DESGN

Designing for Cisco Internetwork Solutions

Version 2.1

Lab Guide

Text Part Number: 97-2918-01

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED “AS IS.” CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

Table of Contents

Lab Guide

Overview

This guide presents the instructions and other information concerning the lab activities for this course. You can find the solutions in the lab activity Answer Key.

Outline

This guide includes these activities:

- Case Study 1-1: ACMC Hospital Network Upgrade Information
- Case Study 2-1: ACMC Hospital Network Structure and Modularity
- Case Study 3-1: ACMC Hospital Network Campus Design
- Case Study 4-1: ACMC Hospital Network WAN Design
- Case Study 5-1: ACMC Hospital Network IP Addressing and Routing Protocol Design.
- Case Study 6-1: ACMC Hospital Network Security Design.
- Case Study 7-1: ACMC Hospital Network Voice Transport Considerations.
- Case Study 8-1: ACMC Hospital Network Wireless Networking Considerations.
- Case Study 8-2: Connecting More Hospitals to the ACMC Hospital Network.
- Answer Key
- Course Worksheets

Case Study Guidelines

Follow these guidelines for each case study:

- Use the scenarios, information, and parameters that are provided with each task of the case study. If there are ambiguities, make reasonable assumptions and proceed. For all the tasks, use the initial customer scenario and build on the solutions that you have developed so far.
- Use any documentation, books, white papers, and so on.
- Use any design strategies that you feel are appropriate.
- In each task of the case study, you act as a network design consultant. Make creative proposals to help the enterprise accomplish its goals. When your ideas differ from the provided solutions, justify your ideas.
- To maximize class interaction and make good use of time, the instructor will ask you to work in groups. Each group should reach consensus on the answers to the questions. If your group is assigned to present a design, pick one member to present. Provide that person with the notes and drawings that are needed to successfully present the design to the class. After a brief presentation of the design, presenters will be expected to answer questions and explain the group design decisions and reasoning.
- To give the student the opportunity to design a modern network, the initial topology was intentional designed with older technology.

Case Study 1-1: ACMC Hospital Network Upgrade Information

This case study enables you to practice the skills and knowledge that you learned in the module.

Activity Objective

In this activity, you will create a high-level design for updating the ACMC Hospital network. After completing this activity, you will be able to meet these objectives:

- Document the requirements of the organization
- Document the existing network
- Identify and request missing information
- Outline the major design tasks for the network

Visual Objective

There is no visual objective for this case study.

Required Resources

The following are the resources and equipment that are required to complete this activity:

- Case study guidelines, presented in the Lab Guide Overview
- ACMC Hospital network upgrade scenario
- A workgroup of two to four learners
- Blank sheets of paper and a pencil

ACMC Hospital Network Upgrade Scenario

This case study analyzes the network infrastructure of Acme County Medical Center (ACMC) Hospital, a fictitious, small, county hospital. Hospital management gave you a short description of the current situation and its plans. It is your job, as an independent network designer, to identify all of the organizational requirements and data that will allow you to provide an effective solution.

Organizational Facts

ACMC is a regional hospital with approximately 500 staff members supporting up to 1000 patients. The hospital is interested in updating its main facility from Brand X equipment in its Layer 2 campus. You are meeting with hospital management to define its requirements.

There are 15 buildings on the hospital campus, plus five small remote clinics. There are seven floors in each of the two main hospital buildings, with four wiring closets per floor in the main buildings. The auxiliary building, the Children’s Place, is connected by fiber to the main buildings. (The three main building switches are connected by fiber into a ring.) The Children’s Place has three floors, with three wiring closets per floor. The other 12 campus buildings are smaller office and support facilities, with 10 to 40 people per building that are located on one or two floors.

The network architect is new to the hospital. The hospital management is aggressively expanding clinic and alternative emergency room presence within Acme County. Due to general population growth, there are also plans to enlarge the main campus. The hospital is doing fairly well financially. It wishes to selectively deploy innovative technology for better patient care and high productivity. Network downtime or slowness has been affecting patient care. Network manageability is important because ACMC has a tradition of basing operations on small support staffs with high productivity. The timeframe for the ACMC upgrade is 6 to 12 months.

Current Situation

The current network uses inexpensive switches that were purchased over time from several vendors. They comply with various standards, depending on when they were purchased. They are not SNMP-manageable switches, although a small amount of information is available from each switch via the web or command-line interface (CLI).

There is a main switch within each of the three main buildings. One floor switch from each floor connects to the main switch. The other switches connect either directly to the floor switch or via a daisy chain of switches, depending on which was most convenient at the time of installation.

The small outlying buildings have one or two 24-port switches. One of these switches connects back to one of the main building switches via fiber. If there is a second switch, it connects via the first switch.

Currently, the staff VLAN spans the entire campus. There is no Layer 3 switching. The address space is 172.16.0.0 /16. Addresses were coded sequentially into PCs as they were deployed. Although the staff would like to deploy DHCP, it has not yet done so.

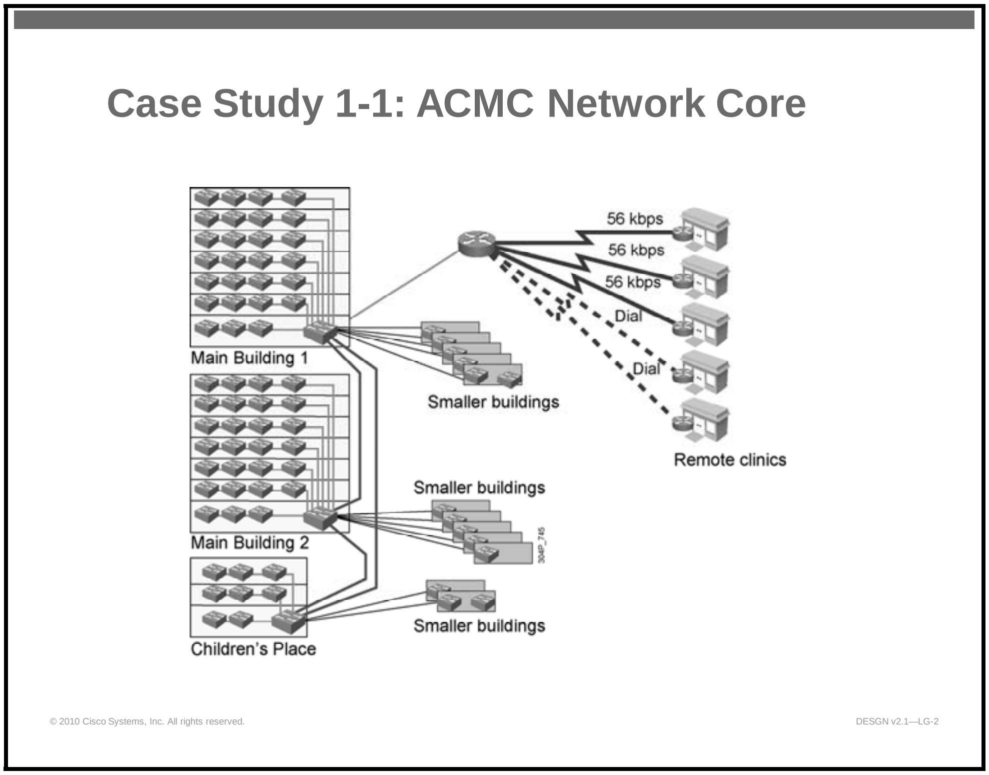
The organization is currently running standard office applications, plus some specialized medical programs running over IP. Radiology, Oncology, and other departments perform medical imaging. As these departments acquire new tools, they are adding real-time motion to the highly detailed medical images. This process requires large amounts of bandwidth. All of the new servers are capable of using Gigabit or GEC connectivity.

Many servers are currently located in various closets. Many of the servers lack UPS or proper environmental controls. The staff rolls a tape backup cart to each server closet to back up each server. There are about 40 centrally located servers in one raised floor server room and 30 other servers that are distributed around the campus near their users. The server room, the cafeteria, and other non-networked areas comprise the first floor of Main Building 1.

Hospital Support Services has been experimenting with workstations on wheels (WoWs). It has proved inefficient to move these WoWs and plug them into an Ethernet jack.

The WAN uses DS0 (56 kb/s) links to three of the remote clinics and PC dialup connectivity to the other two. The one router uses static routing that was configured by a previous network designer.

The staff members have frequently complained about slow response times. There appears to be severe congestion of the LAN, especially during peak hours. The staff provided you with a copy of the recent network diagram.



Case Study 1-1: ACMC Network Core

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-2

You believe that the current situation does not provide for future growth, high reliability, and ease of management.

Plans and Requirements

The introduction of new applications will result in an additional load on the links to remote clinics. The expected tighter integration and growth of remote offices will even further increase the traffic load on the WAN links. The hospital would like to upgrade the WAN infrastructure to provide sufficient bandwidth between the remote clinics and headquarters. At the same time, the hospital would like to find a solution for better convergence during network failures. Management is aware of the drawbacks of the current IP addressing scheme and is seeking a better solution.

ACMC Hospital Network Upgrade Tasks

Complete these steps:

Step 1 Read the ACMC Hospital Network Upgrade scenario information completely before beginning the activity. Allow 10 minutes for reading.

Step 2 Discuss the scenario with your group. Allow 20 minutes for a discussion.

Step 3 Document the ACMC Hospital requirements in the “Requirements” table.

Requirements

Requirement	Comment

Step 4 In the “Missing Items” table, document any information that you think is missing from the scenario and that you consider necessary for the design. Teams ask questions of “the customer” (the instructor) to obtain the missing details. Allow 10 minutes for this step.

Missing Items

Missing Item	Customer Response (Provided by Instructor)

Step 5 Outline the major design areas that you need to address in designing the solution for the given customer scenario. List the tasks, and provide a brief comment for each task in the "Major Design Tasks" table.

Note The Cisco Network Architectures for the Enterprise is covered in "Case Study 2-1: ACMC Hospital Network Structure and Modularity." However, you should already be aware of the terms such as campus, WAN, and server farm, and you may discuss broad areas of design using those terms.

Major Design Tasks

Design Tasks

Step 6 Present your design to the class. Be prepared to justify your design choices.

Activity Verification

You have completed this activity when the instructor has verified your case study solution, and you have justified any major deviations from the solution that is supplied by the instructor.

Case Study 2-1: ACMC Hospital Network Structure and Modularity

This case study enables you to practice the skills and knowledge that you learned in the module.

Activity Objective

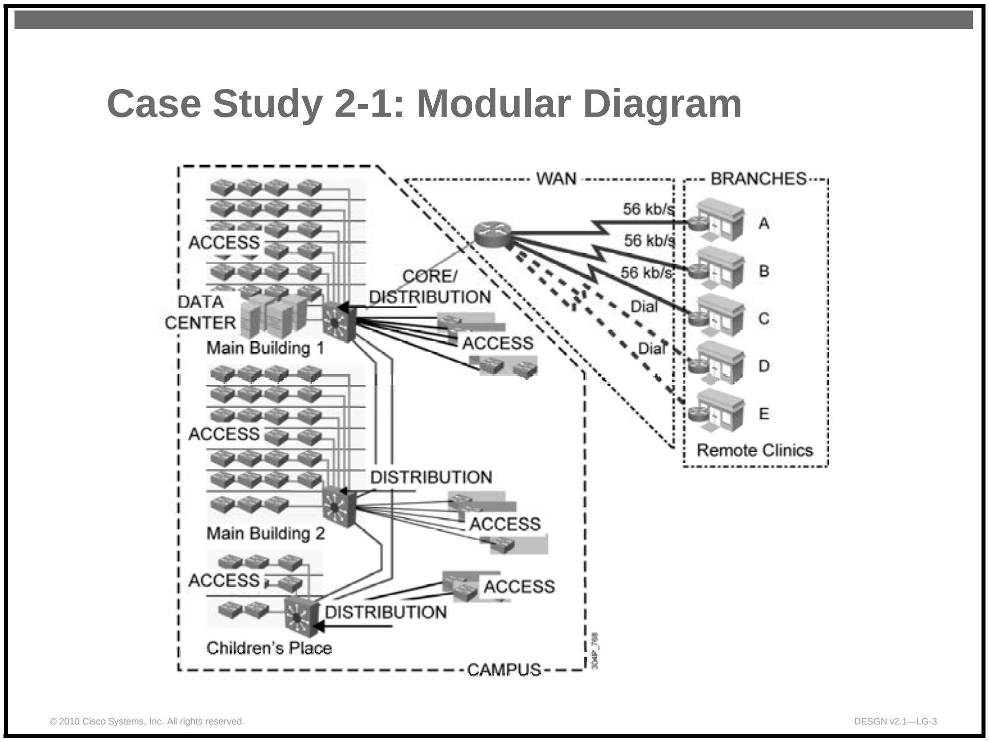
In this activity, you will apply the Cisco Network Architectures for the Enterprise to the ACMC Hospital network requirements. You will develop a high-level sketch of the planned network hierarchy. You will also present your diagram and high-level design features to the class.

After completing this activity, you will be able to meet these objectives:

- Diagram the planned network hierarchy
- Discuss and document some details of the design of each of the modules in the planned design
- Discuss and document the use of infrastructure services within your design at a high level

Visual Objective

The visual objective is to diagram the planned network hierarchy.



Case Study 2-1: Modular Diagram

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-3

Required Resources

The following are the resources and equipment that are required to complete this activity:

- Case study guidelines, presented in the Lab Guide Overview
- ACMC Hospital case study scenario
- A workgroup of two to four learners
- Blank sheets of paper and a pencil

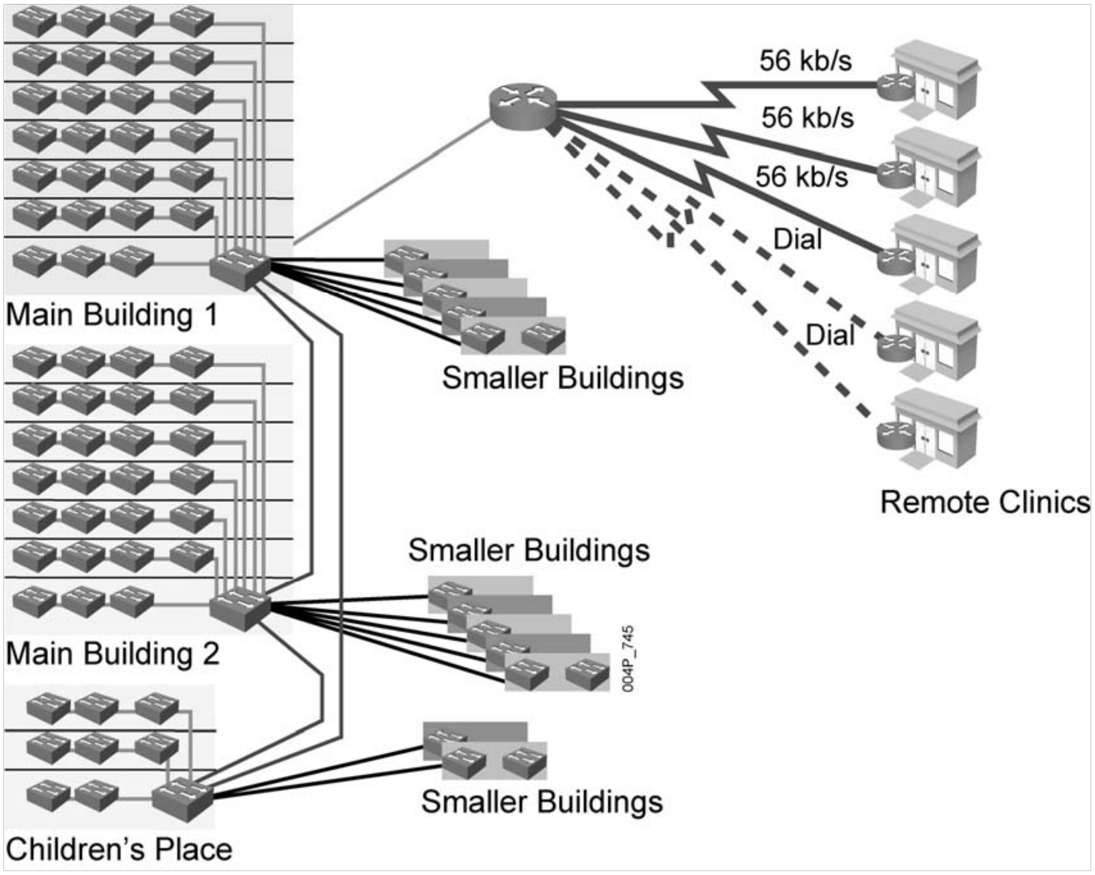
ACMC Hospital Network Structure and Modularity Tasks

Complete these steps.

Step 1 Consider each of the Cisco Network Architectures for the Enterprise modules and components. At a high level, determine how and where they belong in your design for the future ACMC Hospital network.

- Cisco Enterprise Campus Architecture: Campus infrastructure module (campus core layer, building distribution layer, and building access layer) and server farm module
- Cisco Enterprise WAN and MAN Architecture: E-commerce module, Internet connectivity module, remote access and VPN module, and WAN and MAN and site-to-site VPN module
- Cisco Enterprise Branch Architecture
- Cisco Enterprise Data Center Architecture
- wq

Mark up the existing diagram with your conclusions. Identify each of the Cisco Network Architectures for the Enterprise modules. Be as specific as possible. You will add detail to individual modules later.



Step 2 On a piece of paper, list three to five key considerations or functions for each module. If the module is not being used, state that.

Step 3 You provided a written document to the customer, describing the customer requirements you heard during your initial ACMC discussions. Since then, discussions with ACMC have identified these additional requirements:

- The staff needs Internet access for purchasing supplies and reviewing research documents and new medical products.
- ACMC has a web server for patient communications and community relations that is called the “Text a Nurse” service. This service allows a patient to send a text message to the hospital for medical advice.

Step 4 How does this new information change the design? Add the new information to your high-level design, and update your list of modules and considerations.

Step 5 Which of these infrastructure or network services are immediately applicable to your design, based on the ACMC business objectives and technical requirements from “Case Study 1-1: ACMC Hospital Network Upgrade Information”? Are there specific locations or modules where some of these services are particularly relevant? Identify these locations or modules in your diagram. Be prepared to describe these services during your presentation.

- Security services
- Voice services
- Network management
- High availability
- QoS

Step 6 Should your design incorporate redundancy? Does it do so? Make sure that your diagram shows appropriate redundancy or indicates the modules or locations where redundancy is appropriate.

Step 7 Present your design to the class. Be prepared to justify your design choices.

Activity Verification

You have completed this activity when you have created a high-level design diagram and have documented the relevant Cisco Network Architectures for the Enterprise modules, including three to five considerations for each relevant module.

If time permits, the questions and comments in response to your presentation will provide valuable feedback for your design. This feedback offers you an opportunity to see what aspects of this design you might have overlooked.

Case Study 3-1: ACMC Hospital Network Campus Design

This case study enables you to practice the skills and knowledge that you learned in the module.

Activity Objective

In this activity, you will create a high-level design for the Cisco Enterprise Campus Architecture and Cisco Data Center Architecture of the ACMC Hospital network. After completing this activity, you will be able to meet these objectives:

- Describe the proposed campus design
- Document and diagram the proposed campus design

Visual Objective

The visual objective is to diagram the proposed campus design solution.

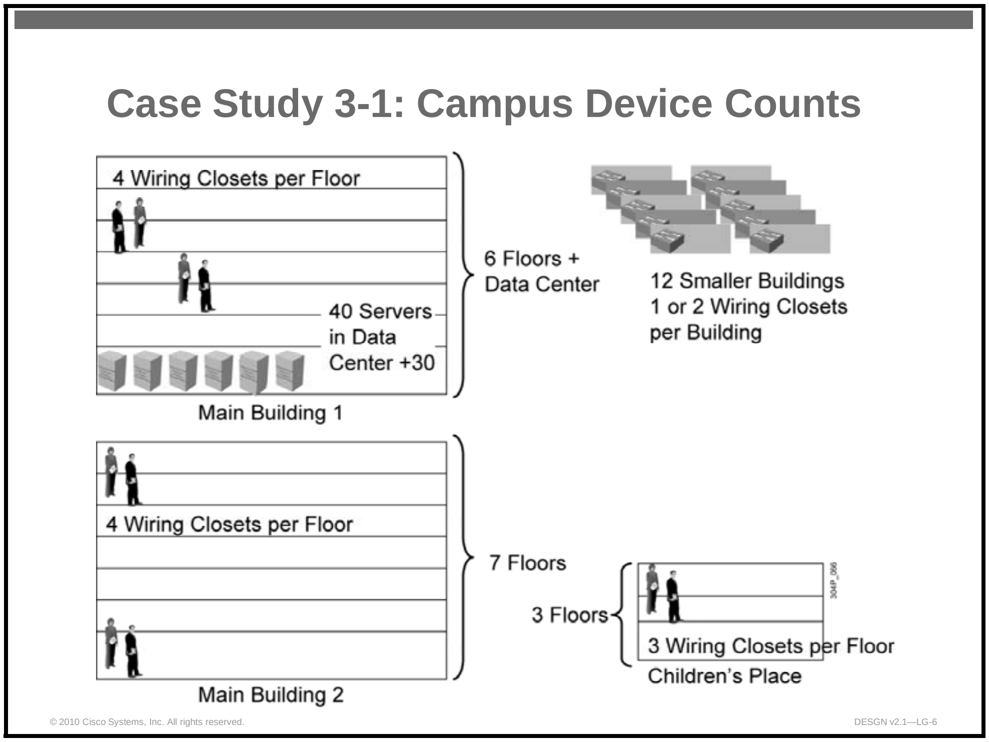
Required Resources

The following are the resources and equipment that are required to complete this activity:

- Case study guidelines, presented in the Lab Guide Overview
- ACMC Hospital case study scenario
- A workgroup of two to four learners
- Blank sheets of paper and a pencil

ACMC Hospital Case Study Scenario

In this section, you will fill in the details of the design, including port counts and cabling. This case study focuses on the enterprise campus and server farm. This diagram shows the campus device counts.



Case Study 3-1: Campus Device Counts

4 Wiring Closets per Floor
40 Servers in Data Center +30
6 Floors + Data Center
Main Building 1
12 Smaller Buildings 1 or 2 Wiring Closets per Building
4 Wiring Closets per Floor
7 Floors
Main Building 2
3 Floors
3 Wiring Closets per Floor
Children's Place

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-6

Port Count Details

The hospital has 500 staff members and 1000 patients. Specifically, buildings A through D have 10 people each, buildings E through J have 20 people each, and buildings K through L have 40 people each. Assume that each building needs as many spare ports as there are people.

Each floor of the Children's Place has 60 people on it. Each floor of the main buildings has about 75 people on it, except the first floor of Main Building 1, which has only the server farm with 40 servers. Assume that each floor needs as many spare ports as there are people. (Each patient room or staff position has two jacks, and spare server ports should be provided to allow for migration of all servers to the server farm.)

Cabling Details

Assume that the hospital has structured cabling with plenty of multimode fiber (MMF) in the risers and plenty of fiber between buildings along all paths that are shown in the diagrams in "Case Study 1-1: ACMC Hospital Network Upgrade" and "Case Study 2-1: Defining Modularity."

Note If there is not enough fiber, either the hospital will have to install the fiber, or you will have to adjust your design to the existing cabling. However, it is best to work out an ideal design before making any adjustments.

ACMC Hospital Network Campus Design Tasks

Complete these steps:

Step 1 Determine the location, quantity, and size of the core switch or switches and what connections there should be within the core.

Step 2 Determine the location of distribution layer switches or whether a collapsed core or a core/distribution approach makes more sense. If you use a design with distribution layer switches, determine their location and size, how they connect to the core, the use of VLANs versus Layer 3 switching, and so on.

Step 3 Determine the location and size of access layer switches. Complete the "Port Counts by Location" table.

Port Counts by Location

Location	Counts	Counts with Spares	Comments
Main Building 1 (Per Floor)			six floors
Main Building Server Farm			
Main Building 2 (Per Floor)			seven floors
Children's Place (Per Floor)			three floors
Buildings A–D			
Buildings E–J			
Buildings K–L			

Step 4 Determine how the access layer switches connect to the distribution layer switches (or to the combined core/distribution switch or switches). Include such information as speeds, cabling type, and location.

Step 5 Verify that you have the correct port counts for all the switches in your design.

Step 6 Determine how you will manage the server farm. Do you propose connecting the servers to the core switch or switches? To server aggregation switches? Other? If you use server access or distribution switches, determine how they all connect to each other and to the core.

Step 7 How do the 12 additional buildings (buildings A through L) affect your design? Be sure to determine what size switches to use in each building, and how they connect back to the distribution or core layers.

Step 8 Other than port counts, speeds, and feeds, is there any other information that would benefit your design?

Step 9 Determine appropriate Cisco switch models for each part of your campus design. Use these links to assist you:

- The Cisco switch main page at http://www.cisco.com/en/US/products/hw/switches/index.html
- The Cisco switch comparison page at http://www.cisco.com/en/US/products/hw/switches/products_category_buyers_guide.html
- The Cisco *Catalyst Switch Solution Finder* at http://www.cisco.com/en/US/partner/products/hw/switches/products_promotion0900aecd8050364f.html

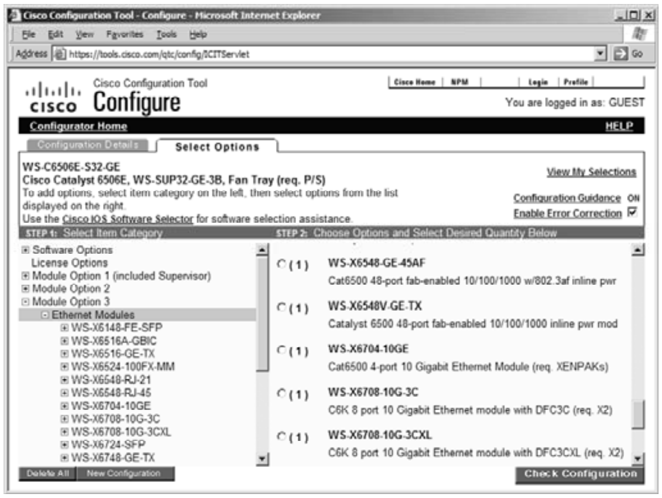
If time permits and you have access to a computer and the Internet, perform Steps 10 and 11.

Step 10 (Optional) Use the Cisco Dynamic Configuration Tool to configure one or more of the switches in your design.

Note This process is easier and faster if you use the same two or three switch models repeatedly in your design, possibly with different numbers of blades in them. Also, there are not many options for the smaller switches in the configuration tool.

- Start at http://www.cisco.com/en/US/ordering/or13/or8/ordering_ordering_help_dynamic_configuration_tool_launch.html. This link requires a valid Cisco.com username and password.
- Click to launch the tool. After you select the product family and the starting bundle or chassis, this screen appears.

Cisco Ordering Dynamic Configuration Tool



Cisco Configuration Tool - Configure - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go
Cisco Home | NPM | Login | Profile
cisco
Configurator Home
HELP
Configuration Details
Select Options
View My Selections
Delete All
New Configuration
Check Configuration

https://tools.cisco.com/qtc/config/ICITServlet

Cisco Configuration Tool
Configure

You are logged in as: GUEST

WS-C6506E-S32-GE
Cisco Catalyst 6506E, WS-SUP32-GE-3B, Fan Tray (req. P/S)
To add options, select item category on the left, then select options from the list displayed on the right.
Use the Cisco IOS Software Selector for software selection assistance.

Configuration Guidance ON
Enable Error Correction ☑

STEP 1: Select Item Category

- ⊞ Software Options
- License Options
- ⊞ Module Option 1 (included Supervisor)
- ⊞ Module Option 2
- ⊟ Module Option 3
  - ⊟ Ethernet Modules
    - ⊞ WS-X6148-FE-SFP
    - ⊞ WS-X6516A-GBIC
    - ⊞ WS-X6516-GE-TX
    - ⊞ WS-X6524-100FX-MM
    - ⊞ WS-X6548-RJ-21
    - ⊞ WS-X6548-RJ-45
    - ⊞ WS-X6704-10GE
    - ⊞ WS-X6708-10G-3C
    - ⊞ WS-X6708-10G-3CXL
    - ⊞ WS-X6724-SFP
    - ⊞ WS-X6748-GE-TX

STEP 2: Choose Options and Select Desired Quantity Below

○ (1) **WS-X6548-GE-45AF**
Cat6500 48-port fab-enabled 10/100/1000 w/802.3af inline pwr

○ (1) **WS-X6548V-GE-TX**
Catalyst 6500 48-port fab-enabled 10/100/1000 inline pwr mod

○ (1) **WS-X6704-10GE**
Cat6500 4-port 10 Gigabit Ethernet Module (req. XENPAKs)

○ (1) **WS-X6708-10G-3C**
C6K 8 port 10 Gigabit Ethernet module with DFC3C (req. X2)

○ (1) **WS-X6708-10G-3CXL**
C6K 8 port 10 Gigabit Ethernet module with DFC3CXL (req. X2)

DESGN v2.1—LG-7

Step 11 (Optional) Develop a Bill of Materials (BOM) that lists switch models, numbers, prices, and total price. If you have access to a PC with spreadsheet software, you may use a spreadsheet to develop the BOM. If not, work on paper. The following is a sample BOM.

Sample Bill of Materials

9/8/2010 11:05

Version 1

Part Number	Description	Unit Price	Qty	Extended Price
WS-C2960S-24TS-L	Catalyst 2960 24 10/100/1000 + 2T/SFP LAN Base Image	$1500	70	$105,000
	Generic SFP	$400	140	$56,000
WS-C3750G-48TS-E	Catalyst 3750 48 10/100/1000T + 4 SFP + IPS Image	$10,000	34	$340,000
	Generic SFP	$400	136	$54,400
WS-C4507R	Catalyst 4500 Chassis (7-Slot), Fan, No Power Supply, Redundant Supervisor Capable	$7000	2	$14,000
PWR-C45-1400AC	Catalyst 4500 1400W AC Power Supply (Data Only)	$1000	2	$2000
WS-X4516	Catalyst 4500 Supervisor V (2 Gigabit Ethernet),Console (RJ-45)	$11,000	2	$22,000
S4KL3E-12220EWA	Cisco IOS Enhanced Layer 3 Catalyst 4500 Supervisor 4/5 (OSPF, EIGRP, IS-IS)	$10,000	2	$20,000
WS-X4306-GB	Catalyst 4500 Gigabit Ethernet Module, 6-Ports (GBIC)	$2100	6	$12,600
Total list price				$626,000
Customer discount				15%
Discounted price				$532,100

Because looking up component prices and building a BOM can be time-consuming, use the “Sample Price List” table for abbreviated and simplified price list information. The prices that are shown are not actual equipment prices and are loosely derived from Cisco list prices at the time this course was written.

Sample Price List

Category	Part Number	Description	Fictional Price
Port Transceiver Modules			
		Generic SFP	$400
		Generic GBIC	$400
		Generic LR Xenpack	$4,000
Cisco Catalyst 2960 Series Workgroup Switches			
	WS-C2960-24LT-L	Catalyst 2960 24 10/100 (8 PoE)+ 2 1000BT LAN Base Image	$2,500
	WS-C2960-24PC-L	Catalyst 2960 24 10/100 PoE + 2 T/SFP LAN Base Image	$1,300
	WS-C2960G-48TC-L	Catalyst 2960 48 10/100/1000, 4 T/SFP LAN Base Image	$4,500
	WS-C2960-48TT-L	Catalyst 2960 48 10/100 Ports + 2 1000BT LAN Base Image	$2,500
	WS-C2960G-24TC-L	Catalyst 2960 24 10/100/1000, 4T/SFP LAN Base Image	$3,300
	WS-C2960G-48TC-L	Catalyst 2960 48 10/100/1000, 4T/SFP LAN Base Image	$6,000
Cisco Catalyst 3560 Series			
	WS-C3560G-48TS-S	Catalyst 3560 48 10/100/1000T + 4 SFP Standard Image	$8,000
	WS-C3560G-24TS-S	Catalyst 3560 24 10/100/1000T + 4 SFP Standard Image	$4,800
	WS-C3560-48TS-S	Catalyst 3560 48 10/100 + 4 SFP Standard Image	$5,000
	WS-C3560-24TS-S	Catalyst 3560 24 10/100 + 2 SFP Standard Image	$3,000
Cisco IOS Upgrades for the Catalyst 3560 (EMI = Layer 3 image)			
	CD-3560-EMI=	Enhanced Multilayer Image upgrade for 3560 10/100 models	$2,000
	CD-3560G-EMI=	Enhanced Multilayer Image upgrade for 3560 Gigabit Ethernet models	$4,000

Category	Part Number	Description	Fictional Price
Cisco Catalyst 3750 Series 10/100/1000, Gigabit Ethernet, 10GE Workgroup Switch			
	WS-C3750G-24T-S	Catalyst 3750 24 10/100/1000T Standard Multilayer Image	$6,000
	WS-C3750G-24TS-S1U	Catalyst 3750 24 10/100/1000 + 4 SFP Std Multilayer 1RU	$7,000
	WS-C3750G-48TS-S	Catalyst 3750 48 10/100/1000T + 4 SFP Standard Multilayer	$14,000
	WS-C3750E-24PD-S	Catalyst 3750E 24 10/100/1000 PoE+2*10GE(X2),750W,IPB s/w	$12,000
	WS-C3750G-12S-S	Catalyst 3750 12 SFP Standard Multilayer Image	$8,000
Cisco Catalyst 3750 Series 10/100 Workgroup Switches			
	WS-C3750-24TS-S	Catalyst 3750 24 10/100 + 2 SFP Standard Multilayer Image	$4,000
	WS-C3750-48TS-S	Catalyst 3750 48 10/100 + 4 SFP Standard Multilayer Image	$7,000
Cisco IOS Upgrades for the Catalyst 3750			
	CD-3750-EMI=	Enhanced Multilayer Image upgrade for 3750 Fast Ethernet models	$2,000
	CD-3750G-EMI=	Enhanced Multilayer Image upgrade for 24-port 3750 Gigabit Ethernet models	$4,000
	CD-3750G-48EMI=	Enhanced Multilayer Image upgrade for 48-port 3750 Gigabit Ethernet models	$8,000
	3750-AISK9-LIC-B=	Advanced IP Services upgrade for 3750 Fast Ethernet models running SMI	$5,000
	3750G-AISK9-LIC-B=	Advanced IP Services upgrade for 3750 Gigabit Ethernet models running SMI	$7,000
	3750G48-AISK9LC-B=	Advanced IP Services upgrade for 3750G-48 running SMI	$11,000
Cisco Catalyst 4948 Switch			
	WS-C4948-S	Catalyst 4948, IPB software, 48-Port 10/100/1000+4 SFP, 1-AC power supply	$10,500
	WS-C4948-E	Catalyst 4948, ES software, 48-Port 10/100/1000+4 SFP, 1-AC power supply	$14,500
	WS-C4948-10GE-S	Catalyst 4948, IPB software, 48*10/100/1000+2*10GE(X2), 1-AC power supply	$17,500
	WS-C4948-10GE-E	Catalyst 4948, ES Image, 48*10/100/1000+2*10GE(X2), 1-AC power supply	$21,500
Cisco Catalyst 4948 Software			
	S49L3K9-12220EWA	Cisco Catalyst 4948 IOS Stand Layer 3 3DES (RIP, St. Routes, IPX, AT)	$0
	S49L3EK9-12220EWA	Cisco Catalyst 4948 IOS Enhanced Layer 3 3DES (OSPF, EIGRP, IS-IS, BGP)	$4,000
	S49ESK9-12225SG	Cisco Catalyst 4900 IOS Enterprise Services SSH	$4,000

Category	Part Number	Description	Fictional Price
Cisco Catalyst 4500 Chassis			
	WS-C4510R	Catalyst 4500 Chassis (10-Slot), fan, no power supply, Redundant Supervisor Capable	$12,500
	WS-C4507R	Catalyst 4500 Chassis (7-Slot), fan, no power supply, Redundant Supervisor Capable	$10,000
	WS-C4506	Catalyst 4500 Chassis (6-Slot),fan, no power supply	$5,000
	WS-C4503-E Cat4500 E-Series 3-Slot Chassis, fan, no ps	Cat4500 E-Series 3-Slot Chassis, fan, no ps	$1,000
	WS-C4506-S2+96	Catalyst 4506 Bundle, 1x 1000AC, 1x S2+, 2x WS-X4148-RJ	$16,800
	WS-C4503-S2+48	Catalyst 4503 Bundle, 1x 1000AC, 1x S2+, 1x WS-X4148-RJ	$10,000
Cisco Catalyst 4500 Non-PoE Power Supplies			
	PWR-C45-1400AC	Catalyst 4500 1400W AC Power Supply (Data Only)	$1,500
	PWR-C45-1000AC	Catalyst 4500 1000W AC Power Supply (Data Only)	$1,000
Cisco Catalyst 4500 Supervisor Engines			
	WS-X4516-10GE	Catalyst 4500 Supervisor V-10GE, 2x10GE (X2) and 4x1GE (SFP)	$20,000
	WS-X4516-10GE/2	Catalyst 45xxR Supervisor V-10GE, 2x10GE (X2) or 4x1GE (SFP)	$20,000
	WS-X4516	Catalyst 4500 Supervisor V (2 Gigabit Ethernet), Console(RJ-45)	$16,500
	WS-X4515	Catalyst 4500 Supervisor IV (2 Gigabit Ethernet), Console(RJ-45)	$12,000
	WS-X4013+10GE	Catalyst 4500 Supervisor II+10GE, 2x10GE (X2), and 4x1GE (SFP)	$12,000
	WS-X4013+	Catalyst 4500 Supervisor II-Plus (IOS), 2GE, Console (RJ-45)	$6,000
	WS-X4013+TS	Catalyst 4503 Supervisor II-Plus-TS, 12 10/100/1000 PoE+8 SFP slots	$6,000
Cisco Catalyst 4500 10/100 line cards			
	WS-X4148-RJ	Catalyst 4500 10/100 Auto Module, 48-Ports (RJ-45)	$4,500
	WS-X4124-RJ45	Catalyst 4500 10/100 Module, 24-Ports(RJ-45)	$2,500
	WS-X4148-RJ21	Catalyst 4500 10/100 Module, 48-Ports Telco (4xRJ21)	$4,500
	WS-X4232-GB-RJ	Catalyst 4500 32-10/100 (RJ-45), 2-Gigabit Ethernet (GBIC)	$4,500
	WS-X4232-RJ-XX	Catalyst 4500 10/100 Module, 32-ports(RJ-45) + Modular uplinks	$3,500
Cisco Catalyst 4500 10/100/1000 line cards			
	WS-X4548-GB-RJ45	Catalyst 4500 Enhanced 48-Port 10BASE-T, 100BASE-T, 1000BASE-T (RJ-45)	$5,500
	WS-X4506-GB-T	Catalyst 4500 6-Port 10/100/1000 PoE or SFP (Optional)	$3,500
	WS-X4448-GB-RJ45	Catalyst 4500 48-Port 10/100/1000 Module (RJ-45)	$6,000

Category	Part Number	Description	Fictional Price
	WS-X4424-GB-RJ45	Catalyst 4500 24-port 10/100/1000 Module (RJ-45)	$3,500
Cisco Catalyst 4500 1000 Base-X Gigabit Ethernet line cards			
	WS-X4448-GB-SFP	Catalyst 4500 48-Port 1000BASE-X (SFPs Optional)	$16,500
Cisco Catalyst 4500 Series Supervisor IOS Software Options			
	S4KL3-12220EWA	Cisco IOS Basic Layer 3 Catalyst 4500 Supervisor 2+/4/5 (RIP, St. Routes, IPX, AT)	$0
	S4KL3E-12220EWA	Cisco IOS Enhanced Layer 3 Catalyst 4500 Supervisor 4/5 (OSPF, EIGRP, IS-IS)	$10,000
Catalyst 6500 Sup720-10G Bundles			
	VS-C6504E-S720-10G	Catalyst Chassis+Fan Tray+Sup720-10G; IP Base ONLY incl. VSS	$33,000
	VS-C6506E-S720-10G	Catalyst Chassis+Fan Tray+Sup720-10G; IP Base ONLY incl. VSS	$43,000
	VS-C6509E-S720-10G	Catalyst Chassis+Fan Tray+Sup720-10G; IP Base ONLY incl. VSS	$49,000
	VS-C6509VE-S72010G	Catalyst Chassis+Fan Tray+Sup720-10G; IP Base ONLY incl. VSS	$49,000
Cisco Catalyst 6500 Series Supervisor 32-10GE Bundles—Top Sellers			
	WS-C6503E-S32-10GE	Cat6503E chassis, WS-Supervisor 32-10GE-3B, Fan Tray (req. power supply)	$23,000
	WS-C6504E-S32-10GE	6504-E Chassis + Fan Tray + Supervisor 32-10GE	$23,000
	WS-C6506E-S32-10GE	Cat6506E chassis, WS-Supervisor 32-10GE-3B, Fan Tray (req. power supply)	$26,000
	WS-C6509E-S32-10GE	Cat6509E chassis, WS-Supervisor 32-10GE-3B, Fan Tray (req. power supply)	$30,000
Cisco Catalyst 6500 Series AC Power Supplies—Top Sellers			
	PWR-2700-AC/4	2700W AC power supply for Cisco 7604/6504-E	$3,000
	WS-CAC-3000W	Catalyst 6500 3000W AC power supply	$3,000
	WS-CAC-6000W	Cat6500 6000W AC power supply	$5,000
Cisco Catalyst 6500 Series 10 Gigabit Ethernet—Top Sellers			
	WS-X6704-10GE	Cat6500 4-port 10 Gigabit Ethernet Module (req. XENPAKs)	$20,000
	S-67-10GE-C2	Cat6500, 1x6704-10 GE, 1xWS-F6700-DFC3B, 2xXENPAK-10GB-SR=	$33,500
Cisco Catalyst 6500 Series Gigabit Ethernet—Top Sellers			
	WS-X6408A-GBIC	Catalyst 6000 8-port Gigabit Ethernet, Enhanced QoS (req. GBICs)	$10,000
	WS-X6516A-GBIC	Catalyst 6500 16-port Gigabit Ethernet Module, fabric-enabled (req. GBICs)	$15,000

Category	Part Number	Description	Fictional Price
	WS-X6724-SFP	Catalyst 6500 24-port Gigabit Ethernet Module, fabric-enabled (req. SFPs)	$15,000
	WS-X6748-SFP	Catalyst 6500 48-port Gigabit Ethernet Module, fabric-enabled (req. SFPs)	$25,000
Cisco Catalyst 6500 Series 10/100/1000—Top Sellers			
	WS-X6148A-GE-TX	Catalyst 6500 48-port 10/100/1000 with Jumbo Frame, RJ-45	$7,000
	WS-X6548-GE-TX	Catalyst 6500 48-port fabric-enabled 10/100/1000 Module	$12,000
	WS-X6748-GE-TX	Cat6500 48-port 10/100/1000 Gigabit Ethernet Module: fabric enabled, RJ-45	$15,000
Cisco Catalyst 6500 Series 10/100—Top Sellers			
	WS-X6148A-RJ-45	Catalyst 6500 48-Port 10/100 with TDR, upgradable to PoE 802.3af	$6,000
	WS-X6148-RJ-21	Catalyst 6500 48-Port 10/100 upgradable to voice, RJ-21	$6,000
	WS-X6196-RJ-21	Catalyst 6500 96-Port 10/100 upgradable to PoE 802.3af	$10,500
Cisco Catalyst 6500 Series Supervisor—Top Sellers			
	S323IBK9-12218SXF	Cisco Catalyst 6000 IP Base SSH	$0
	S323ESK9-12218SXF	Cisco Catalyst 6000 Enterprise Services SSH	$10,000
	S323AEK9-12218SXF	Cisco Catalyst 6000 Advanced Enterprise Services SSH	$15,000

Note For other options not listed, assume a 5 or 10 percent upgrade charge from the components that are shown. For example, if PoE is desired on upgradable modules, include an upgrade charge of 10 percent per module.

Step 12 Present your design to the class. Be prepared to justify your design choices.

Activity Verification

Your case study discussion and solution should include the following:

- Diagram of the proposed design
- Brief documentation giving port counts, types of connections (speeds and feeds), and supporting details
- Brief documentation of the pros and cons of the design choices you made compared to the alternatives
- BOM for your design

You have completed this activity when the instructor has verified your case study solution, and you have justified any major deviations from the solution that is supplied by the instructor.

Case Study 4-1: ACMC Hospital Network WAN Design

This case study enables you to practice the skills and knowledge that you learned in the module.

Activity Objective

In this activity, you will create a high-level design for the WAN portions of the ACMC Hospital network. After completing this activity, you will be able to meet these objectives:

- Determine and document enterprise WAN requirements for an RFP
- Evaluate responses to an RFP and associated costs
- Determine and justify a choice of WAN technology
- Add appropriate redundancy to your design
- Determine appropriate Cisco router models for the WAN

Visual Objective

There is no visual objective for this case study.

Required Resources

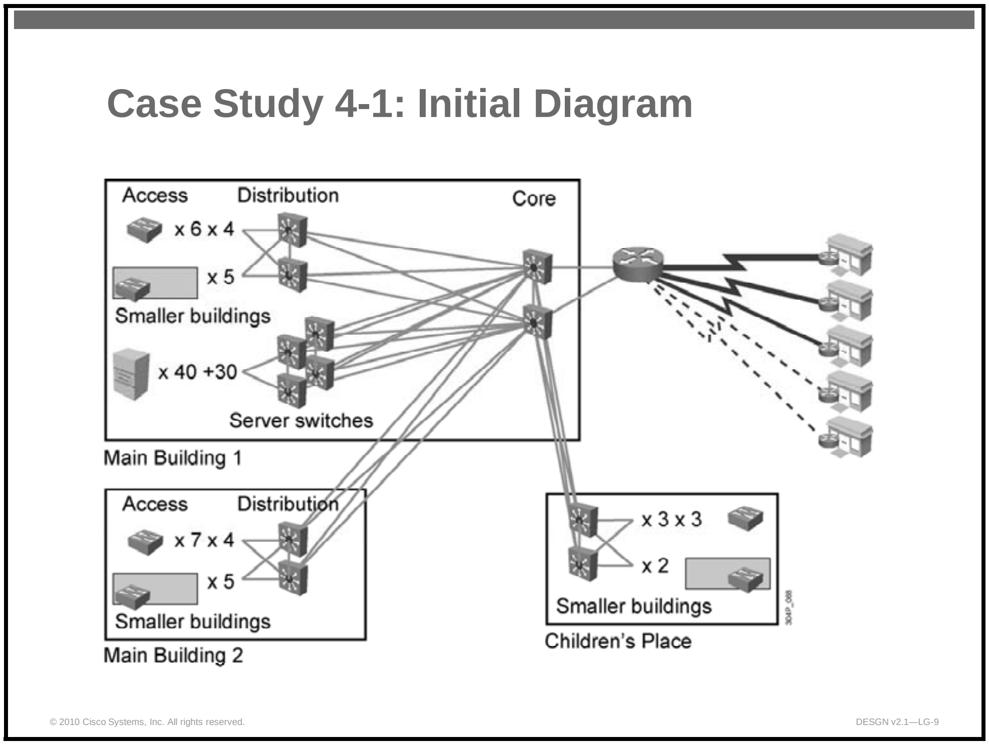
The following are the resources and equipment that are required to complete this activity:

- Case study guidelines, presented in the Lab Guide Overview
- ACMC Hospital case study scenario
- A workgroup of two to four learners
- Blank sheets of paper and a pencil

ACMC Hospital Case Study Scenario

Your site contact initially supplied you with an out-of-date network diagram. The hospital upgraded the DS0s to 128 kb/s a year ago and increased the WAN bandwidth at the largest clinic to 256 kb/s last month.

In this case study, you will begin to fill in the details of your design. This case study focuses on the WAN part of the ACMC Hospital network. This diagram shows the existing WAN links and the planned campus infrastructure.



Case Study 4-1: Initial Diagram

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-9

Business Factors

The ACMC Hospital CIO realizes that WAN performance to the remote clinics is poor. It seems likely that some of the new applications will require more bandwidth. These applications include programs that allow doctors at the central site to access medical images, such as digital X-rays, that are stored locally at the clinics.

The CIO wants to implement a long-term solution. ACMC needs a cost-effective solution that allows high-bandwidth application deployment on the network and that allows for growth for the next two to five years. The CIO also wants you to provide the technical recommendations to ensure that the remote sites all have the same type of access. In addition, the CIO wants you to simplify the planning, pricing, and deployment of future applications.

Technical Factors

TCP adjusts to use the available bandwidth. When there is congestion, there is no way to know how much bandwidth the present applications could ideally use, unless they are tested in a lab situation.

There is also little or no data about the bandwidth requirements of the new applications. Lab testing would provide better data, but ACMC does not have the time or the money for testing.

You know the following information:

- Site A, the largest remote clinic, runs at 256 kb/s.
- Sites B and C are clinics that run at 128 kb/s.
- Sites D and E, the two remaining “small” clinics, run at 56 kb/s.
- You need to increase WAN bandwidth to last for two to five years.

For situations in which you cannot accurately determine how much WAN bandwidth is needed, the general rule is to multiply traffic levels by 1.5 to 2 per year. If you use a higher number than that, you may have to justify this decision. If the customer does not want to be concerned with needing more bandwidth, you should multiply by larger numbers. When there are unknown applications to be installed, you should multiply by larger numbers.

You should proceed assuming that all clinics are upgraded to at least T1 access speed. (Current prices in many areas may even favor T1 over fractional T1 links.)

ACMC Hospital Network WAN Design Tasks

Complete these steps:

Step 1 As a member of the ACMC planning team, develop a short list of requirements and information that is to be provided in the ACMC WAN RFP. Identify any items about which you think the ACMC staff should be concerned.

Step 2 You put out an RFP specifying at least T1 bandwidth at remote clinics, to see what current prices are. You also priced local business-grade DSL and cable service. The responses are shown in the “RFP Results” table.

Note Some technology choices have been omitted, for simplicity. Fractional T1 may cost more than complete T1 in some areas, so it is omitted. DSL is omitted from this case study, since cable has similar characteristics and prices. ATM is also omitted, since multilink T1 or T1-based Frame Relay generally has comparable or lower costs and lower equipment costs. Although a wireless bridged WAN might be applicable, it is not included at this time. It is assumed that Metro Ethernet and dark fiber are not available in the area, which is the case except near major cities.

RFP Results

Option	Technology	Speed	Price per Month
1	Leased-line T1 into central T3 (same LATA)	T1 or T3	$400 for each T1, $8,000 for T3
2	Frame Relay, T1 access, central T3	T1 or T3	$350 for T1 access, $,7000 for T3 access circuit Plus CIR in 5-Mb/s increments times $75 plus $5 per PVC
3	MPLS VPN, T1 access at clinics, central T3	T1 or T3	$500 for T1 access, $8,500 for T3 access circuit
4	High-speed business cable service or Internet at clinics T3 Internet at central site	6 Mb/s downstream or 768 kb/s upstream T3	$90 $4,000

Step 3 Calculate the monthly cost for using each of the approaches and complete the total monthly cost column in the "Monthly Costs" table.

Monthly Costs

Option	Technology	Speed	Price per Month	Monthly Cost
1	Leased-line T1 into central T3 (same LATA)	T1 or T3	$400 for each T1, $8,000 for the T3	5 * $400 = $2,000 1 * $8,000 = $8,000 Total = $10,000 per month
2	Frame Relay, T1 access, central T3	T1 or T3	$350 for T1 access, $7,000 for T3 access circuit Plus CIR in 5-Mb/s increments times $75 plus $5 per PVC	
3	MPLS VPN, T1 access at clinics, central T3	T1 or T3	$500 for T1 access, $8,500 for T3 access circuit	
4	High-speed business cable service or Internet at clinics T3 Internet at central site	6 Mb/s downstream or 768 kb/s upstream T3	$90 $4,000	

Step 4 Which technology do you recommend that ACMC use? Discuss and choose a WAN technology within your workgroup. Remember that Multilink PPP over multiple T1s is also an option. The "ISR Routers and Port Capabilities" table condenses the product information and module information from Cisco.com.

Note To simplify this step, budgetary costs are not included for the routers. Make your choice based on capabilities that are needed, with the understanding that cost is increased if you increase capabilities and options.

ISR Routers and Port Capabilities

Cisco ISR Model	Approx. Mb/s of Layer 3 Fast Ethernet or Cisco Express Forwarding Switching with 64-Byte Packets	LAN Ports	WAN Ports
851	5.12	10/100 four-port switch	10/100 Fast Ethernet
857	5.12	10/100 four-port switch	ADSL
861	12.8	10/100 four-port switch	ADSL
867	12.8	10/100 four-port switch	ADSL2/2+ over POTS (Annex A)
871	12.8	10/100 four-port switch	10/100 Fast Ethernet
876	12.8	10/100 four-port switch	ADSL over ISDN
877	12.8	10/100 four-port switch	ADSL
878	12.8	10/100 four-port switch	G.shdsl
891	12.8	10/100 eight-port switch	V.92 analog modem
1801	35.84	10/100 eight-port switch	one Fast Ethernet, ADSL over POTS
1802	35.84	10/100 eight-port switch	one Fast Ethernet, ADSL over ISDN
1803	35.84	10/100 eight-port switch	one Fast Ethernet, G.shdsl
1811	35.84	10/100 eight-port switch	two Fast Ethernet
1812	35.84	10/100 eight-port switch	two Fast Ethernet
1841	38.40	Two Fast Ethernet, can add four-port switch with HWIC-4ESW	Can add two HWIC modules: ADSL WIC, G.shdsl WIC, cable WIC, WIC-1T (one T1), WIC-2T (two T1)
1941	38.40	Two integrated 10/100/1000 Ethernet ports	2 enhanced High-Speed WAN Interface Card slots that can host 2 single wide or 1 double wide and 1 single wide (e)HWIC
2801	46.08	Two 10/100 Fast Ethernet	Four slots: two slots support HWIC-, WIC-, VIC-, or VWIC-type modules; one slot supports WIC-, VIC-, or VWIC-type modules; one slot supports VIC or VWIC-type modules Can add WIC modules that are listed for 1841, also HWIC-4T (4 T1 HWIC)
2811	61.44	Two 10/100 Fast Ethernet	Four slots: each slot can support HWIC-, WIC-, VIC-, or VWIC-type modules. Can add WIC modules that are listed for 1841, also HWIC-4T (4 T1 HWIC) Plus, one slot supports NM- and NME-type modules Can use NM-1HSSI

Cisco ISR Model	Approx. Mb/s of Layer 3 Fast Ethernet or Cisco Express Forwarding Switching with 64-Byte Packets	LAN Ports	WAN Ports
2821	87.04	Two 10/100 Fast Ethernet	Four slots: each slot can support HWIC-, WIC-, VIC-, or VWIC-type modules. Can add WIC modules that are listed for 1841, also HWIC-4T (4 T1 HWIC) Plus, one slot supports NM-, NME-, and NME-X-type modules Can use NM-1HSSI
2851	112.64	Two 10/100 Fast Ethernet	Four slots: each slot can support HWIC-, WIC-, VIC-, or VWIC-type modules. Can add WIC modules that are listed for 1841, also HWIC-4T (4 T1 HWIC) Plus, one slot supports NM-, NME-, NME-X-, NMD-, and NME-XD-type modules Can use NM-1HSSI
2911	112.64	Three Gigabit Ethernet (10/100/1000)	Embedded hardware-accelerated VPN encryption for secure connectivity and collaborative communications Integrated threat control using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, and Cisco IOS Content Filtering
3825	179.20	Two Gigabit Ethernet (10/100/1000)	Two NM/NME/NME-X modules or one NMD/NME-XD Four HWIC/WIC/VIC/VWIC slots For relevant NM and WIC/HWICs, see modules that are listed for 2851 above
3845	256	Two Gigabit Ethernet (10/100/1000)	Four NM/NME/NME-X modules or two NMD/NME-XDs Four HWIC/WIC/VIC/VWIC slots For relevant NM and WIC/HWICs, see modules that are listed for 2851 above

Switch HWICs for Cisco 1841 Integrated Services Router

Up to two of the four-port HWICs can be used.

Switch HWICs and Network Modules for Cisco 2800 and 3800 Series Integrated Services Routers

Nine-port HWICs are available. Two of them can be used per 2800 or 3800 Series router. Network modules are also available as per the table.

Module	NME-16ES-1G	NME-16ES-1G-P	NME-X-23ES-1G	NME-X-23ES-1G-P	NME-XD-24ES-1S-P	NME-XD-48ES-2S-P
Limitations	2811, 2821, and 2851, 2900 any, Any 3800	2811, 2821, and 2851, only, 2900, 3800	2821 and 2851 only Any 3800	2821 and 2851 only Any 3800	2851 only Any 3800	2851 only Any 3800
Ports	▪ 10/100: 16 ▪ 10/100/1000: 1 ▪ Small Form Factor Pluggable (SFP): 0	▪ 10/100: 16 ▪ 10/100/1000: 1 ▪ Small Form Factor Pluggable (SFP): 0	▪ 0/100: 23 ▪ 10/100/1000: 1 ▪ SFP: 0	▪ 10/100/1000: 1 ▪ 10/100: 23 ▪ SFP: 0	▪ 10/100: 24 ▪ 10/100/1000: 0 ▪ SFP: 1	▪ 10/100: 48 ▪ 10/100/1000: 0 ▪ SFP: 2
Powered Switch Ports	0	16	0	24	24	48
IEEE 802.3af PoE support	No	Yes*	No	Yes*	Yes*	Yes*

Step 5 In a class discussion, each workgroup indicates its choice and reasoning. The instructor will summarize on whiteboard if available. (Ten to 15 minutes of discussion are allowed for this group discussion.)

Step 6 Note that transferring 100-MB images over a T1 takes over 8 minutes. (100 MB * 8 bits/byte / 1.5 Mb/s = 518 seconds.) Does that alter your decision? Why or why not?

Step 7 The CIO indicates that remote site availability is critical, to avoid having to support servers at the clinics. Which redundancy or backup WAN strategy do you recommend?

Step 8 Assume the CIO has chosen to deploy Multilink PPP over two T1s for simple, reliable service. The 6-Mb/s cable service will be used as backup. Select an appropriate Cisco router model to use at the central site and at each remote location. Also, select appropriate switching hardware for each site, remembering that the ISR router models can use integrated switches.

Site	Number of Switch Ports Needed
1	48
2, 3	24
4, 5	16

____

____

____

____

____

Step 9 Which design changes would you make if the CIO wants a second router that is used for the backup link at each site?

Step 10 Present your design to the class. Be prepared to justify your design choices.

____

____

____

____

____

Activity Verification

You have completed this activity when the instructor has verified your case study solution, and you have justified any major deviations from the solution that is supplied by the instructor.

Case Study 5-1: ACMC Hospital Network IP Addressing and Routing Protocol Design

This case study enables you to practice the skills and knowledge learned in the module.

Activity Objective

In this activity, you will create an IP addressing and routing protocol design for the ACMC Hospital network. After completing this activity, you will be able to meet these objectives:

- Determine and document a suitable IP addressing design for ACMC.
- Determine an IP address assignment plan.
- Determine and justify a choice of routing protocol or protocols for ACMC.

Visual Objective

There is no visual objective for this case study.

Required Resources

These are the resources and equipment that are required to complete this activity:

- Case study guidelines, presented in the Lab Guide Overview.
- ACMC Hospital case study scenario.
- A workgroup of two to four learners.
- Blank sheets of paper and a pencil.

ACMC Hospital Case Study Scenario

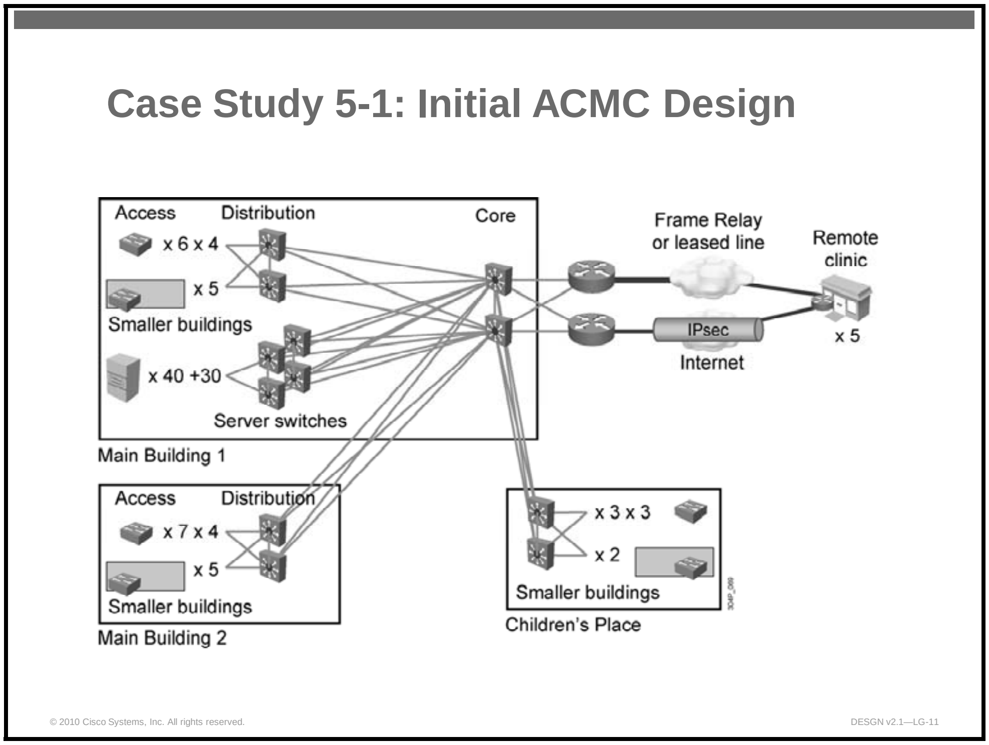
The table lists the port counts by locations.

Port Counts by Location

Location	Counts	Counts with Spares	Comments
Main Building 1 (per floor)	75	150	six floors
Main Building Server Farm	40	80	will connect with dual NICs
Main Building 2 (per floor)	75	150	seven floors
Children’s Place (per floor)	60	120	three floors
Buildings A—D	10 each	20 each	
Buildings E—J	20 each	40 each	
Buildings K—L	40 each	80 each	

Refer to the previous case studies for any additional information you need. You will now start filling in the details of your design.

This diagram shows the planned campus and WAN infrastructure.



Case Study 5-1: Initial ACMC Design

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-11

ACMC Hospital Network IP Addressing and Routing Protocol Design Tasks

Complete these steps:

Step 1 Determine a suitable summarizable IP addressing plan for ACMC. Include the campus, WAN and backup WAN links, and the remote clinics. (Dial-up and IPsec have not yet been covered, so you do not need to consider addressing for them here.)

Step 2 Determine how IP address assignment is to take place.

Step 3 Determine a suitable routing protocol or protocols and routing design.

Step 4 (Optional) Figure out the summary routes for either EIGRP or OSPF from Step 3. What would representative routing tables look like, at various points in the network?

Step 5 (Optional) Go back and rework the design, treating the small buildings as “floors” of a fourth large campus building and the remote clinics as “floors” of a fifth.

Step 6 (Optional) Go back and do the design based on prefix 172.16.0.0 /16.

Step 7 Present your design to the class. Be prepared to justify your design choices.

Activity Verification

You have completed this activity when the instructor has verified your case study solution and you have justified any major deviations from the solution that is supplied by the instructor.

Case Study 6-1: ACMC Hospital Network Security Design

This case study enables you to practice the skills and knowledge learned in the module.

Activity Objective

In this activity, you will create a high-level security design for the ACMC Hospital network. After completing this activity, you will be able to meet these objectives:

- Identify and describe key business security requirements, risks, and threats to ACMC
- Determine and document a secure design for these edge modules for ACMC, and explain how they connect to the rest of the ACMC Hospital network:
  - E-commerce.
  - Internet connectivity.
  - Remote access and VPN.
  - WAN and MAN and site-to-site VPN.
- Determine and document a secure design for remote clinics using Internet with VPN for backup access.
- Determine suitable IP subnetting for the Internet, DMZ, or VPN complex.
- Identify and describe what Cisco Security products and features you would use to secure the three campus layers and data center or server switches.
- Identify some of the other security considerations, products, and features that should be part of deployment and their locations within the network.

Visual Objective

There is no visual objective for this case study.

Required Resources

These are the resources and equipment that are required to complete this activity:

- Case study guidelines, presented in the Lab Guide Overview.
- ACMC Hospital case study scenario.
- A workgroup of two to four learners.
- Blank sheets of paper and a pencil.

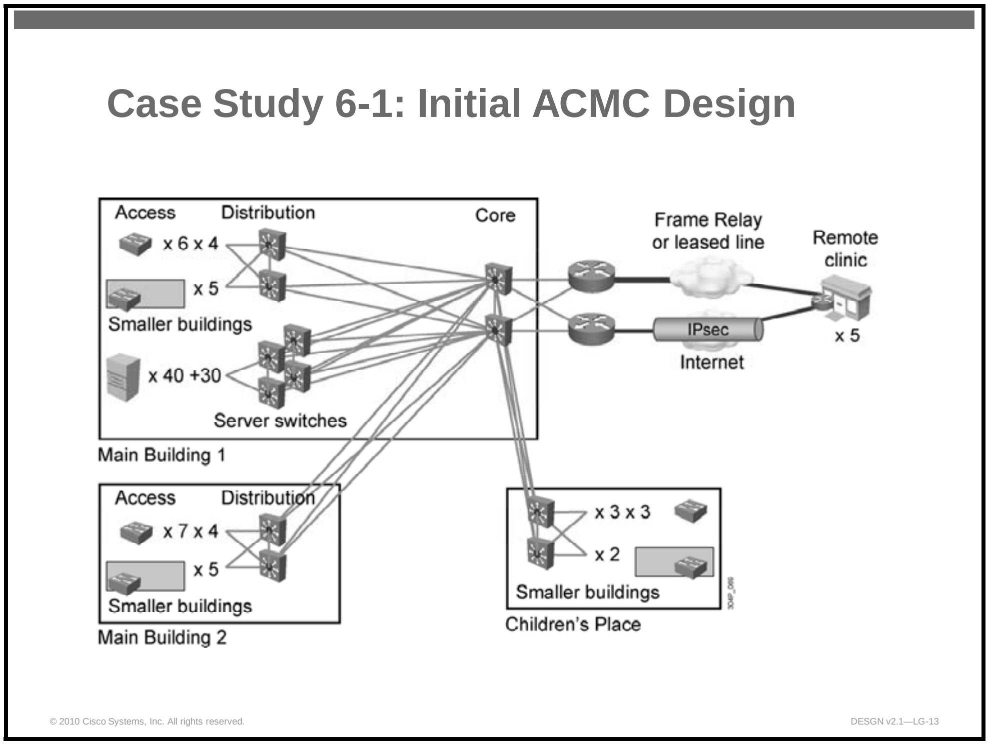
ACMC Hospital Case Study Scenario

In this case study, you will identify what security measures to use to protect the ACMC Hospital network. You will then identify which Cisco Security products to use and where to use them in the network.

The recommended design up to this point (as shown in the case study answer key) should be used. In this case study, you will supplement that design by adding security functionality. These parts of the network already have been designed:

- Core, distribution, access layer, and server switches in the campus.
- WAN routers dual-homed to the core switches.
- IP addressing and routing.

This diagram summarizes the design thus far.



Case Study 6-1: Initial ACMC Design

DESGN v2.1—LG-13

ACMC Hospital Network Security Design Tasks

Complete these steps:

Step 1 Identify key business security requirements, risks, and threats about which ACMC should be concerned.

Step 2 Design these edge modules for ACMC. Also, determine how they should connect to the rest of the ACMC Hospital network. Be prepared to justify your design.

- E-commerce.
- Internet connectivity.
- Remote access and VPN.
- WAN and MAN and site-to-site VPN.

Note Your design can use a consolidated approach in which firewalls are shared between modules.

Step 3 Design security for remote clinics using Internet with VPN for backup access.

Step 4 Determine suitable IP subnetting for the Internet, DMZ, or VPN complex.

Step 5 Identify which Cisco Security products and features you would use to secure the three campus layers and data center or server switches.

____

____

____

____

____

Step 6 Identify some of the other security considerations, products, and features that should be part of deployment and where they should be used. For example, how should you handle infrastructure protection?

____

____

____

____

____

Step 7 Present your design to the group. Be prepared to justify your design choices.

Activity Verification

You have completed this activity when the instructor has verified your case study solution and you have justified any major deviations from the solution that is supplied by the instructor.

Case Study 7-1: ACMC Hospital Network Voice Transport Considerations

This case study enables you to practice the skills and knowledge learned in the module.

Activity Objective

In this activity, you will create a high-level voice support design for the ACMC Hospital network. After completing this activity, you will be able to meet these objectives:

- Reconsider the design in “Case Study 6-1: Security Design” based on voice requirements, and determine key aspects that impact the ability to support voice.
- Select an appropriate IP telephony design model and defend this choice.
- Identify appropriate IP telephony components to meet specific design goals.
- Discuss suitability of Internet VPN access for voice support.
- Perform simple voice bandwidth calculations, being aware of the impact of header overhead in addition to codec payload bandwidth.
- Draw conclusions about using the WAN for voice transport.

Visual Objective

There is no visual objective for this case study.

Required Resources

These are the resources and equipment that are required to complete this activity:

- Case study guidelines, presented in the Lab Guide Overview.
- ACMC Hospital case study scenario.
- A workgroup consisting of two to four learners.
- Blank sheets of paper and a pencil.

ACMC Hospital Case Study Scenario

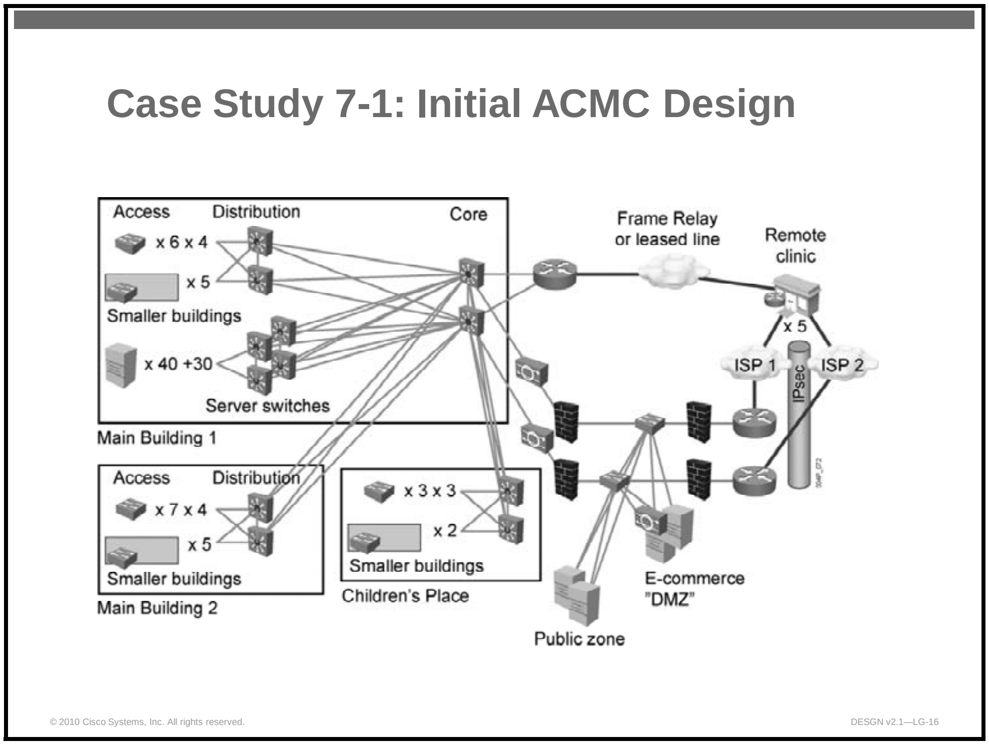
In this case study, you will identify what voice support the ACMC Hospital network requires. You will then identify how to provide that Voice Support in your design.

The ACMC staff wants to replace its PBX and key systems and is eager to achieve cost reduction while providing better service to remote clinics. The replacement system needs to offer at least as many features as the present system. The staff is also very interested in unified voice-mail services for busy doctors and the potential for using phones with web-based menus as part of a quality care system.

Current features include standard PBX features, call conferencing, voice mail, and local calls.

Remote clinics currently use some form of key system or remote PBX shelf with limited features.

This diagram summarizes the ACMC design up to this point.



Case Study 7-1: Initial ACMC Design

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-16

ACMC Hospital Network Voice Transport Consideration Tasks

Complete these steps:

Step 13 Based on the ACMC design up to this point, what are the infrastructure issues that affect voice deployment that you should consider (ignore the IPsec for now)?

Step 14 Select the IP telephony design model most appropriate to ACMC. Justify your recommendation based on your understanding of the ACMC requirements. Indicate where you would place the various IP telephony components.

Step 15 If each remote clinic is to be able to place local calls without going through the main campus, what will be needed at each site? What needs to be added to support local conference calls?

Step 16 WAN backup is by IPsec VPN across the Internet. What service characteristics might IPsec or Internet lack? What could you add to your design to remedy this?

Step 17 The ACMC current phone system uses a PBX or remote shelf at each clinic, together with phone trunks back to the main campus PBX. The Director of Telephony just had a call study done and is convinced she has sufficient capacity. The table summarizes how many calls are currently supported per remote site.

Remote Clinic	Number of Calls on Trunk to Main Campus
1	8
2, 3, 4, 5	4

Look at the call bandwidth, taking into account all Layer 2 and other header overhead, plus 5percent for signaling. Assume Ethernet and no tunnel overhead. In this case, a G.729 call uses about 25 kbps with 30 ms digitization interval. A G.711 call with overhead uses about 92 kbps with a 20 ms digitization interval. Use these numbers to estimate how much WAN bandwidth each ACMC site would need for each of the two codecs.

Remote Clinic	Number of Calls on Trunk to Main Campus	G.711 Bandwidth (kbps)	G.729 Bandwidth (kbps)
1	8		
2, 3, 4, 5	4		

What conclusions about the ACMC WAN does the previous calculation in the table imply? Is there enough bandwidth?

Step 18 Present your design to the group. Be prepared to justify your design choices.

Activity Verification

You have completed this activity when the instructor has verified your case study solution, and you have justified any major deviations from the solution that is supplied by the instructor.

Case Study 8-1: ACMC Hospital Network Unified Wireless Networking Considerations

This case study enables you to practice the skills and knowledge learned in the module.

Activity Objective

In this activity, you will create a high-level unified wireless design for the ACMC Hospital network. After completing this activity, you will be able to meet these objectives:

- Complete a design using the RF survey results.
- Determine the location and number of wireless controllers, which models to use, and whether to use the CAPWAP WLC Discovery approach.
- Design the wireless network to separate traffic from different user communities and allow enforcement of HIPAA access restrictions.
- Provide an IP addressing design for the resulting WLANs.
- Provide a design concerning a mobility group or groups.
- Design a wireless solution for the remote clinics.
- Provide a design for secure guest wireless access.
- Present your designs and discuss benefits and drawbacks.

Visual Objective

There is no visual objective for this case study.

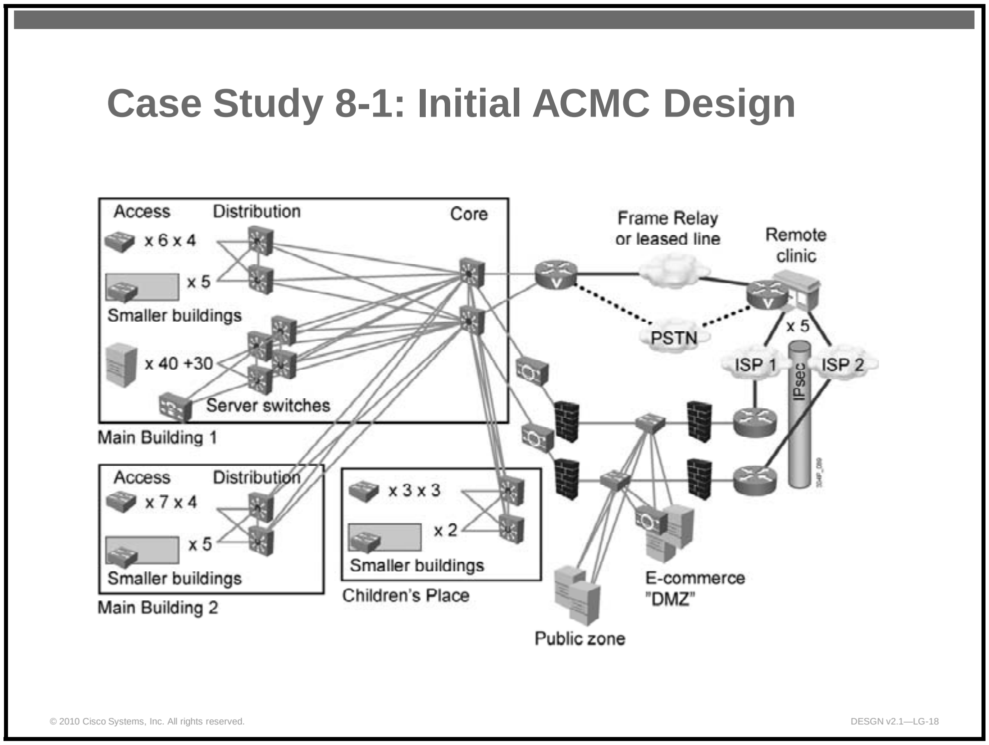
Required Resources

These are the resources and equipment that are required to complete this activity:

- Case study guidelines, presented in the Lab Guide Overview.
- ACMC Hospital case study scenario.
- A workgroup consisting of two to four learners.
- Blank sheets of paper and a pencil.

ACMC Hospital Case Study Scenario

In this case study, you will develop a high-level unified wireless design for the ACMC Hospital network. This diagram summarizes the design up to this point.



Case Study 8-1: Initial ACMC Design

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-18

Note	A site survey customarily is required to determine RF propagation characteristics, select AP locations and antennas, look for interference (possibly a major factor in hospitals), and so on. In hospitals, there also may be areas where radio signals would interfere with critical equipment, areas that must be protected from wireless AP signals. These details all lie outside the scope of this course.

Assume that the site survey has been performed and is summarized in the table. Assume that no sources of interference or RF prohibitions have been discovered. For this design, wireless devices are estimated to match current Ethernet ports. Wireless coverage in the cafeteria on floor 1 of Main Building 1 has been added as well.

Building	Ethernet Ports	Access Point Information	Counts
Main Building 1	150 per floor, 7 floors (plus server farm)	8 per floor, 7 floors 4 in the server farm (for administrator convenience)	60
Main Building 2	150 per floor, 7 floors	8 per floor, 7 floors	56
Children's Place	120 per floor, 3 floors	6 per floor	18
Buildings A—D	20	1 per building, 4 buildings	4
Buildings E—J	40	2 per building, 6 buildings	12
Buildings K—L	80	4 per building, 2 buildings	8
Remote Clinic 1	48	3	3
Remote Clinics 2 and 3	24	1 per building, 2 buildings	2
Remote Clinics 4 and 5	16	1 per building, 2 buildings	2
Total			165

The ACMC CIO has indicated no desire to implement any outdoor wireless support at this time.

ACMC Hospital Network Unified Wireless Networking Tasks

Complete these steps:

Step 1 Determine the location and number of wireless controllers and which models to use. How are you going to handle CAPWAP WLC discovery? Be prepared to justify your choices.

Step 2 The hospital wishes to separate traffic based on its three staff organizations: Financial, Medical, and Support. The intent is to enforce HIPAA compliance by only allowing staff to authenticate to the appropriate SSID based on the type of access the staff needs. How does this affect your wireless design? What could you do to enforce the HIPAA access restrictions?

Step 3 How will you support the WLANs in terms of IP addressing? How should you modify or extend your IP addressing scheme to the various wireless groups?

Step 4 What will your mobility group or groups be?

Step 5 Determine how to handle wireless for the remote clinics.

Step 6 Determine how to supply secure guest wireless access.

Step 8 Present your design to the group. Be prepared to justify your design choices.

Activity Verification

You have completed this activity when the instructor has verified your case study solution and you have justified any major deviations from the solution that is supplied by the instructor.

Case Study 8-2: Connecting More Hospitals to the ACMC Hospital Network

This case study enables you to practice the skills and knowledge learned in the course.

Activity Objective

In this activity, you will update your high-level design as the ACMC Hospital network evolves. After completing this activity, you will be able to meet these objectives:

- Discuss pros and cons of ACMC being assigned address block 10.1.0.0 /16 for communications on the state hospital network.
- Provide a revised addressing scheme for ACMC.
- Identify key issues to fix in redesigning Hospital Omega to modernize its network and allow robust access to the ACMC data center.
- Propose a new design for Hospital Omega.
- Extend the IP addressing scheme to cover Hospital Omega.
- Identify the key security issue for the Hospital Omega network and two ways to resolve this issue.
- Provide a design to standardize the Hospital Beta network and allow robust access to the ACMC data center.
- Identify design issues for Hospital Beta.
- Identify issues involved in centralizing Hospital Beta server to ACMC.
- The impact of inexpensive Metro Ethernet between ACMC and Hospital Beta on server consolidation.
- Analyze whether the Hospital Beta Cisco Unified CallManager and Cisco Unity servers should be moved to the ACMC data center.
- Analyze whether the wireless controllers at Hospital Beta should be moved to the ACMC campus.
- Provide a recommendation on overall routing protocol and routing design for the merged networks
- List additional steps that can be taken to improve security in the combined ACMC-OB network.
- Provide technical comments to the CIO concerning moving Hospital Omega from Centrex service to IP telephony for large savings.

Visual Objective

There is no visual objective for this case study.

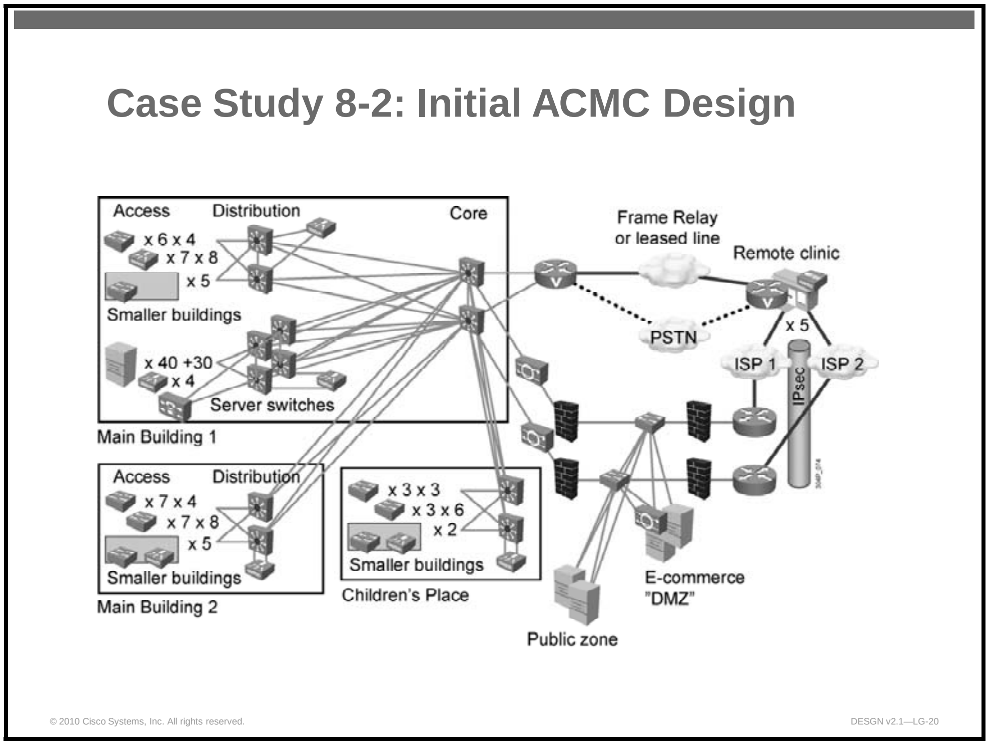
Required Resources

These are the resources and equipment that are required to complete this activity:

- Case study guidelines, presented in the Lab Guide Overview.
- ACMC Hospital case study scenario.
- A workgroup consisting of two to four learners.
- Blank sheets of paper and a pencil.

ACMC Hospital Case Study Scenario

In this case study, revise your previous design to incorporate changes in the business environment in and around ACMC Hospital. This diagram shows the current ACMC design.



Case Study 8-2: Initial ACMC Design

DESGN v2.1—LG-20

The state in which ACMC operates wishes to improve patient service by networking hospitals. The legislature hopes to leverage large city medical expertise for telemedicine at smaller locations. The network will be called MedNet. Short-term TDM circuits funded. MedNet will move to Metro Ethernet service after terms for provider construction and contract are agreed upon. Clinics will be associated with and connected via county hospitals.

Connecting More Hospitals to the ACMC Hospital Network Tasks

Complete these steps:

Step 1 ACMC has been assigned address block 10.1.0.0 /16. The CIO wants you to determine how to react to this. What alternatives are there to re-addressing all of ACMC? What are their pros and cons? Could ACMC re-address within 10.1.0.0 /16? Assuming it can do so, provide a revised addressing scheme.

Address Assignments

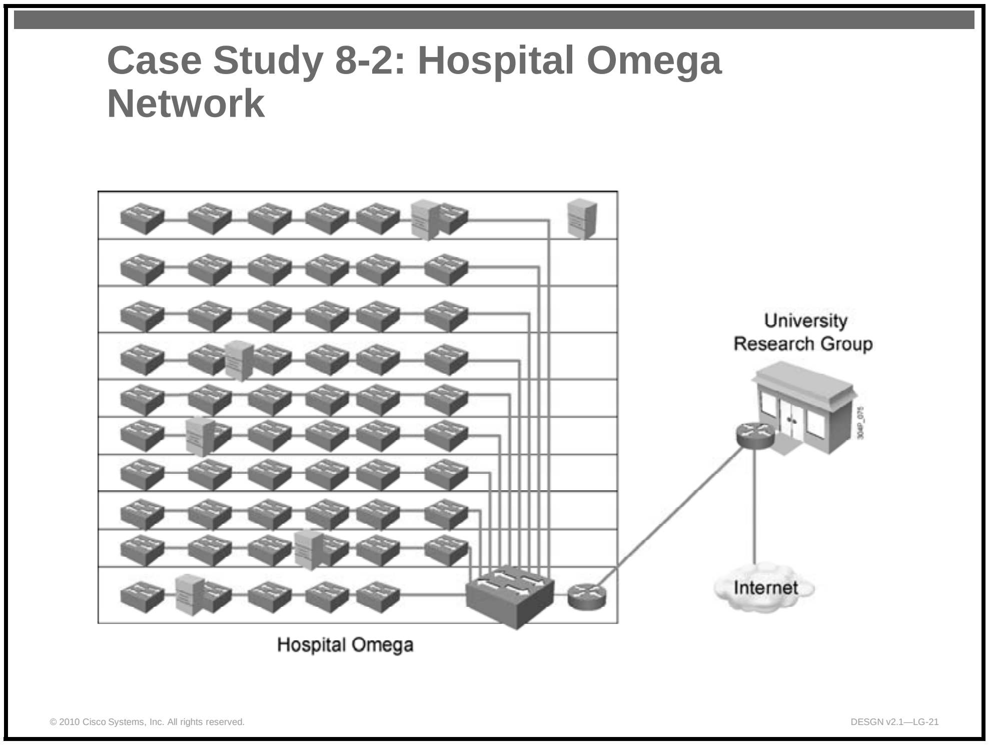
Building or Site	Address Block	Details
Main Building 1		
Building A		
Building B		
Building C		
Building D		
Building E		
Reserved		
Main Building 2		
Building F		
Building G		
Building H		
Building I		
Building J		
Reserved		
Children's Place		
Building K		
Building L		
Reserved		

Building or Site	Address Block	Details
Remote site 1		
Remote site 2		
Remote site 3		
Remote site 4		
Remote site 5		
Reserved		
Future space		

Hospital Omega is a nearby hospital that has been having financial difficulties. It is facing large licensing and application development costs to bring its financial and other applications up to date. To cut costs and stabilize finances, Hospital Omega will merge with ACMC. All data services will move to the ACMC data center and gradually migrate to the modern applications ACMC already has in place. The Hospital Omega network was deployed between 7 and 10 years ago, and in many cases, the equipment vendors no longer exist. Here is some information about Hospital Omega:

- Hospital Omega does not use DHCP.
- Hospital Omega is one building of 10 floors, with less than 250 computers per floor.
- Hospital Omega uses static routing.
- The Hospital Omega network is flat and Layer 2 switched.
- The switching equipment is from a third-party vendor and is 6 to 9 years old.
- The Hospital Omega network uses old copper and fiber cabling that was added by various people in a random manner over the years. For any given closet, about 50 percent of the cable (copper or fiber) goes to unknown locations and is of unknown quality.
- Servers are scattered around the building in random closets near the department that originally installed them.

This diagram shows the Hospital Omega network.



Case Study 8-2: Hospital Omega Network

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-21

Step 2 The CIO wants a design to modernize the Hospital Omega network and allow robust access to the ACMC data center. What issues can you identify? What would you propose to the CIO as your design?

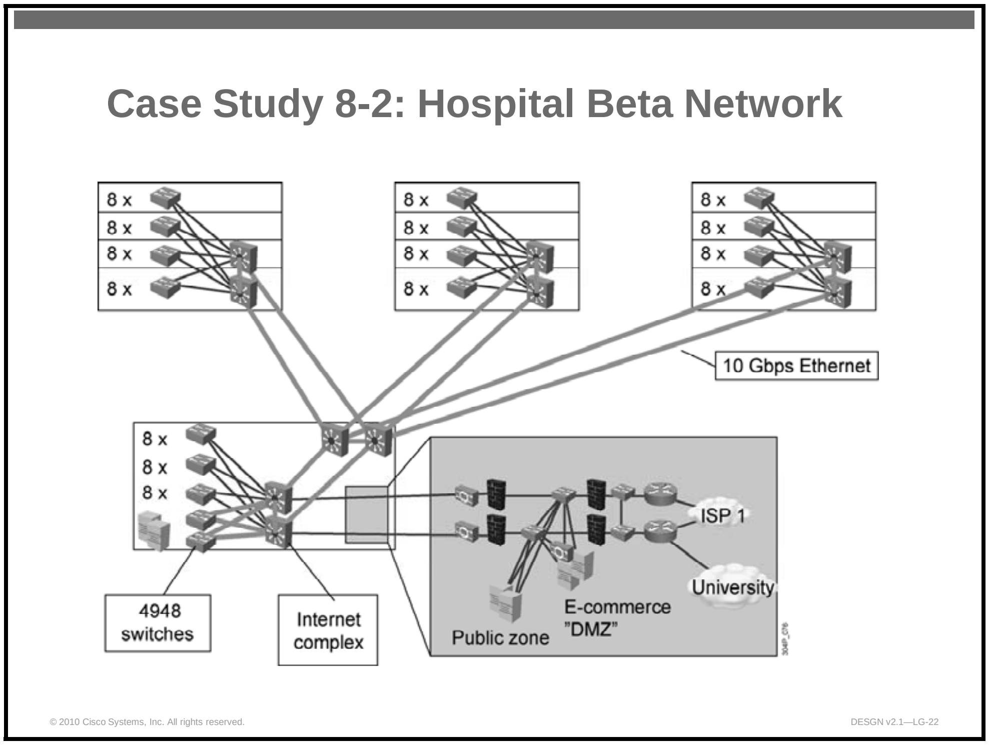
Step 3 Extend the IP addressing scheme to cover Hospital Omega.

Step 4 What is the key security issue for the Hospital Omega network? What are two ways to resolve this issue?

Hospital Beta is another nearby hospital. Both ACMC and Hospital Beta duplicate several areas of medical expertise and feel that pooling talent and facilities should lead to better depth of medical expertise and better patient care. Sharing financial and other applications should also reduce overhead costs. Here is some information about Hospital Beta:

- DHCP is in use.
- Hospital Beta consists of four buildings, each with four large floors (less than 250 Ethernet users and ports each). Each floor uses eight 24-port 3560 switches in IDF closets, with dual uplinks to the distribution layer switches. The data center and Internet complex is in one floor of one of the four buildings.
- Each building uses two 6506 switches as distribution layer. These are dual-homed via single-mode fiber at 10 Gbps to the core switches.
- The two 6506 core switches have 10 Gbps interconnect and dual connections to two 4948 switches for the servers.
- The campus network is based on high-speed Layer 3 Cisco switches.
- Wireless is supported using Cisco wireless LAN controllers.
- Hospital Beta has a DMZ, dual firewalls in each of two layers, IPS monitoring DMZ and internal access, and so on.
- Cisco IP telephony is in place.

This diagram shows the Hospital Beta network.



Case Study 8-2: Hospital Beta Network

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-22

Step 5 The CIO wants a design to standardize the Hospital Beta network and allow robust access to the ACMC data center. What issues can you identify? What do you propose to the CIO as your design?

Step 6 The CIO wishes to consolidate servers in the ACMC data center. What issues need to be examined before proceeding with such a?

Step 7 Suppose inexpensive Metro Ethernet is available between ACMC and Hospital Beta. How does this change your answer to the question in Step 6?

Step 8 Hospital Beta already has deployed Cisco Unified CallManager, IP phones, voice gateways, and so on. Should the Cisco Unified CallManager and Cisco Unity servers be moved to the ACMC data center? If so, what would be the pros and cons of moving them? If not, how should they interact with a Cisco Unified CallManager on the ACMC campus?

Step 9 Should the wireless controllers at Hospital Beta be moved to the ACMC campus?

Hospital Omega is using static routes on its one Internet router. Hospital Beta is using IS-IS protocol.

Step 10 Make a recommendation on overall routing protocol and routing design for the merged networks.

The CIO at ACMC is concerned about HIPAA compliance and general security. She and you agree on running all Internet connectivity through ACMC and Hospital Beta. Assume firewalls, firewall rules, DMZs, and properly configured IPsec VPN access are all in place.

Step 11 What additional steps can be taken to improve security in the combined ACMC-Omega-Beta (ACMC-OB) network?

Step 12 Hospital Omega is paying a large amount per phone for Centrex service. The CIO urgently wishes to cut costs by moving to IP phones for Hospital Omega. The ROI on doing this indicates that it would pay for itself in under a year. So, the CIO has asked you for technical comments on doing this. What do you tell her?

Step 13 Present your design to the group. Be prepared to justify your design choices.

Activity Verification

You have completed this activity when the instructor has verified your case study solution and you have justified any major deviations from the solution that is supplied by the instructor.

Answer Key

The correct answers and expected solutions for the activities that are described in this guide appear here.

Case Study 1-1 Answer Key: ACMC Hospital Network Upgrade Information

Your case study discussion and solution should include these items:

- Documentation of the ACMC Hospital requirements
- Documentation of the existing network
- A list of missing information
- An outline of the major design tasks for the network

Based on the scenario, this section includes the proposed solutions. According to the case study guidelines, there may be some minor variations in your solutions.

Case Study Solutions

The steps that require solutions are listed here.

Step 1 Read the ACMC Hospital network upgrade scenario information completely before beginning the activity.

No answers are required for this step.

Step 19 Discuss the scenario with your group.

No answers are required for this step.

Step 20 Document the ACMC Hospital requirements in the “Requirements” table.

Requirement	Comment
Structured cabling	
High availability, redundancy	
Higher campus speeds, at least Gigabit Ethernet core	Medical images are huge.
Higher WAN speeds	
More uniform WAN	
IPsec VPN for teleworkers	Not stated but useful, common
Designated server farm, improved "data center" area	
Wireless for WoWs	
Network management capabilities	
DHCP	
Scalable IP addressing scheme	
QoS-capable equipment	To allow VoIP, IP telephony without replacing network equipment

Step 21 In the “Missing Items” table, document any information that you think is missing from the scenario and that you consider necessary for the design. Teams ask questions of the “customer” (the instructor) to obtain the missing details. Allow 10 minutes for this step.

Missing Items

Missing Item	Customer Response (Provided by Instructor)
Bandwidth information	Not available, because staff has not had time to conduct measurements. Many 100-Mb/s trunks between switches. Servers on 100-Mb/s ports.
Bandwidth use	No data due to unmanageable equipment. Congestion is estimated by observing 80 to 100% use on some uplinks using network taps and Ethereal (current version is Wireshark).
IP telephony, video, videoconferencing, and multimedia plans	All are possible in the two- to five-year timeframe.
Security requirements	HIPAA an important driver. Need "good security."
Wireless already on site? Plans? Requirements? Security requirements for wireless?	Several departmental experiments; generally the hospital suspects they are not adequately secured. Network team has had no time to explore wireless.
QoS needs	ACMC does not know what QoS is.
IP multicast needs	Right now, the hospital is using VoD for some training, continuing education. IP multicast might help reduce bandwidth used and make more efficient use of servers.
Security cameras	Already have coaxial cable plant in place.
Staff mobility requirements?	Secure mobile access is a real need, but ACMC needs to improve the infrastructure before solving that problem.
WAN application usage data	There is no data, due to unmanageable equipment and lack of time.
Network management tools	Ethereal (current version is Wireshark)
Does ACMC headquarters have Internet access today? Do the remote WAN sites require Internet access?	CIO will need to respond to this issue.
What are the future plans for the server farm? Will servers be consolidated to one location? Will that be the present location?	Assume the current location, in Main Building 1, will be used.
Type of WAN that is currently in use	The three existing DS0 circuits are point-to-point links.
WAN backup	There is currently no WAN backup.
Technical constraints (availability of certain WAN services at the remote clinics)	Frame Relay and MPLS are also available to the remote clinics.
Budget available for new solutions	Unknown; perhaps about $500,000
Responsible people	Dwayne Welcher: network architect Dennis Reece: MIS manager
Business constraints, such as policies, goals, and criticality of applications	Medical imaging is identified as the most critical application.

Step 22 Outline the major design areas that you need to address in designing the solution for the given customer scenario. List the tasks, and provide a brief comment for each in the “Major Design Tasks” table.

Major Design Tasks

Design Tasks
1. Identify the relevant applications and their logical connectivity requirements.
2. Divide the network into modules.
3. Identify the scope, that is, which modules are relevant to be redesigned.
4. Identify design alternatives for each module.
4.1 Redesign the campus LAN. The current campus LAN is shared and interconnects three buildings. Because there is also no redundancy, the designer needs to entirely redesign the campus, including the placement of servers.
4.2 Redesign the IP addressing scheme. The flat addressing scheme and static routes are certainly not features of scalable growing networks. New hierarchical addressing is required.
4.3 Design a new routing protocol. The hospital is aware of the drawbacks of static routes. You should implement a dynamic routing protocol that is more scalable and that better fits into the planned hierarchical addressing scheme.
4.4 Upgrade the WAN links. The upgrade of the WAN links is essential because, according to the company, the current bandwidth seems insufficient. The introduction of new applications will result in a higher load because the existing applications will remain.
Note: There are many other ways in which one could improve the customer design. These options will be discussed in later case studies. So, if you do not see your answer on this list, that does not mean that it is incorrect.
5. Identify network applications and services that are required as part of the initial design, as well as what might be added later.
6. (Planning implementation and similar issues would be moving beyond design.)

Case Study 2-1 Answer Key: ACMC Hospital Network Structure and Modularity

Your case study discussion and solution should include these items:

- A high-level diagram of the network, indicating the Cisco Network Architectures for the Enterprise modules
- Notes describing three to five key considerations for each relevant module

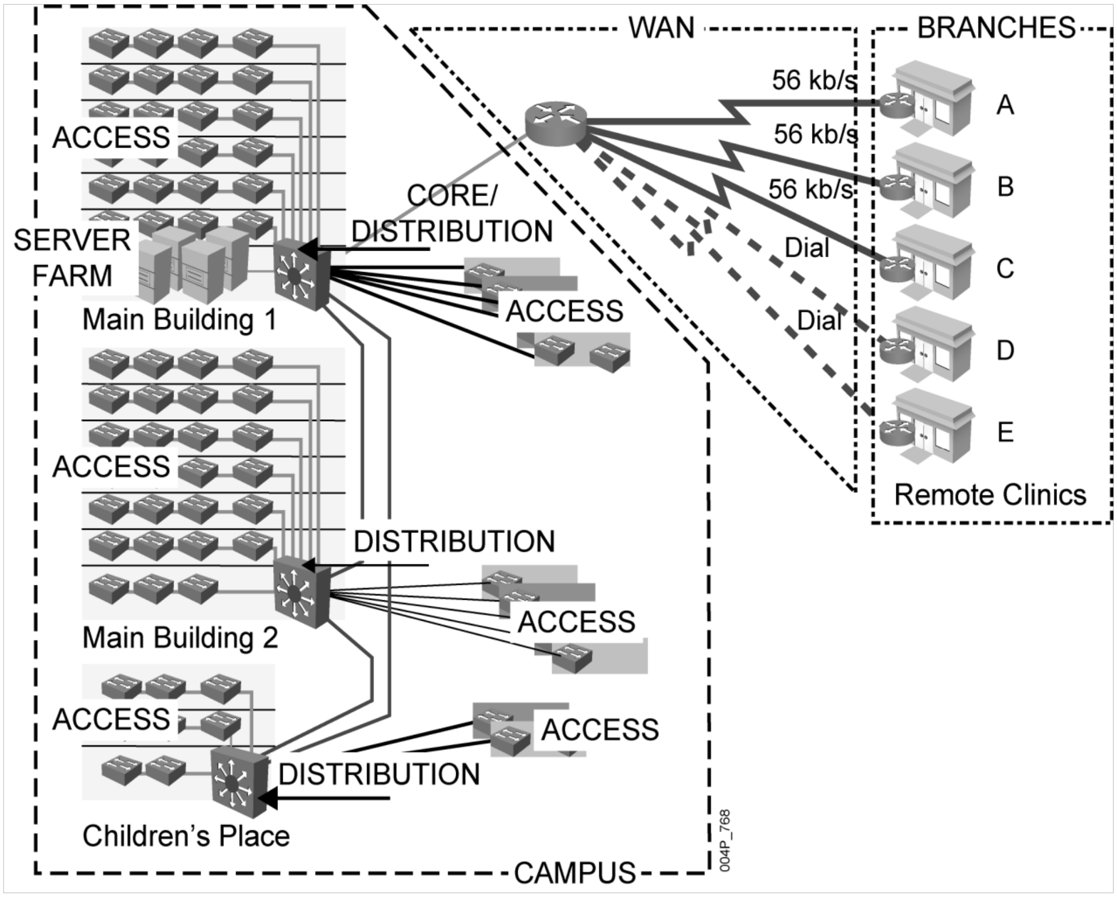
Based on the scenario, this section includes the proposed solutions. According to the case study guidelines, there may be some minor variations in your solutions.

Case Study Solutions

The steps that require solutions are listed here.

Step 1 Consider each of the Cisco Network Architectures for the Enterprise modules and components. At a high level, determine how and where they belong in your design for the future ACMC Hospital network.

The diagram shows the location of each of the Cisco Network Architectures for the Enterprise modules within the network.



Step 2 On a piece of paper, list three to five key considerations or functions for each module. If the module is not being used, state that information.

- Cisco Enterprise Campus Architecture
  - Building access layer
    - This layer supports important services such as broadcast suppression, protocol filtering, network access, IP multicast, and QoS.
    - For high availability, the access switches are dual-attached to the distribution layer switches.
    - This layer can provide PoE and auxiliary VLANs to support voice services.
    - Layer 2 functions such as VLANs and spanning tree can be supported here.
  - Building distribution layer
    - This layer aggregates access networks using multilayer switching.
    - You need this layer for the three main buildings.
    - You may want to combine this layer with the core in at least one building.
    - This layer performs routing, QoS, and access control.
    - Redundancy and load balancing with the building access and campus core layers are recommended.
  - Campus core layer
    - This layer comprises common switches that interconnect the campus buildings and the modules that are located on the campus.
    - This layer provides redundant and fast-converging connectivity between buildings and with the server farm and edge distribution modules.
    - This layer routes and switches traffic as fast as possible from one module to another.
    - This layer uses multilayer switches for high-throughput functions with added routing, QoS, and security features.
  - Server farm module
    - This layer also supports network management services for the enterprise.
    - This layer contains internal email and corporate servers that provide application, file, print, email, and DNS services to internal users.
    - Because access to these servers is vital, as a best practice the servers are connected to two different switches, enabling complete redundancy and load sharing.
    - The server farm module switches are cross-connected with the campus core layer switches for high reliability and availability for servers.
- Cisco Enterprise WAN and MAN Architecture (or Cisco Enterprise Edge Architecture)
  - This module provides reliable WAN connectivity.

  - This module supports traditional media (leased lines) and circuit-switched data link technologies (Frame Relay and ATM), SONET or Synchronous Digital Hierarchy (SDH), cable, DSL, MPLS, and wireless.
  - All Cisco devices that support these WAN technologies, in addition to routing, access control, and QoS mechanisms, can be used in this module.
  - Although security is not as critical when all links are enterprise-owned, you should consider security in the network design.
  - The PSTN module represents the dialup infrastructure for accessing the enterprise network using ISDN, analog, and wireless telephony (cellular) technologies.
- Cisco Enterprise Data Center Architecture
  - This module includes networked infrastructure such as gigabit or 10 Gb, InfiniBand, storage switching, and optical transport.
  - This module includes interactive services such as storage fabric, computer, security, and application optimization services.
  - This module includes management devices such as Fabric Manager (element and network management) and Cisco VFrame (server and service provisioning).
- Cisco Enterprise Branch Architecture
  - This module must be able to connect to the central site to access company information.
  - This module comprises the remote site, remote office, or sales office.
  - This module can benefit from high-speed Internet access, VPN connectivity to corporate intranets, telecommuting capabilities for work-at-home employees, video conferencing, and economical PSTN-quality voice and fax calls over the managed IP networks.
  - The enterprise branch typically uses a simplified version of the enterprise campus network infrastructure.

Step 3 How does this new information change the design? Add to your high-level design, and update your list of modules and considerations.

You will need to add an Internet module and an e-commerce module.

- Enterprise Edge
  - E-commerce module
    - Scalability, security, and high availability within the overall e-commerce network design
    - Web servers
    - Application servers
    - Database servers
    - Firewall or firewall routers
- Internet connectivity module
  - This module provides Internet users with access to information that is published on the enterprise public servers, such as HTTP and FTP servers.

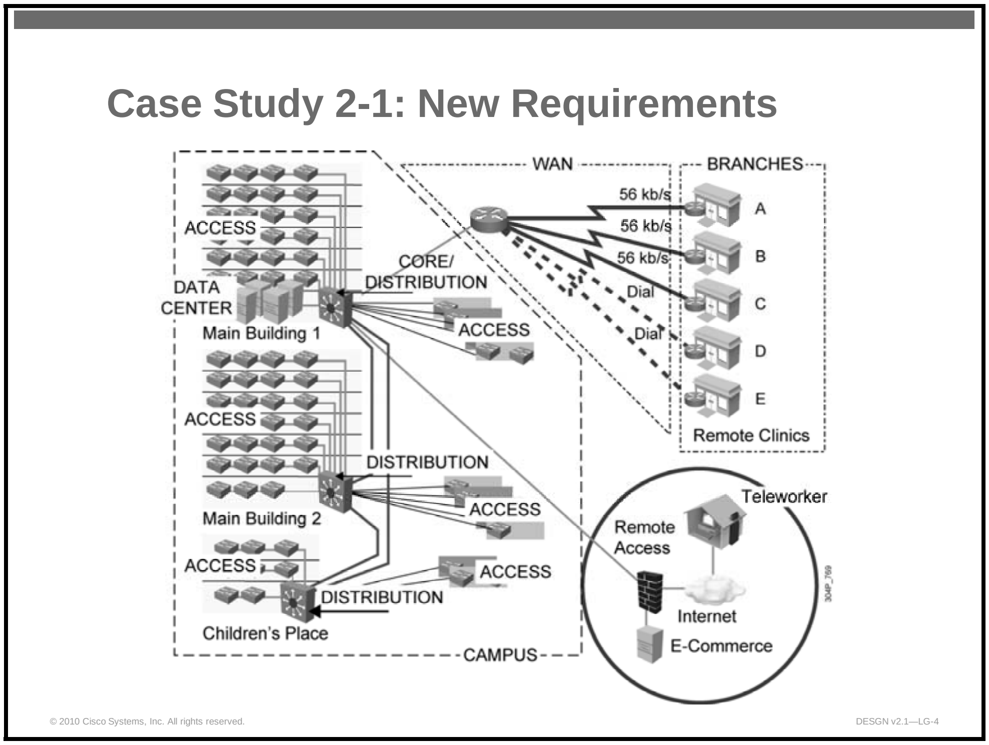
  - This module can accept VPN traffic from remote users and forwards it to the remote access and VPN module, where VPN termination takes place.
  - This module does not serve e-commerce applications.
  - This module can include the following servers and network devices:
    - SMTP mail servers
    - DNS servers
    - Public servers (FTP and HTTP)
    - Firewall or firewall routers that provide network-level protection of resources, stateful filtering of traffic, and VPN termination for remote sites and users
    - Edge routers
- Remote access and VPN module
  - This module initiates VPN connections to remote sites using the Internet connectivity module.
  - This module terminates dial-in connections that are received through the PSTN, and grants dial-in users access to the network.
  - This module can support:
    - Dial-in access concentrators
    - Adaptive Security Appliances
    - Firewalls that provide network-level protection of resources and stateful filtering of traffic, provide differentiated security for remote-access users, authenticate trusted remote sites, and provide connectivity using IPsec tunnels
    - NIDS appliances
- Cisco Enterprise Teleworker Architecture

Note The Cisco Enterprise Teleworker Architecture will be discussed in Module 4 of this course, and it is probably of interest to the customer. Check with the customer before putting in significant effort on teleworker support. Reviewing the Cisco Network Architectures for the Enterprise modules can help you discover the customer requirements.

  - This module comprises a small office with one to several employees or the home office of a telecommuter.
  - This module may also consist of traveling users.
  - Telecommuters working from home tend to use dialup and broadband services, or they may also use a VPN tunnel to the company intranet.
  - Traveling users tend to access the company network via an asynchronous dialup connection through the telephone company, or they may use broadband Internet service and VPN Client software on their laptops.
  - An optional IP phone can be provided to make use of the benefits of a centralized IP communications system.

New Requirements

The planned new modules are shown in this diagram.



Case Study 2-1: New Requirements

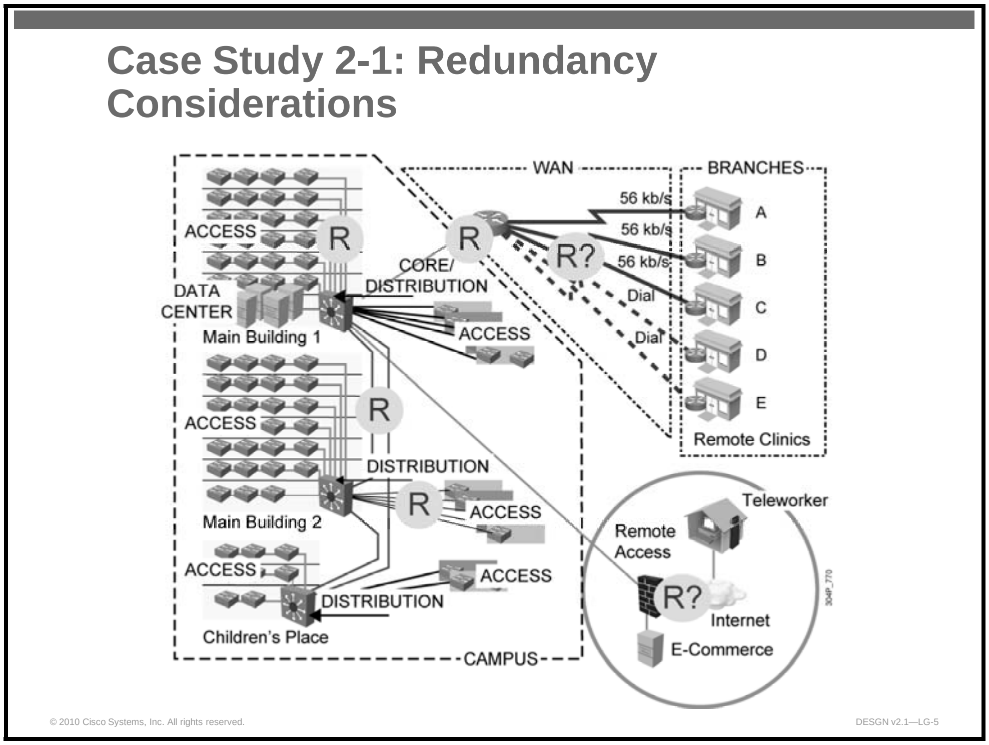
DESGN v2.1—LG-4

Step 1 Which of these infrastructure or network services are immediately applicable to your design, based on the ACMC business objectives and technical requirements from "Case Study 1-1: ACMC Hospital Network Upgrade"? Are there specific locations or modules where some of these services are particularly relevant? Identify these locations or modules in your diagram. Be prepared to describe these services during your presentation.

- Security services should support the Internet, e-commerce, and remote VPN modules. Firewall and IDS may be appropriate.
- Voice services are not immediately applicable.
- Wireless services are not immediately applicable.
- One or two basic network management tools are appropriate.
- High availability is definitely applicable in the campus, and possibly it is needed in the WAN.
- There is no indication that QoS is needed; however, you should build an infrastructure that will support QoS if and when it is needed.
- The customer has indicated some possible uses of IP multicast; therefore, the infrastructure must support IP multicast.

Step 2 Should your design incorporate redundancy? Does it do so? Make sure that your diagram shows appropriate redundancy or indicates the modules or locations where redundancy is appropriate.

The circled “R” in the diagram indicates where redundancy is appropriate.



Case Study 2-1: Redundancy Considerations

DESGN v2.1—LG-5

- The campus needs redundancy as one component of high availability an d reliability. Redundancy is most critical at the core, then at the distribution layer. The access layer is seldom redundant, but redundant uplinks are common.
- You could make the WAN router redundant; the value and cost of making the WAN router redundant depends on the actual WAN technology in use. Doubling the number of WAN links is generally costly. Therefore, the “R?” in the diagram is shown on the WAN links. One common approach is to back up WAN links with site-to-site IPsec VPN. If you are implementing a remote access module anyway, you add minimal cost by using it for backup WAN links.
- The firewall and e-commerce module could be redundant, depending on cost-benefit-risk analysis. Ask the customer about the criticality of e-commerce services, the monetary value to ACMC, and how ACMC values the costs of downtime in comparison to the costs of redundancy.
- If teleworker access is required for productivity rather than convenience, then you should consider redundancy for that module. This is another question to ask the customer.
- Similarly, the Internet module may or may not be redundant, depending on how critical Internet access is for ACMC. This is another question to ask the customer.

Case Study 3-1 Answer Key: ACMC Hospital Network Campus Design

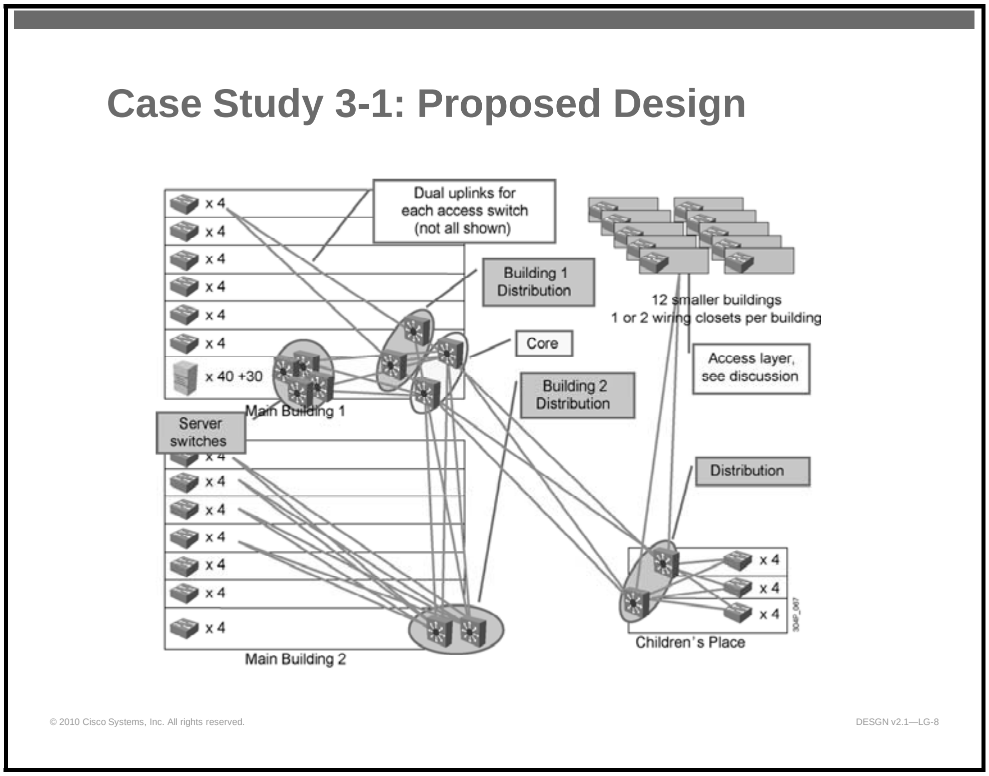
Your case study discussion and solution should include these items:

- A diagram of the proposed design
- Brief documentation giving port counts, types of connections (speeds and feeds), and supporting details
- Brief documentation of pros and cons of the design choices you made compared to the alternatives
- A BOM for your design

Based on the scenario, this section includes the proposed solutions. According to the case study guidelines, there may be some minor variations in your solutions.

Case Study Solutions

The steps that require solutions are listed here. The diagram shows the recommended design.



Case Study 3-1: Proposed Design

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-8

Step 1 Determine the location, quantity, and size of the core switch or switches and what connections there should be within the core.

- Use two core switches for high availability.
- Putting the core switches in the main building with the servers and future data center is best. The server farm or data center is generally the focus of network traffic.
- You could split the switches between two buildings for geographic diversity.
- The precise location of the switches within the building depends on space, where fibers terminate, and so on.

- Two ports are needed for every distribution switch to support uplinks to both core switches. If you count the server switches as combined access and distribution switches, the core switches each need 16 ports (four times four). (Increase this number if more than two server switches are used.)
- Use 1 Gb/s, Gigabit EtherChannel (GEC), or 10-Gb/s links from distribution to core. Note that N-way EtherChannel multiplies the number of ports that are needed by N. For example, four GEC uplinks would mean that 64 ports (4 * 16) are needed.
- You should consider dual power supplies for high availability.
- You should consider dual supervisors in each switch, route processing in the supervisors, or dual supervisors with route processing modules in each switch for even higher availability.

Step 2 Determine the location of distribution layer switches or whether a collapsed core/distribution approach makes more sense. If you use a design with distribution layer switches, determine their location and size, how they connect to the core, the use of VLANs versus Layer 3 switching, and so on.

- Use distribution switches in the three main buildings. You can implement separate core switches and the distribution switches in Main Building 1, because you are consolidating three buildings and a server farm. However, combining the core and distribution layers here is an alternate design.
- Use a redundant pair for high availability in each building.
- Use dual uplinks from each distribution switch to each core switch.
- Use Layer 3 switching at core and distribution layers.
- Note that there would not be enough aggregation if you put distribution or aggregation switches on each floor.
- The following are the port counts from access switch uplinks:
  - — Main Building 1: 6 * 4 = 24 access switches (You also need to add in the server farm switch counts.)
  - — Main Building 2: 7 * 4 = 28 access switches
  - — Children’s Place: 3 * 3 = 9 access switches
- You should consider dual power supplies for high availability.
- You should consider dual supervisor, route processing, or both modules for even higher availability.

Step 3 Determine the location and size of access layer switches. Complete the “Port Counts by Location” table.

Port Counts by Location

Location	Counts	Counts with Spares	Comments
Main Building 1 (Per Floor)	75	150	Six floors
Main Building Server Farm	70	140	Will connect with dual NICs; allows for planned migration of all servers to server farm
Main Building 2 (Per Floor)	75	150	Seven floors
Children’s Place (Per Floor)	60	120	Three floors
Buildings A—D	10 each	20 each	
Buildings E—J	20 each	40 each	
Buildings K—L	40 each	80 each	

- There will be an access switch in every closet. They should all be dual-homed into distribution layer switches.
- For the main buildings, 150 ports are needed (75 people per floor times 2). Dividing the number of ports by four closets means that you need about 38 ports per closet. Round up to 48 and use a 48-port switch. Treat all closets the same for simplicity and common models.
- For the Children’s Place, 120 ports are needed (60 people per floor times 2). Dividing the number of ports by three closets means that you need 40 ports per closet. Also use a 48-port switch at the Children’s Place.
- The following are the port counts for the other buildings:
  - Buildings A–D: 10 people, 20 ports; use a 24-port switch.
  - Buildings E–J: 20 people, 40 ports; use one 48-port switch or two 24-port switches.
  - Buildings K–L: 40 people, 80 ports; use one 96-port switch, two 48-port switches, or four 24-port switches.
- Which combination to use depends on where local cabling terminates. (This issue was not discussed in the case study.) Use one large switch where possible, because one switch is easiest to manage. Use two switches if necessary. You probably do not need four switches, because the case study says that the sites use one or two Brand X switches already.
- If there is sufficient fiber, dual-home all other building access switches to one of the three pairs of distribution layer switches. Because the current fiber runs may go to various main buildings, connect to whichever main building distribution layer switch the fiber goes to. If there is not enough fiber, consider adding more. The less preferable alternative is to dual-home a “primary” switch in any such building to the distribution layer, and daisy-chain the second switch off that.

Step 4 Determine how the access layer switches connect to the distribution layer switches (or to the combined distribution or the core switch). Include such information as speeds, cabling type, and location.

- Assume that the other building connections are as shown in the diagram in “Case Study 1-1: ACMC Hospital Network Upgrade”: Five connections to Main Building 1, five to Main Building 2, and two to the Children’s Place.
- At the time this course was written, the access layer switches would most likely connect via gigabit uplinks.
- For the two main buildings, there are 24 or 28 access switches from the building wiring closets, plus five uplinks from the remote building to each distribution switch, making the port count 29 to 33 ports. (Multiply by N for N-way EtherChannel.)
- For the Children’s Place, there are nine access uplinks from the building wiring closets plus two uplinks from the remote buildings, making the total 11. So, a 12-port distribution switch will suffice, but 16 to 24 ports would allow for growth.
- Assume that all uplinks in buildings are multimode fiber, with distances under 550 m and single-mode fiber between buildings.

Step 5 Verify that you have the correct port counts for all the switches in your design.

Check the port counts from Step 4.

Step 6 Determine how you will manage the server farm. Do you propose connecting the servers to the core switch or switches? To server aggregation switches? Other? If you use server access or distribution switches, determine how they all connect to each other and to the core.

- There are three reasonable options:
  - — Connect servers directly to the core switches.
  - — Connect servers directly to the distribution switches.
  - — Implement separate server switches (two large ones or multiple smaller ones).
- The last option is preferred because it keeps server link transitions and spanning-tree requirements far from the Layer 3 core. For that reason, if you want to reduce cost, you should connect servers to the building distribution switches rather than connecting the server directly to the core switches. If the servers are connected to the distribution switches, you should implement a trunk link between the two distribution switches to avoid black-holing of traffic that is returning to a server VLAN.
- The server switches should start with 48 ports and allow for expansion as servers are consolidated into the server farm or data center and as the number of servers grows.
- You should consider dual power supplies for high availability.
- You should consider dual supervisor, route processing, or both modules for even higher availability.

Step 7 How do the 12 additional buildings (buildings A through L) affect your design? Be sure to determine what size switches to use in each building, and how they connect back to the distribution or core layers.

See Step 6 for specifics.

Step 8 Other than port counts, speeds, and feeds, is there any other information that would benefit your design?

PoE needs and power supply sizing is another level of complexity that the authors of the course decided not to introduce at this point.

Step 9 Determine appropriate Cisco switch models for each part of your campus design.

- You would use the Cisco Catalyst 6500 or 4500 Series Switches for the core and distribution layers.
- You could use the 6500, 4500, 4948, 3750, or 3560 models for server switches. Only the first two of these allow dual power supplies in the chassis.
  - The 4948 switch may be a cost-effective alternative for the server farm. However, it does not provide much in the way of server migration and expansion capacity. You could use a second pair of 4948 switches for that, although the 6506 model switches would provide expansion within a single pair of chassis. For this design, you should initially implement four server switches to allow capacity for the complete server migration.
  - The 6500 and 4500 Series would allow room for growth.
  - You could use the 3750 and 3560 models at rack top and bottom. This approach reduces cabling tangle but increases the number of server switches and the number of uplinks that you must manage.

The table shows one solution that falls somewhere in the middle of the price spectrum.

Layer	Location	Ports	Model	Quantity
Core or Distribution	Main Building 1	20 x N for distribution layer termination	C6506E-S32-GE, power supply (or 2 supplies), 3 WS-X6724-SFP	2
Distribution	Main Building 1	29	C6506E-S32-GE, power supply (or 2 supplies),WS-X6724-SFP (two, or the 6748 48-port SFP blade instead)	2
Distribution	Main Building 2	33	C6506E-S32-GE, power supply (or 2 supplies),WS-X6724-SFP (two, or the 6748 48-port SFP blade instead)	2
Distribution	Children’s Place	11	C3750G-24TS	2
Servers	Main Building 1	40 dual NIC connected, + expansion	C4948-E	4
Access	Main Building 1, 2, CP closets	40	C3560G-48TS-S	62
Access	Buildings A—D	20	C3560G-24TS-S	4
Access	Buildings E—J	40	C3560G-48TS-S	6
Access	Buildings K—L	80	C3560G-48TS-S	4

Note Using 10 Gb/s for distribution or server farm to core would increase performance (and cost). You would also need a Cisco Catalyst 6500 Series Supervisor Engine 720 with integrated switch fabric to realize the performance in the core.

One budget approach would be to use Cisco Catalyst 3750 Series Switches in the core and distribution layers and Cisco Catalyst 2960 Series Switches for closet switches. This design approach is not recommended, however, because it would not provide a distinctive speed advantage in the core. It would also be limited in terms of increasing performance. The Cisco Catalyst 4500 and 6500 models are usually recommended for use in the core and distribution layers in medium to large enterprises.

If time permits, and you have access to a computer and the Internet, complete Steps 10 and 11.

Step 10 (Optional) Use the Cisco Ordering Dynamic Configuration Tool to configure one or more of the switches in your design.

No specific results are desired.

Step 11 (Optional) Develop a BOM that lists switch models, numbers, prices, and total price. If you have access to a PC with spreadsheet software, you may use a spreadsheet to develop the BOM. If not, do your work on paper.

See the sample BOM from the case study. Be aware that it does not represent a complete design.

Case Study 4-1 Answer Key: ACMC Hospital Network WAN Design

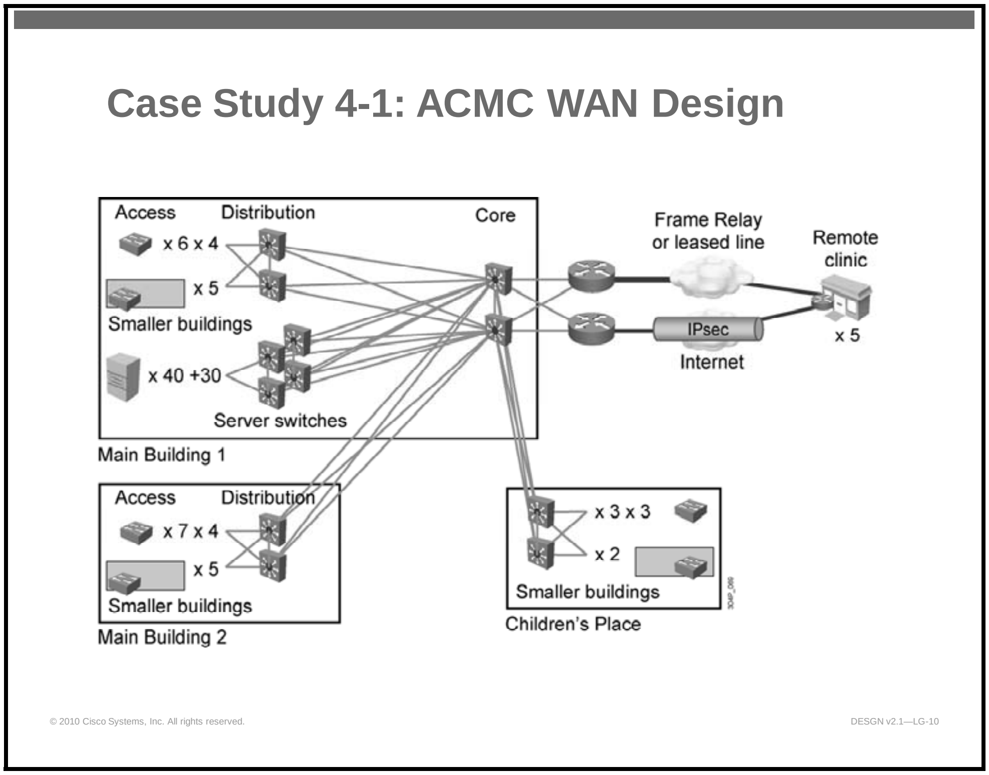
Your case study discussion and solution should include these items:

- A list of requirements to be provided in the ACMC WAN RFP
- The costs for those requirements
- Your recommendation on which technology would best suit ACMC
- Your recommendation on redundancy or a backup WAN strategy
- The appropriate Cisco router model to use at the central site and the appropriate switching hardware for each site
- Any design changes you would make if the CIO wants a second router to be used for the backup link at each site

Based on the scenario, this section includes the proposed solutions. According to the case study guidelines, there may be some minor variations in your solutions.

Case Study Solutions

The steps that require solutions are listed here. The diagram shows the recommended design.



Case Study 4-1: ACMC WAN Design

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-10

Step 1 As a member of the ACMC planning team, develop a short list of requirements and information to be provided in the ACMC WAN RFP. Identify any items about which you think ACMC should be concerned.

- Include the number of sites and the amount of minimum bandwidth that is required to each site. Specifically, you should calculate that each remote site needs at least 256 kb/s, or at least five times the sum of the remote site bandwidths at the central site.
- Include the level of mean time to repair (MTTR) that is acceptable under the SLA.
- Include the level of packet loss, latency, and jitter that is acceptable under the SLA.
- Include how the SLA variables are measured.
- Include the service level that is guaranteed (or that the provider will deliver).
- Include information on any penalties for SLA noncompliance.

Step 2 Calculate the monthly cost for using each of the approaches, and complete the total monthly cost column in the "Monthly Costs" table.

Monthly Costs

Option	Technology	Speed	Price per Month	Monthly Cost
1	Leased-line T1 into central T3 (same LATA)	T1 or T3	$400 for each T1, $8000 for the T3	5 * $400 = $2000 1 * $8000 = $8000 Total = $10,000 per month
2	Frame Relay, T1 access, central T3	T1 or T3	$350 for T1 access, $7000 for T3 access circuit Plus CIR in 5-Mb/s increments times $75 plus $5 per PVC	5 * $350 = $1750 1 * $7000 = $7000 5 * 1.544/5 * $75 = $115.80 5 * $5 = $25 Total = $8890.80 per month
3	MPLS VPN, T1 access at clinics, central T3	T1 or T3	$500 for T1 access, $8500 for T3 access circuit	5 * $500 = $2500 1 * $8500 = $8500 Total = $11,000 per month
4	High-speed business cable service or Internet at clinics	6 Mb/s downstream or 768 kb/s upstream	$90	5 * $90 = $450 1 * $4000 = $4000 Total = $4450 per month
	T3 Internet at central site	T3	$4000	

Step 3 Which technology do you recommend that ACMC use? Remember that Multilink PPP over multiple T1s is also an option.

Here are some things to consider as you prepare your recommendation:

- Leased-line commoditization is reflected in the pricing.
- Frame Relay appears to be cheaper than leased lines (per Mb/s), but the providers are probably oversubscribing their trunks between Frame Relay switches. That is, the CIR is not guaranteed bandwidth.
- MPLS VPN costs more than Frame Relay, at least in the ACMC area.
- Cable is quite competitive on price and bandwidth, but it does not provide the same level of service.
- In regard to the Business Objectives listed in this case study, the issue with cable (and asymmetric DSL [ADSL]) is that moving images from the remote office to the central office is limited to the 768-kb/s upstream speed. You should mention this issue to the customer. Alternatives are to make sure that images are transferred and cached at the main hospital (local access) or to use another WAN technology.
- When you do not know how much bandwidth you actually need, being able to add more "on demand" is attractive. This aspect of Metro Ethernet is currently popular, when it is available. You can shift to multiples of 10, 50, or 100 Mb/s (up to 1000 Mb/s) speeds easily. Inverse Multiplexing over ATM (IMA) allows adding T1 ATM links. Including Multilink PPP on T1 leased lines or multilink Frame Relay over multiple T1 access circuits also allows for some bandwidth growth.
- Note that most hospitals will want a solid SLA.

T1 Frame Relay into T3 at the central site is recommended. This approach should provide guaranteed bandwidth with a good SLA. Assuming that the carrier supports it, multilink Frame Relay can add bandwidth up to 6 Mb/s. Multilink PPP over T1s is also attractive. These two are similar enough and comparable enough in price to be roughly equivalent.

Note This answer is somewhat subjective. There is no perfect answer, because cost may cause some customers to rethink their requirements. For some, cost is more important than SLA. Ultimately, the consultant or designer presents the options and makes a recommendation, and then the customer (or management) makes the choice.

Step 4 Note that transferring a 100-MB image over a T1 takes over 8 minutes. (100 MB * 8 bits/byte / 1.5 Mb/s = 518 seconds.) Does that alter your decision? Why or why not?

This calculation suggests that more bandwidth would be useful, as soon as it becomes affordable. Going from 256 kb/s to 1.5 Mb/s is six times as much bandwidth. Few administrators will authorize the purchase of such a large expansion if there are cheaper alternatives. They are likely to want to try something around four times the bandwidth first. One practical approach to convincing administrators that there may be a lack of bandwidth is to arrange a lab demonstration. You want to show the hospital administrators how long it takes for the medical image to display, and then present the costs for a higher bandwidth solution.

The medical images should probably be prestaged or automatically uploaded and stored centrally. Some imaging applications allow the doctor to mark images for transfer and then view them later when they become available locally. Until Metro Ethernet becomes available, ACMC really will have no other cost-effective option than one of the choices in the Monthly Cost table together with software that is smart about WAN usage.

Step 5 The CIO indicates that remote site availability is critical, to avoid having to support servers at the clinics. Which redundancy or backup WAN strategy do you recommend?

This instance is where IPsec VPN over Internet has become attractive as a lower-cost approach for the backup link. Part of the justification for the lesser SLA is that in an outage, some connectivity is better than none. If the service is bad enough to compromise VoIP or other services, that assumption becomes questionable.

Step 6 Assume that the CIO has chosen to deploy Multilink PPP over two T1s for simple, reliable service. The 6-Mb/s cable service will be used as backup. Select an appropriate Cisco router model to use at the central site and at each remote location. Also, select appropriate switching hardware for each site, remembering that the ISR router models can use integrated switches.

- The Cisco 870, 1800, 2800, and 3800 Series Routers can manage the necessary traffic levels. The 870 router does not support serial ports or ATM WAN.
- The Cisco 1841 router can be used with two-port serial WIC and Fast Ethernet to a cable modem.
- All of the 2800 Series models except the 2801 router can be used with High-Speed Serial Interface (HSSI) T3 links. All of the 2800 Series models support the four-port high-speed T1 HWIC. You could also use the 3800 Series models.
- In conclusion, use the 2800 Series with the four T1 HWIC serial ports at remote sites to allow growth. If cost is an issue, use the 1841 router, but realize that this option limits growth to two T1 ports (which is not a large amount of bandwidth).
- Use an external switch with the 2800 Series, or trade up to the 3800 Series with switching network modules to cover the number of needed ports at each remote

site. Using an external switch preserves options, if you are considering adding a second backup router in the future.

- Use a Cisco 2821 router or 3800 Series model with central site T3 links (one for the leased line and one for the Internet connection).

Step 7 Which design changes would you make if the CIO wants a second router that is used for the backup link at each site?

With two routers, you could use an 870 router for the cable (or DSL) link at each remote site. You would still need a 2800 Series router for four T1 links. At the central site, use two 2800 Series models: one for T3 or ATM T3 and the other for Internet T3.

With two routers at the remote clinics, it makes more sense to use an external switch with two uplinks than to use an integrated switch network module in a 3800 Series router.

Note A routing protocol, Hot Standby Router Protocol (HSRP) or other first-hop routing protocol, and other design features would also be appropriate for your design. These topics are covered in the “Designing Basic Campus and Data Center Networks” module of this course.

Case Study 5-1 Answer Key: ACMC Hospital Network IP Addressing and Routing Protocol Design

Your case study discussion and solution should include these items:

- An IP addressing design.
- An IP address assignment plan.
- Your routing protocol selection and design.

Based on the scenario, this section includes the proposed solutions. According to the case study guidelines, there may be some minor variations in your solutions.

Case Study Solutions

The steps that require solutions are listed here.

Step 1 Determine a suitable summarizable IP addressing plan for ACMC. Include the campus, WAN and backup WAN links, and the remote clinics.

Here are some IP addressing considerations, based on previous case study answers:

- The main buildings have 150 ports per floor, which equals about 48 ports per closet. Seven floors multiplied by 150 ports is 1050 ports total in each building. (These counts include the server farm in Main Building 1.)
- The Children’s Place has 120 ports per floor divided by three closets, which equals 40 ports per closet. Forty ports multiplied by three floors equals 360 ports total.
- Buildings A through D have one 24 port switch each.
- Buildings E through J each have one 48-port switch each or two 24-port switches.
- Buildings K through L each have one switch with 96 ports, two 48-port switches, or four 24-port switches.

- Use 98 ports on the server switches to allow for growth.
- Connections from the access to distribution layers, distribution layer to the core, and the WAN router or routers to the core are all Layer 3 connections, so you can use /30 addressing.
- Each remote clinic WAN link could be a /30. You allow summarization by choosing the links from a common prefix. It would be wise to allow for expansion to more remote sites.
- Recall that five of the small buildings are cabled (connected) to Main Building 1, five to Main Building 2, and two to the Children’s Place. For simplicity, assume small buildings A through E connect to Main Building 1, F through J to Main Building 2, and K through L to the Children’s Place.

The total number of addresses that are needed should fit easily into a Class B address (up to 65,534 hosts). You could use private address 172.16.0.0 /16. Alternatively, using network 10.0.0.0 /8 means you do not have to manipulate bits in the third octet; you can use entire octets. The drawback to using network 10 is that if ACMC ever merges with another organization, and the other party is using network 10, then re-addressing will be needed.

One simple approach is to use the second octet for the building or site number. (The leading four bits of the third octet in 172.16.0.0 could be used in a similar fashion.) The third octet then indicates the floor number, which will provide enough addresses per floor. Use a 24-bit mask on the network 10 addresses to keep addressing simple and divide by four for the number of closets.

As a more complex approach, you could treat buildings A through L as “floors” of a fictitious building. The same thing could be done for remote clinics. This would be less wasteful of address space. However, network 10 provides so much space that you do not need a complex approach.

In the address assignment, treat buildings A through E as connected to Main Building 1, F through J to Main Building 2, and K through L to the Children’s Place. If the actual connectivity were different (for example, Building G connects to Main Building 1), then the building numbers in the “Address Assignments” table could be swapped around to match.

Address Assignments

Building or Site	Address Block	Details
Main Building 1	10.1.0.0 /16	Third octet = floor number, /24 Fourth octet divided into /26 blocks (multiples of 64), one per closet The servers can be addressed as a separate "floor", floor 8.
Building A	10.2.0.0 /16	Put these with Main Building 1 so they can be summarized along with it.
Building B	10.3.0.0 /16	
Building C	10.4.0.0 /16	
Building D	10.5.0.0 /16	
Building E	10.6.0.0 /16	
Reserved	10.7 through 15	Allow room for growth within summarizable block.

Building or Site	Address Block	Details
Main Building 2	10.16.0.0 /16	Third octet = floor number, /24 Fourth octet divided into /26 blocks (multiples of 64), one per closet
Building F	10.17.0.0 /16	
Building G	10.18.0.0 /16	
Building H	10.19.0.0 /16	
Building I	10.20.0.0 /16	
Building J	10.21.0.0 /16	
Reserved	10.22 through 31	Allow room for growth
Children's Place	10.32.0.0 /16	Third octet = floor number, /24 Fourth octet divided into /26 blocks (multiples of 64), one per closet (last one not used)
Building K	10.33.0.0 /16	
Building L	10.34.0.0 /16	
Reserved	10.35 through 47	Some room for future buildings

Building or Site	Address Block	Details
Remote site 1	10.48.0.0 /16	Moving to 10.48 allows room in this block and the prior block to summarize 16 building or site prefixes. For each remote site, reserve 10.xx.0.0 /24 for purposes such as providing /30 subnets for one or two WAN links to the main site.
Remote site 2	10.49.0.0 /16	
Remote site 3	10.50.0.0 /16	
Remote site 4	10.51.0.0 /16	
Remote site 5	10.52.0.0 /16	
Reserved	10.53 through 63	Expansion
Future space	10.64 through 255	Unused space

The necessary /30 blocks to interconnect locations can come from 10.*building*.255.0. For small buildings and remote sites, use addressing from the small building or remote site block, so the connection summarizes with the building or clinic to which it connects.

For access to distribution links, use these port counts:

- The uplink port count for the main buildings is 30 to 33 ports (multiply by N if you perform N-way EtherChannel) for each of the two distribution switches. So, you need two /30 blocks from each of the five small buildings connecting in, plus up to 56 (28 times 2) /30 blocks for closet switches. 10.1.255.0 /24 or 10.16.255.0 /24 provides 64 blocks of four addresses, or 64 /30 blocks, which is enough for those sets of 56 uplink subnets.
- Children’s Place has an uplink port count of 11 for each of two switches. For each of the two small buildings, use two /30 blocks from 10.*building*.255.0 for the small building uplinks. That leaves nine uplinks to each of two distribution

switches, or 18 /30 subnets. 10.32.255.0 provides 64 /30 blocks, so you can use the first 18 of these.

- The WAN router or routers have five remote links to the five remote sites. Multiply by two if redundant WAN routers are used. The /30 blocks can easily come from 10.*building*.255.0 for each remote site.

Six distribution switches, four server switches, plus possibly two WAN routers are redundantly connected to each core switch. That equals a minimum of 24 uplinks to core. For each of the two main buildings and the Children's Place, you could use /30 blocks from the building range. In Main Building 1, you would then have used all the /30 blocks. Another approach is to draw from 10.1.253.0 for all distribution or WAN router to core links, which seems like better option in this instance.

Step 2 Determine how IP address assignment is to take place.

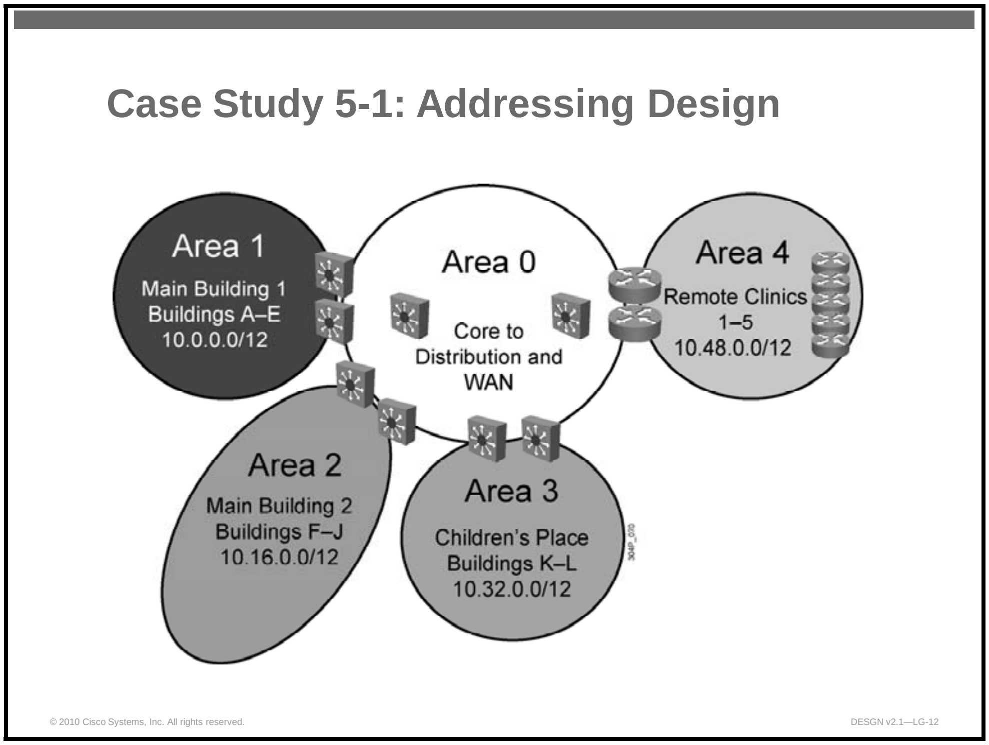
- Use DHCP for the edges (access layer) and static IP addresses between network devices, for management ports, WAN links, and so on.
- Remote clinics could use local DHCP off the router. The alternative is DHCP from the central site. In a WAN outage, the central site DHCP would not be available.

Step 3 Determine a suitable routing protocol or protocols and routing design.

- EIGRP or OSPF fast convergence is recommended.
- Summarization is quite possible within the above addressing scheme.
- If desired, and if there is no backup link, you could use static routes for small buildings and remote clinics. If you use IPsec VPN over Internet, then you would need a static route for 10.0.0.0 /8 through the IPsec tunnel (because 0.0.0.0 /0 points out to the Internet).
- If you use OSPF, make Area 0 cover the links from the core to the distribution layer switches. Use one area for each main building and one for the WAN. You could then summarize everything in the three larger buildings and attached buildings at the distribution layer ABRs: One summary prefix for Main Building 1 and connected small buildings, another for Main Building 2 and connected small buildings, and a third summary for the Children's Place and connected small buildings. Similarly, you could summarize the WAN at the WAN router, which acts as ABRs to the WAN area. This is why addresses were assigned as such, grouping small buildings with large buildings.
- The same summarization boundaries would work for EIGRP.
- In any case, all the remote clinics need for routing is "IP classless" plus a summary route to the rest of network 10.

Step 4 (Optional) Figure out the summary routes for either EIGRP or OSPF from Step 3. What would representative routing tables look like, at various points in the network?

This diagram shows the planned summarizable addressing with OSPF areas.



Case Study 5-1: Addressing Design

Area 1
Main Building 1
Buildings A–E
10.0.0.0/12

Area 0
Core to
Distribution and
WAN

Area 4
Remote Clinics
1–5
10.48.0.0/12

Area 2
Main Building 2
Buildings F–J
10.16.0.0/12

Area 3
Children's Place
Buildings K–L
10.32.0.0/12

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-12

Step 5 (Optional) Go back and rework the design, treating the small buildings as "floors" of a fourth large campus building and the remote clinics as "floors" of a fifth.

The addresses would follow this scheme: 10.*small building prefix*.*small building number*.0 /24 or 10.*WAN prefix*.*clinic number*.0 /24. Build a table as in Step 1.

Step 6 (Optional) Go back and do the design that is based on prefix 172.16.0.0 /16. Use leading bits of the third octet as the "building number."

Case Study 6-1 Answer Key: ACMC Hospital Network Security Design

Your case study discussion and solution should include these items:

- A list of key business security requirements, risks, and threats to ACMC
- Diagrams and text for a secure design for these enterprise edge modules for ACMC, and how they connect to the rest of the ACMC Hospital network:
  - E-commerce .
  - Internet connectivity.
  - Remote access and VPN.
  - WAN and MAN and site-to-site VPN.
- A list of pros and cons of your design.
- A Diagram or notes that document a secure design for remote clinics using Internet with an IPsec VPN for backup access.
- A scheme for suitable IP subnetting for the Internet, DMZ, or VPN complex.
- A list of Cisco Security products and features you would use to secure the three campus layers and data center or server switches.

- A list of some of the other security considerations, products, and features that should be part of deployment, and their locations within the network.

Based on the scenario, this section includes the proposed solutions. According to the case study guidelines, there may be some minor variations in your solutions.

Case Study Solutions

The steps that require solutions are listed here.

Step 1 Identify key business security requirements, risks, and threats about which ACMC should be concerned.

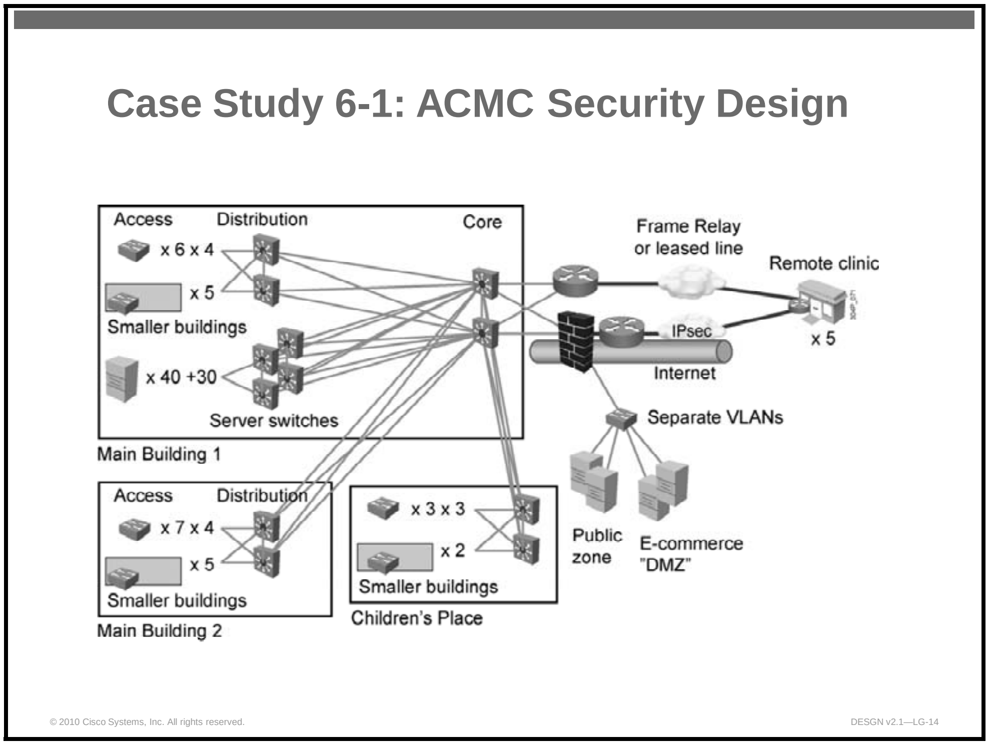
- HIPAA, which is about patient confidentiality and the costs for failure to provide adequate security and confidentiality.
- Denial of service, which could be life-threatening.
- Alteration of records, which could be life-threatening.
- Illicit system or network access, which could lead to denial of service or records alteration.
- Worms, viruses, patch management issues, and other system threats that could deny service or breach record confidentiality.

Step 2 Design these edge modules for ACMC. Also, determine how they should connect to the rest of the ACMC Hospital network. Be prepared to justify your design.

- E-commerce.
- Internet connectivity.
- Remote access and VPN.
- WAN and MAN and site-to-site VPN.

Note Your design can use a consolidated approach in which firewalls are shared between modules.

This diagram shows the single Cisco PIX Firewall (or ASA) approach. Notice that the Internet router is needed to connect to the T3 link, so the PIX Firewall or ASA goes between the router and the core switches.



Case Study 6-1: ACMC Security Design

DESGN v2.1—LG-14

With a suitable PIX Firewall model, you can trunk the VLANs to a switch, with the VLANs separating the public zone and the e-commerce zone or DMZ. The firewall would also secure outbound Internet traffic from ACMC (Internet access for the main campus).

The firewall could terminate IPsec tunnels or pass them through to one or both Cisco Catalyst 6500 Series Switches (as shown in the figure). The device terminating the IPsec tunnels should be equipped with hardware IPsec encryption acceleration.

In both instances, you could use router-to-router GRE tunnels over IPsec to allow simple use of dynamic routing.

Use an ASA if there is significant interest in SSL VPN. ACMC has not mentioned this interest, but asking them about it would be a good idea. (When unsure, always present the options, and pros and cons of each option, to the design customer.)

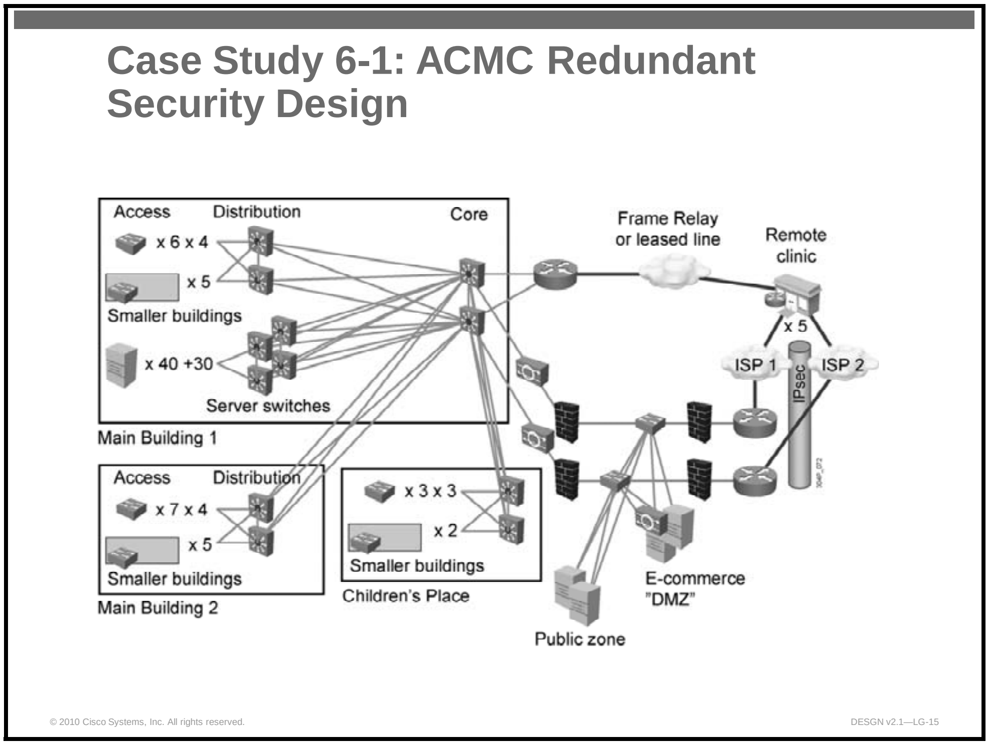
You could use an IPS and add it behind the firewall. You could place another one outside the firewall, but it would then be subject to many alarms. You could also use a FlexWAN module and Cisco Catalyst 6500 Series FWSM instead of a separate Internet router.

You could use IPsec to encrypt the Frame Relay or leased-line links. Some medical organizations use this approach for enhanced HIPAA confidentiality. Others reason that Frame Relay or leased lines are generally secure. Banks or government, judiciary, and law enforcement agencies might use encryption on such links.

Some sites, usually larger sites, prefer a "firewall sandwich" approach. In this approach, two firewalls are used, with one or more switches in between. The idea is that if the outer firewall should somehow be compromised, there is defense in depth. Some security personnel might even use this approach with firewalls from two vendors, to avoid common failure modes and gain support complexity.

Another consideration is Internet redundancy. If Internet access or e-commerce availability is sufficiently important, ACMC should consider headend links to two different ISPs. You might then use dual firewalls and Internet routers to increase availability. This approach increases the routing complexity, including the mechanism to failover from one ISP to another.

This diagram shows a more redundant version of the enterprise edge module, specifically the PIX 500 Series Firewalls or ASA and DMZ functions. While this approach is costly and increases the number of devices to manage, many sites now consider e-commerce (and email) sufficiently important for such a design to be worth the cost.



Case Study 6-1: ACMC Redundant Security Design

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-15

IPS devices were added to this design because an organization investing in this kind of redundancy would probably consider security important enough to want to use IPS devices. Note that an IDS also monitors accesses to the e-commerce servers. Client VPNs can easily be terminated at the firewalls or the IPsec router or routers, to add remote access for doctors or other users.

Step 3 Design security for remote clinics using Internet with VPN for backup access.

- Use the Cisco IOS Firewall and Cisco IOS IPS features in the ISR products to secure remote campuses.
- Use IPsec VPN acceleration for high-performance secure connectivity on backup links across the Internet.
- Use VPN split tunneling so remote Internet traffic does not have to go across an IPsec tunnel and then back out to the Internet from the main campus.
- Optional URL filtering can improve security for remote users.
- NAC and Cisco Security Agent can be added to increase security.

Step 4 Determine suitable IP subnetting for the Internet, DMZ, or VPN complex.

These answers are for the deluxe design (dual firewalls, and so on). The same sort of approach will work for the simpler design.

- One approach is to use 10.7.0.0 /16 for this deluxe design. It is far more address space than you need, which has long-term benefits.
- Use 10.7.1.0 /28 for the VLAN that connects the two inside firewalls to the core switches (four connected devices).
- You need two VLANs between the firewall pairs: one for Public Zone, and one for the e-commerce DMZ. You could use 10.7.2.0 /24 and 10.7.3.0 /24 for these, to provide lots of room for additional servers in each zone.
- You can use 10.7.1.16 /28 for the connections from outer firewalls to routers. Ideally, these should run through switches in a common VLAN to allow HSRP, VRRP, or GLBP.
- The addresses from the routers to the ISPs are provided by the ISPs.
- If you have a GRE tunnel over IPsec to each remote clinic, then you need a subnet for each tunnel. You can use 10.7.1.32, .36, .40, .44, and .48 as /30 subnets. Reserve through .60 for additional (future) tunnels. An alternative is to use /30 subnets from a block allocated for WAN /30 subnets for each site.
- If you allow remote VPN Client access, you need a block of addresses, 107.4.0 /24 for example, for the VPN Client pool.

Step 5 Identify which Cisco Security products and features you would use to secure the three campus layers and data center or server switches.

- IPS for intrusion protection in the campus, particularly for traffic going to or from the servers.
- Cisco Security MARS for event correlation.
- NetFlow, NBAR, and syslog for monitoring and event detection.
- Cisco NAC Appliance for quarantine or patch enforcement, and identity-based access control.
- 802.1x for identity-based networking.
- Endpoint protection (CSA, antivirus, and so on).
- Guest, clerical, and other VLANs can use ACLs to limit the information to which outsiders and selected staff have access.
- Anomaly detection module.

- Cisco Security Management Suite.

Step 6 Identify some of the other security considerations, products, and features that should be part of deployment and where they should be used. For example, what should be done about infrastructure protection?

- Physical protection of devices, including protecting against physical access and theft.
- Cisco IOS security features.
- Infrastructure hardening measures, such as using access classes on Telnet, using access lists on SNMP and web devices, using SSH instead of Telnet, using SCP instead of FTP (requires current Cisco IOS code), and so on.
- Layer 2 security measures, such as out-of-band campus device management, DHCP snooping, ARP inspection, controlling trunking and native VLANs on access ports, and so on.
- Layer 3 (“control plane”) security, such as routing authentication.

Case Study 7-1 Answer Key: ACMC Hospital Network Voice Transport Considerations

Your case study solution should include these items:

- A list of key aspects from the design in “Case Study 6-1: Security Design” that impact the ability to support voice.
- An appropriate IP telephony design model and points in favor of this choice.
- The appropriate IP telephony components that meet the specified design goals.
- Discussion of key points regarding suitability of Internet VPN access for voice support.
- The results of performing simple voice bandwidth calculations, being aware of the impact of header overhead in addition to codec payload bandwidth.
- Your conclusions about using WAN for voice transport.

Based on the scenario, this section includes the proposed solutions. According to the case study guidelines, there may be some minor variations in your solutions.

Case Study Solutions

The steps that require solutions are listed here.

Step 1 Based on the ACMC design up to this point, what are the infrastructure issues that affect voice deployment that you should consider (ignore the IPsec for now)?

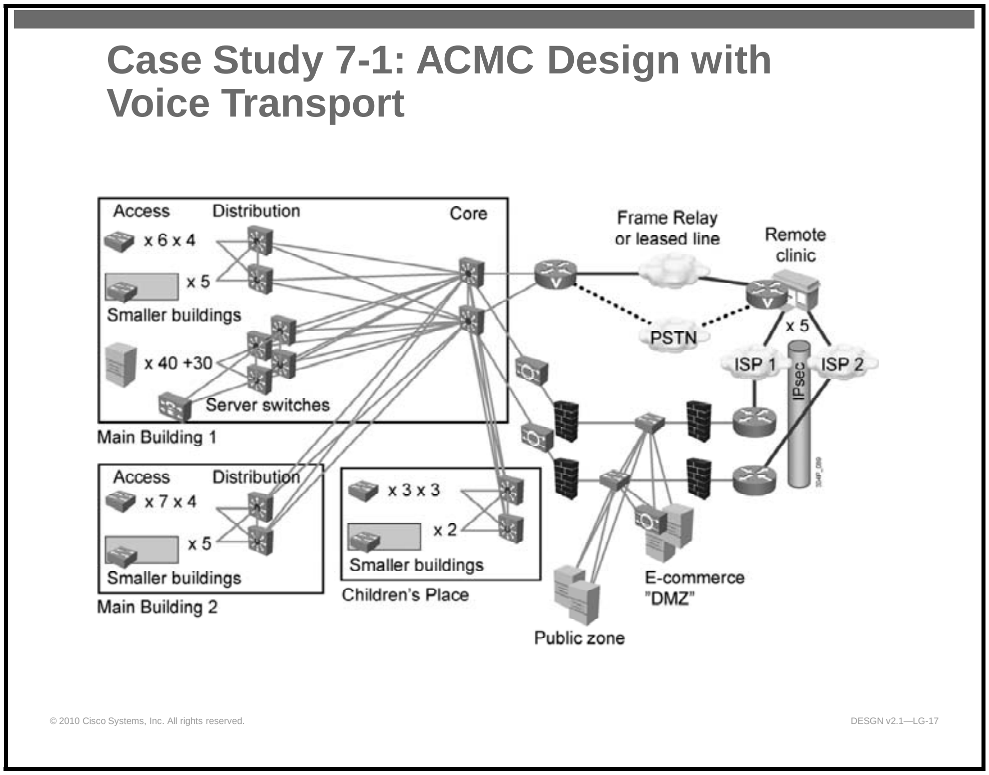
- You should consider using switch and power supplies that support PoE, unless ACMC does not wish to do so.
- You need to review building closet power, cooling, and space. It is wise to collect all possibly relevant data when doing closet surveys (you may want to take photos if possible) because going back for missing information is costly.
- Consider QoS capabilities, even in the campus switches. Make sure switches support the level of QoS ACMC desires.
- Perform an infrastructure assessment. Deployments must use proper cabling, avoid duplex mismatches, and generally be clean, which is something to note with deploying the proposed design.

- You need call data to identify how much WAN bandwidth is needed to support VoIP.
- You need to plan for and configure WAN QoS, which includes CAC for calls from clinics to the main campus. It also includes features such as RTP header compression and LFI.

Step 2 Select the IP telephony design model most appropriate to ACMC. Justify your recommendation that is based on your understanding of the ACMC requirements. Indicate where you would place the various IP telephony components that we have discussed.

- The most appropriate design is multisite WAN with centralized call processing. It potentially reduces costs and simplifies administration. Placing the Cisco Unified CallManager in the server farm is a recommended practice.
- Use SRST and local PSTN connections for survivability at the remote clinics.

This diagram shows the voice transport features in the design.



Case Study 7-1: ACMC Design with Voice Transport

© 2010 Cisco Systems, Inc. All rights reserved. DESGN v2.1—LG-17

Step 3 If each remote clinic is to be able to place local calls without going through the main campus, what will be needed at each site? What needs to be added to support local conference calls?

- Voice gateways.
- DSP resources.
- Local configurations.

Step 4 WAN backup is by IPsec VPN across the Internet. What service characteristics might IPsec or Internet lack? What could you add to your design to remedy this?

- Internet best effort does not support any SLA. Packet loss, high latency, and high jitter can all be expected. This implies poor-quality voice if the IPsec VPN is used for VoIP.

- The dial plan design could route calls via the PSTN if the WAN fails or exhibits poor QoS.
- Another alternative would be to add a second Frame Relay or WAN provider instead of IPsec VPN or Internet for backup. While this would add cost, it would also make the network more robust overall.

Step 5 Look at the call bandwidth, taking into account all Layer 2 and other header overhead, plus 5 percent for signaling. Assume Ethernet and no tunnel overhead. In this case, a G.729 call uses about 25 kb/s with 30-ms digitization interval. A G.711 call with overhead uses about 92 kb/s with a 20-ms digitization interval. Use these numbers to estimate how much WAN bandwidth each ACMC site would need for each of the two codecs.

Remote Clinic	Number of Calls on Trunk to Main Campus	G.711 Bandwidth (kb/s)	G.729 Bandwidth (kb/s)
1	8	8 x 92 = 736	8 x 25 = 200
2, 3, 4, 5	4	4 x 92 = 368	4 x 25 = 100

What conclusions about the ACMC WAN does the calculation in the table imply? Is there enough bandwidth?

- With G.729, bandwidth should not be a big problem.
- With G.711, voice might consume up to one-quarter of the bandwidth on two T1 links.

Case Study 8-1 Answer Key: ACMC Hospital Network Unified Wireless Networking Considerations

Your case study discussion and solution should include these items:

- A design for the location and number of wireless controllers and which models to use, and a plan for managing CAPWAP WLC discovery.
- Design notes for how the hospital separation of traffic requirement affects your wireless design, and a plan to enforce the HIPAA access restrictions.
- Your design for IP addressing for the WLANs.
- Your design for the mobility group or groups.
- Your wireless solution for the remote clinics.
- A design concerning secure guest wireless access.

Based on the scenario, this section includes the proposed solutions. According to the case study guidelines, there may be some minor variations in your solutions.

Case Study Solutions

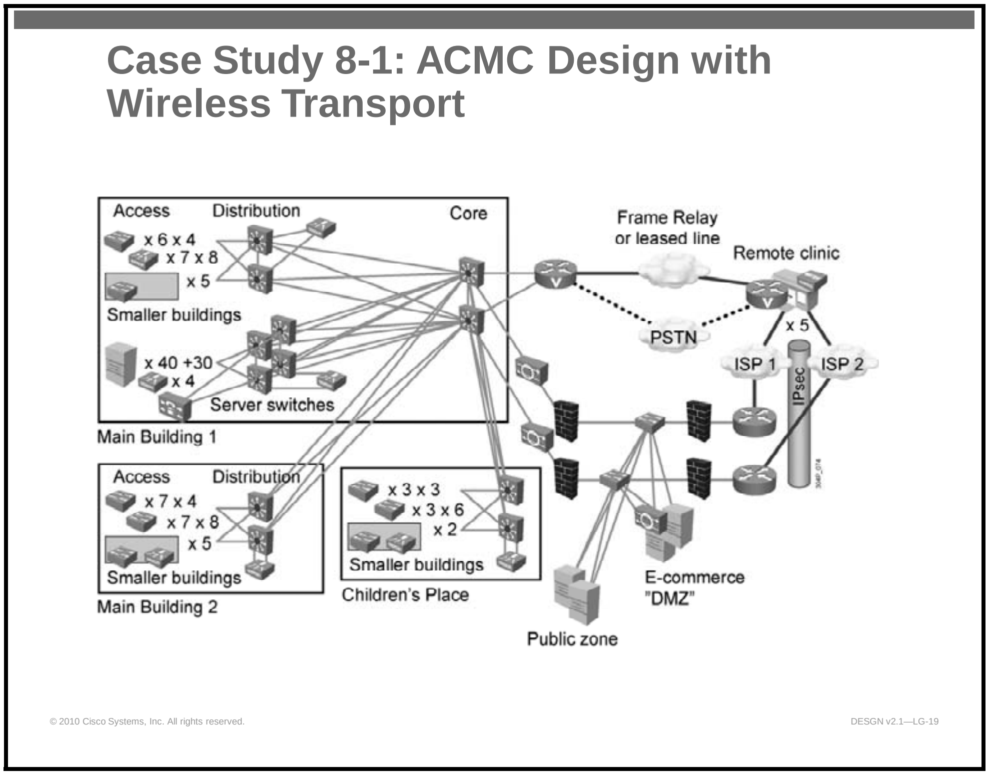
The steps that require solutions are listed here.

Step 1 Determine the location and number of wireless controllers and which models to use. How are you going to manage WLC Discovery? Be prepared to justify your choices.

Note Redundancy requirements were not addressed. In a real-world situation, you should ask the customer so that you would catch this omission.

- One design option is to use Cisco 4404 Wireless LAN Controller with a LAG to support up to 100 access points. This option would allow a distributed approach, with one controller in each main building and the Children's Place. There would be enough capacity so any two controllers could support all 165 access points. You could add another 4404 for additional redundancy. Attach these at the distribution layer in each building.
- As another design option, Remote Clinic 1 may have enough users to support a WLC in the ISR. This option would provide wireless support at the clinic if the WAN link failed.
- Another choice is to use a Wireless Services Module (WiSM) blade in the distribution layer of Main Building 1. If desired, add another blade in a distribution layer switch for redundancy. You need to prioritize wireless control traffic on the WAN.
- Cisco WCS could be added to centralize controller management and provide RF heat maps.
- The CAPWAP WLC discovery process will be Layer 3.

This diagram shows the wireless transport features in the design.



Case Study 8-1: ACMC Design with Wireless Transport

© 2010 Cisco Systems, Inc. All rights reserved.

DESGN v2.1—LG-19

Step 2 The hospital wishes to separate traffic based on its three staff organizations: Financial, Medical, and Support. The intent is to enforce HIPAA compliance by only allowing staff to authenticate to the appropriate SSID based on the type of access the staff needs. How does this affect your wireless design? What could you do to enforce the HIPAA access restrictions?

- You could add WLANs at the controllers. Tie these to the VLANs, which will be subnets at the distribution layer.
- You could have distinctive subnets on the WLANs. Use access lists to control which servers each such subnet (user group) can reach.

Step 3 How will you support the WLANs in terms of IP addressing? How should you modify or extend your IP addressing scheme to the various wireless groups?

- View the WLANs as subnets attached to the network at the distribution switch or switches. Because the VLANs are separated by the Layer 3 core, each building will need different subnets for the VLANs.
- Subnets for each VLAN should come out of the relevant building block of addresses.
- Wired ports are limited by the number of physical ports. With wireless, you have to make some working assumptions to determine how many users to assign per WLAN or VLAN. In this case, you know that each VLAN will be limited to the building. There are 1050 ports in Building 2, corresponding to roughly 500 users. Of these, probably about one-third to one-half is in any one VLAN. If you allow for 500 users per VLAN, there is room for growth or flexibility.
- One approach is to use 10.1.24.0-10.125.255 /23 for one VLAN, 10.1.26 and 10.1.27 for the second, and10.1.28 and 10.1.29 for the third.
- Another approach would be to use pairs of third octet values out of 10.6.0.0 /16 for this, although there is no particular benefit to this approach.
- Another approach would be to use 10.6.0.0 /16 for one VLAN, 10.7.0.0 /16 for the second, and 10.8.0.0 /16 for the third. This approach is an inefficient use of address space. However, the original addressing scheme was also inefficient because the small buildings could have been managed as “pseudo-floors” of the buildings they are attached to.
- If desired, to allow for addition of access points for greater density of coverage, you could use four /24 blocks for 1022 addresses for the VLAN.

Step 4 What will your mobility group or groups be?

Because there are only three or four controllers, it makes sense to put them all in one mobility group.

Step 5 Determine how to manage wireless for the remote clinics.

Run the wireless for the remote clinics off the central controllers, in Building 1 for instance. Use H-REAP access points.

Step 6 Determine how to supply secure guest wireless access.

- Put a controller, a 4402 model for example, in the DMZ, and make it the anchor for the guest WLAN. Note that the 2206 model cannot be used for this.
- A separate guest DMZ would be the best place for secure guest wireless access to protect the formal DMZ servers from hacking.

- You need to assign a subnet for guest wireless access. (This course did not discuss details for IP addressing for public zone and DMZ subnets, VPN Client address pools, GRE over IPsec VPN subnets, and so on.) A suitably sized block of pseudo-floors, such as 10.1.20-23.0, might be used for such purposes.

Case Study 8-2 Answer Key: Connecting More Hospitals to the ACMC Hospital Network

Your case study discussion and solution should include these items:

- Your reaction to ACMC being assigned address block 10.1.0.0 /16.
- A revised addressing scheme for ACMC.
- Key issues to fix in redesigning Hospital Omega to modernize its network and allow robust access to the ACMC data center, and your design proposal.
- An extended IP addressing scheme covering Hospital Omega.
- The key security issue for the Hospital Omega network and two ways to resolve this issue.
- A design to standardize the Hospital Beta network and allow robust access to the ACMC data center.
- The issues involved in centralizing the Hospital Beta server
- The impact if inexpensive Metro Ethernet is available between ACMC and Hospital Beta on server consolidation.
- Your recommendation on whether the Hospital Beta Cisco Unified CallManager and Cisco Unity servers should be moved to the ACMC data center, why they should or should not be moved, and, if they are not moved, how they should interact with a Cisco Unified CallManager on the ACMC campus.
- Your recommendation on whether wireless controllers at Hospital Beta should be moved to the ACMC campus.
- Your recommendation on overall routing protocol and routing design for the merged networks.
- A short list of additional steps that can be taken to improve security in the combined ACMC-OB network.
- Technical comments for the CIO concerning moving Hospital Omega from Centrex service to IP telephony for large savings.

Based on the scenario, this section includes the proposed solutions. According to the case study guidelines, there may be some minor variations in your solutions.

Case Study Solutions

The steps that require solutions are listed here.

Step 1 ACMC has been assigned address block 10.1.0.0 /16. The CIO wants you to determine how to react to this. What alternatives are there to re-addressing all of ACMC? What are their pros and cons? Could ACMC re-address within 10.1.0.0 /16? Assuming it can do so, provide a revised addressing scheme.

- There are two alternatives to re-addressing:
  - — Re-address into 10.1.0.0 /16. Take the list of /24 blocks that were assigned previously and assign them out of summarizable sub-blocks of 10.1.0.0 /16.
  - — NAT all inbound traffic from other hospitals using overlapping parts of network 10. You would also have to NAT outbound ACMC traffic going to other hospitals, into the assigned 10.1.0.0 /16 blocks. This two-way NAT creates complexity and later challenges in troubleshooting.

- Readdressing is preferred to either of the alternatives. The table provides the revised addressing scheme for ACMC.

Address Assignments

Building or Site	Address Block	Details
Main Building 1	10.1.0-7.0 /24	Third octet = floor number, /24 Fourth octet divided into /26 blocks (multiples of 64), one per closet The servers can be addressed as a separate "floor", floor 0.
Reserved	10.1.8.0 /24 10.1.9.0 /24	
Building A	10.1.10.0 /24	These have been put with Main Building 1 so that they can be summarized along with it.
Building B	10.1.11.0 /24	
Building C	10.1.12.0 /24	
Building D	10.1.13.0 /24	
Building E	10.1.14.0 /24	
Reserved	10.1.15.0 /24	Allow room for growth within summarizable block
Main Building 2	10.1.16-22.0 /24	Third octet = 15 + floor number, /24 Fourth octet divided into /26 blocks (multiples of 64), one per closet
Building F	10.1.24.0 /24	
Building G	10.1.25.0 /24	
Building H	10.1.26.0 /24	
Building I	10.1.27.0 /24	
Building J	10.1.28.0 /24	
Reserved	10.1.29-31	Allow room for growth
Children's Place	10.1.32-34.0 /24	Third octet = 31 + floor number, /24 Fourth octet divided into /26 blocks (multiples of 64), one per closet (last one not used)
Building K	10.1.35.0.0 /24	
Building L	10.1.36.0.0 /24	
Reserved	10.1.37-39	Room for growth
WAN and Firewall Links	10.1.40-47	Provides plenty of /30 and other-sized subnets in a summarizable block. Specifically, use 40-44 for the five remote clinic sites, with a /25 or /26 mask, and take WAN /30 subnets from the last 16 address part of the /24. Or, to keep things simpler and to allow for up to 254 hosts at a remote site, take /30 blocks from 10.1.47.0 /24, for use on WAN, GRE tunnel, etc., interfaces. 10.1.48-63 might be used instead if many new remote sites are likely to be added.

Step 2 The CIO wants a design to modernize the Hospital Omega network and allow robust access to the ACMC data center. What issues can you identify? What would you propose to the CIO as your design?

- A flat Layer 2 network is one issue. Stabilize the network by adding Layer 3 switching at the core and gradually work it deeper into the network. Due to lack of DHCP, this will be a long process. Make sure that the Hospital Omega spanning tree issues are isolated behind a Layer 3 device connecting to the other hospitals.
- Old equipment is another issue, and you should propose modernizing it.
- Old cabling is another issue. Conduct random testing of 10 to 20 percent of the cabling to get an idea of its condition. If the cabling is sub-standard, rewire it to bring it up to modern standards. Make sure the new cabling is done in standard structured cabling fashion, not in random runs to odd locations.
- Add redundancy to improve network robustness.
- Move the servers into a controlled environment.

Step 3 Extend the IP addressing scheme to cover Hospital Omega.

- Use 10.1.48-57.0 /24, assigning each floor third octet equal to 47 plus the floor number (where the bottom floor is floor number 1).
- Reserve 10.1.58-63 for things at or connected to Hospital Omega.

Step 4 What is the key security issue for the Hospital Omega network? What are two ways to resolve this issue?

- The main security issue is a lack of firewalling to an external entity (the university, the Internet, and so on).
- Adding a firewall or using Cisco IOS Firewall features will resolve this issue.

Step 5 The CIO wants a design to standardize the Hospital Beta network and allow robust access to the ACMC data center. What issues can you identify? What do you propose to the CIO as your design?

- Having much greater network speed might be an issue in the merger.
- The Hospital Beta network appears advanced and secure.

Step 6 The CIO wishes to consolidate servers in the ACMC data center. What issues need to be examined before proceeding with such a migration?

- You would need a fair amount of WAN bandwidth between Hospital Beta ACMC to relocate servers. Metro Ethernet may or may not provide enough bandwidth.
- If those servers and users are actually using most of that 10 Gb/s core, then relocating the servers is counter-productive.

Step 7 Suppose inexpensive Metro Ethernet is available between ACMC and Hospital Beta. How does this change your answer to the question Step 6?

A 100 Mb/s or 1 Gb/s Metro Ethernet connection may or may not provide enough bandwidth.

Step 8 Hospital Beta already has deployed Cisco Unified CallManager, IP phones, voice gateways, and so on. Should the Cisco Unified CallManager and Cisco Unity servers be moved to the ACMC data center? If so, what would the pros and cons of moving them be? If not, how should they interact with a Cisco Unified CallManager on the ACMC campus?

- Moving the Beta Cisco Unified CallManager means that the two hospitals need to be connected, for example, with dual Metro Ethernet or fiber from two providers over diverse paths. In the short term, leaving the Cisco Unified CallManager where it is would be a lot simpler and less prone to disruption of this critical service.
- Standalone Cisco Unified CallManager systems offer survivability advantages.
- Removing a Cisco Unified CallManager might eventually lower licensing and support costs. Trading the survivability for small savings might not be a good idea.
- The two Cisco Unified CallManager systems can interact via H.323.

Step 9 Should the wireless controllers at Hospital Beta be moved to the ACMC campus?

This issue is similar to the one presented in Step 8. There is no advantage to moving the wireless controllers. Although there may be some slight savings on support if they are eliminated, Hospital Beta would lose wireless if the inter-hospital link were experiencing problems.

Step 10 Make a recommendation on overall routing protocol and routing design for the merged networks.

- Implement EIGRP or OSPF.
- Each hospital address can be summarized.
- Perform these optional tasks:
  - — Determine appropriate addressing for Hospital Beta.
  - — What are the routing summaries each hospital should be advertising to the others?

Step 11 What additional steps can be taken to improve security in the combined ACMC-Omega-Beta (ACMC-OB) network?

- Set up IDS monitoring of traffic between hospitals in case a weakness at one leads to attack on another.
- Use NetFlow or anomaly detection to look for odd traffic flows.
- Consider internal firewalling, either on links between hospitals or in the path to servers. Only those who require access under the security policy should be granted access to patient financial or medical records.

Step 12 Hospital Omega is paying a large amount per phone for Centrex service. The CIO urgently wishes to cut costs by moving to IP phones for Hospital Omega. The ROI on doing this indicates that it would pay for itself in under a year. So, the CIO has asked you for technical comments on doing this. What do you tell her?

Until the Hospital Omega infrastructure is fixed, it would be unwise to deploy IP telephony. The quality of calls would probably be poor and subject to failures. A better plan would be to conduct pilot testing and ramp up staff skills on IP telephony during the infrastructure mitigation project. Then rapidly deploy IP telephony once the cabling and switching are updated.

Course Worksheets

This section includes the worksheets that are discussed in the course materials.

Site Contact Form

1. What is the site location or name?	
2. What is the site address?	
3. What is the shipping address?	
4. Who is the site contact?	Name:
	Title:
	Telephone:
	Mobile:
	Fax:
	Pager:
	Email:
	After hours contact number:
5. Is this site owned and maintained by the customer?	Yes or No
6. Is this a manned site?	Yes or No
7. What are the hours of operation?	
8. What are the building and room access procedures?	
9. Are there any special security or safety procedures?	Yes or No What:
10. Are there any union or labor requirements or procedures?	Yes or No What:
11. What are the locations of the equipment cabinets and racks?	Floor: Room: Position:

Decision Table Worksheet

Use this table to record options for various network parameters.

Option Parameter				Required Network Parameters

Network Locations Worksheet

Use this table to record your own network information.

Location	Type	Comments

Network Locations Size Worksheet

Use this table to record the size of each network location.

Location	Office Type	Work-stations	Servers	IP Phones	Router Inter-faces	Switches Layer 3 Ports	Firewall or Net Devices	Reserve	Total
Total									

Risk Index Calculation Worksheet

Use this table to develop your risk index calculations.

Risk	Probability P (1–3)	Severity S (1–3)	Control C (1–3)	Risk Index (P x S) / C (1–9)

Address Blocks by Location Worksheet

Use this table to develop your own address block information.

Location	Counts	Rounded Power of 2	Address Blocks

Address Assignments

Use this table to record the address assignment blocks.

Location	Address Block	Details