses
ICMP Utility: Ping by IP

- Available on all Cisco devices & most OS
- Pings last host in path to destination
-Reports time to destination host as round trip in milliseconds

```bash
C:\>ping 206.190.36.105

Pinging 206.190.36.105 with 32 bytes of data:
Reply from 206.190.36.105: bytes=32 time=34ms TTL=50
Reply from 206.190.36.105: bytes=32 time=32ms TTL=50
Reply from 206.190.36.105: bytes=32 time=38ms TTL=50
Reply from 206.190.36.105: bytes=32 time=40ms TTL=50

Ping statistics for 206.190.36.105:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
     Minimum = 32ms, Maximum = 40ms, Average = 36ms
```
ICMP Utility: Ping by Name

• Same result as pinging by name
• Host must first resolve name to IP
  • Proves DNS is working
  • ICMP utilities can use name or IP of host!
ICMP Utility: Ping Options


Options:
- **-t**
  - Ping the specified host until stopped.
  - To see statistics and continue - type control-Break;
  - To stop - type control-C.
- **-a**
  - Resolve addresses to hostnames.
- **-n count**
  - Number of echo requests to send.
- **-l size**
  - Send buffer size.
- **-f**
  - Set Don’t Fragment flag in packet (IPv4-only).
- **-i TTL**
  - Time To Live.
- **-v TOS**
  - Type of Service (IPv4-only. This setting has been deprecated and has no effect on the type of service field in the IP Header).
- **-r count**
  - Record route for count hops (IPv4-only).
- **-s count**
  - Timestamp for count hops (IPv4-only).
- **-j host-list**
  - Loose source route along host-list (IPv4-only).
- **-k host-list**
  - Strict source route along host-list (IPv4-only).
- **-w timeout**
  - Timeout in milliseconds to wait for each reply.
- **-R**
  - Use routing header to test reverse route also (IPv6-only).
- **-S srcaddr**
  - Source address to use.
- **-4**
- **-6**

Example:
```
c:\> ping www.yahoo.com -n 10 -i 90
```

Ping statistics for 206.190.36.45:
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
Minimum = 36ms, Maximum = 110ms, Average = 52ms
ICMP Utility: Trace Route

- Available on all Cisco devices & most OS
- Pings each L3 host in path to destination
- Reports time to each host as round trip in milliseconds

```
c:\>tracert www.yahoo.com
Tracing route to ds-any-fp3-real.wa1.b.yahoo.com [206.190.36.45]  
over a maximum of 30 hops:
1     7 ms  9 ms  9 ms 192.168.1.1
2    20 ms 19 ms 20 ms 10.101.56.1
3    15 ms 19 ms 22 ms dtr01rsbgor-tge-0-0-0-2.rsbg.or.charter.com [96.34.105.80]
4    28 ms 16 ms 25 ms dtr01grpsor-tge-0-1-0-1.grpe.or.charter.com [96.34.105.213]
5    20 ms 29 ms 29 ms dtr03mrdor-bue-1.mrdor.or.charter.com [96.34.104.164]
6    29 ms 23 ms 25 ms bbr01mrdor-bue-3.mrdor.or.charter.com [96.34.104.34]
7    38 ms 39 ms 39 ms bbr02sttlwa-bue-4.sttl.wa.charter.com [96.34.0.56]
8    28 ms 33 ms 40 ms prr01sttlwa-bue-2.sttl.wa.charter.com [96.34.3.39]
9    31 ms 49 ms 39 ms pat2.swt.yahoo.com [198.32.134.35]
10    33 ms 39 ms 29 ms ae-2.pat1.ggp.yahoo.com [216.115.101.111]
11    38 ms 40 ms 29 ms ae-1.msr2.gq1.yahoo.com [66.196.67.3]
12  137 ms 37 ms 32 ms x4-8-0-0.ctr1-a-gdc.gq1.yahoo.com [68.180.253.131]
13    39 ms 39 ms 39 ms et-17-1.fab3-1-gdc.gq1.yahoo.com [98.137.31.172]
14    31 ms 39 ms 34 ms po-11.bas2-7-prd.gq1.yahoo.com [206.190.32.33]
15    50 ms 39 ms 119 ms tr1.fp.vip.gq1.yahoo.com [206.190.36.45]
Trace complete.
```
ICMP Utility: Traceroute (cont’d)

- Not all intermediate hosts send echo replies
- Destination times out when host refuses to reply
  - Why does this occur?

```
c:\>tracert www.google.com
Tracing route to www.google.com [74.125.141.147] 
over a maximum of 30 hops:

1     6 ms   11 ms  5 ms  192.168.1.1
2    12 ms   19 ms  31 ms  10.101.56.1
3    20 ms   29 ms  19 ms  dtr01rsbgor-tge-0-0-0-2.rsbg.or.charter.com [96.34.105.80]
4    18 ms  19 ms  29 ms  dtr01grpsor-tge-0-1-0-1.grps.or.charter.com [96.34.105.213]
5    18 ms  19 ms  29 ms  dtr03mdfdo-com-four-1.mdff.rd.charter.com [96.34.104.164]
6    18 ms  25 ms  39 ms  bbr01mdfdo-bue-3.mdff.or.charter.com [96.34.104.34]
7    23 ms  40 ms  40 ms  bbr02mdfdo-bue-4.mdff.or.charter.com [96.34.0.56]
8    22 ms  39 ms  29 ms  prr01mdfdo-bue-2.mdff.or.charter.com [96.34.3.39]
9    33 ms   26 ms  24 ms  72.14.195.46
10   53 ms   89 ms  43 ms  66.249.94.214
11   22 ms   39 ms  39 ms  66.249.94.197
12   48 ms  41 ms  37 ms  216.239.46.208
13   34 ms  38 ms  41 ms  64.233.174.126
14 * Request timed out.
15  41 ms  37 ms  32 ms  da-in-f147.1e100.net [74.125.141.147]
Trace complete.
c:\>
```
ICMP Utility: Traceroute Options

- Use similar to ping options
ICMP Utility: Pathping

- Available in host OS but not Cisco IOS
- Pings each L3 host in path to destination
- Reports time to each host as round trip in milliseconds
ICMP Utility: Pathping Options

- Use similar to ping options
What Was That All About?

- ICMP tools useful in solving common reachability problems
- Example: PC1 unable to open file on File Server
- How would you solve this?
Ask Questions & Think!

• Host connecting to server by name or IP address?
  • Can you ping the server by IP address and name?
  • Ping by IP proves that addressing works
  • Ping by name proves that DNS works

• Can host ping its default gateway?
  • Host & gateway must be in same subnet
  • Best if both have same mask

• Can default gateway ping the server
  • As before, ping by IP and name
Ping IP – Can’t Ping Name

• Proves that DHCP or manual assignment functioning properly
• Need to investigate DNS for more data
  • Data in DNS A record is wrong?
    – Name and/or IP address entered incorrectly
  • No A record exists for the server?
  • Server & host in different subnets?
Ping Name – Can’t Ping IP

• Proves that DNS **may be** functioning properly
  • Maybe not too!
• Need to investigate further
  • Reply might be coming from host other than server
Host Configuration

- Is each host configured properly?
Host Configuration (cont’d)

- Other methods to obtain data:
  - `ipconfig`
  - Host address
  - Host mask
  - Default gateway
  - `ipconfig /all`
  - All of the above
  - Host name
  - MAC address
Is Router Configured Properly?

- Matches host subnet?
Ping Via Router

- Ping host using router interface that is not the host’s default gateway

```
Router2#ping
Protocol [ip]:
Target IP address: 192.168.100.20
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.250.1

[some command options omitted]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.20, timeout is 2 seconds:
Packet sent with a source address of 192.168.250.1
U.U.U
Success rate is 0 percent (0/5)

Router2#
```
Other Considerations

• Switch port set for access?
• Switchport in correct VLAN?
• ACL blocking the traffic?
  • Outgoing traffic can be blocked -- and/or --
  • Incoming traffic can be blocked
• Host & default gateway have different masks?
• If host does not have DHCP addressing, is DHCP server up & running
  • Is DHCP server connected to same router interface?
  • Do other hosts in same subnet have issues?
Other Considerations (cont’d)

• ROAS caused issues?
  • DHCP server on different subinterface?
• Does router have path to destination?

```
Router2#show ip route 192.168.150.1
% Network not in table
Router2#

Router2#show ip route 192.168.1.1
Routing entry for 192.168.1.0/24
Known via "eigrp 100", distance 90, metric 2707456, type internal
  Redirecting via eigrp 100
Last update from 192.168.10.5 on Serial0/0, 00:02:12 ago
Routing Descriptor Blocks:
  * 192.168.10.5, from 192.168.10.5, 00:02:12 ago, via Serial0/0
    Route metric is 2707456, traffic share count is 1
    Total delay is 41000 microseconds, minimum bandwidth is 1544 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 2
Router2#
```
Subnetting vs. VLSM

- Any problems here?

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Network Address</th>
<th>Mask</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet 1</td>
<td>192.168.10.0</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>Host 1</td>
<td>192.168.10.100</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>Subnet 2</td>
<td>192.168.10.64</td>
<td>255.255.255.192</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>Host 1</td>
<td>192.168.10.62</td>
<td>255.255.255.192</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>Host 2</td>
<td>192.168.10.63</td>
<td>255.255.255.240</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>Subnet 3</td>
<td>10.0.0.128</td>
<td>255.255.255.128</td>
<td>10.0.0.129</td>
</tr>
<tr>
<td>Host 1</td>
<td>10.0.0.162</td>
<td>255.255.255.128</td>
<td>10.0.0.1</td>
</tr>
</tbody>
</table>
Troubleshooting Basic LANs & Routing
Summary – Unit 01

• Explain the ICMP and identify its role as a messaging protocol
• Differentiate between the ping and trace route utilities
• Use OS utilities to identify L2 & L3 issues
• Use OS and IOS utilities to reveal host configurations
• Use basic subnetting & VLSM techniques to identify a host’s network
• Explain how DHCP & DNS work together and separately to facilitate locating network resources
Troubleshooting Basic LANs & Routing

References – Unit 01

References

CCNA 3: Intermediate LANs & Routing

Unit 02: 02
Building Scalable Networks
Building Scalable Networks

Learning Objectives

• Explain the need for redundancy in a modern network and the STP
• Describe and explain IEEE 802.1D operations in a switched network
• Differentiate between PVST, PVST+, and RPVST, explaining the operations and use of each
• Configure PVST+ and RPVST on a Cisco switch
• Identify and troubleshoot common STP configuration and operations issues
• Explain the need for, varieties of, and operations of first hop redundancy protocols such as GLBP and HSRP
• Use the Cisco CLI to troubleshoot and verify STP, GLBP, and HSRP
No Redundancy

- Network has no redundant links
- Subject to single failure
- Loss of connectivity & productivity
Full Redundancy

- Network has redundant links
- Single failure will not disrupt network traffic
- Adds potential for L2 traffic looping
Spanning Tree Protocol

• STP guarantees loop-free topology in switched network
• Implements IEEE 802.1D (ca. 1990) algorithm
• Creates logical spanning tree & disables redundant links between L2 devices
  • Disabled ports are amber on switch face
• Enables disabled ports dynamically when primary path fails
• Prevents frames from being forwarded in perpetuity
STP At Work

- PC1 pings PC3
- PC1’s switch records PC1’s MAC & port
- Switch forwards ping to its primary Distribution switch

**KEY:**
- Primary connections represented by solid lines
- Redundant connections represented by dotted lines
STP At Work (cont’d)

- Primary Distribution switch forward ping to its primary Core switch
- Primary Core switch forwards ping to PC3’s primary Distribution switch
- Primary Distribution switch forwards ping to PC3’s primary Access switch
- Access switch forwards ping to PC3
STP At Work (cont’d)

• Without STP PC1’s primary Access switch forwards ping to both Distribution switches.
• Each Distribution switch forwards traffic to same Core switch.
• Core switch believes it has two paths to PC3.
• Creates mess for broadcast & multicast traffic!
STP Eliminates L2 Loops

- Ensures only one logical path between all destinations by dynamically blocking redundant paths (ports)
- Port considered blocked when switch does not permit traffic to enter/exit port
- If redundant port is needed, STP recalculates spanning tree paths & unblocks port(s) to keep network communication moving
STP Key Terms

• Bridge – vintage name for today’s switch
• STA – spanning tree algorithm
• Root bridge – control point switch used to determine paths to/from all destinations
• Root port – port on non-root bridge offering shortest path to root bridge
• Designated port – port permitted to forward traffic
  • All ports on root bridge are designated ports
STP Key Terms (cont’d)

• Port Roles determined by STA
• Port roles based on relationship to root bridge
  • Root port – port on any non-root bridge offering shortest path to Root bridge
    – Each switch will have only one root port
  • Designated port – non-root port(s) permitted to forward traffic
    – Each switch may have > 1 Designated port
  • Non-Designated port – port not permitted to forward traffic
    – Each switch may have > 1 Non-Designated port
STP Root Port

- Root Port selected by STA based on port cost
- Root bridge has no Root ports
STP Designated Port

- All ports on root bridge are Designated ports
  - (Not shown in graphic to conserve space!)
- Port allowed to forward traffic
STP Non-Designated Port

- Port is not allowed to forward traffic
STP Port/Bridge States

• Disabled
  • Port not UP/UP and ignored by STA
  • Port does not forward frames
• Listening for & processing BPDUs
  • Not forwarding frames via any port
  • Lasts approx. 15 seconds
• Learning MAC addresses and populating MAC address table
  • Not forwarding frames via any port
  • Lasts approx. 15 seconds
STP Port/Bridge States (cont’d)

• Forwarding:
  • All ports on Root switch are always set to forwarding state
  • Port can forward traffic onto network
  • Examples: Designated & Root ports

• Blocking:
  • Port stopped by STA from forwarding frames onto network
  • Takes approx. 20 seconds to block ports
  • Examples: Non-Designated ports
Switch STP Messaging

• STA uses fields in STP message between switches called BPDU
  • BPDU = Bridge Protocol Data Unit
  • BPDU encapsulated inside L2 frame
  • BPDU sent out every 2 seconds
• BPDU contains 12 fields
• Key fields are:
  • Root [Bridge] ID
  • [Sending] Bridge ID
  • [Sending] Bridge Root Cost
  • Timing values for BPDU communications
Key Bridge Data

• Each bridge possess two key pieces of information necessary to elect and identify the Root bridge:
  • Two-part Bridge ID
    – Part I: Bridge Priority Number
    – Part II: MAC address of management VLAN
    – Example: 32768:00-cd-ef-01-c4-b5
  • Part I default value set to 32,769
    – Lower priority number than default increases election chances!
    – Should rig election by manually altering this value
    – (Example shown later)
Key Bridge Data (cont’d)

- Part II MAC address value matters too:
  - Lower MAC address number breaks tie when priority values create a tie
- Convert MAC address from HEX -> Binary -> Decimal to determine MAC address numerical value

<table>
<thead>
<tr>
<th>Base Bridge Priority ID</th>
<th>Extended Bridge Priority ID</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>(4 bits)</td>
<td>(12 bits)</td>
<td>(48 bits)</td>
</tr>
</tbody>
</table>

TOTAL = 64 bits or 8 Bytes
Electing the Root Bridge

• At boot, bridges send Hello BPDUs out all UP/UP interfaces

• STA elects bridge based on Priority ID & MAC address calculation

• Non-root bridges determine Root, Designated, and Non-Designated ports
  • Based on accumulated path cost from Non-root bridge to Root bridge
    – 100 Mbps port - default path cost of 19
    – 1 Gbps port – default path cost of 4
    – 10 Gbps port – default path cost of 2
Some STP Revisions

- STP – original 1990 (802.1D) standard, discussed so far
  - Supports max. of one STP instance for entire LAN, regardless of number of VLANs
- RSTP – Rapid STP
  - Replaces 802.1D standard & replaces it with 802.1w
  - Reduces convergence time from ~ 50 seconds to ~ 6 seconds
- PVST+ – Cisco proprietary and allows STP instance per VLAN
PVST+ Key Elements

• Default STP mode for Cisco Catalyst switch
• Slower switch convergence than industry-standard RSTP
• Allows STP instance to run in each VLAN
  • Reduces size of spanning tree
• Default values (some, not all):
  • Defaults to VLAN 1
  • Priority default of 32,768
  • Same port costs as STP
PVST+ Graphic

- All switches connected via 802.1Q trunks
PVST+ Configurations

- SW1 set as root bridge
- SW2 priority number change
- SW3 set as secondary root bridge
- SW4 not altered
Verify Configurations

- Privileged mode `show` commands:

```
Switch#show spanning-tree ?
  active Report on active interfaces only
detail Detailed information
inconsistports Show inconsistent ports
interface Spanning Tree interface status and configuration
summary Summary of port states
vlan VLAN Switch Spanning Trees
<cr>
Switch#show spanning-tree
```

```
Switch>en
Switch#sh spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID  Priority 32769
Address 03d4.F765.1234
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 03d4.F765.1234
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/4</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.4</td>
<td>P2p</td>
</tr>
<tr>
<td>Fa0/2</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.2</td>
<td>P2p</td>
</tr>
<tr>
<td>Fa0/3</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.3</td>
<td>P2p</td>
</tr>
<tr>
<td>Fa0/18</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.18</td>
<td>P2p</td>
</tr>
<tr>
<td>Fa0/1</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.1</td>
<td>P2p</td>
</tr>
<tr>
<td>Fa0/6</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.6</td>
<td>P2p</td>
</tr>
<tr>
<td>Fa0/11</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.11</td>
<td>P2p</td>
</tr>
</tbody>
</table>
```
Verify Configurations (cont’d)

- Privileged mode `show` commands
  - Can always use `show run` for help too!
Verify Configurations (cont’d)

• Privileged mode `show` commands:

```
Switch#sh spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree Protocol
Bridge Identifier has priority of 32768, sysid 1, 0123.234F.9876
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32769
Topology change flag not set, detected flag not set
Number of topology changes 0 last change occurred 00:00:00 ago
from FastEthernet0/1
Times:  hold 1, topology change 35, notification 2
       hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

Port 1 (FastEthernet0/1) of VLAN0001 is designated forwarding
Port path cost 19, Port priority 128, Port Identifier 128.1
Designated bridge has priority 32769, address 0123.234F.9876
Designated port id is 128.1, designated path cost 19
Timers: message age 16, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
[Output omitted to conserve space]
```
Global Config. Commands

• Global Configuration mode **settings** commands:

```
Switch(config)#spanning-tree ?
  mode   Spanning tree operating mode
  portfast   Spanning tree portfast options
  vlan   VLAN Switch Spanning Tree
Switch(config)#spanning-tree mode ?
  pvst   Per-Vlan spanning tree mode
  rapid-pvst   Per-Vlan rapid spanning tree mode
Switch(config)#spanning-tree
```
Setting: PORTFAST

- Port transitions from state of blocking to forwarding instantly
- Use when port connects end station to switch

```bash
Switch(config)#int fa0/1
Switch(config-if)#spanning-tree?
  bpduguard  Don't accept BPDUs on this interface
  guard     Change an interface's spanning tree guard mode
  link-type Specify a link type for spanning tree protocol use
  portfast Enable an interface to move directly to forwarding on link up
  vlan      VLAN Switch Spanning Tree
Switch(config-if)#spanning-tree portfast?
  disable  Disable portfast for this interface
  trunk    Enable portfast on the interface even in trunk mode
<cr>
Switch(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only have effect when the interface is in a non-trunking mode.
Switch(config-if)#
```
Setting: BPDUGUARD

• if a portfast port receives a BPDU, the port is set to an err-disable state
  • Must manually enable the port to enable it

• Global enable:
  • SW1(config)# spanning-tree portfast bpduguard default

• Interface specific enable:
  • SW1(config-if)# spanning-tree portfast bpduguard enable
Setting: ROOTGUARD

• Prevents a new switch from becoming the root
  • Guards current root from hostile takeover!
  • Enabled on ports that will never receive BPDUs from the root
• Enable on switches not the root bridge, on ports that are not root ports:
  • SW1(config-if)# spanning-tree guard root
There is One More Thing...

- Single link trunk failure forces STA to run
- EtherChannel trunk links to prevent STA from running when a single link fails
  - If one physical cable in the logical group fails, STA does not run
  - STP treats EtherChannel as one single unit
- If multiple links between switches are not EtherChannelled, redundant links blocked by STP
EtherChannel Configuration

• Simple configuration example
  • Assumes other switch configurations in place...

```
Switch1(config)# interface port-channel 1
Switch1(config-if)# exit
Switch1(config)# interface fa0/0
Switch1(config-if)# channel-group 1 mode on
Switch1(config-if)# exit
Switch1(config)# interface fa0/1
Switch1(config-if)# channel-group 1 mode on
Switch1(config-if)# exit
Switch1(config)# interface port-channel 1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk native vlan 20
```

```
Switch1# show running-config
Building configuration...
Current configuration : 4500 bytes

[Other output omitted to conserve space!]

interface Port-channel1
switchport trunk native vlan 20
switchport mode trunk
no ip address
flowcontrol send off

interface FastEthernet0/0
switchport trunk native vlan 20
switchport mode trunk
no ip address

interface FastEthernet0/1
switchport trunk native vlan 20
switchport mode trunk
no ip address
channel-group 1 mode on
```
Redundancy = Availability

- Hosts always configured with one default gateway
- When gateway not available, host loses connectivity beyond LAN
- Need dynamic solution that replaces unavailable gateway with replacement gateway
- FHRP – First Hop Redundancy Protocol
  - Family of protocols
  - Eliminates single point of default gateway failure
FHRP Options

- **VRRP** – Virtual Router Redundancy Protocol
  - IETF ratified
  - Virtualized team of routers

- **GLBP** – Gateway Load Balancing Protocol
  - Cisco proprietary

- **HSRP** – Hot Standby Router Protocol
  - Cisco proprietary
  - Permits primary & secondary default-gateway
    - Primary gateway is “active”
    - Secondary gateway is “on standby”
HSRP Operations

- PC1 unable to reach Internet via its default gateway (R1)
- HSRP acts to forward traffic to R2, which was on standby and ready to take over for R1
- Transparent to host
HSRP – Behind the Scenes

- Manually create group of two HSRP routers
- Virtual L2 & L3 address shared amongst all members of HSRP group
- Hosts forward traffic to virtual address
- Primary HSRP router responds as usual
- Standby HSRP router responds if Primary HSRP router fails
  - HSRP messages between the routers determine which router responds to host traffic
HSRP Configuration

• Basic HSRP configurations for R1 & R2
  • R1 set as primary router with lower priority
  • R2 set as standby router with higher priority

```
R1# config t
R1(config)# interface fa0/0
R1(config-if)# ip addr 10.1.1.254 255.255.255.0
R1(config-if)# standby 1 ip 10.1.1.1
R1(config-if)# standby 1 priority 100
R1(config-if)# no shut
R1(config-if)# end
```

```
R2# config t
R2(config)# interface fa0/1
R2(config-if)# ip addr 10.1.1.253 255.255.255.0
R2(config-if)# standby 1 ip 10.1.1.1
R2(config-if)# standby 1 priority 200
R2(config-if)# no shut
R2(config-if)# end
```
Verify your Work!

- Use show commands to verify and troubleshoot
  - Show running-config
  - Show standby [brief]
Building Scalable Networks
Summary – Unit 02

• Explain the need for redundancy in a modern network and the STP
• Describe and explain IEEE 802.1D operations in a switched network
• Differentiate between PVST, PVST+, and RPVST, explaining the operations and use of each
• Configure PVST+ and RPVST on a Cisco switch
• Identify and troubleshoot common STP configuration and operations issues
• Explain the need for, varieties of, and operations of first hop redundancy protocols such as GLBP and HSRP
• Use the Cisco CLI to troubleshoot and verify STP, GLBP, and HSRP
References


CIS154C Course Schedule:
Please see below for a week-by-week listing of this term's activities and homework.

Abbreviations used:
PT = Packet Tracer (latest version)
SG = Study Guide
PTSIC = PT Skills Integration Challenge

<table>
<thead>
<tr>
<th>Week</th>
<th>Topics</th>
<th>Chapter Readings</th>
<th>Labs &amp; Exams</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction to WANs</td>
<td>Chapter 1</td>
<td>PTSIC 1.5.1</td>
</tr>
<tr>
<td>2</td>
<td>Point-to-Point Protocol (PPP)</td>
<td>Chapter 2</td>
<td>Lab 2.5.1 (Basic PPP) and PTSIC 2.6.1</td>
</tr>
<tr>
<td>3</td>
<td>Frame Relay</td>
<td>Chapter 3</td>
<td>Lab 3.5.3 (Troubleshooting FR) and PTSIC 3.6.1</td>
</tr>
<tr>
<td>4</td>
<td>Network Security</td>
<td>Chapter 4</td>
<td>Lab 4.6.1 (Basic Security Config.) and PTSIC 4.7.1</td>
</tr>
<tr>
<td>5</td>
<td>Access Control Lists (ACLs)</td>
<td>Chapter 5</td>
<td>Any one extra lab after Chapter 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NOTE: you must look ahead and not submit a lab that is assigned later this term.</td>
</tr>
<tr>
<td>6</td>
<td>Access Control Lists (ACLs) Continued</td>
<td>Chapter 5</td>
<td>Lab 5.5.1 (Basic ACLs) and Lab 5.5.2 (ACLs Challenge)</td>
</tr>
<tr>
<td>7</td>
<td>Teleworker Services</td>
<td>Chapter 6</td>
<td>PTSIC 5.6.1, &amp; PTSIC 6.4.1</td>
</tr>
<tr>
<td>8</td>
<td>IP Addressing Services</td>
<td>Chapter 7</td>
<td>Lab 7.4.1 (Basic DHCP and NAT Config.)</td>
</tr>
<tr>
<td>9</td>
<td>IP Addressing Services Continued</td>
<td>Chapter 7</td>
<td>PTSIC 7.5.1 &amp; any extra lab after chapter 4</td>
</tr>
<tr>
<td></td>
<td>Network Troubleshooting</td>
<td>Chapter 8</td>
<td>Lab 8.3.7 (TS Role)</td>
</tr>
</tbody>
</table>
| 10 | Monday, June 10, TC 101  
     Time: 8 AM - 10 AM  
*Skills Exam and multiple-choice online exam  
    - Make appointment with instructor in week 9 | Play) or PTSIC 8.6.1 |
| 11 | Study Guide | Final Exams |

*Must take skills final exam on or before the online final exam date!
Syllabus

CIS 154C - Accessing the WAN (Cisco 4)
Spring 2013

Class Hours:        Lecture: M, T, W: 9:00 - 9:50 AM, TC101 and Lab: F 10:00-
11:50, TC101
Credits:                4
Instructor:           John Blackwood
Office:                 Tower #3
Office Hours:       See schedule posted in Angel (under Lessons link)
Phone:                 541-440-7686
Email:                john.blackwood@umpqua.edu

Cisco Networking Academy Link:
http://cisco.netacad.net/staticcontentassets/choice/multilogin.html

Course Description:
This is the fourth and final course in the UCC's offering of Cisco Networking Academy courses and continues to provide students with classroom and laboratory experience in current and emerging networking technology that will empower them to enter employment or further education and training in the rapidly evolving networking field.

Instruction, includes a review of local area network (LAN) switching, virtual LANs, LAN design, routing protocols, access control lists (ACLs), wide area networks (WANs), the open system interconnection (OSI) reference model, networking, point-to-point (PPP) protocols, frame relay, network address translation, and general network management. Particular emphasis is given to students being able to demonstrate the ability to apply information from Cisco 1 - 3 to a network and to be able to explain how and why a particular strategy is employed. In addition, students will prepare for the CCNA Exam.

Course Outcomes:
Upon completion of this course the student should be able to:

- Ability to differentiate between various WAN services including: LAPB, Frame Relay, LAPD, HDLC, PPP, and DDR.
- Ability to configure Frame Relay and subinterfaces.
- Ability to monitor Frame Relay operation.
- Ability to configure PPP on WAN.
- Explain how Access Control Lists (ACLs) are used to promote network security.
Differentiate between standard and extended ACLs.
Ability to configure standard and extended ACLs to implement network security.
Troubleshoot and solve ACL issues.
Connect to a router using Cisco's Secure Device Manager (SDM) HTML tool.
Install and use SDM to apply an auto security configuration to a router.
Configure DHCP on a router.
Explain Network Address Translation (NAT).
Explain Port Address Translation (PAT).
Differentiate between NAT and PAT, explaining how these technologies work together to reduce IP address use and deliver network security.
Configure a router for NAT and PAT.
Understand IPv6 concepts
Configure IPv6 on a router
Use Packet Tracer to build and test a robust network containing routers, switches, and end devices.
Use industry-accepted troubleshooting methodologies and tools to resolve router, switch, and end device connectivity issues.

Course Prerequisite(s):
To take this course you should:

- Previously have completed CIS 153 with a grade of C or better; or have instructor approval.

Required Text:
ISBN: 9781118217146
CCNA: Cisco Certified Network Associate Study Guide 7E (includes CD-ROM) with CCNA Review Guide (640-802) Set. Special pricing is available at the book store. Both books are required for this class. This is the same bundle you purchased in CIS 151C (Cisco 1).


Supplies:
At least one (1) 32 GB USB portable hard disk drive, and five (5) rewriteable DVDs.

Equipment:
It is intended that students will use UCC lab computers, routers, switches, and the Packet Tracer simulation software provided by Cisco. Please talk to your instructor prior to purchasing any hardware or software for this class.

Homework (AKA “Lab Work”):
Students should plan to spend an average of 10-12 hours per week working in class lecture, assigned materials and reading. Lab work will be graded primarily on timely, complete, and accurate completion. Late assignments will be penalized up to 20% of that assignment’s grade. **Assignments turned in after graded work has been returned to class will not be accepted for grading.**

Much of your homework will be completed using Cisco’s Packet Tracer (PT) simulation program. Your other homework will be done by working through your lab manual. Lab manual work revolves around expressing what you’ve learned in written format.

**Quizzes:**
There will be eight quizzes during the term. Quizzes are available through Cisco’s Networking Academy link (the link is near the top of this document). Quizzes are taken weekly, up to two times. The last (not highest) score is the one that counts.

**Grading & Points:**
Grades will be assigned based on the total points (pts) earned as follows; 90 to 100% = A, 80 to 89% = B, 70 to 79% = C, 60 to 69% = D, and less than 60% = F.
Points are distributed as follows:

<table>
<thead>
<tr>
<th>Description</th>
<th>Pts</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 lab assignments @ 8 pts. ea.</td>
<td>144</td>
<td>31.0%</td>
</tr>
<tr>
<td>8 quizzes @ 15 pts. ea.</td>
<td>120</td>
<td>25.9%</td>
</tr>
<tr>
<td>Skills final exam</td>
<td>75</td>
<td>16.2%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>125</td>
<td>26.9%</td>
</tr>
<tr>
<td>TOTAL POSSIBLE POINTS</td>
<td>464</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

It should be pointed out here that you are to select two additional labs to complete before the end of the term. You can select any lab not previously assigned beginning with Chapter 3. These two extra labs are included in the 18 lab assignments listed above.

**Course Outline:**
This outline is a plan for the term. It is subject to change should the need arise. Any such changes will be noted during assigned class or lab time. It is your responsibility to note changes in the syllabus schedule as presented in class or via Angel announcements during the term. Lab assignments are due by 1:15 PM on the Monday following each week’s assignment. For example, labs for Week 1 are due on or before 1:15 PM on Monday, April 8th, 2013. You are to submit printed lab work for grading, and you must place your lab manual in my mailbox as I won’t accept them in class (too many to carry!). I do not take responsibility for (real or imagined) lost labs! Always keep a backup of your homework in your possession until I return your graded work back to you.
Since you are assigned a lot of homework, this class will not include a midterm exam. The final exam will be comprehensive, will cover all chapters, and will be in our regular classroom as noted in the finals schedule.

Quizzes are to be taken weekly. For example the quiz for Chapter 1 must be completed no later than Monday, April 8th, 2013. The time that the quiz expires depends on exactly when I turn it on. You are responsible for logging into the Academy site and keeping track of quiz closure date/times. It is important to point out that while you can take each quiz twice, your last score will be the one that is recorded in the gradebook.

**Important note: All labs are due no later than Monday, June 10th, by 1:15 PM.**

**Lab Grading Rubric:**
Labs are to be completed in a professional manner. Network administrators must learn to write neatly and succinctly so that steps can be repeated and/or understood by others. Some governing bodies require documentation for auditing purposes. Please review the lab rubric posted in Angel under Lessons for details about how your work will be graded.

**Use of Online Components**
Angel will be used only to provide you access to class files, chapter quizzes (assessments), the final exam, and an online grade book.

In addition, we will utilize Cisco's Networking Academy site. Your chapter quizzes, simulation tools, student review material, and your final exam. Please see the URL near the top of this document for the link to the Academy.

The Angel Learning Management System is compliant with ADA standards.

**Course Policies**
If you have problems completing an assignment, it is your responsibility to contact me to resolve the situation. The college has a zero tolerance policy (721.1 Academic Integrity) regarding all forms of academic dishonesty. Students caught (and/or involved in) copying—or any of the other noted violations of academic dishonesty—will receive a zero (0) on that assignment, project, or test. Continued violations of this policy may result in student suspension from classes. Note that this policy specifically addresses plagiarism as it applies to students at UCC. The policy on academic integrity is posted throughout the campus; please take the time to read it!

Although it is not normal procedure—after corrected materials have been returned to class, late assignments may be accepted at the instructor’s discretion.

I will generally grade your homework each week. For example, week 1 homework will be graded some time during week 2. When your homework is graded, your instructor will send you
an email with comments on your work, when applicable, along with a grade for each assignment. Then, grades are posted in Angel later that same day.

Students are responsible for running weekly grade reports to verify that what is in the gradebook is correct. Gradebook entries may be challenged within one week after homework is graded except for grades issued for week 10 homework, which must be challenged no later than Thursday at noon of week 11 (finals week).

You may work at your own pace throughout this course. For example, you can complete the whole course in less than ten weeks if you have the time to do so. However, your instructor will grade homework and answer course material questions weekly. Therefore, if you ask a week 8 question in week 2, your instructor may defer answering that question until that answer benefits the entire class.

Students are responsible for material presented in lecture, flash presentations, assigned reading, activities, handouts, videos, required presentations, and class assignments. Any of these materials can and will be used by the instructor as the basis for test questions.

Since quizzes are taken through Cisco's Networking Academy site, quiz scores will be copied to Angel within one week after the quiz ceases to be available to students. Students are responsible for material presented in flash presentations, assigned readings, activities, handouts, videos, required presentations, and class assignments. Any of these materials can and will be used by the instructor as the basis for test questions.

Make up tests will only be given in two circumstances:

1) The student contacts the instructor with a valid excuse prior to the scheduled test. (Examples of valid excuses are documented health problems, emergency medical appointments, “special” family events, etc.).

2) There was a personal, family, or medical emergency at the time of the test that prevented contact with instructor. (Examples of valid excuses are car accidents, death in the immediate family, or serious injury just prior to the test.)

I retain the right to refuse non-health and/or family emergency excuses which appear to be avoidable or optional choices made by the student. The alternate test time will be set by me and will be offered at my convenience. Make-up options for pop quizzes or class activities will be extremely limited and at the instructor’s discretion.

**Student Notice**

UCC is committed to supporting all students. Any student who feels he or she may need an accommodation for any type of disability should make contact with the Disability Services
Office in the Advising and Career Service Center of the Campus Center Building.

If you plan to use academic accommodations for this course, please contact your instructor and the Disability Services Office as soon as possible to discuss your needs. Accommodations are not retroactive; they begin when the instructor receives the “Approved Academic Accommodations” letter.

To request academic accommodations for a disability, please contact a Disability Service Coordinator.

Phone (541) 440-7655 or (541) 440-4610 or Oregon Relay 1-800-735-2900.

Additional information may be found at the Disability Services web page at:  http://www.umpqua.edu/disability-services-home

New and returning students may access information at: http://www.umpqua.edu/your-first-term
Objectives

- Describe the general methods used to mitigate security threats to Enterprise networks
- Configure Basic Router Security
- Explain how to disable unused Cisco router network services and interfaces
- Explain how to use Cisco SDM
- Manage Cisco IOS devices
Why is Network Security Important

- Today’s hackers do not need much skill to use what are called ‘Script Kiddie’ hacker tools
How Attacks Occur

- The attacker's goal is to compromise a network target or an application running within a network. Many attackers use this seven-step process to gain information and state an attack.

- Step 1. Perform footprint analysis (reconnaissance). A company webpage can lead to information, such as the IP addresses of servers. From there, an attacker can build a picture of the security profile or "footprint" of the company.

- Step 2. Enumerate information. An attacker can expand on the footprint by monitoring network traffic with a packet sniffer such as Wireshark, finding information such as version numbers of FTP servers and mail servers. A cross-reference with vulnerability databases exposes the applications of the company to potential exploits (AKA doing the 'enum hack').

- Step 3. Manipulate users to gain access. Sometimes employees choose passwords that are easily crackable. In other instances, employees can be duped by talented attackers into giving up sensitive access-related information. (AKA Social Engineering)

- Step 4. Escalate privileges. After attackers gain basic access, they use their skills to increase their network privileges.

- Step 5. Gather additional passwords and secrets. With improved access privileges, attackers use their talents to gain access to well-guarded, sensitive information.

- Step 6. Install backdoors. Backdoors provide the attacker with a way to enter the system without being detected. The most common backdoor is an open listening TCP or UDP port.

- Step 7. Leverage the compromised system. After a system is compromised, an attacker uses it to stage attacks on other hosts in the network.
Open vs. Closed Networks

- The overall security challenge facing network administrators is balancing two important needs:
  - Keeping networks open to support evolving business requirements
  - Protecting private, personal, and strategic business information.

A change in access policy may be as simple as asking a network administrator to enable a service.

Depending on the company, a change could require an amendment to the enterprise security policy before the administrator is allowed to enable the service.

For example, a security policy could disallow the use of instant messaging (IM) services, but demand from employees may cause the company to change the policy.
Develop a Security Policy

- The **first step** any organization should take to protect its data and itself from a liability challenge is to develop a security policy.

ISO/IEC 27002 is intended to be a common basis and practical guideline for developing organizational security standards and effective security management practices.

The document consists of 12 sections:

- Risk assessment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

Common Security Threats

- When discussing network security, three common factors are vulnerability, threat, and attack.
  - There are three primary vulnerabilities or weaknesses:
    - Technological weaknesses
    - Configuration weaknesses
    - Security policy weaknesses

Technological weaknesses:
- TCP/IP protocol weakness
  - Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) and Internet Control Message Protocol (ICMP) are inherently insecure.
  - Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP), and Syn Floods are related to the inherently insecure structure upon which TCP was designed.

Operating system weakness
- Each operating system has security problems that must be addressed.
  - UNIX, Linux, Mac OS, Mac OS X, Windows NT, 9x, 2K, XP, and Vista.
  - They are documented in the Computer Emergency Response Team (CERT) archives at http://www.cert.org.

Network equipment weakness
- Various types of network equipment, such as routers, firewalls, and switches have security weaknesses that must be recognized and protected against. Their weaknesses include password protection, lack of authentication, routing protocols, and firewall holes.
Common Security Threats (cont’d)

- When discussing network security, three common factors are vulnerability, threat, and attack.
  - There are three primary vulnerabilities or weaknesses:
    - ✓ Technological weaknesses
    - ✓ Configuration weaknesses
    - ✓ Security policy weaknesses

<table>
<thead>
<tr>
<th>Configuration Weakness</th>
<th>How the weakness is exploited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsecured user accounts</td>
<td>User account information may be transmitted insecurely across the network, exposing usernames and passwords to snoopers.</td>
</tr>
<tr>
<td>System accounts with easily guessed passwords</td>
<td>This common problem is the result of poorly selected and easily guessed user passwords.</td>
</tr>
<tr>
<td>Misconfigured Internet services</td>
<td>A common problem is to turn on JavaScript in Web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites. IIS, FTP, and Terminal Services also pose problems.</td>
</tr>
<tr>
<td>Unsecured default settings within products</td>
<td>Many products have default settings that enable security holes.</td>
</tr>
<tr>
<td>Misconfigured network equipment</td>
<td>Misconfigurations of the equipment itself can cause significant security problems. For example, misconfigured access lists, routing protocols, or SNMP community strings can open up large security holes.</td>
</tr>
</tbody>
</table>
Common Security Threats (cont’d)

- When discussing network security, three common factors are vulnerability, threat, and attack.
  
  - There are three primary vulnerabilities or weaknesses:
    
    ✓ Technological weaknesses
    ✓ Configuration weaknesses
    ✓ Security policy weaknesses

<table>
<thead>
<tr>
<th>Policy Weakness</th>
<th>How the weakness is exploited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of written security policy</td>
<td>An unwritten policy cannot be consistently applied or enforced.</td>
</tr>
<tr>
<td>Politics</td>
<td>Political battles and turf wars can make it difficult to implement a consistent security policy.</td>
</tr>
<tr>
<td>Lack of authentication continuity</td>
<td>Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network.</td>
</tr>
<tr>
<td>Logical access controls not applied</td>
<td>Inadequate monitoring and auditing allow attacks and unauthorized use to continue, wasting company resources. This could result in legal action or termination against IT technicians, IT management or even company leadership that allows these unsafe conditions to persist.</td>
</tr>
<tr>
<td>Software and hardware installation and changes do not follow policy</td>
<td>Unauthorized changes to the network topology or installation of unapproved applications create security holes.</td>
</tr>
<tr>
<td>Disaster recovery plan is nonexistent</td>
<td>The lack of a disaster recovery plan allows chaos, panic, and confusion to occur when someone attacks the enterprise.</td>
</tr>
</tbody>
</table>
Common Security Threats (cont’d)

- Computer crimes can usually be grouped into four categories:

  **Unstructured** - inexperienced hackers using easily available hacking tools, such as shell scripts and password crackers.

  **Structured** - individuals or groups that are more highly motivated and technically competent.

  **External** - arise from individuals or organizations working outside of a company.

  **Internal** - someone has authorized access to the network with either an account or physical access.
Common Security Threats (cont’d)

- The easiest hack involves no computer skill at all…

**Phishing** is a type of social engineering attack that involves using e-mail or other types of messages in an attempt to trick others into providing sensitive information.

The figure is an email that I recently received, appearing to be from eBay.

Notice the email address from which this email originated?

I right-clicked the link to view it and saw this was not an eBay link.

After pasting the URL in IE, the Address Bar turned **RED** and this message appeared on the screen.

**YIKES!**
Types of Network Attacks

- **Reconnaissance** is the unauthorized discovery and mapping of systems, services, or vulnerabilities.

- **System access** is the ability for an intruder to gain access to a device for which the intruder does not have an account or a password.

- **Denial of service (DoS)** is when an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks are the most feared.

- **Malicious software** can be inserted onto a host to damage or corrupt a system, replicate itself, or deny access to networks, systems, or services. Common names for this type of software are worms, viruses, and Trojan horses.
## Types of Network Attacks

- **DoS attacks** are the most publicized form of attack and also among the most difficult to eliminate.

Because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators.

### A SYN flood

A **SYN flood** attack exploits the TCP three-way handshake. It involves sending multiple SYN requests (1,000+) to a targeted server.

The server replies with the usual SYN-ACK response, but the malicious host never responds with the final ACK to complete the handshake.

This ties up the server until it eventually runs out of resources and cannot respond to a valid host request.

### The Smurf attack

The **Smurf attack** uses spoofed broadcast ping messages to flood a target system. It starts with an attacker sending a large number of ICMP echo requests to the network broadcast address from valid spoofed source IP addresses.

A router could perform the Layer 3 broadcast-to-Layer 2 broadcast function, most hosts will each respond with an ICMP echo reply, multiplying the traffic by the number of hosts responding.

On a multi-access broadcast network, there could potentially be hundreds of machines replying to each echo packet.
General Mitigation Techniques

- Device Hardening is the process of applying specific settings and software to an object to protect it from attack

  It is critical to protect network hosts, such as workstation PCs and servers. These hosts need to be secured as they are added to the network, and should be updated with security patches as these updates become available.

Personal computers connected to the Internet through a dialup connection, DSL, or cable modems are as vulnerable as corporate networks.

**Personal firewalls:**
- Reside on the PC of the user and attempt to prevent attacks.
- Are not designed for LAN implementations, such as appliance-based or server-based firewalls.
- May prevent network access if installed with other networking clients, services, protocols, or adapters.

Some personal firewall software vendors include McAfee, Microsoft, Norton, Symantec, and Zone Labs.
General Mitigation Techniques (cont’d)

- Intrusion detection systems (IDS) detect attacks against a network and send logs to a management console
- Intrusion prevention systems (IPS) prevent attacks against the network
  
  IPS tries to stop attacks (prevention) and tries to immunize against future attacks (reaction)

**Cisco Security Agent (CSA)** is a security software agent that provides threat protection for server and desktop computing systems.

CSA agents can be managed by CiscoWorks VMS Management Center for Cisco Security Agents or can be standalone agents running on Cisco IP Communications application servers.

Standalone agents for Cisco IP Communications application servers must be manually installed on the IP Communications application server.
The Network Security Wheel

- Most security incidents occur because system administrators do not implement available countermeasures, and attackers or disgruntled employees exploit the oversight.

The Security Wheel promotes retesting and reapplying updated security measures on a continuous basis.

1. Secure the network by applying the security policy and implementing threat defense and packet filtering.
2. Monitoring security involves both active and passive methods of detecting security violations.
3. Test what you did in steps 1 and 2!
4. The improvement phase of the Security Wheel involves analyzing the data collected during the monitoring and testing phases.

With the information collected from the monitoring and testing phases, IDSs can be used to implement improvements to the security. The security policy should be adjusted as new security vulnerabilities and risks are discovered.
The Enterprise Security Policy

A security policy is a set of guidelines established to safeguard the network from attacks, both from inside and outside a company. Forming a policy starts with asking questions.

- How does the network help the organization achieve its vision, mission, and strategic plan?
- What implications do business requirements have on network security.
- How do those requirements get translated into the purchase of specialized equipment and the configurations loaded onto devices?

A security policy is a living document, meaning that the document is never finished and is continuously updated as technology and employee requirements change. It acts as a bridge between management objectives and specific security requirements.
Components of A Security Policy

- The following are general security policies that an organization may invoke:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement of authority and scope</td>
<td>This section specifies who sponsors the security policy and what areas the policy covers.</td>
</tr>
<tr>
<td>Acceptable Use Policy</td>
<td>This section specifies what technologies, equipment, or the combination of the two the company will and will not allow regarding its information infrastructure.</td>
</tr>
<tr>
<td>Identification and authentication policy</td>
<td>This section specifies only authorized individuals have access to its data.</td>
</tr>
<tr>
<td>Internet access policy</td>
<td>This section specifies what the company considers ethical and proper use of its Internet access capabilities.</td>
</tr>
<tr>
<td>Campus access policy</td>
<td>This section specifies how on-campus users will use the company data infrastructure.</td>
</tr>
<tr>
<td>Remote access policy</td>
<td>This section specifies how remote users will access the company's data infrastructure.</td>
</tr>
<tr>
<td>Incident handling procedure</td>
<td>This section specifies how the company will create an incident response team and the procedures it will use during and after incident occurs.</td>
</tr>
</tbody>
</table>
The Enterprise Security Policy

- Let’s do the 4.1.6.4 Activity 1

Solution on the next slide…
# The Enterprise Security Policy

## Activity 1 Solution!

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>____ is a general term that has historically been used to describe a computer programming expert.</td>
<td></td>
<td>Hacker</td>
</tr>
<tr>
<td>____ is generally regarded as the more accurate term to describe someone who tries to gain unauthorized access to network resources with malicious intent.</td>
<td></td>
<td>Cracker</td>
</tr>
<tr>
<td>____ is a term used to describe an individual that manipulates the phone network in order to cause it to perform a function that is normally not allowed.</td>
<td></td>
<td>Phreaker</td>
</tr>
<tr>
<td>____ is a term used to describe an individual that sends large quantities of unsolicited e-mail messages.</td>
<td></td>
<td>Spammer</td>
</tr>
<tr>
<td>____ is a term used to describe an individual that uses e-mail or other means in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords.</td>
<td></td>
<td>Phisher</td>
</tr>
<tr>
<td>____ is a term used to describe individuals that use their abilities to find vulnerabilities in systems or networks, and then report these vulnerabilities to the owners of the system so that they can be fixed.</td>
<td></td>
<td>White hat</td>
</tr>
<tr>
<td>____ is another term for individuals that use their knowledge of computer systems to break into systems or networks that they are not authorized to use.</td>
<td></td>
<td>Black hat</td>
</tr>
</tbody>
</table>
Router Security Issues

Because routers provide gateways to other networks, they are obvious targets, and are subject to a variety of attacks. Here are some examples of various security problems:

- Compromising the access control can expose network configuration details, thereby facilitating attacks against other network components.
- Compromising the route tables can reduce performance, deny network communication services, and expose sensitive data.
- Misconfiguring a router traffic filter can expose internal network components to scans and attacks, making it easier for attackers to avoid detection.

Note: This section focuses on securing routers. Most of the best practices discussed can also be used to secure switches.

However, this section does not cover Layer 2 threats, such as MAC address flooding attacks and STP attacks, because these are covered in CCNA Exploration: LAN Switching and Wireless.
Router Security Issues (cont’d)

- Securing routers at the network perimeter is an important first step in securing the network.

Think about router security in terms in these categories:

- Physical security
- Update the router IOS whenever advisable
- Backup the router configuration and IOS
- Harden the router to eliminate the potential abuse of unused ports and services

Provision the router with the maximum amount of memory possible.

Harden the router to make it as secure as possible. A router has many services enabled by default. Many of these services are unnecessary and may be used by an attacker for information gathering or exploitation. You should harden your router configuration by disabling unnecessary services.

Note: Slide 32 illustrates how to disable services
Securing Cisco Routers

Before you configure security features on a router, you need a plan for all the Cisco IOS security configuration steps:

- Step 1. Manage router security
- Step 2. Secure remote administrative access to routers
- Step 3. Logging router activity
- Step 4. Secure vulnerable router services and interfaces
- Step 5. Secure routing protocols
- Step 6. Control and filter network traffic
Manage Router Security

- Basic router security consists of configuring passwords. A strong password is the most fundamental element in controlling secure access to a router. For this reason, strong passwords should always be configured.

- A recommended method for creating strong complex passwords is to use passphrases.
  - A passphrase is basically a sentence or phrase that serves as a more secure password.
  - Make sure that the phrase is long enough to be hard to guess but easy to remember and type accurately.
Manage Router Security (cont’d)

- By default, Cisco IOS software leaves passwords in plain text when they are entered on a router. This is not secure!

Cisco recommends that Type 5 encryption be used instead of Type 7 whenever possible. MD5 encryption is a strong encryption method. It should be used whenever possible. It is configured by replacing the keyword password with secret.

The local database usernames should be also configured using the username username secret password global configuration command. For example:

```
R1(config)# username Student secret cisco
R1(config)# do show run | include username
username Student secret 5
$1$z245$IVSTJzuYgdQDJiacwP2Tv/
R1(config)#
```
Manage Router Security (cont’d)

- Cisco IOS Software Release 12.3(1) and later allow administrators to set the minimum character length for all router passwords:

  This command provides enhanced security access to the router by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as "lab" and "cisco."

  This command affects any new user passwords, enable passwords and secrets, and line passwords created after the command was executed.

  The command does not affect existing router passwords.
Securing Remote Administrative Access

Traditionally, remote administrative access on routers was configured using Telnet on TCP port 23.

Telnet was developed in the days when security was not an issue. For this reason, all Telnet traffic is forwarded in plain text.

SSH has replaced Telnet as the best practice for providing remote router administration with connections that support strong privacy and session integrity. SSH uses port TCP 22.

It provides functionality that is similar to that of an outbound Telnet connection, except that the connection is encrypted.

With authentication and encryption, SSH allows for secure communications over an insecure network.

Not all Cisco IOS images support SSH. Only cryptographic images can. Typically, these images have image IDs of k8 or k9 in their image names.

Image names are discussed in Section 5.
Configuring SSH Security

To enable SSH on the router, the following parameters must be configured:

- Hostname
- Domain name
- Asymmetrical keys
- Local authentication

**Disable Telnet: & enable SSH**

```plaintext
R2(config)# username student secret cisco
R2(config)# line vty 0 4
R2(config-line)# transport input ssh
R2(config-line)# login local
```

Generate asymmetric keys - create a key that the router uses to encrypt its SSH management traffic with the `crypto key generate rsa` command from configuration mode. The router responds with a message showing the naming convention for the keys.

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. As a best practice, Cisco recommends using a minimum modulus length of 1024.

A longer modulus takes longer to generate and to use, but it offers stronger security.
The Enterprise Security Policy

- Let’s do the 4.2.4.5 Activity

Solution on the next slide…
The Enterprise Security Policy

Activity Solution!

Step 1: Set Router Parameters
- `hostname R1`
- `ip domain-name cisco.com`
- `crypto key generate rsa`

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: Enter
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

*Sep 21 15:41:51.015: %SSH-5-ENABLED: SSH 1.5 has been enabled

Step 2: Generate Asymmetric Keys
- `ip ssh timeout 15`
- `ip ssh authentication-retries 2`
- `username student secret cisco`

Step 3: Configure SSH Timeouts and Username
- `line vty 0 4`
- `transport input ssh`
- `login local`

Step 4: Configure Local Authentication and vty
Vulnerable Router Services and Interfaces

- Cisco routers support a large number of network services as described in the figure:

Turning off an automatic network feature usually prevents a certain kind of network traffic from being processed by the router, or prevents it from traversing the router.

For example, **IP source routing** is a little-used feature of IP that can be utilized in network attacks. Unless it is required for the network to operate, IP source routing should be disabled.
Router Security Issues (cont’d)

- **Examples…**
  - Small services such as echo, discard, and chargen - Use the no service tcp-small-servers or no service udp-small-servers command.
  - BOOTP - Use the no ip bootp server command.
  - Finger - Use the no service finger command.
  - HTTP - Use the no ip http server command.
  - SNMP - Use the no snmp-server command.

It is also important to disable services that allow certain packets to pass through the router, send special packets, or are used for remote router configuration.

- Cisco Discovery Protocol (CDP) - Use the no cdp run command.
- Remote configuration - Use the no service config command.
- Source routing - Use the no ip source-route command.
- Classless routing - Use the no ip classless command.

The interfaces on the router can be made more secure by using certain commands in interface configuration mode:

- Unused interfaces - Use the shutdown command.
- No SMURF attacks - Use the no ip directed-broadcast command.
- Ad hoc routing - Use the no ip proxy-arp command.
Router Security Issues (cont’d)

- How to disable unnecessary services, enable SSH, and disable telnet:

```
Router(config)# no cdp run
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
Router(config)# no ip finger
Router(config)# no ip identd
Router(config)# no service finger
Router(config)# no ip source-route
Router(config)# no ftp-server enable
Router(config)# no ip http server
Router(config)# no ip http secure-server
Router(config)# no snmp-server community public RO
Router(config)# no snmp-server community private RW
Router(config)# no snmp-server enable traps
Router(config)# no snmp-server system-shutdown
Router(config)# no snmp-server trap-auth
Router(config)# no snmp-server
Router(config)# no ip domain-lookup
Router(config)# no ip bootp server
Router(config)# no service dhcp
Router(config)# no service pad
Router(config)# no boot network
Router(config)# no service config
Router(config)# interface ethernet 0
Router(config-if)# no ip proxy-arp
```

```
Router(config-if)# no ip directed-broadcast
Router(config-if)# no ip unreachable
Router(config-if)# no ip redirect
Router(config-if)# no ip mask-reply
Router(config-if)# exit
Router(config)# interface ethernet 1
Router(config-if)# no ip proxy-arp
Router(config-if)# no ip directed-broadcast
Router(config-if)# no ip unreachable
Router(config-if)# no ip redirect
Router(config-if)# no ip mask-reply
Router(config-if)# exit
Router(config)# service tcp-keepalives-in
Router(config)# service tcp-keepalives-out
Router(config)# username admin1 privilege 15 secret geekboy
Router(config)# hostname Bullmastiff
Bullmastiff(config)# ip domain-name quizware.com
Bullmastiff(config)# crypto key generate rsa
Bullmastiff(config)# line vty 0 4
Bullmastiff(config-line)# login local
Bullmastiff(config-line)# transport input ssh
Bullmastiff(config-line)# transport output ssh
```

Some services are turned on here to enhance security!
Vulnerable Router Services and Interfaces

- The figure describes three management services which should also be secured.
  - The methods for disabling or tuning the configurations for these services are beyond the scope of this course.
  - SNMP is the standard Internet protocol for automated remote monitoring and administration.
  - Cisco routers and other hosts use NTP to keep their time-of-day clocks accurate.
  - Cisco IOS software supports looking up hostnames with the Domain Name System (DNS).

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>Versions 1 and 2 pass management information and community strings (passwords) in clear text</td>
</tr>
<tr>
<td>NTP</td>
<td>NTP leaves listening ports open and vulnerable</td>
</tr>
<tr>
<td>DNS</td>
<td>Can help attackers connect IP addresses to domain names</td>
</tr>
</tbody>
</table>
Securing Routing Protocols

Routing protocol authentication should also be configured for other routing protocols such as EIGRP and OSPF:

Create a key chain to be used by all routers in your network.

Enable MD5 authentication in EIGRP packets traversing an interface.

The first command specifies the key that will be used for MD5 authentication.

The next command enables MD5 authentication.

```
R1(config)#key chain EIGRP_KEY
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco
R1(config-keychain-key)#exit
R1(config-keychain)#exit
R1(config)#interface s0/0/0
R1(config-if)#ip authentication mode eigrp 1 md5
R1(config-if)#ip authentication key-chain eigrp 1 EIGRP_KEY
```

```
R1(config)#interface s0/0/0
R1(config-if)#ip ospf message-digest-key 1 md5 cisco
R1(config-if)#ip ospf authentication message-digest
R1(config-if)#exit
R1(config)#router ospf 10
R1(config-router)#area 0 authentication message-digest
```
Packet Tracer Exploration:
Configuring OSPF Authentication

- This activity covers both OSPF simple authentication and OSPF MD5 (message digest 5) authentication.
- In this activity, you will configure simple authentication between R1 and R2, and MD5 authentication between R2 and R3.

Let’s do PT 4.3.2.4 (~10 min.)
Cisco AutoSecure

- Cisco AutoSecure uses a single command to disable non-essential system processes and services, eliminating potential security threats.

```
RING1#auto secure
Is this router connected to internet? [no]: y
Enter the number of interfaces facing internet [1]: 1
Enter the interface name that is facing internet: Serial0/1/0
Securing Management plane services..
Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
(output omitted)
```
Cisco SDM Overview

- The Cisco Router and Security Device Manager (SDM) is an easy-to-use, web-based device-management tool.

Cisco SDM supports a wide range of Cisco IOS software releases. It ships preinstalled by default on all new Cisco integrated services routers.

If it is not preinstalled, you will have to install it. The SDM files can be installed on the router, a PC, or on both. An advantage of installing SDM on the PC is that it saves router memory, and allows you to use SDM to manage other routers on the network.

If Cisco SDM is pre-installed on the router, Cisco recommends using Cisco SDM to perform the initial configuration.
To configure Cisco SDM on a router already in use, without disrupting network traffic, follow these steps:

Step 1. Access the router's Cisco CLI interface using Telnet or the console connection

Step 2. Enable the HTTP and HTTPS servers on the router

Step 3 Create a user account defined with privilege level 15 (enable privileges).

Step 4 Configure SSH and Telnet for local login and privilege level 15.

See the next slide for a CLI example!
How to Configure for Cisco SDM (cont’d)

- The screen output shows an example of the configuration needed to ensure you can install and run Cisco SDM on a production router without disrupting network traffic.

```plaintext
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# ip http authentication local
R1(config)# username Student privilege 15 secret cisco
R1(config)# line vty 0 4
R1(config-line)# privilege level 15
R1(config-line)# login local
R1(config-line)# transport input telnet ssh
R1(config-line)# exit
```
Starting Cisco SDM

- Cisco SDM is stored in the router flash memory. It can also be stored on a local PC.

To launch the Cisco SDM use the HTTPS protocol and put the IP address of the router into the browser.

The figure shows the browser with an address of https://198.162.20.1 and the launch page for Cisco SDM. The http:// prefix can be used if SSL is not available. When the username and password dialog box appears (not shown), enter a username and password for the privileged (privilege level 15) account on the router.

After the launch page appears a signed Cisco SDM Java applet appears which must remain open while Cisco SDM is running.

Because it is a signed Cisco SDM Java applet you may be prompted to accept a certificate. The certificate security alert appears in the bottom right of the figure.
Cisco SDM Home Page Overview

- After Cisco SDM has started and you have logged in, the first page displayed is the Overview page.

This page displays the router model, total amount of memory, the versions of flash, IOS, and SDM, the hardware installed, and a summary of some security features, such as firewall status and the number of active VPN connections.

Note: The menu bar, tool bar, and current mode are always displayed at the top of each screen. The other areas of the screen change based upon the mode and function you are performing.

Configuration overview - Summarizes the configuration settings. To view the running configuration, click the View Running Config button (see arrow to left).
Cisco SDM Wizards

- Cisco SDM provides a number of wizards to help you configure a Cisco ISR router.

Once a task is selected from the task area in the Cisco SDM GUI, the task pane allows you to select a wizard.

The figure shows various Cisco SDM GUI screens for the Basic NAT wizard.

NAT is discussed later in the IP Addressing Services sections course.
Explain How to Use Cisco SDM

The Cisco SDM one-step lockdown wizard implements almost all of the security configurations that Cisco AutoSecure offers.

The one-step lockdown wizard is accessed from the Configure GUI interface by clicking the Security Audit task.

The one-step lockdown wizard tests your router configuration for potential security problems and automatically makes any necessary configuration changes to correct any problems found.

Do not assume that the network is secure simply because you executed a one-step lockdown.

Not all the features of Cisco AutoSecure are implemented in Cisco SDM.
Manage Cisco IOS Devices

- The availability of the network can be at risk if a router configuration or operating system is compromised.

The figure displays the output of the show file systems command which lists all of the available file systems on a Cisco 1841 router.

This command provides insightful information such as the amount of available and free memory, the type of file system and its permissions. Permissions include read only (ro), write only (wo), and read and write (rw).

Although there are several file systems listed, of interest to us will be the tftp, flash and nvram file systems. The remainder of the file systems listed are beyond the scope of this course.

Network file systems include using FTP, trivial FTP (TFTP), or Remote Copy Protocol (RCP). This course focuses on TFTP.

Notice that the flash file system also has an asterisk preceding it which indicates that this is the current default file system.

Recall that the bootable IOS is located in flash, therefore the pound symbol (#) appended to the flash listing indicates that this is a bootable disk.
Manage Cisco IOS Devices (cont’d)

- This figure lists the content of the current default file system, which in this case is flash:

```
R1# dir

Directory of flash:/

1  -rw-    720  Sep 11 2007 15:59:54 +00:00  pre_autosec.cfg
2  -rw-   1821  Jul 11 2006 10:30:42 +00:00  sdmconfig-18xx.cfg
3  -rw-  4734464  Jul 11 2006 10:31:20 +00:00  sdm.tar
4  -rw-  833024  Jul 11 2006 10:31:44 +00:00  es.tar
5  -rw-  1052160  Jul 11 2006 10:32:14 +00:00  common.tar
6  -rw-   1038  Jul 11 2006 10:32:36 +00:00  home.shtml
7  -rw-  102400  Jul 11 2006 10:32:58 +00:00  home.tar
8  -rw-  491213  Jul 11 2006 10:33:20 +00:00  128MB.sdf
9  -rw-  1684577  Jul 11 2006 10:34:00 +00:00  securedesktop-ios-3.1.1.27-k9.pkg
10 -rw-  398305  Jul 11 2006 10:34:34 +00:00  sslclient-win-1.1.0.154.pkg
11 -rw- 22149320  Mar 28 2007 16:02:28 +00:00  cl841-advipservicesk9-mz.124-13a.bin

31932416 bytes total (462848 bytes free)
R1#
```

There are several files located in flash, but of specific interest is the last listing.

This last file is the file image name of the current IOS running in RAM.
Manage Cisco IOS Devices (cont’d)

- To view the contents of NVRAM, you must change the current default file system using the `cd` (change directory) command.

  The `pwd` present working directory command verifies that we are located in the NVRAM directory.

  Finally, the `dir` command lists the contents of NVRAM.

  Although there are several configuration files listed, of specific interest to us is the startup-configuration file.
Manage Cisco IOS Devices (cont’d)

- Good practice for maintaining system availability is to ensure you always have backup copies of the startup configuration files and IOS image files.

Copy the running configuration from RAM to a remote location:

R2# copy running-config tftp:
R2# copy system:running-config tftp:

Copy a configuration from a remote source to the startup configuration:

R2# copy tftp: startup-config
R2# copy tftp: nvram:startup-config
The Cisco IOS image file is based on a special naming convention. The name for the Cisco IOS image file contains multiple parts, each with a specific meaning.

For example, the filename in the figure is explained as follows:

- The first part, **c1841**, identifies the platform on which the image runs. In this example, the platform is a Cisco 1841.
- The second part, **ipbase**, specifies the feature set. In this case, "ipbase" refers to the basic IP internetworking image. Other feature set possibilities include:
  - **i** - Designates the IP feature set
  - **j** - Designates the enterprise feature set (all protocols)
  - **s** - Designates a PLUS feature set (extra queuing, manipulation, or translations)
  - **56i** - Designates 56-bit IPsec DES encryption
  - **3** - Designates the firewall/IDS
  - **k2** - Designates the 3DES IPsec encryption (168 bit)
- The third part, **mz**, indicates where the image runs and if the file is compressed. In this example, "mz" indicates that the file runs from RAM and is compressed.
- The fourth part, **12.3-14.T7**, is the version number.
- The final part, **bin**, is the file extension. The .bin extension indicates that this is a binary executable file.

```
c1841-ipbase-mz.123-14.T7.bin
```

Platform - Cisco 1841 ISR
Feature set - IP Base
File format - m (runs in RAM)
File extension - binary executable
Version number - 12.3(14)T7
z (compressed or "zipped")
Backing Up IOS Software Images

A software backup image file is created by copying the image file from a router to a network TFTP server.

Step 1. Ping the TFTP server to make sure you have access to it.

Step 2. Verify that the TFTP server has sufficient disk space to accommodate the Cisco IOS software image. Use the show flash: command on the router to determine the size of the Cisco IOS image file.

Step 3. Copy the current system image file from the router to the network TFTP server, using the copy flash: tftp: command in privileged EXEC mode. The command requires that you to enter the IP address of the remote host and the name of the source and destination system image files.
Upgrading IOS Software Images

- Upgrading a system to a newer software version requires a different system image file to be loaded on the router.

Use the `copy tftp: flash:` command to download the new image from the network TFTP server.

The command prompts you for the IP address of the remote host and the name of the source and destination system image file. Enter the appropriate filename of the update image just as it appears on the server.

After these entries are confirmed, the Erase flash: prompt appears. Erasing flash memory makes room for the new image. Erase flash memory if there is not sufficient flash memory for more than one Cisco IOS image. If no free flash memory is available, the erase routine is required before new files can be copied. The system informs you of these conditions and prompts for a response.

Each exclamation point (!) means that one UDP segment has successfully transferred.

Note: Make sure that the Cisco IOS image loaded is appropriate for the router platform. If the wrong Cisco IOS image is loaded, the router could be made unbootable, requiring ROM monitor (ROMmon) intervention.
Restoring IOS Software Images

- Because the router does not have a valid Cisco IOS image, the router boots automatically into **ROMmon** mode.

```
rommon7> tftpdmld

IP_ADDRESS: 192.168.1.2
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 192.168.1.1
TFTP_SERVER: 192.168.1.1

Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n: [n]: y <CR>

Receiving c1841-ipbase-mz.123-14.T7.bin from 192.168.1.1
!!!!!!!!!!!!! (output omitted) !!!!!!!!!!
File reception completed.
Erasing flash at 0x607c0000
program flash location 0x605a0000
```
Another method for restoring a Cisco IOS image to a router is by using Xmodem. However, the file transfer is accomplished using the console cable and is therefore very slow when compared to the tftpdnld command.

If the Cisco IOS image is lost, the router goes into ROMmon mode when it boots up. ROMmon supports Xmodem. With that capability, the router can communicate with a terminal emulation application, such as HyperTerminal, on a PC.

A system administrator who has a copy of the Cisco IOS image on a PC can restore it to the router by making a console connection between the PC and the router and running Xmodem from HyperTerminal.
Troubleshooting Cisco IOS Configs

- Two commands that are extensively used in day-to-day network administration are show and debug. The difference between the two is significant.
  
  • Use the **show** command to verify configurations.
  
  • Use the **debug** command to identify traffic flows through interfaces and router processes.

<table>
<thead>
<tr>
<th></th>
<th>show</th>
<th>debug</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing characteristic</td>
<td>Static</td>
<td>Dynamic</td>
</tr>
<tr>
<td>Processing load</td>
<td>Low overhead</td>
<td>High overhead</td>
</tr>
<tr>
<td>Primary use</td>
<td>Gather facts</td>
<td>Observe processes</td>
</tr>
</tbody>
</table>
Recovering a Lost Router Password

- The first thing that you have to know about password recovery is that for security reasons, you need physical access to the router. You connect your PC to the router through a console cable.

In a router, a configuration register, represented by a single hexadecimal value, tells the router what specific steps to take when powered on.

Configuration registers have many uses, and password recovery is probably the most used.

Example on next slide!
Recovering a Lost Router Password

To recover a router password, do the following:

Step 1. Connect to the console port.

Step 2. If you have lost the enable password, you would still have access to user EXEC mode. Type *show version* at the prompt, and record the configuration register setting.

Step 3. Use the power switch to turn off the router, and then turn the router back on.

Step 4. Issue a **Break** signal from the terminal within 60 seconds of power up to put the router into ROMmon. A Break signal is sent using a break key sequence appropriate for the terminal program and the operating system.

Step 5. Type `confreg 0x2142` at the rommon 1> prompt. This causes the router to bypass the startup configuration where the forgotten enable password is stored.

Step 6. Type `reset` at the rommon 2> prompt. The router reboots, but ignores the saved configuration.

Step 7. Type no after each setup question, or press Ctrl-C to skip the initial setup procedure.

Step 8. Type `enable` at the Router> prompt. This puts you into enable mode, and you should be able to see the Router# prompt.

Step 9. Type `copy startup-config running-config` to copy the NVRAM into memory.

Step 10. Type `show running-config`. You must change encrypted passwords to a new password and change others you do not want to keep. **<Steps omitted to save space!>**

Step 11. Type `config-register configuration_register_setting`. The configuration_register_setting is either the value you recorded in Step 2 or 0x2102. For example:  

R1(config)#config-register 0x2102
Recovering a Lost Router Password

To recover a router password, do the following: (cont’d)

Step 12. Press Ctrl-Z or type end to leave configuration mode. The R1# prompt appears.
Step 13. Type copy running-config startup-config to commit the changes.

You have now completed password recovery. Entering the show version command will confirm that the router will use the configured config register setting on the next reboot.
This activity is a cumulative review of the chapter covering OSPF routing, authentication, and upgrading the Cisco IOS image.

Let’s do PT 4.7.1.3 (~30 min.)
Summary

- Security Threats to an Enterprise network include:
  - Unstructured threats
  - Structured threats
  - External threats
  - Internal threats

- Methods to lessen security threats consist of:
  - Device hardening
  - Use of antivirus software
  - Firewalls
  - Download security updates
Summary

- Basic router security involves the following:
  - Physical security
  - Update and backup IOS
  - Backup configuration files
  - Password configuration
  - Logging router activity

- Disable unused router interfaces & services to minimize their exploitation by intruders

- Cisco SDM
  - A web based management tool for configuring security measures on Cisco routers
Summary

- Cisco IOS Integrated File System (IFS)
  - Allows for the creation, navigation & manipulation of directories on a Cisco device
Access Control Lists

Accessing the WAN – Chapter 5
Objectives

- Explain how ACLs are used to secure a medium-size Enterprise branch office network.

- Configure standard ACLs in a medium-size Enterprise branch office network.

- Configure extended ACLs in a medium-size Enterprise branch office network.

- Describe complex ACLs in a medium-size Enterprise branch office network.

- Implement, verify and troubleshoot ACLs in an enterprise network environment.
Using ACLs to Secure Networks

- TCP provides a connection-oriented, reliable, byte stream service.
  
i.e. the two applications using TCP must establish a TCP connection with each other before they can exchange data.

TCP packets are marked with flags that denote their purpose:
- a SYN starts (synchronizes) the session;
- an ACK is an acknowledgment that an expected packet was received, and
- a FIN finishes the session.

A SYN/ACK acknowledges that the transfer is synchronized.

TCP data segments include the higher level protocol needed to direct the application data to the correct application.

A TCP Conversation

- "Let's talk."
  - TCP SYN packet
    - "Sure, let's talk."
  - TCP SYN/ACK packet
    - "Great, we have a connection."
  - TCP ACK packet
    - "I need you to send me some data."
  - TCP data segment
    - "Thanks, I received your request."
  - TCP ACK packet
    - "Here is the data you want."
  - TCP data segment(s)
    - "Thanks. I received my data."
  - TCP ACK packet
    - "I am finished and have no more data to send."
  - TCP FIN/ACK packet
    - "I am finished as well. Thanks."
Using ACLs to Secure Networks (cont’d)

- Packet filtering, sometimes called static packet filtering, controls access to a network by analyzing the incoming and outgoing packets and passing or halting them based on stated criteria.

An ACL is a **sequential** list of permit or deny statements that apply to IP addresses or upper-layer protocols.

The ACL can extract the following information from the packet header, test it against its rules, and make "allow" or "deny" decisions based on:
- Source IP address
- Destination IP address
- ICMP message type

The ACL can also extract upper layer information and test it against its rules. Upper layer information includes:
- TCP/UDP source port
- TCP/UDP destination port
Using ACLs to Secure Networks (cont’d)

- To understand the concept of how a router uses packet filtering, imagine that a guard has been posted at a locked door…

The guard's instructions are to allow only people whose names appear on a list to pass through the door. The guard is filtering people based on the criterion of having their names on the authorized list.

For example, you could say, "Only permit web access to users from network A. Deny web access to users from network B, but permit them to have all other access."

Refer to the figure to examine the decision path the packet filter uses to accomplish this task.

Let’s walk through it logically.
Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- An ACL is a router configuration script that controls whether a router permits or denies packets to pass based on criteria found in the packet header.

As each packet comes through an interface with an associated ACL, the ACL is checked from top to bottom, one line at a time, looking for a pattern matching the incoming packet. The ACL enforces one or more corporate security policies by applying a permit or deny rule to determine the fate of the packet. ACLs can be configured to control access to a network or subnet.

By default, a router does not have any ACLs configured and therefore does not filter traffic. Traffic that enters the router is routed according to the routing table. If you do not use ACLs on the router, all packets that can be routed through the router pass through the router to the next network segment.
ACLs Operation – Inbound Traffic Example

- ACL statements operate in sequential order. They evaluate packets against the ACL, from the top down, one statement at a time.

Inbound ACLs –
Incoming packets are processed before they are routed to the outbound interface.

An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded.

If the packet is permitted by the tests, it is then processed for routing.

The figure shows the logic for an inbound ACL.

If a packet header and an ACL statement match, the rest of the statements in the list are skipped, and the packet is permitted or denied as determined by the matched statement.

A final implied statement covers all packets for which conditions did not test true. This final test condition matches all other packets and results in a "deny" instruction.
ACLs Operation – Outbound Traffic Example

- ACL statements operate in sequential order. They evaluate packets against the ACL, from the top down, one statement at a time.

**Outbound ACLs** -
Incoming packets are routed to the outbound interface, and then they are processed through the outbound ACL.

The figure shows the logic for an outbound ACL. Before a packet is forwarded to an outbound interface, the router checks the routing table to see if the packet is routable. If the packet is not routable, it is dropped. Next, the router checks to see whether the outbound interface is grouped to an ACL.

For outbound lists, "to permit" means to send the packet to the output buffer, and "to deny" means to discard the packet.
Types of Cisco ACLs

- **Standard ACLs** allow you to permit or deny traffic from source IP addresses.
- The destination of the packet and the ports involved do not matter.

The example allows all traffic from network 192.168.30.0/24 network. Because of the implicit "deny any" at the end, all other traffic is blocked with this ACL.

Standard ACLs are created in global configuration mode.
Types of Cisco ACLs (cont’d)

- **Extended ACLs** filter IP packets based on several attributes, for example:
  - Source and destination IP addresses
  - Source and destination TCP and UDP ports
  - Protocol type (IP, ICMP, UDP, TCP, or protocol number)

In the figure, ACL 103 permits traffic originating from any address on the 192.168.30.0/24 network to any destination host port 80 (HTTP).

Extended ACLs are created in global configuration mode.
Numbering & Naming ACLs

- Using numbered ACLs is an effective method for determining the ACL type on smaller networks with more homogeneously defined traffic.

  However, a number does not inform you of the purpose of the ACL. For this reason, starting with Cisco IOS Release 11.2, you can use a name to identify a Cisco ACL.

Why are numbers 200 to 1299 skipped? Because those numbers are used by other protocols. This course focuses only on IP ACLs. Numbers 600 to 699 are used by AppleTalk, and numbers 800 to 899 are used by IPX.
Where to Place ACLs

The proper placement of an ACL to filter undesirable traffic makes the network operate more efficiently.

Where you place ACLs can reduce unnecessary traffic. For example, traffic that will be denied at a remote destination should not use network resources along the route to that destination.

Every ACL should be placed where it has the greatest impact on efficiency. The basic rules are:

• Locate extended ACLs as close as possible to the source of the traffic denied. This way, undesirable traffic is filtered without crossing the network infrastructure.

• Because standard ACLs do not specify destination addresses, place them as close to the destination as possible.
Where to Place ACLs – Standard Example

- Let us consider an example of where to place a standard ACL in our network.

  **Standard ACLs** do not specify destination addresses, place them as close to the destination as possible.

In the figure, the administrator wants to prevent traffic originating in the 192.168.10.0/24 network from getting to the 192.168.30.0/24 network.

An ACL on the outbound interface of R1 denies R1 the ability to send traffic to other places as well.

The solution is to place a standard ACL on the inbound interface of R3 to stop all traffic from the source address 192.168.10.0/24.

A standard ACL meets the needs because it is only concerned with source IP addresses.
Where to Place ACLs – Extended Example

- Let us consider an example of where to place an extended ACL in our network.

  Locate extended ACLs as close as possible to the source of the traffic denied. This way, undesirable traffic is filtered without crossing the network infrastructure.

In this figure, the administrator of the 192.168.10.0/24 and 192.168.11.0/24 networks wants to deny Telnet and FTP traffic from Eleven to the 192.168.30.0/24 network.

At the same time, other traffic must be permitted to leave Ten.

The best solution is to move closer to the source and place an extended ACL on the inbound Fa0/2 interface of R1. This ensures that packets from Eleven do not enter R1, and subsequently cannot cross over into Ten, or even enter R2 or R3.

Traffic with other destination addresses and ports is still permitted through R1.
ACL Best Practices

- Using ACLs requires attention to detail and great care.
  - Mistakes can be costly in terms of downtime, troubleshooting efforts, and poor network service.
  - Before starting to configure an ACL, basic planning is required.
  - The figure presents guidelines that form the basis of an ACL best practices list.

<table>
<thead>
<tr>
<th>Guideline</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base your ACLs on the security policy of the organization.</td>
<td>This will ensure you implement organizational security guidelines.</td>
</tr>
<tr>
<td>Prepare a description of what you want your ACLs to do.</td>
<td>This will help you avoid inadvertently creating potential access problems.</td>
</tr>
<tr>
<td>Use a text editor to create, edit and save ACLs.</td>
<td>This will help you create a library of reusable ACLs.</td>
</tr>
<tr>
<td>Test your ACLs on a development network before implementing them on a production network.</td>
<td>This will help you avoid costly errors.</td>
</tr>
</tbody>
</table>
General Guidelines for Creating ACLs

- Let’s do the 5.1.9.2 Activity 3

Solution on the next slide…
General Guidelines for Creating ACLs

Activity 3 Solution!
Entering Criteria Statements

- Criteria statement order in an ACL is important

When traffic comes into the router, it is compared to ACL statements based on the order that the entries occur in the router.

The router continues to process the ACL statements until it has a match. For this reason, you should have the most frequently used ACL entry at the top of the list.

If no matches are found when the router reaches the end of the list, the traffic is denied because ACLs have an implied deny for all traffic not meeting any of the tested criteria.

A single-entry ACL with only one deny entry has the effect of denying all traffic. You must have at least one permit statement in an ACL or all traffic is blocked.
Configuring a Standard ACL

- Remember that statement order is critical!

In the figure, packets that come in Fa0/0 are checked for their **source addresses**:

```
access-list 2 deny host 192.168.10.1
access-list 2 permit 192.168.10.0 0.0.0.255
access-list 2 deny 192.168.0.0 0.0.255.255
access-list 2 permit 192.0.0.0 0.255.255.255
```

If packets are permitted, they are **routed** through the router to an output interface. If packets are not permitted, they are **dropped** at the incoming interface.

**Standard ACL access-list Command Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-number</td>
<td>Number of an ACL. This is a decimal number from 1 to 99, or 1300 to 1999 (for standard ACL).</td>
</tr>
<tr>
<td>deny</td>
<td>Denies access if the conditions are matched.</td>
</tr>
<tr>
<td>permit</td>
<td>Permits access if the conditions are matched.</td>
</tr>
<tr>
<td>remark</td>
<td>Add a remark about entries in an IP access list to make the list easier to understand and scan.</td>
</tr>
</tbody>
</table>
| source         | Number of the network or host from which the packet is being sent. There are two ways to specify the source:  
                       - Use a 32-bit quantity in four-part, dotted-decimal format.  
                       - Use the keyword **any** as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255. |
| source-wildcard | (Optional) Wildcard bits to be applied to the source. There are two ways to specify the source-wildcard:  
                       - Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.  
                       - Use the keyword **any** as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255. |
| log            | (Optional) Causes an informational logging message about the packet that matches the |
ACL Wildcard Masking

- ACLs statements include masks, also called wildcard masks.
  - Wildcard masks use the following rules to match binary 1s and 0s:
    - Wildcard mask bit 0 – Must match the corresponding bit value in the source address
    - Wildcard mask bit 1 - Ignore the corresponding bit value in the source address
Applying Standard ACLs

- ACL 1 only permits hosts from the 192.168.10.0 /24 network to exit router R1.
  It denies any other network including the 192.168.11.0 network.

Procedure for Configuring Standard ACLs

Step 1 Use the access-list global configuration command to create an entry in a standard IPv4 ACL.

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```

Step 2 Use the interface configuration command to select an interface to which to apply the ACL.

```
R1(config)# interface FastEthernet 0/0
```

Step 3 Use the ip access-group interface configuration command to activate the existing ACL on an interface.

```
R1(config-if)# ip access-group 1 out
```

To remove an IP ACL from an interface, enter the no ip access-group command on the interface. This example activates the standard IPv4 ACL 1 on the interface as an outbound filter.
Applying Standard ACLs – More Complex

Below is an example of an ACL that denies a specific host and permits a number of subnets.

The first command deletes the previous version of ACL 1 and the next ACL statement denies the PC1 host located at 192.168.10.10.

The third line is new and permits all hosts from the 192.168.x.x /16 networks. This now means that all hosts from the 192.168.10.0 /24 network still match but now the hosts from the 192.168.11.0 network also match.

The ACL is again reapplied to interface S0/0/0 in an outbound direction. Therefore, both LANs attached to router R1 may exit the S0/0/0 interface with the exception of the PC1 host.

This ACL blocks traffic from the host PC1. It also permits all other LAN traffic to exit from router R1.
Editing Numbered ACLs

- There is no built-in editing feature that allows you to edit a change in an ACL. You cannot selectively insert or delete lines.

Construct ACLs in a text editor such as Microsoft Notepad.

**Step 1.** Display the ACL using the `show running-config` command. The example in the figure uses the `include` keyword to display only the ACL statements.

**Step 2.** Highlight the ACL, copy it, and then paste it into Microsoft Notepad. Edit the list as required. Once the ACL is correctly displayed in Microsoft Notepad, highlight it and copy it.

**Step 3.** In global configuration mode, disable the access list using the `no access-list` command. Otherwise, the new statements would be appended to the existing ACL. Then paste the new ACL into the configuration of the router.
Creating Standard Named ACLs

- The steps to create a standard named ACL:

```
R1(config)#ip access-list standard NO_ACCESS
R1(config-std-nacl)#deny host 192.168.11.10
R1(config-std-nacl)#permit 192.168.11.0 0.0.0.255
R1(config-std-nacl)#interface Fa0/0
R1(config-if)#ip access-group NO_ACCESS out
```

In the figure to the right, the screen output shows the commands used to configure a standard named ACL on router R1, interface Fa0/0 that denies host 192.168.11.10 access to the 192.168.10.0 network.

Capitalizing ACL names is not required, but makes them stand out when viewing the running-config output.
Monitoring & Verifying ACLs

- When you finish an ACL configuration, ALWAYS use the Cisco IOS show commands to verify the configuration.

The example below shows the result of issuing the show access-lists command on router R1. The capitalized ACL names, SALES and ENG stand out in the screen output:

```
R1# show access-lists
Standard IP access list SALES
  10 deny 10.1.1.0 0.0.0.255
  20 permit 10.3.3.1
  30 permit 10.4.4.1
  40 permit 10.5.5.1
Extended IP access list ENG
  10 permit tcp host 192.168.10.2 any eq telnet (25 matches)
  20 permit tcp host 192.168.10.2 any eq ftp
  30 permit tcp host 192.168.10.2 any eq ftp-data
```

Now that you have verified that the ACLs are configured as you intended, the next step is to confirm that the ACLs work as planned.
Editing Named ACLs

- Named ACLs have a big advantage over numbered ACLs in that they are easier to edit.

Starting with Cisco IOS Software Release 12.3, named IP ACLs allow you to delete individual entries in a specific ACL.

- In the first show command output, you can see that the ACL named WEBSERVER has three numbered lines indicating access rules for the webserver.
- To grant another workstation access in the list only requires inserting a numbered line. In the example, the workstation with the IP address 192.168.11.10 is being added.
- The final show command output verifies that the new workstation is now allowed access.
Standard ACLs are router configuration scripts that control whether a router permits or denies packets based on the source address.

This activity focuses on defining filtering criteria, configuring standard ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation.

Let’s do PT 5.2.8.2 (~15 min.)
Extended ACLs

- For more precise traffic-filtering control, you can use extended ACLs numbered 100 to 199 and 2000 to 2699 providing a total of 800 possible extended ACLs.
  - Extended ACLs can also be named.
  - Extended ACLs are used more often than standard ACLs because they provide a greater range of control.
  - Extended ACLs check the source packet addresses, but they also check the destination address, protocols and port numbers (or services).
  - This gives a greater range of criteria on which to base the ACL. For example, an extended ACL can simultaneously allow e-mail traffic from a network to a specific destination while denying file transfers and web browsing.

- Let’s walk through Graphic 5.3.1.1
Extended ACL Examples

- The ability to filter on protocol and port number allows you to build very specific extended ACLs.
- Using the appropriate port number, you can specify an application by configuring either the port number or the name of a well-known port.

The figure shows some examples of how an administrator specifies a TCP or UDP port number by placing it at the end of the extended ACL statement.

Logical operations can be used, such as equal (eq), not equal (neq), greater than (gt), and less than (lt).
The procedural steps for configuring extended ACLs are the same as for standard ACLs, you first create the extended ACL and then activate it on an interface.

The command syntax and parameters are more complex to support the additional features provided by extended ACLs.

```
access-list access-list-number {deny | permit | remark} protocol source [source-wildcard] [operator operand] [port port-number or name] destination [destination-wildcard] [operator operand] [port port-number or name] [established]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list-number</code></td>
<td>Identifies the access list using a number in the range 100 to 199 (for an extended IP ACL) and 2000 to 2699 (expanded IP ACLs).</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>Denies access if the conditions are matched.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Permits access if the conditions are matched.</td>
</tr>
<tr>
<td><code>remark</code></td>
<td>Indicates whether this entry allows or blocks the specified address. Could also be used to enter a remark.</td>
</tr>
<tr>
<td><code>protocol</code></td>
<td>Name or number of an Internet protocol. Common keywords include icmp, ip, tcp, or udp. To match any Internet protocol (including ICMP, TCP, and UDP) use the ip keyword.</td>
</tr>
<tr>
<td><code>source</code></td>
<td>Number of the network or host from which the packet is being sent.</td>
</tr>
<tr>
<td><code>source-wildcard</code></td>
<td>Wildcard bits to be applied to source.</td>
</tr>
<tr>
<td><code>destination</code></td>
<td>Number of the network or host to which the packet is being sent.</td>
</tr>
<tr>
<td><code>destination-wildcard</code></td>
<td>Wildcard bits to be applied to the destination.</td>
</tr>
</tbody>
</table>
Configuring Extended ACLs - Example

- In this example, the network administrator needs to restrict Internet access to allow only website browsing.

  ACL 103 applies to traffic leaving the 192.168.10.0 network, and ACL 104 to traffic coming into the network.

ACL 103 accomplishes the first part of the requirement. It allows traffic coming from any address on the 192.168.10.0 network to go to any destination, subject to the limitation that traffic goes to ports 80 (HTTP) and 443 (HTTPS) only.

The nature of HTTP requires that traffic flow back into the network, but the network administrator wants to restrict that traffic to HTTP exchanges from requested websites. The security solution must deny any other traffic coming into the network.

ACL 104 does that by blocking all incoming traffic, except for the established connections. HTTP establishes connections starting with the original request and then through the exchange of ACK, FIN, and SYN messages.

With the established parameter, the router will allow only the established traffic to come back in and block all other traffic.
Applying Extended ACLs to Ints

- Here - we want to allow users to browse both insecure and secure websites.

First consider whether the traffic you want to filter is going in or out. Trying to access websites on the Internet is traffic going out. Receiving e-mails from the Internet is traffic coming in.
Creating Named Extended ACLs

- You can create named extended ACLs in essentially the same way you created named standard ACLs.
  
The commands to create a named ACL are different for standard and extended ACLs.
Extended ACLs are router configuration scripts that control whether a router permits or denies packets based on their source or destination address as well as protocols or ports.

Extended ACLs provide more flexibility and granularity than standard ACLs.

This activity focuses on defining filtering criteria, configuring extended ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation.

Let’s do PT 5.3.4.2 (~25 min.)
Complex ACLs

- Standard and extended ACLs can become the basis for complex ACLs that provide additional functionality.

The table in the figure summarizes the three categories of complex ACLs, which are all discussed next:

<table>
<thead>
<tr>
<th>Complex ACL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic ACLs (lock-and-key)</td>
<td>Users that want to traverse the router are blocked until they use Telnet to connect to the router and are authenticated</td>
</tr>
<tr>
<td>Reflexive ACLs</td>
<td>Allows outbound traffic and limits inbound traffic in response to sessions that originate inside the router</td>
</tr>
<tr>
<td>Time-based ACLs</td>
<td>Allows for access control based on the time of day and week</td>
</tr>
</tbody>
</table>

Lock-and-key is available for IP traffic only.

Dynamic ACLs are dependent on Telnet connectivity, authentication (local or remote), and extended ACLs.

Some common reasons to use dynamic ACLs are as follows:
- When you want a specific remote user or group of remote users to access a host within your network, connecting from their remote hosts via the Internet.
- When you want a subset of hosts on a local network to access a host on a remote network that is protected by a firewall.

In the figure the user at PC1 is an administrator that requires a back door access to the 192.168.30.0 /24 network located on router R3. A dynamic ACL has been configured to allow FTP and HTTP on router R3 access but only for a limited time.
Complex ACLs - Dynamic

- Lock-and-key is a traffic filtering security feature that uses dynamic ACLs, which are sometimes referred to as lock-and-key ACLs.
- Lock-and-key is available for IP traffic only.
- Dynamic ACLs are dependent on Telnet connectivity, authentication (local or remote), and extended ACLs.
- Some common reasons to use dynamic ACLs are as follows:
  - When you want a specific remote user or group of remote users to access a host within your network, connecting from their remote hosts via the Internet.
  - When you want a subset of hosts on a local network to access a host on a remote network that is protected by a firewall.
Complex ACLs – Dynamic Example

In the figure the user at PC1 is an administrator that requires a back door access to the 192.168.30.0 /24 network located on router R3.

A dynamic ACL has been configured to allow FTP and HTTP on router R3 access but only for a limited time.
Complex ACLs - Reflexive

- Reflexive ACLs force the reply traffic from the destination of a known recent outbound packet to go to the source of that outbound packet.

- Network administrators use reflexive ACLs to allow IP traffic for sessions originating from their network while denying IP traffic for sessions originating outside the network.

- Reflexive ACLs provide a truer form of session filtering than an extended ACL that uses the established parameter introduced earlier. Although similar in concept to the established parameter, reflexive ACLs also work for UDP and ICMP, which have no ACK or RST bits.

- Reflexive ACLs can be defined only with extended named IP ACLs.
Complex ACLs – Reflexive Example

- The figure shows an example for which the administrator needs a reflexive ACL that permits ICMP outbound and inbound traffic, while it permits only TCP traffic that has been initiated from inside the network.

Assume that all other traffic will be denied.

The reflexive ACL is applied to the outbound interface of R2.
Complex ACLs – Reflexive Example

- Continuing our example from the previous slide...

  Although the complete configuration for reflexive ACLs is outside the scope of this course, the figure shows an example of the steps that are required to configure a reflexive ACL.

```
R2(config)#ip access-list extended OUTBOUNDFILTERS
R2(config-ext-nacl)# permit tcp 192.168.0.0 0.0.255.255 any reflect TCPTRAFFIC
R2(config-ext-nacl)# permit icmp 192.168.0.0 0.0.255.255 any reflect ICMPTRAFFIC

R2(config)#ip access-list extended INBOUNDFILTERS
R2(config-ext-nacl)# evaluate TCPTRAFFIC
R2(config-ext-nacl)# evaluate ICMPTRAFFIC

R2(config)#interface S0/1/0
R2(config-if)#ip access-group INBOUNDFILTERS in
R2(config-if)#ip access-group OUTBOUNDFILTERS out
```
Complex ACLs – Time-based

- Time-based ACLs are similar to extended ACLs in function, but they allow for access control based on time.

To implement time-based ACLs, you create a time range that defines specific times of the day and week. You identify the time range with a name and then refer to it by a function. The time restrictions are imposed on the function itself.
Complex ACLs – Time-based Example

- In the example, a Telnet connection is permitted from the inside network to the outside network on Monday, Wednesday, and Friday during business hours.

Although the complete configuration details for time-based ACLs are outside the scope of this course, the following example shows the steps that are required.

<table>
<thead>
<tr>
<th>Step</th>
<th>Configuration</th>
</tr>
</thead>
</table>
| Step 1 | R1(config)#time-range EVERYOTHERDAY  
R1(config-time-range)#periodic Monday Wednesday Friday 8:00 to 17:00 |
| Step 2 | R1(config)#access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range EVERYOTHERDAY |
| Step 3 | R1(config)#interface s0/0/0  
R1(config-if)#ip access-group 101 out |
Troubleshoot Common ACL Errors

- What’s wrong here?

```
# show access-lists 10
10 deny tcp 192.168.10.0 0.0.0.255 any
20 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
30 permit ip any any
```

Error 1:
Host 192.168.10.10 has no connectivity with 192.168.30.12
Troubleshoot Common ACL Errors

- What’s wrong here?

Troubleshooting Common ACL Errors

```
# show access-lists 120
Extended IP access list 120
  10 deny tcp 192.168.10.0 0.0.255.255 any eq telnet
  20 deny tcp 192.168.1.0 0.0.0.255 host 10.100.100.1 eq smtp
  30 permit tcp any
```

Error 2:
The 192.168.10.0 /24 network cannot use TFTP to connect to the 192.168.30.0 /24.
Troubleshoot Common ACL Errors

- What’s wrong here?
In this activity, you will design, apply, test and troubleshoot basic access list configurations.

Packet Tracer may not support all the tasks specified in the hands-on lab. **BEWARE!**

Let’s do **PT 5.5.1.2 (~15 min.)**
Summary

- An Access List (ACL) is:
  A series of permit and deny statements that are used to filter traffic

- **Standard ACL**
  - Identified by numbers 1 - 99 and 1300 - 1999
  - Filter traffic based on source IP address

- **Extended ACL**
  - Identified by number 100 -199 & 2000 - 2699
  - Filter traffic based on
    - Source IP address
    - Destination IP address
    - Protocol
    - Port number
Summary

- Named ACL
  - Used with IOS 11.2 and above
  - Can be used for either standard or extended ACL

- ACL’s use Wildcard Masks (WCM)
  - Described as the inverse of a subnet mask
    - Reason
      - 0 → check the bit
      - 1 → ignore the bit
Summary

- Implementing ACLs
  - 1st create the ACL
  - 2nd place the ACL on an interface
    - Standard ACL are placed nearest the destination
    - Extended ACL are placed nearest the source

- Use the following commands for verifying & troubleshooting an ACL
  - Show access-list
  - Show interfaces
  - Show run
Summary

- Complex ACL
  - Dynamic ACL
  - Reflexive ACL
  - Time based ACL
RJ-45 PINOUTS

Straight-Through Cable

**FLUKE MAP**

<table>
<thead>
<tr>
<th>T568B</th>
<th>T568A</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2 3 4 5 6 7 8</td>
<td>1 2 3 6 4 5 7 8</td>
</tr>
</tbody>
</table>

**Graphic Map**

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

Cross Connect or Cross-Over Cable

**FLUKE MAP**

<table>
<thead>
<tr>
<th>T568B</th>
<th>T568A</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2 3 4 5 6 7 8</td>
<td>1 2 3 6 4 5 7 8</td>
</tr>
</tbody>
</table>

**Graphic Map**

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

Roll-Over or Console Cable

**FLUKE MAP**

<table>
<thead>
<tr>
<th>T568B</th>
<th>T568A</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2 3 4 5 6 7 8</td>
<td>8 7 6 5 4 3 2 1</td>
</tr>
</tbody>
</table>

**Graphic Map**

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>
Lab – Building a Switched Network with Redundant Links

Topography

Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>VLAN 1</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>S2</td>
<td>VLAN 1</td>
<td>192.168.1.2</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>S3</td>
<td>VLAN 1</td>
<td>192.168.1.3</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

Objectives

Part 1: Build the Network and Configure Basic Device Settings
Part 2: Determine the Root Bridge
Part 3: Observe STP Port Selection Based on Port Cost
Part 4: Observe STP Port Selection Based on Port Priority

Background / Scenario

Redundancy increases the availability of devices in the network topology by protecting the network from a single point of failure. Redundancy in a switched network is accomplished through the use of multiple switches or multiple links between switches. When physical redundancy is introduced into a network design, loops and duplicate frames can occur.

The Spanning Tree Protocol (STP) was developed as a Layer 2 loop-avoidance mechanism for redundant links in a switched network. STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop.

In this lab, you will use the `show spanning-tree` command to observe the STP election process of the root bridge. You will also observe the port selection process based on cost and priority.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.
Lab – Building a Switched Network with Redundant Links

Required Resources
- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings
In Part 1, you will set up the network topology and configure basic settings on the switches.

Step 1: Cable the network as shown in the topology.
Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Initialize and reload the switches as necessary.

Step 3: Configure basic settings for each switch.
  a. Disable DNS lookup.
  b. Configure the device name as shown in the topology.
  c. Assign class as the encrypted privileged EXEC mode password.
  d. Assign cisco as the console and vty passwords and enable login for console and vty lines.
  e. Configure logging synchronous for the console line.
  f. Configure a message of the day (MOTD) banner to warn users that unauthorized access is prohibited.
  g. Configure the IP address listed in the Addressing Table for VLAN 1 on all switches.
  h. Copy the running configuration to the startup configuration.

Step 4: Test connectivity.
Verify that the switches can ping one another.
Can S1 ping S2? _____________
Can S1 ping S3? _____________
Can S2 ping S3? _____________
Troubleshoot until you are able to answer yes to all questions.

Part 2: Determine the Root Bridge
Every spanning-tree instance (switched LAN or broadcast domain) has a switch designated as the root bridge. The root bridge serves as a reference point for all spanning-tree calculations to determine which redundant paths to block.

An election process determines which switch becomes the root bridge. The switch with the lowest bridge identifier (BID) becomes the root bridge. The BID is made up of a bridge priority value, an extended system ID, and the MAC address of the switch. The priority value can range from 0 to 65,535, in increments of 4,096, with a default value of 32,768.
Step 1: Deactivate all ports on the switches.

Step 2: Configure connected ports as trunks.

Step 3: Activate ports F0/2 and F0/4 on all switches.

Step 4: Display spanning tree information.

Issue the `show spanning-tree` command on all three switches. The Bridge ID Priority is calculated by adding the priority value and the extended system ID. The extended system ID is always the VLAN number. In the example below, all three switches have equal Bridge ID Priority values (32769 = 32768 + 1, where default priority = 32768, VLAN number = 1); therefore, the switch with the lowest MAC address becomes the root bridge (S2 in the example).

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
  Address     0cd9.96d2.4000
  Cost        19
  Port        2 (FastEthernet0/2)
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
  Address     0cd9.96e8.8a00
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time  300 sec
  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/2               Root FWD 19        128.2    P2p
  Fa0/4               Altn BLK 19        128.4    P2p

S2# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
  Address     0cd9.96d2.4000
  This bridge is the root
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
  Address     0cd9.96d2.4000
  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time  300 sec
```
### Interface Table

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Status</th>
<th>Cost</th>
<th>Priority</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/2</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.2</td>
<td>P2p</td>
</tr>
<tr>
<td>Fa0/4</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.4</td>
<td>P2p</td>
</tr>
</tbody>
</table>

```
S3# show spanning-tree
```

#### VLAN0001

Spanning tree enabled protocol ieee

<table>
<thead>
<tr>
<th>Root ID</th>
<th>Priority</th>
<th>Address</th>
<th>Cost</th>
<th>Port</th>
<th>Hello Time</th>
<th>Max Age</th>
<th>Forward Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32769</td>
<td>0cd9.96d2.4000</td>
<td>19</td>
<td>2 (FastEthernet0/2)</td>
<td>2 sec</td>
<td>20 sec</td>
<td>15 sec</td>
</tr>
</tbody>
</table>

Bridge ID: 32769 (priority 32768 sys-id-ext 1)

<table>
<thead>
<tr>
<th>Address</th>
<th>0cd9.96e8.7400</th>
</tr>
</thead>
</table>

| Hello Time | 2 sec |
| Max Age    | 20 sec |
| Forward Delay | 15 sec |

| Aging Time | 300 sec |

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Status</th>
<th>Cost</th>
<th>Priority</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/2</td>
<td>Root</td>
<td>FWD</td>
<td>128.2</td>
<td>P2p</td>
<td></td>
</tr>
<tr>
<td>Fa0/4</td>
<td>Desg</td>
<td>FWD</td>
<td>128.4</td>
<td>P2p</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The default STP mode on the 2960 switch is Per VLAN Spanning Tree (PVST).

In the diagram below, record the Role and Status (Sts) of the active ports on each switch in the Topology.
Based on the output from your switches, answer the following questions.

Which switch is the root bridge? ____________
Why did spanning tree select this switch as the root bridge?
_______________________________________________________________________________________
_______________________________________________________________________________________
Which ports are the root ports on the switches? ___________________________________________
Which ports are the designated ports on the switches? _______________________________________
What port is showing as an alternate port and is currently being blocked? _________________________
Why did spanning tree select this port as the non-designated (blocked) port?
_______________________________________________________________________________________
_______________________________________________________________________________________
_______________________________________________________________________________________

Part 3: Observe STP Port Selection Based on Port Cost

The spanning tree algorithm (STA) uses the root bridge as the reference point and then determines which ports to block, based on path cost. The port with the lower path cost is preferred. If port costs are equal, then spanning tree compares BIDs. If the BIDs are equal, then the port priorities are used to break the tie. Lower values are always preferred. In Part 3, you will change the port cost to control which port is blocked by spanning tree.
**Lab – Building a Switched Network with Redundant Links**

**Step 1: Locate the switch with the blocked port.**

With the current configuration, only one switch should have a port that is blocked by STP. Issue the `show spanning-tree` command on both non-root switches. In the example below, spanning tree is blocking port F0/4 on the switch with the highest BID (S1).

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID  Priority  32769
  Address  0cd9.96d2.4000
  Cost     19
  Port     2 (FastEthernet0/2)
  Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/2               Root FWD 19        128.2    P2p
  Fa0/4               Altn BLK 19        128.4    P2p

S3# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID  Priority  32769
  Address  0cd9.96d2.4000
  Cost     19
  Port     2 (FastEthernet0/2)
  Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority  32769  (priority 32768 sys-id-ext 1)
  Address   0cd9.96e8.7400
  Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time  15  sec

  Interface           Role Sts Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/2               Root FWD 19        128.2    P2p
  Fa0/4               Desg FWD 19        128.4    P2p
```

**Note:** Root bridge and port selection may differ in your topology.
Step 2: Change port cost.

In addition to the blocked port, the only other active port on this switch is the port designated as the root port. Lower the cost of this root port to 18 by issuing the `spanning-tree cost 18` command.

```
S1(config)# interface f0/2
S1(config-if)# spanning-tree cost 18
```

Step 3: Observe spanning tree changes.

Re-issue the `show spanning-tree` command on both non-root switches. Observe that the previously blocked port (S1 - F0/4) is now a designated port and spanning tree is now blocking a port on the other non-root switch (S3 - F0/4).

```
S1# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID   Priority  32769
  Address   0cd9.96d2.4000
  Cost      18
  Port      2 (FastEthernet0/2)
  Hello Time     2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority  32769 (priority 32768 sys-id-ext 1)
  Address   0cd9.96e8.8a00
  Hello Time     2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time   300 sec

  Interface           Role Sts  Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/2               Root FWD 18        128.2    P2p
  Fa0/4               Desg FWD 19        128.4    P2p

S3# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID   Priority  32769
  Address   0cd9.96d2.4000
  Cost      19
  Port      2 (FastEthernet0/2)
  Hello Time     2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority  32769 (priority 32768 sys-id-ext 1)
  Address   0cd9.96e8.7400
  Hello Time     2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time   300 sec

  Interface           Role Sts  Cost      Prio.Nbr Type
  ------------------- ---- --- --------- -------- --------------------------------
  Fa0/2               Root FWD 18        128.2    P2p

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.
Why did spanning tree change the previously blocked port to a designated port, and block the port that was a designated port on the other switch?

---

**Step 4: Remove port cost changes.**

a. Issue the `no spanning-tree cost 18` interface configuration mode command to remove the cost statement that you created earlier.

```
S1(config)# interface f0/2
S1(config-if)# no spanning-tree cost 18
```

b. Re-issue the `show spanning-tree` command to verify that STP has reset the port on the non-root switches back to the original port settings. It takes approximately 30 seconds for STP to complete the port transition process.

**Part 4: Observe STP Port Selection Based on Port Priority**

If port costs are equal, then spanning tree compares BIDs. If the BIDs are equal, then the port priorities are used to break the tie. The default port priority value is 128. STP aggregates the port priority with the port number to break ties. Lower values are always preferred. In Part 4, you will activate redundant paths to each switch to observe how STP selects a port using the port priority.

a. Activate ports F0/1 and F0/3 on all switches.

b. Wait 30 seconds for STP to complete the port transition process, and then issue the `show spanning-tree` command on the non-root switches. Observe that the root port has moved to the lower numbered port linked to the root switch, and blocked the previous root port.

```
S1# show spanning-tree
```

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID   Priority 32769
            Address 0cd9.96d2.4000
            Cost    19
            Port    1 (FastEthernet0/1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
            Address 0cd9.96e8.8a00
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 15 sec

  Interface Role Sts Cost      Prio.Nbr Type
  ------------------------- ------ --------- -------- --------------------------------
  Fa0/1               Root FWD 19        128.1    P2p
  Fa0/2               Altn BLK 19        128.2    P2p
  Fa0/3               Altn BLK 19        128.3    P2p
  Fa0/4               Altn BLK 19        128.4    P2p
```
S3# `show spanning-tree`

```
VLAN0001
 Spanning tree enabled protocol ieee
 Root ID  Priority  32769
    Address 0cd9.96d2.4000
    Cost 19
    Port 1 (FastEthernet0/1)
    Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority  32769  (priority 32768 sys-id-ext 1)
    Address 0cd9.96e8.7400
    Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
    Aging Time 15 sec

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Sts</th>
<th>Cost</th>
<th>Prio.Nbr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>Root</td>
<td>FWD</td>
<td>19</td>
<td>128.1</td>
<td>P2p</td>
</tr>
<tr>
<td>Fa0/2</td>
<td>Altn</td>
<td>BLK</td>
<td>19</td>
<td>128.2</td>
<td>P2p</td>
</tr>
<tr>
<td>Fa0/3</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.3</td>
<td>P2p</td>
</tr>
<tr>
<td>Fa0/4</td>
<td>Desg</td>
<td>FWD</td>
<td>19</td>
<td>128.4</td>
<td>P2p</td>
</tr>
</tbody>
</table>
```

What port did STP select as the root port on each non-root switch? _________________________________

Why did STP select these ports as the root port on these switches?
_______________________________________________________________________________________
_______________________________________________________________________________________

**Reflection**

1. After a root bridge has been selected, what is the first value STP uses to determine port selection?
_______________________________________________________________________________________

2. If the first value is equal on the two ports, what is the next value that STP uses to determine port selection?
_______________________________________________________________________________________

3. If both values are equal on the two ports, what is the next value that STP uses to determine port selection?
_______________________________________________________________________________________
Powerful Protocols

Objective
A review of EIGRP and OSPF routing protocol configuration and verification commands.

Scenario
At the end of this course, you are asked to complete two Capstone Projects where you will create, configure, and verify two network topologies using the two main routing protocols taught in this course, EIGRP and OSPF.

To make things easier, you decide to create a chart of configuration and verification commands to use for these two design projects. To help devise the protocol charts, ask another student in the class to help you.

Refer to the PDF for this chapter for directions on how to create a design for this modeling project. When complete, share your work with another group or with the class. You may also want to save the files created for this project in a network portfolio for future reference.

Resources
- Previous curriculum chapter content for EIGRP and OSPF
- Word processing software

Directions

Step 1: Create a matrix for each routing protocol (EIGRP and OSPF).

a. Within each routing protocol matrix, design two sections.
   1) one section for configuration commands
   2) one section for verification or show commands

b. Use a word processing program to save your matrix designs, or in the space provided below, one for EIGRP and one for OSPF.

Step 2: Review the chapters in this curriculum.

a. Refer to the different sections and activities presented in the curriculum.
   1) Content
   2) Labs
   3) Packet Tracer Activities

b. Record configuration commands for each protocol on their respective matrix. Note: Some commands are universal, and some are used only for IPv4 or IPv6.

c. Record verification commands used for each protocol on their respective matrix. Note: Some of these commands are universal, and some are used only with IPv4 or IPv6.

d. Leave extra, blank rows for the group or classroom portion of this activity.

Step 3: Meet as a class or with another group.

a. Compare configuration commands.

b. Compare verification commands.
c. Add any commands to each matrix mentioned in the full- or group-setting that you did not record in your own group.

d. Save your work for use with the two Capstone projects which summarize this entire course.
PT Activity 7.2.8: Scaling Networks with NAT

Topology Diagram

Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Fa0/0</td>
<td>192.168.10.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>S0/0/0</td>
<td>10.1.1.1</td>
<td>255.255.255.252</td>
</tr>
<tr>
<td>R2</td>
<td>Fa0/0</td>
<td>192.168.20.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>S0/0/0</td>
<td>10.1.1.2</td>
<td>255.255.255.252</td>
</tr>
<tr>
<td></td>
<td>S0/0/1</td>
<td>10.2.2.1</td>
<td>255.255.255.252</td>
</tr>
<tr>
<td></td>
<td>S0/1/0</td>
<td>209.165.200.225</td>
<td>255.255.255.224</td>
</tr>
<tr>
<td>R3</td>
<td>Fa0/0</td>
<td>192.168.30.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>S0/0/1</td>
<td>10.2.2.2</td>
<td>255.255.255.252</td>
</tr>
</tbody>
</table>

Addressing Table continued on next page
Addressing Table continued

<table>
<thead>
<tr>
<th>Inside Web Server</th>
<th>NIC</th>
<th>Local: 192.168.20.254</th>
<th>255.255.255.252</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NIC</td>
<td>Global: 209.165.202.131</td>
<td>255.255.255.252</td>
</tr>
<tr>
<td>PC1</td>
<td>NIC</td>
<td>192.168.10.10</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>PC3</td>
<td>NIC</td>
<td>192.168.30.10</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Outside Host</td>
<td>NIC</td>
<td>209.165.201.14</td>
<td>255.255.255.240</td>
</tr>
<tr>
<td>Public Web Server</td>
<td>NIC</td>
<td>209.265.201.30</td>
<td>255.255.255.240</td>
</tr>
</tbody>
</table>

Learning Objectives

- Configure an ACL to permit NAT.
- Configure static NAT.
- Configure dynamic NAT Overload.
- Configure the ISP router with static route.
- Test connectivity.

Introduction

NAT translates non-routable private, internal addresses into routable, public addresses. NAT has an added benefit of providing a degree of privacy and security to a network because it hides internal IP addresses from outside networks. In this activity, you will configure dynamic and static NAT. The user EXEC password is `cisco`, and the privileged EXEC password is `class`.

Task 1: Configure an ACL to Permit NAT

Step 1. Create a named standard ACL.

To define the internal addresses that are translated to public addresses in the NAT process, create a named standard ACL called R2NAT. This list is used in the NAT configuration steps that follow.

<enter your commands in PT>

Step 2. Check results.

Your completion percentage should be 11%. If not, click Check Results to see which required components are not yet completed.

Task 2: Configure Static NAT

Step 1. Configure static NAT for an inside web server.

The Inside Web Server needs to have a public IP address that never changes so that it can be accessed from outside the network. Configuring a static NAT address allows the web server to be configured with a private internal address. The NAT process then always maps packets using the public address of the server to the private address.

<enter your commands in PT>

Step 2. Check results.

Your completion percentage should be 22%. If not, click Check Results to see which required components are not yet completed.
Task 3: Configure Dynamic NAT Overload

In addition to the public IP address assigned to Inside Web Server, the ISP has assigned three public addresses for your use. These addresses are mapped to all other internal hosts that access the Internet. To allow more than three internal hosts to access the Internet at the same time, configure NAT with overload to accommodate the additional hosts. NAT overload, also called Port Address Translation (PAT), uses port numbers to distinguish packets from different hosts that are assigned the same public IP address.

Step 1. Define the address pool and configure dynamic NAT.

Enter the following commands to configure the pool of public addresses that are dynamically mapped to the internal hosts.

The first command defines the pool of three public addresses that are mapped to internal addresses. Name the pool R2POOL.

The second command instructs the NAT process to map the addresses in the pool to the addresses defined in the access list you created in Task 1.

<enter your commands in PT>

Step 2. Configure the interfaces on R2 to apply NAT.

In interface configuration mode on R2, configure each of the interfaces using the `ip nat {inside | outside}` command. Because the internal addresses are on networks connected to the Fa0/0, Serial 0/0/0, and Serial0/0/1 interfaces, use the `ip nat inside` command in configuring these interfaces. The Internet is connected to Serial0/1/0, so use the `ip nat outside` command on this interface.

Step 3. Check results.

Your completion percentage should be 89%. If not, click Check Results to see which required components are not yet completed.

Task 4: Configure the ISP with a Static Route

Step 1. Configure ISP with a static route to R2.

ISP needs a static route to the public addresses of R2. Use the following command to configure this route.

<enter your commands in PT>

Step 2. Check results.

Your completion percentage should be 100%. If not, click Check Results to see which required components are not yet completed.

Task 5: Test Connectivity

You should now be able to ping from any inside host to Outside Host or Public Web Server.
Linking Up

Objective
Describe link aggregation.

Scenario
Many bottlenecks occur on your small- to medium-sized business network, even though you have configured VLANs, STP, and other network traffic options on the company’s switches.

Instead of keeping the switches as they are currently configured, you would like to try EtherChannel as an option for, at least, part of the network to see if it will lessen traffic congestion between your access and distribution layer switches.

Your company uses Catalyst 3560 switches at the distribution layer and Catalyst 2960 and 2950 switches at the access layer of the network. To verify if these switches can perform EtherChannel, you visit the System Requirements to Implement EtherChannel on Catalyst Switches. This site allows you to gather more information to determine if EtherChannel is a good option for the equipment and network currently in place.

After researching the models, you decide to use a simulation software program to practice configuring EtherChannel before implementing it live on your network. As a part of this procedure, you ensure that the equipment simulated in Packet Tracer will support these practice configurations.

Resources
- World Wide Web connectivity
- Packet Tracer software
- Word processing or spreadsheet software

Directions

Step 1: Visit System Requirements to Implement EtherChannel on Catalyst Switches.
   a. Pay particular attention to the Catalyst 3560, 2960, and 2950 model information.
   b. Record any information you feel would be useful to deciding whether to use EtherChannel in your company.

Step 2: Create a matrix to record the information you recorded in Step 1b, including:
   a. Number of ports allowed to bundled for an EtherChannel group
   b. Maximum group bandwidth supported by bundling the ports
   c. IOS version needed to support EtherChannel on the switch model
   d. Load balancing availability
   e. Load balancing configuration options
   f. Network layers supported for EtherChannel operation

Step 3: Open Packet Tracer.
   a. Notice how many ports are available to bundle for EtherChannel on all three switch models.
   b. Check all three models to see how many EtherChannel groups you could create on each model.
   c. Make sure the IOS version is recent enough to support all EtherChannel configurations.
d. Do not configure your simulated network, but do check the models available in the Packet Tracer to make sure they will support all the EtherChannel configuration options.

Step 4: Share your matrix with another group or the class.
Digital Trolleys

Objective
Use CLI commands to verify operational status of a multiarea OSPF network.

Scenario
Your city has an aging digital trolley system based on a one-area design. All communications within this one area are taking longer to process as trolleys are being added to routes serving the population of your growing city. Trolley departures and arrivals are also taking a little longer, because each trolley must check large routing tables to determine where to pick up and deliver residents from their source and destination streets.

A concerned citizen has come up with the idea of dividing the city into different areas for a more efficient way to determine trolley routing information. It is thought that if the trolley maps are smaller, the system might be improved because of faster and smaller updates to the routing tables.

Your city board approves and implements the new area-based, digital trolley system. But to ensure the new area routes are more efficient, the city board needs data to show the results at the next open board meeting.

Complete the activity directions as stated below.

Save your work and explain the differences between the old, single area and new, multiarea system to another group or the entire class.

Required Resources
- Packet Tracer software
- Word processing software

Directions

Step 1: Map the single-area city trolley routing topology.
   a. Use Packet Tracer to map the old routing topology for the city. Cisco 1941 Integrated Services Routers (ISRs) are preferred.
   b. Create a core area and place one of the routers in the core area.
   c. Connect at least two routers to the core area router.
   d. Choose to connect two more routers to the routers from Step 1c or create loopback addresses for the LAN interfaces on the routers from Step 1c.
   e. Address the connected links or interfaces using IPv4 and VLSM.
   f. Configure OSPF on each router for area 0 only.
   g. Ping all routers to ensure full connectivity within the entire area.

Step 2: Map the multiarea city trolley routing topology.
   a. Use your cursor to highlight all devices from Step 1, and copy and paste them to another area of the Packet Tracer desktop.
b. Assign at least three areas to your topology. One must be the backbone (or core area) and the other two areas will be joined to the backbone area using current routers, which will now become area border routers.

c. Configure the appropriate routers to their new area assignments. Remove old area configuration commands and assign new area commands to the appropriate interfaces.

d. Save each router’s changes as you make changes.

e. When complete, you should have three areas represented on the topology and all routers should be able to ping each other throughout the network.

f. Use the drawing tool and identify your areas by drawing circles or rectangles around the three areas.

g. Save your work.

**Step 3: Verify the network for city council members.**

a. Use at least three commands learned (or used in this chapter) to help the city council prove that the new area, digital trolley routing topology works.

b. Save a copy of topology graphics and verification commands comparisons in table format to a word processing file or in the space provided below.

c. Share your work with another group or the class. You may also want to add this activity and its files to a portfolio for this course.