



**Faculty of Computers and Information**  
**Computer Science Department**  
**2014 / 2015**

**Dynamic Uniform Network Distribution**

**Presented by:**

Mahmoud Adel Ahmed  
Mohamed Nabil Radwan  
Mahmoud Wageh Mohamed  
Hamdallah Ramadan  
Hussein Abdullah  
Mohamed Khames

**Supervisor:**

Dr.Amira Idrees  
Dr.Shereen Taie

**Dean:** Dr. Nabila Mohammed Hassan

**Vice Dean:** Dr. Mohamed Alrabeey

**Vice Dean:** Dr. Naglaa

# Acknowledgment

---

## Thanks to Allah

The success of any project depends largely on the encouragement and guidelines of many others. So that we would like to present our deep thanks to many people who guided us through the four years of the faculty.

At first we would like to thank Prof Dr. Nabila Mohamed Hassan dean of the faculty of computer and information sciences at Fayoum University for her continues support and her keenness to encourage us to spread the spirit of interest and initiating, in addition to her great effort in upgrading the faculty to a better level.

We would also like to thank our professors for their efforts and their permanent desire to improve the educational process in the college.

The special thank goes to our helpful supervisors, Dr.Amira Idrees and Dr.Shereen Taie. The supervision and support they gave us truly helped in the progression of our graduation project.

Our regards to the faculty team teaching assistants for their efforts in educating and guiding us.  
Our regards to the college management team and employees

## Abstract

---

Computer networks have become increasingly ubiquitous. However, with the increase in networked applications, there has also been an increase in difficulty to manage and secure these networks.

Most of Universities, Faculties, Units of information technology in faculties, Units of e-learning in universities, Companies using networks, Banks and Insurance companies need networks with High performance and security with low costs to manage and secure their departments (Data).

We have developed Dynamic Uniform Network Distribution, Provide VLANs to connect each department on its VLAN to manage Group of departments on one Switch (Provide Low Costs), Build load balancing and distribution in DUND and chat Allow to departments to speak with each other.

# Content

---

## Chapter 1: Introduction

- **Introduction**
- **Motivation**
  - **Advantages of Dynamic Uniform Network Distribution**
- **System Requirements**
- **System Overview**
- **Documentation Structure**

## Chapter 2: Project Planning

- **SDLC**
  - **Overview**
  - **System Development Phases**
- **Planning**
  - **Planning Steps**
  - **The milestone for the planning phase**
- **Project time plane**
- **Project Scheduling**
- **Requirement Gathering**
- **Project Management**
- **Risk Identification**

## Chapter 3: Background

- **Operation of IP Data Networks**
  - **Recognize the purpose and functions of various network devices such as Routers, Switches, Bridges and Hubs**
  - **Select the components required to meet a given network specification**
  - **Identify common applications and their impact on the network**
  - **Describe the purpose and basic operation of the protocols in the OSI and TCP/IP**
  - **models Predict the data flow between two hosts across a network**
  - **Identify the appropriate media, cables, ports, and connectors to connect Cisco network devices to other network devices and hosts in a LAN**
  
- **LAN Switching Technologies**
  - **Identify basic switching concepts and the operation of Cisco switches**
  - **Describe how VLANs create logically separate networks and the need for routing between them**
  - **Explain network segmentation and basic traffic management concepts**
  - **Configure and verify VLANs**
  - **Configure and verify trunking on Cisco switches**
  - **IP Routing Technologies**
  - **Describe basic routing concepts**
  - **Configure and verify interVLAN routing (Router on a stick)**

- **Network Device Security**
  - **Configure and verify network device security features such as**
  - **Configure and verify Switch Port Security features such as**
- **LAN Switching Technologies**
  - **Identify enhanced switching technologies**
  - **RSTP**
  - **PVSTP**
  - **Ether channels**
  - **Configure and verify PVSTP operation**
  - **Describe root bridge election**
  - **Spanning tree mode**
- **IP Services**
  - **VRRP**
  - **HSRP**
  - **GLBP Load Balancing**
- **Servers**
  - **Domain controller vs. workgroup**
  - **Distributed File System (DFS)**
  - **File Sharing and security**
  - **Security issues (file replications)**

## Chapter 4: System Analysis

- **Overview**
- **System Requirement**
  - **Functional Requirements**
  - **Non- Functional Requirements**
- **USE CASE Diagram**
- **Scenario**

## Chapter 5: System Design

- **Overview**
- **Process Modeling**
  - **Sequence Diagram**

## Chapter 6: Implementation

- **Overview**
- **Implementation**
  - **Server**
  - **Network**
  - **Chatting**

## Chapter 7: Case Study

## Chapter 8: Gain Experiences

- **VRRP, HSRP and GLBP.**
- **Round Robin and weight Round Robin.**

## Reference

# Chapter 1

## Introduction

### 1.1 Introduction

- **Introduction**
- **Motivation**
- **System Requirements**
- **System Overview**
- **Documentation Structure**



For such an extensive and involved subject, which includes so many different technologies, hardware devices and protocols, the definition of networking is actually quite simple. A network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

Networks are used for an incredible array of different purposes. In fact, the definitions above are so simple for the specific reason that networks can be used so broadly, and can allow such a wide variety of tasks to be accomplished. While most people learning about networking focus on the interconnection of PCs and other “true” computers, you use various types of networks every day. Each time you pick up a phone, use a credit card at a store, get cash from an ATM machine, or even plug in an electrical appliance, you are using some type of network.

In fact, the definition can even be expanded beyond the world of technology altogether: I'm sure you've heard the term “networking” used to describe the process of finding an employer or employee by talking to friends and associates. In this case too, the idea is that independent units are connected together to share information and cooperate.

The widespread networking of personal computers is a relatively new phenomenon. For the first decade or so of their existence, PCs were very much “islands unto themselves”, and were rarely connected together. In the early 1990s, PC networking began to grow in popularity as businesses realized the advantages that networking could provide. By the late 1990s, networking in homes with two or more PCs started to really take off as well.

This interconnection of small devices represents, in a way, a return to the “good old days” of mainframe computers. Before computers were small and personal, they were large and centralized machines that were shared by many users operating remote terminals. While having all of the computer power in one place had many disadvantages, one benefit was that all users were connected because they shared the central computer.

Individualized PCs took away that advantage, in favor of the benefits of independence. Networking attempts to move computing into the middle ground, providing PC users with the best of both worlds: the independence and flexibility of personal computers, and the connectivity and resource

sharing of mainframes. In fact, networking is today considered so vital that it's hard to conceive of an organization with two or more computers that would not want to connect them together!

You have undoubtedly heard the “the whole is greater than the sum of its parts”. This phrase describes networking very well, and explains why it has become so popular. A network isn't just a bunch of computers with wires running between them. Properly implemented, a network is a system that provides its users with unique capabilities, above and beyond what the individual machines and their software applications can provide.

Most of the benefits of networking can be divided into two generic categories: connectivity and sharing. Networks allow computers, and hence their users, to be connected together. They also allow for the easy sharing of information and resources, and cooperation between the devices in other ways. Since modern business depends so much on the intelligent flow and management of information, this tells you a lot about why networking is so valuable.

Here, in no particular order, are some of the specific advantages generally associated with networking:

- **Connectivity and Communication:** Networks connect computers and the users of those computers. Individuals within a building or work group can be connected into local area networks (LANs); LANs in distant locations can be interconnected into larger wide area networks (WANs). Once connected, it is possible for network users to communicate with each other using technologies such as electronic mail. This makes the transmission of business (or non-business) information easier, more efficient and less expensive than it would be without the network.
- **Data Sharing:** One of the most important uses of networking is to allow the sharing of data. Before networking was common, an accounting employee who wanted to prepare a report for her manager would have to produce it on his PC, put it on a floppy disk, and then walk it over to the manager, who would transfer the data to her PC's hard disk. (This sort of “shoe-based network” was sometimes sarcastically called a “sneaker net”.)

True networking allows thousands of employees to share data much more easily and quickly than this. More so, it makes possible applications that rely on the ability of many people to access and share the same data, such as databases, group software development,

and much more. [Intranets and extranets](#) can be used to distribute corporate information between sites and to business partners.

- **Hardware Sharing:** Networks facilitate the sharing of hardware devices. For example, instead of giving each of 10 employees in a department an expensive color printer (or resorting to the “sneaker net” again), one printer can be placed on the network for everyone to share.
- **Internet Access:** The Internet is itself an enormous network, so whenever you access the Internet, you are using a network. The significance of the Internet on modern society is hard to exaggerate, especially for those of us in technical fields.
- **Internet Access Sharing:** Small computer networks allow multiple users to share a single Internet connection. Special hardware devices allow the bandwidth of the connection to be easily allocated to various individuals as they need it, and permit an organization to purchase one high-speed connection instead of many slower ones.
- **Data Security and Management:** In a business environment, a network allows the administrators too much better manage the company's critical data. Instead of having this data spread over dozens or even hundreds of small computers in a haphazard fashion as their users create it, data can be centralized on shared servers. This makes it easy for everyone to find the data, makes it possible for the administrators to ensure that the data is regularly backed up, and also allows for the implementation of security measures to control who can read or change various pieces of critical information.
- **Performance Enhancement and Balancing:** Under some circumstances, a network can be used to enhance the overall performance of some applications by distributing the computation tasks to various computers on the network.
- **Entertainment:** Networks facilitate many types of games and entertainment. The Internet itself offers many sources of entertainment, of course. In addition, many multi-player games exist that operate over a local area network. Many home networks are set up for this reason, and gaming across wide area networks (including the Internet) has also become quite popular. Of course, if you are running a business and have easily-amused employees, you might insist that this is really a **disadvantage** of networking and not an advantage.

## 1.2 Motivation

---

Most of Corporates face problems in load balancing and distribution need networks with High performance and security with low costs to manage and secure their departments (Data).

### 1.2.1 Advantages of Dynamic Uniform Network Distribution

---

Networks is considered one of the most important factor to Success Enterprises in their communication so it is the backbone to enterprises, Enterprises face High-risk in management of network, Such as security and quality of communication that improve easy reach to data. These provide the core motivation for DYND:

- Load balance in Routers provide high quality of communication in delivering data to destination quickly, and have role in security when one of two Router break down not lead to break down in network.
- Management of departments by defining roles for everyone in enterprise and identify relation between departments (access list in routers).
- Distributed File server provide improving management to data, when do update in files do that's update in same files in other Servers.

## 1.3 System Requirements

---

### **Domain controller (DC):**

Is a server that responds to security authentication requests (logging in, checking permissions, etc.) within the Windows Server Domain

One domain controller per domain was configured as the Primary Domain Controller (PDC); all other domain controllers were Backup Domain Controllers (BDC).

A BDC could authenticate the users in a domain, but all updates to the domain (new users, changed passwords, group membership, etc.) could only be made via the PDC, which would then propagate these changes to all BDCs in the domain. If the PDC was unavailable (or unable to communicate with the user requesting the change), the update would fail. If the PDC was permanently unavailable (e.g. if the machine failed), an existing BDC could be promoted to be a PDC. Because of the critical nature of the PDC, best practices dictated that the PDC should be dedicated solely to domain services, and not used for file/print/application services that could slow down or crash the system. Some network administrators took the additional step of having a dedicated BDC online for the express purpose of being available for promotion if the PDC failed

### **File server:**

is a computer attached to a network that has the primary purpose of providing a location for shared disk access, i.e. shared storage of computer files (such as documents, sound files, photographs, movies, images, databases, etc.) that can be accessed by the workstations that are attached to the same computer network. The term server highlights the role of the machine in the client–server scheme, where the clients are the workstations using the storage. A file server is not intended to perform computational tasks, and does not run programs on behalf of its clients. It is designed primarily to enable the storage and retrieval of data while the computation is carried out by the workstations.

### **DNS server:**

Is any computer registered to join the Domain Name System? A DNS server runs special-purpose networking software, features a public IP

address, and contains a database of network names and addresses for other Internet hosts.

### **VLAN Overview:**

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

VLANs are usually associated with IP sub networks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. LAN port VLAN membership is assigned manually on a port-by-port basis.

### **Inter-Van Routing:**

Is the capability to route traffic between VLANs? This functionality could be on the Switch itself (for Layer 3 Switches), on another module or card on the switch (for modular switches) or even an external router.

### **Distributed File System (DFS):**

Is a client/server -based application that allows clients to access and process data stored on the server as if it were on their own computer? When a user accesses a file on the server, the server sends the user a copy of the file, which is cached on the user's computer while the data is being processed and is then returned to the server.

Ideally, distributed file system organizes file and directory services of individual servers into a global directory in such a way that remote data access is not location-specific but is identical from any client. All files are accessible to all users of the global file system and organization is hierarchical and directory-based.

Since more than one client may access the same data simultaneously, the server must have a mechanism in place (such as maintaining information about the times of access) to organize updates so that the client always receives the most current version of data and that data conflicts do not arise.

Distributed file systems typically use file or database replication (distributing copies of data on multiple servers) to protect against data access failures.

Sun Microsystems' Network File System (NFS), Novell NetWare, Microsoft's Distributed File System, and IBM/Transacts DFS are some examples of distributed file systems.

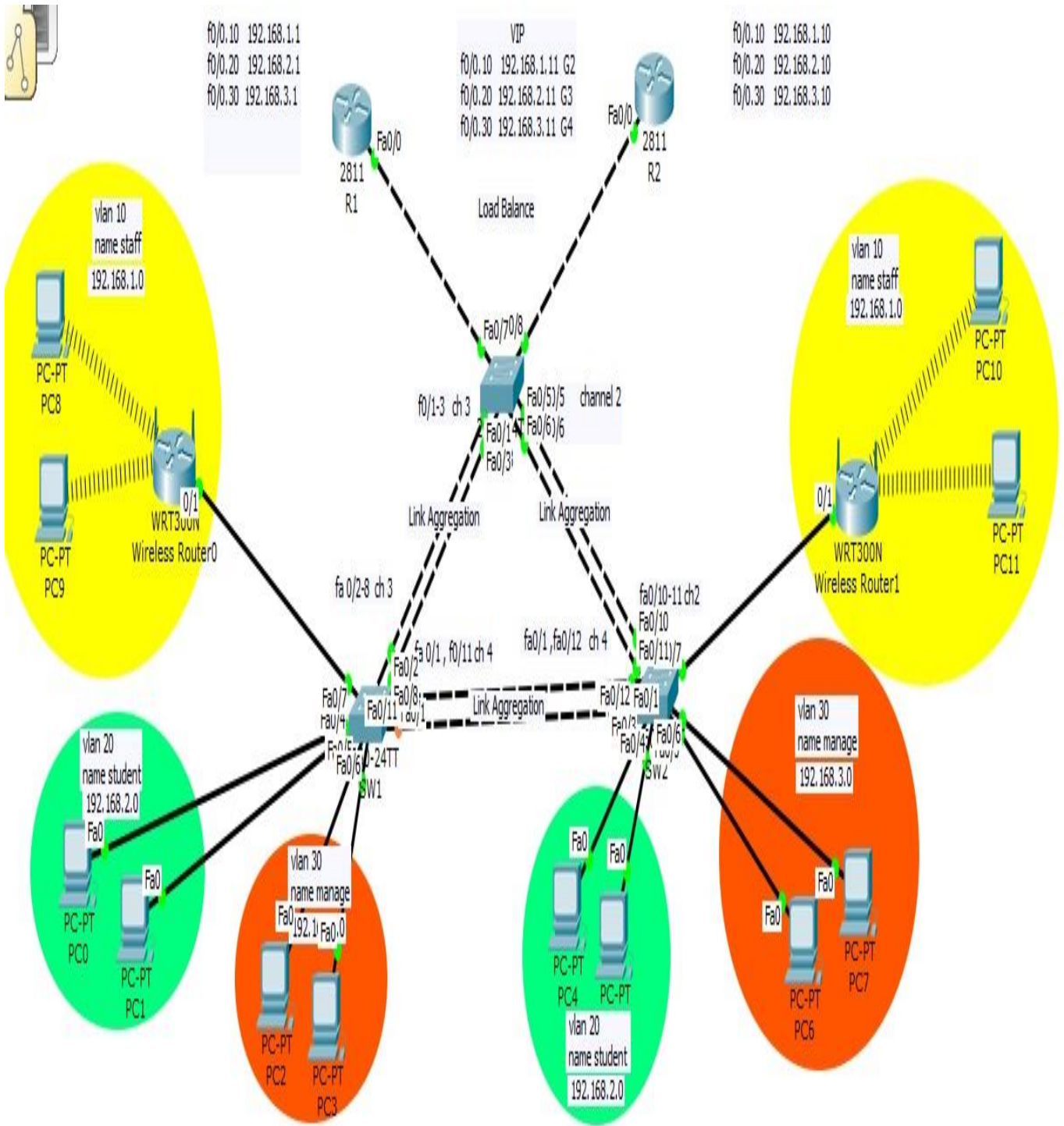
<u>Sno</u>	Input	Quantity	Output
1	Windows server 2012 Data center	2	Domain Controller
2	Windows 7	10	Radius Server
3	Configuration Files	4	File Server
4	Cisco Router	2	Backup Domain Control
5	Cisco Switches	3	DHCP Server
6	Cisco Access point	4	DNS Server
7	Cables	20	VLAN
8	Visual studio		InterVlan
			High Availability
			Security
			Fault tolerance
			Scalability
			<u>Distributed File System</u>
			<u>Voice Chat</u>
			<u>Network Access Protection</u>
			Load Balance

## 1.4 System Overview

---

In our project we have 3 Switches one of them is a core switch and this core switch Joins two another switches with double cables one of them is redundancy of another because if one of them had a problem the second work automatic and this will make high Availability of our network and another switches both of them have Cisco Access point to make us add many numbers of computers , two servers and we can increase number of servers to make a load Balance on them one of these servers is A domain controller and the second is a backup for it and we have DHCP server to distribute IP addresses on computers automatic and we have DNS server to entered on any computers with name rather than IP address and we will create any number of VLANS as we need on both switches for example each department has A VLAN and we will join core switch to two Cisco router to make as Inter-VLAN and we make a load Balance between Two Routers and we will make a distributed file system that when we add ,delete or update on one server it can change them for all servers automatic and we will make NAP that make or support security in our network that checks each computer on the network if it hasn't antivirus it setup antivirus on this computer then enters on the network , our project support high availability ,security , fault tolerance and Scalability , Scalability : that we can increase our network in any time easily by adding any numbers of switches to our core switch . And we will **make chat in our networks to make departments speak to each other.**





**Figure 1.1 System overview**

## 1.5 Documentation Structure

---

At this section, this document is briefed. This document consists of seven chapters that are organized as follows:

**Chapter 1** introduces “Dynamic Uniform Network Distribution” and presents its objectives and features.

**Chapter 2** presents planning

**Chapter 3** provides a background about the technologies and techniques used in the system, and present some of the similar related systems.

**Chapter 4** presents the analysis phase of the system.

**Chapter 5** presents the design phase of the system.

**Chapter 6** focuses on implementation and technical parts issues of the system.

**Chapter 7** describes test case scenarios for the system.

**Chapter 8** describes Gain Experiences for the system

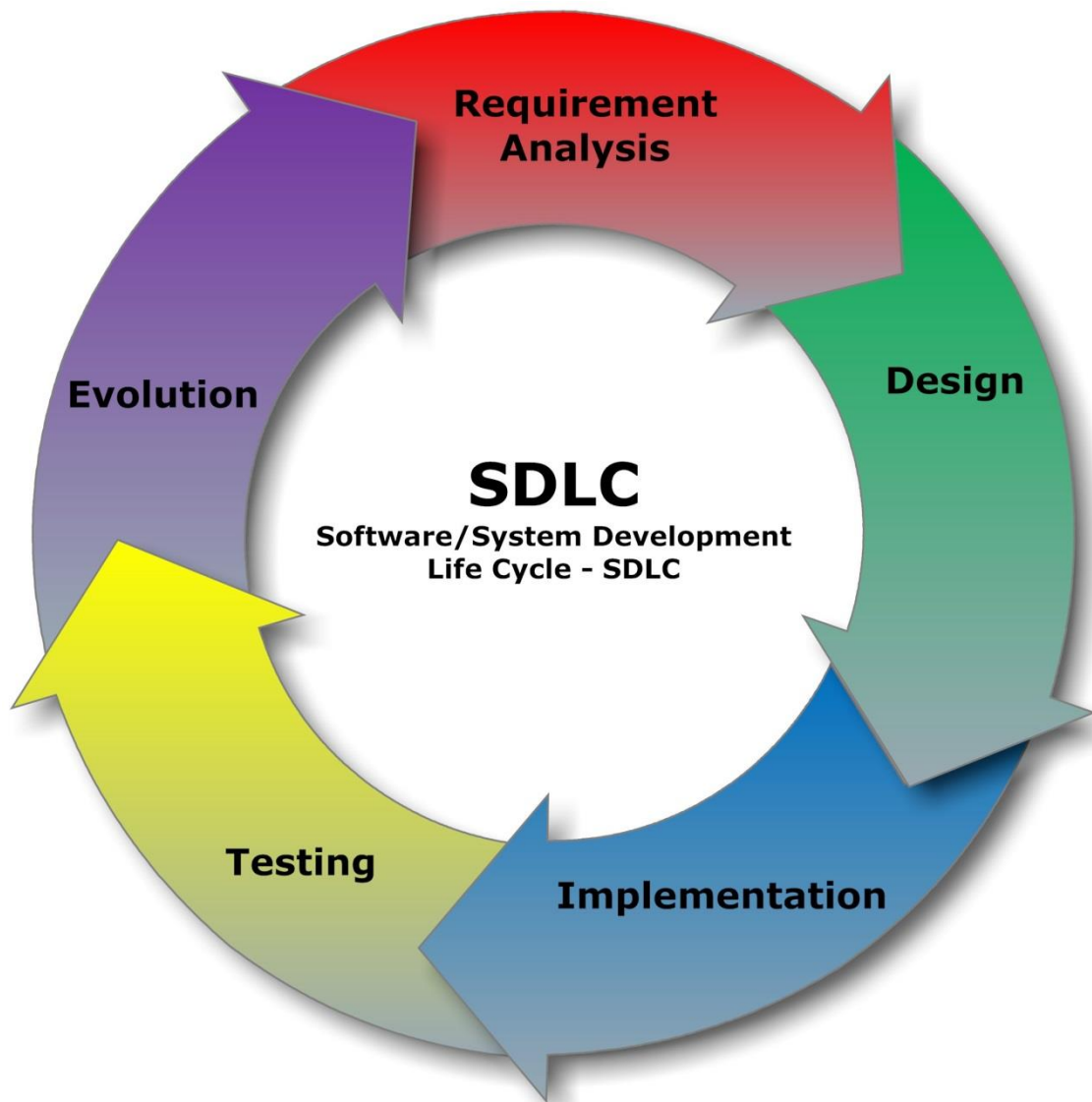
# Chapter 2

## Introduction

- **SDLC**
- **Planning**
- **Project Time Plan**
- **Project Scheduling**
- **Requirement Gathering**
- **Project Management**
- **Risk Identification**

## 2.1 SDLC

---



The **Systems Development Life Cycle (SDLC)**, or Software Development Life Cycle in systems engineering, information systems and software engineering, is the process of creating or altering systems, and the models and methodologies that people use to develop these systems.

The concept generally refers to computer or information systems. Emphasis on this article (SLDC) is on man-made technological life-cycle. But there are many other life-cycle models to choose from. This includes ecological life

cycles, for every life cycle, whether biological or technological, has a beginning and an end. In software engineering the SDLC concept underpins many kinds of software development methodologies. These methodologies form the framework for planning and controlling the creation of an information system.

### 2.1.1 Overview

---

**Systems Development Life Cycle (SDLC)** is a process used by a systems analyst to develop an information system, including requirements, validation, training, and user (stakeholder) ownership.

Any SDLC should result in a high quality system that meets or exceeds customer expectations, reaches completion within time and cost estimates, works effectively and efficiently in the current and planned Information Technology infrastructure, and is inexpensive to maintain and cost-effective to enhance.

Computer systems are complex and often (especially with the recent rise of Service-Oriented Architecture) link multiple traditional systems potentially supplied by different software vendors. To manage this level of complexity, a number of SDLC models or methodologies have been created, such as "waterfall"; "spiral"; "Agile software development"; "rapid prototyping"; "incremental"; and "synchronize and stabilize".

SDLC models can be described along a spectrum of agile to iterative to sequential. Agile methodologies, such as XP and Scrum, focus on lightweight processes which allow for rapid changes along the development cycle.

Iterative methodologies, such as Rational Unified Process and Dynamic Systems Development Method, focus on limited project scope and expanding or improving products by multiple iterations.

Sequential or big-design-up-front (BDUF) models, such as Waterfall, focus on complete and correct planning to guide large projects and risks to successful and predictable results.

Other models, such as Anamorphic Development, tend to focus on a form of development that is guided by project scope and adaptive iterations of feature development.

In project management a project can be defined both with a project life cycle (PLC) and an SDLC, during which slightly different activities occur.

According to Taylor (2004) "the project life cycle encompasses all the activities of the project, while the systems development life cycle focuses on realizing the product requirements.

### 2.1.2 Systems development phases

---

The System Development Life Cycle framework provides a sequence of activities for system designers and developers to follow.

It consists of a set of steps or phases in which each phase of the SDLC uses the results of the previous one.

A Systems Development Life Cycle (SDLC) adheres to important phases that are essential for developers, such as planning, analysis, design, and implementation, and are explained in the section below.

A number of system development life cycle (SDLC) models have been created: waterfall, fountain, and spiral build and fix, rapid prototyping, incremental, and synchronize and stabilize.

The oldest of these, and the best known, is the waterfall model: a sequence of stages in which the output of each stage becomes the input for the next.

*These stages can be characterized and divided up in different ways, including the following:-*

- **Project planning, feasibility study:** Establishes a high-level view of the intended project and determines its goals.
- **Systems analysis, requirements definition:** Defines project goals into defined functions and operation of the intended application. Analyzes end-user information needs.
- **Systems design:** Describes desired features and operations in detail, including screen layouts, business rules, process diagrams, pseudo code and other documentation.
- **Implementation:** The real code is written here.
- **Integration and testing:** Brings all the pieces together into a special testing environment, then checks for errors, bugs and interoperability.
- **Acceptance, installation, deployment:** The final stage of initial development, where the software is put into production and runs actual business.
- **Maintenance:** What happens during the rest of the software's life: changes, correction, additions, and moves to a different

computing platform and more? This, the least glamorous and perhaps most important step of all, goes on seemingly forever.

## 2.2 Planning

---

Planning is a process for accomplishing purposes. It is a blue print of business growth and a road map of development. It helps in deciding objectives both in quantitative and qualitative terms. It is setting of goals on the basis of objectives and keeping in the resources.

### What should a plan be?

A plan should be a realistic view of the expectations. Depending upon the activities, a plan can be long range, intermediate range or short range. It is the framework within which it must operate. For management seeking external support, the plan is the most important document and key to growth. Preparation of a comprehensive plan will not guarantee success, but lack of a sound plan will almost certainly ensure failure.

### 2.2.1 Planning Steps

---

*Planning can be summarized in 3 easy steps:*

- choosing a destination,
- evaluating alternative routes, and
- Deciding the specific course of your plan.



Helps management to clarify, focus, and research their businesses or project's development and prospects.

- Provides a considered and logical framework within which a business can develop and pursue business strategies over the next three to five years.
- Offers a benchmark against which actual performance can be measured and reviewed.

The term is also used for describing the formal procedures used in such an endeavor, such as the creation of documents, diagrams, or meetings to discuss the important issues to be addressed, the objectives to be met, and the strategy to be followed .

Beyond this, planning has a different meaning depending on the political or economic context in which it is used.

### **Two attitudes to planning need to be held in tension:**

- On the one hand we need to be prepared for what may lie ahead, which may mean contingencies and flexible processes .
- On the other hand, our future is shaped by consequences of our own planning and actions.

This initial phase starts by defining the need. The objective may vary a great deal in nature and form .

In the planning phase the team needs to thoroughly understand the business model of the customer and their current IT state. They document the customer's inventorying application, information, and technology resources, record their locations, and analyze and prioritize their usefulness to business process.

After considering many businesses and IT factors, the team documents a plan, which identifies and prioritizes projects that will move the organization closer to the desired architecture.

## 2.2.2 The milestone for the planning phase

---

**The milestone for the planning phases** the Project Plan Approved milestone, in which the customer approves of the plan of action and authorizes the next step .

During the Release Planning phase, feasibility studies are performed, user requirements are defined, high level estimates are produced and compared to forecasts of the Performing Organization's capacity, business cases are prepared and all possible projects are prioritized to assist in project selection.

Scenarios may be created to investigate possible combinations of projects (features) that would be affordable based on the capacity of the Performing Organization. Many of these activities are performed on an ongoing basis as new customer requests are submitted.

**The Release Planning Review Board** is responsible for evaluating, prioritizing, and determining which service requests will be included in the next release. They ultimately direct the fate of the release and are the key decision-makers in the relative prioritization of requests and resource commitments.

**The Release Planning Review Board** is appointed by the OCE and should include the Project Sponsor and representative(s) (Director/V.P.

level) from Product Management, Channel Marketing, Engineering, Technical Support, and Program/Project Management .

With the exception of the Project Sponsor and Program manager assigned to the release, the Release Planning Review Board members remain constant release after release. The Release Planning Review Board may or may not be the same the Gate Review Board defined below depending on how the organization structure is defined.

The planning stage of the system development life cycle begins with a request to the system analyst; this is known as the system request.

## 2.3 Project time plan

Analysis			
Tasks	Start Date	FinishDate	Persons
▪ Switch 1	20/10/2014	27/10/2014	Mahmoud Adel Mohamed Nabil Mahmoud Wageh
Basic Switch configuration	20/10/2014	22/10/2014	
Create Vlan	23/10/2014	24/10/2014	
Switch configuration	25/10/2014	27/10/2014	
▪ Switch 2	28/10/2014	5/11/2014	
Basic Switch configuration	28/10/2014	30/10/2014	
Create Vlan	1/11/2014	2/11/2014	
Switch configuration	3/11/2014	5/11/2014	
▪ Servers	6/11/2014	20/11/2014	
Root Server	6/11/2014	8/11/2014	
DHCP Server	9/11/2014	10/11/2014	
DNS Server	11/11/2014	12/11/2014	
Web Server	13/11/2014	14/11/2014	
NAP	15/11/2014	16/11/2014	
DFS	17/11/2014	18/11/2014	
Backup Server	19/11/2014	20/11/2014	Hussein Abdalaah Hamdalah Ramadan Mohammed Khamis
▪ Router	21/11/2014	28/11/2014	
Basic Router Configuration	21/11/2014	23/11/2014	
Router Configuration	24/11/2014	28/11/2014	
▪ Programming	29/11/2014	12/12/2014	
Voice Chat	29/11/2014	6/12/2014	
Web Site	7/12/2014	12/12/2014	

Project	11/12/2014	12/12/2014	
Design			
Tasks	Start Date	Finish Date	Persons
• Switch 1	13/12/2014	20/12/2014	Mahmoud Adel
Basic Switch configuration	13/12/2014	14/12/2014	Mohamed Nabil
Create Vlans	15/12/2014	16/12/2014	Mahmoud Wageh
Switch configuration	17/12/2014	20/12/2014	
• Switch 2	13/12/2014	20/12/2014	
Basic Switch configuration	13/12/2014	14/12/2014	
Create Vlans	15/12/2014	16/12/2014	
Switch configuration	17/12/2014	20/12/2014	
• Servers	21/12/2014	12/1/2014	
Root Server	21/12/2014	24/12/2014	
DHCP Server	25/12/2014	27/12/2014	
DNS Server	28/12/2014	30/12/2014	
Web Server	1/1/2014	3/1/2014	
NAP	4/1/2014	7/1/2014	
DFS	8/1/2014	9/1/2014	
Backup Server	10/1/2014	12/1/2014	
• Router	13/1/2014	20/1/2014	Hussein Abdalaah
Basic Router Configuration	13/1/2014	15/1/2014	Hamdalah Ramadan
Router Configuration	16/1/2014	20/1/2014	Mohammed Khamis
• Programming	21/1/2014	12/2/2014	
Voice Chat	21/1/2014	30/1/2014	
Web Site	1/2/2014	12/2/2014	

Implementation			
Tasks	Start Date	Finish Date	Persons
• <b>Switch 1</b>	13/2/2014	27/2/2014	Mahmoud Adel
Basic Switch configuration	13/2/2014	17/2/2014	Mohamed Nabil
Create <u>Vlans</u>	18/2/2014	22/2/2014	<u>Mahmoud Wageh</u>
Switch configuration	23/2/2014	27/2/2014	
• <b>Switch 2</b>	28/2/2014	12/3/2014	
Basic Switch configuration	28/2/2014	2/3/2014	
Create <u>Vlans</u>	3/3/2014	7/3/2014	
Switch configuration	8/3/2014	12/3/2014	
• <b>Servers</b>	13/3/2014	27/4/2014	
Root Server	13/3/2014	22/3/2014	
DHCP Server	23/3/2014	27/3/2014	
DNS Server	28/3/2014	2/4/2014	
Web Server	3/4/2014	10/4/2014	
NAP	11/4/2014	17/4/2014	
DFS	18/4/2014	22/4/2014	
Backup Server	23/4/2014	27/4/2014	
• <b>Router</b>	28/4/2014	5/5/2014	Hussein Abdalaah
Basic Router Configuration	28/4/2014	1/5/2014	<u>Hamdalah Ramadan</u>
Router Configuration	2/5/2014	5/5/2014	Mohammed Khamis
• <b>Programming</b>	13/2/2014	27/4/2014	
Voice Chat	13/2/2014	16/3/2014	
Web Site	17/3/2014	27/4/2014	
• <b>Network Established</b>	28/4/2014	5/5/2014	Mahmoud Adel Mohamed Nabil <u>Mahmoud Wageh</u> <u>Hussein Abdalaah</u> <u>Hamdalah Ramadan</u> <u>Mohammed Khamis</u>



Testing			
Tasks	Start Date	Finish Date	Persons
• Switch 1	6/5/2014	13/5/2014	Mahmoud Adel
Basic Switch configuration	6/5/2014	7/5/2014	Mohamed Nabil
Create Vlans	8/5/2014	9/5/2014	Mahmoud Wageh
Switch configuration	10/5/2014	13/5/2014	
• Switch 2	6/5/2014	13/5/2014	
Basic Switch configuration	6/5/2014	7/5/2014	
Create Vlans	8/5/2014	9/5/2014	
Switch configuration	10/5/2014	13/5/2014	
• Servers	14/5/2014	3/6/2014	
Root Server	14/5/2014	18/5/2014	
DHCP Server	19/5/2014	22/5/2014	
DNS Server	23/5/2014	25/5/2014	
Web Server	26/5/2014	27/5/2014	
NAP	28/5/2014	29/5/2014	
DFS	30/5/2014	1/6/2014	
Backup Server	2/6/2014	3/6/2014	
• Router	4/6/2014	15/6/2014	Hussein Abdalaah
Basic Router Configuration	4/6/2014	7/6/2014	Hamdalah Ramadan
Router Configuration	8/6/2014	15/6/2014	Mohammed Khamis
• Programming	28/4/2014	15/6/2014	
Voice Chat	28/4/2014	15/5/2014	
Web Site	16/5/2014	15/6/2014	
• Network Established	15/6/2014	22/6/2014	Mahmoud Adel Mohamed Nabil Mahmoud Wageh Hussein Abdalaah Hamdalah Ramadan Mohammed Khamis

## 2.4 Requirement Gathering

Requirements gathering are an essential part of any project and project management, understanding fully what a project will deliver is critical to its success. In addition to it is one of our biggest and most important tasks to try and get the most out of when engaging with stakeholders. This is really an important phase/ milestone in the project life cycle. Requirements help establish a clear and common understanding of what the product must accomplish. Good requirements start with good sources; primary sources of are the Stakeholders: Customers – Users –Report –Procedures.

## Techniques to Gather Requirements

- **Brainstorming**

Project began when one of the team members suggested the idea a Dynamic Uniform Network Distribution), and it seemed searched for and a general idea about the configuration and determine the possibility implemented. Both of them brainstorm the idea of collective and clarify the vision each one how he sees the idea. The ideas are collected can review, analyze and prioritize the ones, the resulting consensus of best ideas is used for the initial Requirements.

- **Group interviews / meetings**

More than one person is being interviewed -- usually two to four. Group interviews can be more productive if interviewees are at a similar level or from the same section within a department and the same level or has the same role.

Team member was held a meeting with an expert who works in Networking and other one works in cloud computing. They started to give us some ideas about both of them (Networking and Cloud Computing) .They described for us the techniques about them. We discussed with them about our idea and availability to build it and they motivated us to work hard in our project and return to them when we need.

- **Prototyping**

Prototyping comprises collection of requirements without function. It enables to see a potential solution and get a better feel for what they require. In addition to the possibility of adding or modifying the requirement. With the prototype being reworked on an iterative basis, until requirements are taken root.

**Advantages:** Good for exploring how a particular software function requirement. It can identify problems with requirements and can improve the quality of requirements and hence the Final solution.

## 2.5 Project Management

---

Due to the multifaceted nature of projects, there are many activities that fall under the umbrella term –project management.|| To oversee a project from its initial stages through to its completion requires a number of skills, including the ability to manage resources, set dates, and facilitate communication. The following is a list of common project-management related activities:

Project management is the process of defining, planning, organizing, leading and controlling the development of an information system project. It is necessary to track or measure the progress we have achieved towards a goal we wish to accomplish. We use project management to aid us in maximizing and optimizing our resources to accomplish our goals

- Setting goals within the overall framework of the project and ensuring that they are complete on time and in a satisfactory way.
- Establishing timetables for the project and its various subtasks. Monitoring the use of time for maximum efficiency.
- Estimating the resources, both material and human, required by the project and ensuring that they are distributed and used properly. Setting a budget for the project and keeping it within that budget.
- Organizing relevant documents and records so that they may be conveniently consulted by those working on the project.



- Analyzing the current conditions of the project and predicting future trends so as not to be caught off-guard by changes.
- Identifying potential risks to the project. Developing a risk management plan to deal with unfavorable contingencies.
- Assigning short-term tasks to specific groups or individuals and recording the progress made toward their completion.
- Managing any issues that affect the project; keeping an issue log that organizes issues by type and priority.
- Managing the quality of the products of the project. Providing adequate quality control and quality assurance. Finding ways to improve quality.
- Properly monitoring the closing stages of a project that is near completion.

## 2.6 Risk Identification

---

The main risks types' facing development of this system are the follows:

### Time risks

- This is due to compression of schedule of the project.
- Optimistic evaluation of time estimates.
- Dropping off important tasks from estimates.

### Budget risks

- This is due to un-predictable developing cost since project requires several experiments which can't be determined at earlier stages.

### Requirement risks

- This can happen due to incomplete, incorrect, inconsistent, volatile or unclear requirements.

Risks facing the project are the following:-

**-Network Connection failed**

# Chapter 3

## Background

- **Operation of IP Data Networks**
- **LAN Switching Technologies**
- **Network Device Security**
- **LAN Switching Technologies**
- **IP Services**
- **Servers**

## 3.1 Operation of IP Data Networks

---

### **Recognize the purpose and functions of various network devices such as Routers, Switches, Bridges and Hubs**

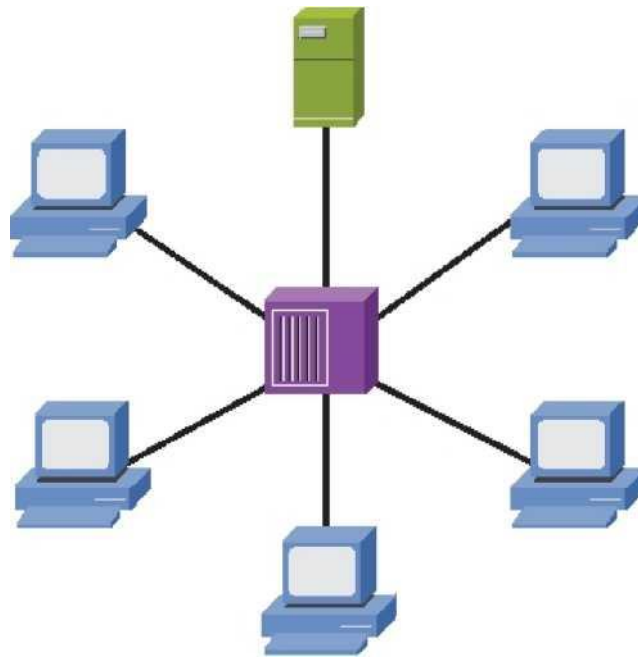
#### Repeaters

Repeaters are Layer 1 devices utilizing the Physical Layer and are considered as outdated technology today. They have been replaced by Hubs and Switches. But for the purposes of understanding; a repeater consists of a transmitter and a receiver. The function of a repeater is to receive the signal, amplify it and retransmit it enabling the signal to be transmitted over a longer distance.

Repeaters are essential to maintain the quality of signals as they degrade over a distance. Repeaters regenerate and retiming the signal, helping it travel a longer distance. Repeaters may be single port or multi port. The figure given below illustrates a repeater.

#### **Figure 1: A Repeater Hubs**

A Multiple Port Repeater is termed as a Hub. It is also a Layer 1 device utilizing the Physical Layer. It can comprise of ports varying from 2 to 24 in number and may also be known as a workgroup hub. Its main job is cleaning up signals. By isolating the end points, Hubs increase the network reliability. A hub retransmits data on all the other ports. A twisted pair cable is used for achieving physical connectivity. The figure given below illustrates a HUB



**Figure 2: A Hub**

### **Types of Hubs**

Hubs can be of two types; Active and Passive hubs. The difference between the two is that Active Hubs regenerate the incoming signal, whereas the Passive Hubs do not do so. Active Hubs need individual power supply to help with the gain of signal before the data is forwarded to all ports. Gain is an electrical term, representing the ratio of signal output to signal input of a system.

The advantage of Hubs is that they are inexpensive. If more efficient use of bandwidth and its distribution among the ports is required, hubs may not be the best option. Traffic congestion because of collisions on the network is indispensable while using hubs. The best solution in this case is to use a switch.

### **Network Interfaces:**

Network interfaces provide connectivity between an end-user computers to the public network. Depending on the interface that is being used, up to three light-emitting diodes (LEDs) may appear. These diodes help to determine the status of the connection.

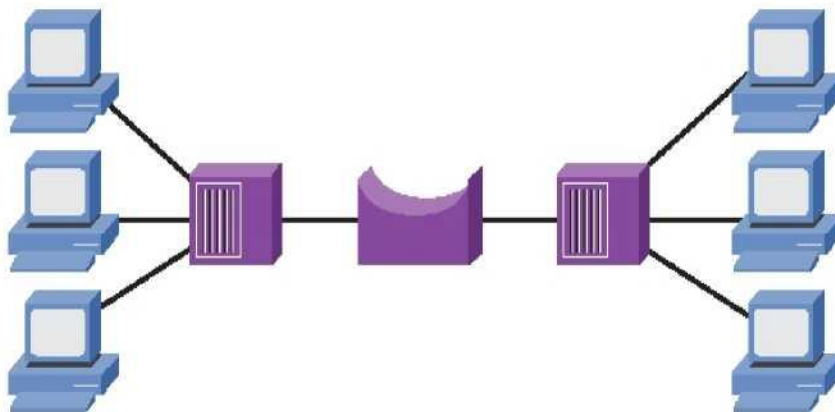
- The Link Light LED: It lights up when the connectivity is there;
- The Activity Light LED: It flickers if some activity is taking place on

- the line;
- The Speed Light LED: This light indicates the connection speed. It may be there on the interface, it may not be there.

Blinking lights and colors other than green are indicative of error conditions.

### **Bridges:**

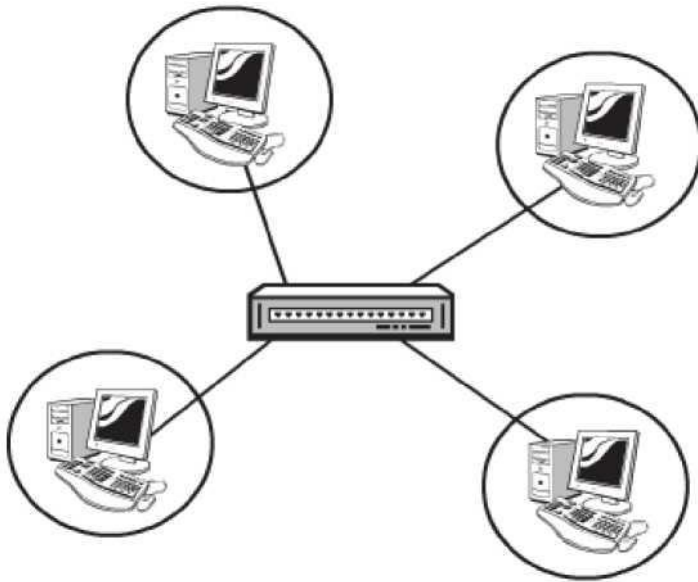
Bridges were used as a solution for issues relating to network congestion. Hubs and Repeaters were longer proving sufficient to meet the challenges provided by systems growing complex. In comparison to Repeaters and Hubs and Bridges used the concept of segmentation. Repeaters and Hubs which do not use segmentation, share the same bandwidth and hence the traffic congestion on a network. When the other device on the network is not aware of the existence of a Bridge, it is called a Transparent Bridge. Figure 3 given below illustrates a Bridge.



**Figure 3: A Bridge**

### **Switches:**

Switches are very smart Bridges with the characteristics of being multi port and high speed. They differ from bridges in the point that bridges process frames in software whereas switches process frames in hardware. Switches do so by using application integrated circuits (ASIC's). Figure 4 given below illustrates a Switch.



**Figure 4: A Switch.**

In addition to the above mentioned Switches have the following features:

- **Speed Back Plane:** this function increases the speed of the network; it allows monitoring of multiple conversations.
- **Data Buffering:** This function allows storage of frames and later forwarding the frame to the right port.
- **High Port Density:** Switches can support multiple ports at one time.
- **High Port Speed:** Switches can support high speeds varying from speeds from 10 Mbps to 10Gbps.
- **Lower Latency:** Latency is a term that is used to measure the time it takes an incoming frame to come back out of a switch. In the case of switches latency is low.
- **VLAN's:** This feature allows segmentation of networks into separate broadcast domains.

These features permit micro segmentation.

### **Micro segmentation:**

Micro segmentation means that a dedicated switch ports are created for every end station; meaning that dedicated paths for sending and receiving transmission with each connected hosts are created. These reduce traffic congestion to a great extent for the reason that separate collision domain and individual bandwidth is available for every host. But faster computers, broadcasts and multicasts can still cause congestion.

Bridges and Switches perform the following tasks:

- **Ascertainment of MAC Address:** Examine the source MAC address of every inbound frame to ascertain its MAC address;
- **Filtration/Forwarding:** Depending on the destination of the MAC

- address, filtration or forwarding of frames as the case may demand;
- Elimination: Eliminating loops caused by superfluous connections.

## **Select the components required to meet a given network specification**

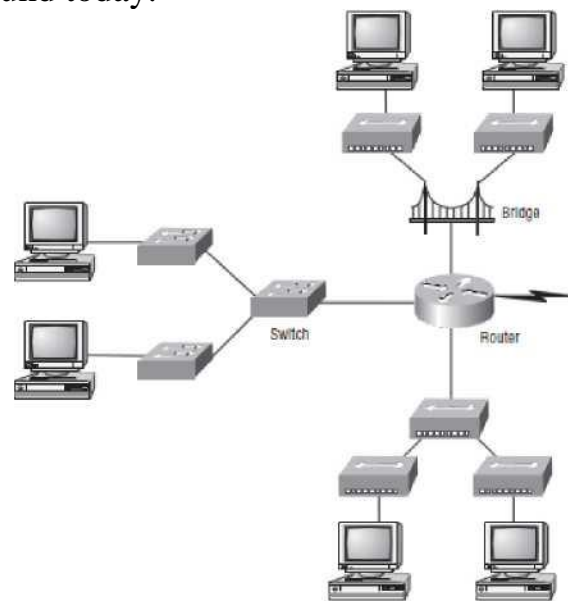
Select the components required to meet a network specification  
As mentioned in the previous objectives, we use routers, bridges, and switches in an internetwork. Figure 1.5 shows how a network would look with all these internetwork devices in place. Remember that the router will not only break up broadcast domains for every LAN interface, it will break up collision domains as well.

When you looked at Figure 1.5, did you notice that the router is found at center stage and that it connects each physical network together? We have to use this layout because of the older technologies involved—bridges and hubs.

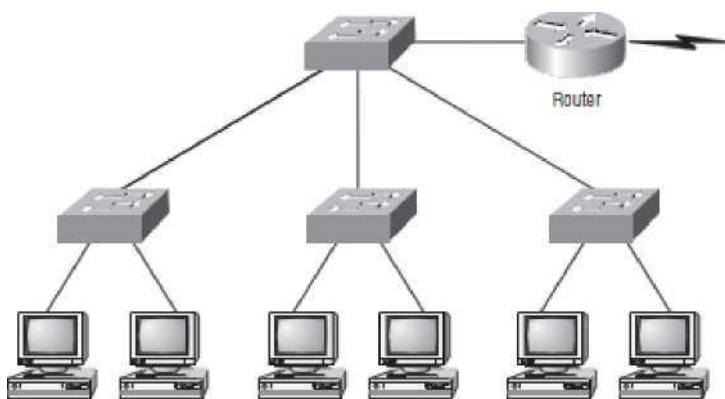
On the top internetwork in Figure 1.5, you'll notice that a bridge was used to connect the hubs to a router. The bridge breaks up collision domains, but all the hosts connected to both hubs are still crammed into the same broadcast domain. Also, the bridge only created two collision domains, so each device connected to a hub is in the same collision domain as every other device connected to that same hub. This is actually pretty lame, but it's still better than having one collision domain for all hosts.

Notice something else: The three hubs at the bottom that are connected also connect to the router, creating one collision domain and one broadcast domain. This makes the bridged network look much better indeed! The best network connected to the router is the LAN switch network on the left. Why? Because each port on that switch breaks up collision domains. But it's not all good—all devices are still in the same broadcast domain. Do you remember why this can be a really bad thing? Because all devices must listen to all broadcasts transmitted, that's why. And if your broadcast domains are too large, the users have less bandwidth and are required to process more broadcasts, and network response time will slow to a level that could cause office riots.

Once we have only switches in our network, things change a lot! Figure 1.6 shows the network that is typically found today.



*FIGURE 1. 5 Internetworking devices*



**FIGURE 1. 6** Switched networks creating an internetwork

Here, I've placed the LAN switches at the center of the network world so that the routers are connecting only logical networks together. If I implemented this kind of setup, I've created virtual LANs (VLANs). But it is really important to understand that even though you have a switched network, you still need a router to provide your inter-VLAN communication, or internetworking.



Obviously, the best network is one that's correctly configured to meet the business requirements of the company it serves. LAN switches with routers, correctly placed in the network, are the best network design.

Let's go back to Figure 1.6. Looking at the figure, how many collision domains and broadcast domains are in this internetwork? Hopefully, you answered nine collision domains and three broadcast domains! The broadcast domains are definitely the easiest to see because only routers break up broadcast domains by default. And since there are three connections, that gives you three broadcast domains. But do you see the nine collision domains? Just in case that's a no, I'll explain. The all-hub network is one collision domain; the bridge network equals three collision domains. Add in the switch network of five collision domains—one for each switch port—and you've got a total of nine.

So now that you've gotten an introduction to internetworking and the various devices that live in an internetwork, it's time to head into internetworking models.

## **Identify common applications and their impact on the network**

Describe the impact of applications (Voice over IP and Video over IP) on a network

The main purpose of the Host-to-Host layer is to shield the upper-layer applications from the complexities of the network. This layer says to the upper layer, "Just give me your data stream, with any instructions, and I'll begin the process of getting your information ready to send."

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

By understanding how TCP and UDP work, you can interpret the impact of applications on networks when using Voice and Video over IP.

Transmission Control Protocol (TCP) takes large blocks of information from an application and breaks them into segments. It numbers and sequences each segment so that the destination's TCP stack can put the segments back into the order the application intended. After these segments are sent, TCP (on the transmitting host) waits for an acknowledgment of the receiving end's TCP virtual circuit session, retransmitting those that aren't acknowledged.

Before a transmitting host starts to send segments down the model, the sender's TCP stack contacts the destination's TCP stack to establish a

connection. What is created is known as a virtual circuit. This type of communication is called connection-oriented. During this initial handshake, the two TCP layers also agree on the amount of information that's going to be sent before the recipient's TCP sends back an acknowledgment. With everything agreed upon in advance, the path is paved for reliable communication to take place.

TCP is a full-duplex, connection-oriented, reliable, and accurate protocol, but establishing all these terms and conditions, in addition to error checking, is no small task. TCP is very complicated and, not surprisingly, costly in terms of network overhead. And since today's networks are much more reliable than those of yore, this added reliability is often unnecessary.

**TCP Segment Format**  
Since the upper layers just send a data stream to the protocols in the Transport layers, I'll demonstrate how TCP segments a data stream and prepares it for the Internet layer. When the Internet layer receives the data stream, it routes the segments as packets through an internetwork. The segments are handed to the receiving host's Host-to-Host layer protocol, which rebuilds the data stream to hand to the upper-layer applications or protocols.

Figure 1.7 shows the TCP segment format. The figure shows the different fields within the TCP header.

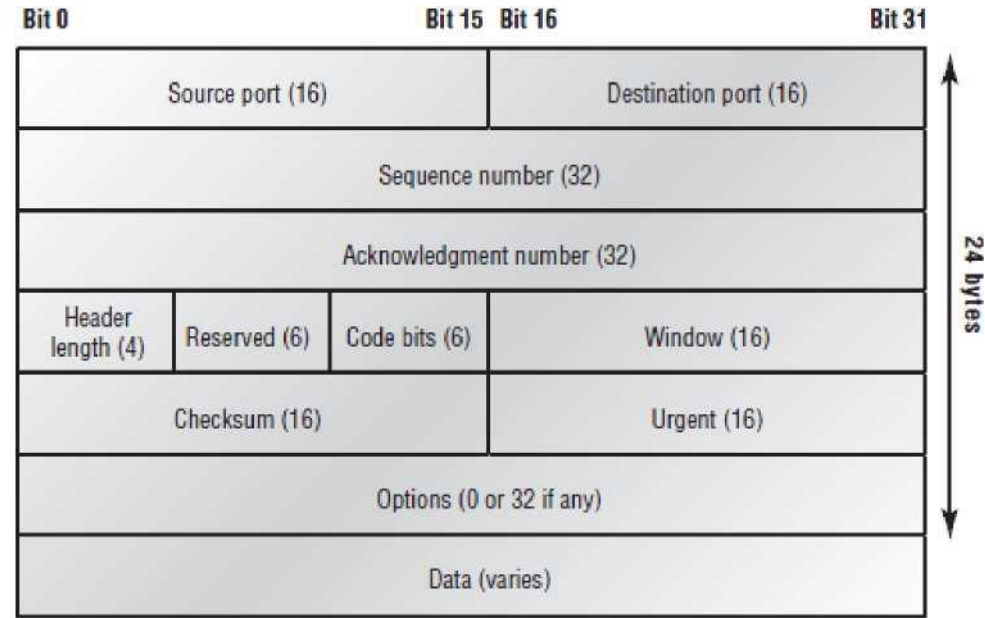


FIGURE 1.7 TCP segment format

The TCP header is 20 bytes long, or up to 24 bytes with options. You need to understand what each field in the TCP segment is:

- Source port the port number of the application on the host sending the data.
- Destination port the port number of the application requested on the destination host. Sequence number a number used by TCP that puts the data back in the correct order or retransmits missing or damaged data, a process called sequencing.
- Acknowledgment number The TCP octet that is expected next.
- Header length the number of 32-bit words in the TCP header. This indicates where the data begins. The TCP header (even one including options) is an integral number of 32 bits in length. Reserved Always set to zero.
- Code bits Control functions used to set up and terminate a session.
- Window The window size the sender is willing to accept, in octets.
- Checksum The cyclic redundancy check (CRC), because TCP doesn't trust the lower layers and checks everything. The CRC checks the header and data fields.
- Urgent a valid field only if the Urgent pointer in the code bits is set. If so, this value indicates the offset from the current sequence number, in octets, where the first segment of non-urgent data begins.
- Options May be 0 or a multiple of 32 bits, if any. What this means is that no options have to be present (option size of 0). However, if any options are used that do not cause the option field to total a multiple of 32 bits, padding of 0s must be used to make sure the data begins on a 32-bit boundary.

Data handed down to the TCP protocol at the Transport layer, which includes the upper layer headers.

Let's take a look at a TCP segment copied from a network analyzer:

TCP - Transport Control Protocol

**Source Port: 5973**  
**Destination Port: 23**  
**Sequence Number: 1456389907**  
**ACK Number: 1242056456**  
**Offset: 5**  
**Reserved: %000000**  
**Code: %011000**  
**ACK is valid**  
**Push Request**  
**Window: 61320**  
**Checksum: 0x61a6**  
**Urgent Pointer: 0**  
**No TCP Options**

**TCP Data Area:**

**VL.5. +.5. +.5. +.5 76 4c 19 35 11 2b 19 35 11 2b 19 35 11  
2b 19 35 +. 11 2b 19**

**Frame Check Sequence: 0x0d00000f**

Did you notice that everything I talked about earlier is in the segment? As you can see from the number of fields in the header, TCP creates a lot of overhead. Application developers may opt for efficiency over reliability to save overhead, so the User Datagram Protocol was also defined at the Transport layer as an alternative.

**User Datagram Protocol (UDP)**

If you were to compare the User Datagram Protocol (UDP) with TCP, the former is basically the scaled-down economy model that's sometimes referred to as a thin protocol. Like a thin person on a park bench, a thin protocol doesn't take up a lot of room—or in this case, much bandwidth on a network.

UDP doesn't offer all the bells and whistles of TCP either, but it does do a fabulous job of transporting information that doesn't require reliable delivery—and it does so using far fewer network resources. (UDP is covered thoroughly in Request for Comments 768.)

There are some situations in which it would definitely be wise for developers to opt for UDP rather than TCP. Remember the watchdog SNMP up there at the Process/Application layer? SNMP monitors the network, sending intermittent messages and a fairly steady flow of status updates and alerts, especially when running on a large network. The cost in overhead to establish, maintain, and close a TCP connection for each one of those little messages would reduce what would be an otherwise healthy, efficient network to a dammed-up bog in no time!

Another circumstance calling for UDP over TCP is when reliability is already handled at the Process/Application layer. Network File System (NFS) handles its own reliability issues, making the use of TCP both impractical and redundant. But ultimately, it's up to the application developer to decide whether to use UDP or TCP, not the user who wants to transfer data faster.

UDP does not sequence the segments and does not care in which order the segments arrive at the destination. But after that, UDP sends the segments off and forgets about them. It doesn't follow through, check up on them, or even allow for an acknowledgment of safe arrival—complete abandonment. Because of this, it's referred to as an unreliable protocol.

This does not mean that UDP is ineffective, only that it doesn't handle issues of reliability. Further, UDP doesn't create a virtual circuit, nor does it contact the destination before delivering information to it. Because of this, it's also considered a connectionless protocol. Since UDP assumes that the application will use its own reliability method, it doesn't use any. This gives an application developer a choice when running the Internet Protocol stack: TCP for reliability or UDP for faster transfers.

So if you're using Voice over IP (VoIP), for example, you really don't want to use UDP, because if the segments arrive out of order (very common in IP networks), they'll just be passed up to the next OSI (DOD) layer in whatever order they're received, resulting in some seriously garbled data. On the other hand, TCP sequences the segments so they get put back together in exactly the right order—something that UDP just can't do.

UDP Segment Format

Figure 1.8 clearly illustrates UDP's markedly low overhead as compared to TCP's hungry usage. Look at the figure carefully—can you see that UDP doesn't use windowing or provide for acknowledgments in the UDP header?

It's important for you to understand what each field in the UDP segment is:

- Source port number of the application on the host sending the data
- Destination port number of the application requested on the destination host
- Length of UDP header and UDP data
- Checksum of both the UDP header and UDP data fields
- Data Upper-layer data

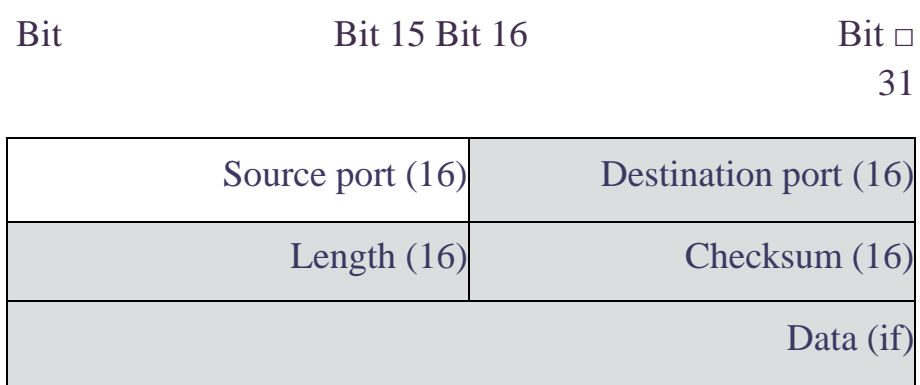


FIGURE 1.8 UDP segment

UDP, like TCP, doesn't trust the lower layers and runs its own CRC. Remember that the Frame Check Sequence (FCS) is the field that houses

the CRC, which is why you can see the FCS information. The following shows a UDP segment caught on a network analyzer:

UDP - User Datagram Protocol

**Source Port: 1085 Destination Port: 5136 Length: 41 Checksum: 0x7a3c**  
**UDP Data Area:**  
**..Z ..... 00 01 5a 96 00 01 00 00 00 00 11 0000 00**  
**...C...2. C. C 2e 03 00 43 02 1e 32 0a 00 0a 00 80 43 00 80**  
**Frame Check Sequence: 0x00000000**

Notice that low overhead! Try to find the sequence number, ACK number, and window size in the UDP segment. You can't because they just aren't there!

### Key Concepts of Host-to-Host Protocols

Since you've seen both a connection-oriented (TCP) and connectionless (UDP) protocol in action, it would be good to summarize the two here.

Table 1. 2 highlight some of the key concepts that you should keep in mind regarding these two protocols. You should memorize this table.

***TABLE 1.2 Key Features of TCP and UDP***

TCP	UDP
<b>Sequenced</b>	<b>Un sequenced</b>
<b>Reliable</b>	<b>Unreliable</b>
<b>Connection-oriented</b>	<b>Connectionless</b>
<b>Virtual circuit</b>	<b>Low overhead</b>
<b>Acknowledgments</b>	<b>Mo acknowledgment</b>
<b>Windowing flow control</b>	<b>Mo windowing or flow control</b>

A telephone analogy could really help you understand how TCP works. Most of us know that before you speak to someone on a phone, you must first establish a connection with that other person—wherever they are. This is like a virtual circuit with the TCP protocol. If you were giving someone important information during your conversation, you might say, “You know?” or ask, “Did you get that?” Saying something like this is a lot like a TCP acknowledgment—it's designed to get you verification. From time to time (especially on cell phones), people also ask, “Are you still there?”

They end their conversations with a “Goodbye” of some kind, putting closure on the phone call. TCP also performs these types of functions.

Alternately, using UDP is like sending a postcard. To do that, you don’t need to contact the other party first. You simply write your message, address the postcard, and mail it. This is analogous to UDP’s connectionless orientation. Since the message on the postcard is probably not a matter of life or death, you don’t need an acknowledgment of its receipt. Similarly, UDP does not involve acknowledgments.

### **Describe the purpose and basic operation of the protocols in the OSI and TCP/IP models**

#### Overview of the TCP/IP Networking Model

The TCP/IP model both defines and references a large collection of protocols that allow computers to communicate. To define a protocol, TCP/IP uses documents called Requests for Comments (RFC). (You can find these RFCs using any online search engine.) The TCP/IP model also avoids repeating work already done by some other standards body or vendor consortium by simply referring to standards or protocols created by those groups.

For example, the Institute of Electrical and Electronic Engineers (IEEE) defines Ethernet LANs; the TCP/IP model does not define Ethernet in RFCs, but refers to IEEE Ethernet as an option.

An easy comparison can be made between telephones and computers that use TCP/IP. You go to the store and buy a phone from one of a dozen different vendors. When you get home and plug in the phone to the same cable in which your old phone was connected, the new phone works. The phone vendors know the standards for phones in their country and build their phones to match those standards.

Similarly, when you buy a new computer today, it implements the TCP/IP model to the point that you can usually take the computer out of the box, plug in all the right cables, turn it on, and it connects to the network. You can use a web browser to connect to your favorite website. How? Well, the OS on the computer implements parts of the TCP/IP model. The Ethernet card, or wireless LAN card, built into the computer implements some LAN standards referenced by the TCP/IP model. In short, the vendors that created the hardware and software implemented TCP/IP.

To help people understand a networking model, each model breaks the functions into a small number of categories called layers. Each layer includes protocols and standards that relate to that category of functions. TCP/IP actually has two alternative models, as shown in Figure 1.9.



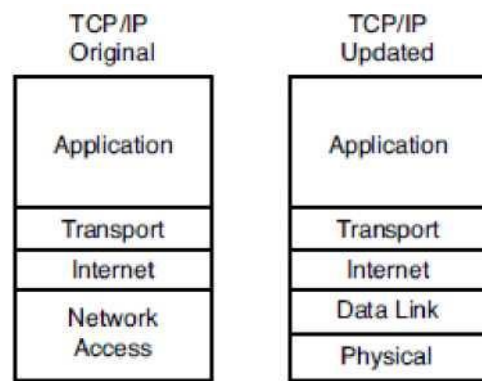


Figure 1.9 the Two TCP/IP Networking Models

The model on the left, the original TCP/IP model, breaks TCP/IP into four layers. The top layers focus more on the applications that need to send and receive data, whereas the lower layers focus more on the need to somehow transmit the bits from one device to another. The model on the right is a newer version of the model, formed by expanding the network access layer on the left into two separate layers: data link and physical. Note that the model on the right is used more often today.

Many of you will have already heard of several TCP/IP protocols, like the examples listed in

Table 1.3 TCP/IP Architectural Model and Example Protocols

<b>TCP/IP Architecture Layer</b>	<b>Example Protocols</b>
<b>Application</b>	<b>HTTP. POP3. SMTP</b>
<b>Transport</b>	<b>TCP. UDP</b>
<b>Internet</b>	<b>IP</b>
<b>Network Access</b>	<b>Ethernet, Point-to-Point Protocol (PPP), I7/i</b>

### TCP/IP Application Layer

TCP/IP application layer protocols provide services to the application software running on a computer. The application layer does not define the application itself, but it defines services that applications need. For example, application protocol HTTP defines how web browsers can pull the contents of a web page from a web server. In short, the application layer provides an interface between software running on a computer and the network itself.

Table 1.3 TCP/IP Architectural Model and Example Protocols Arguably, the most popular TCP/IP application today is the web browser. Many major



software vendors either have already changed or are changing their application software to support access from a web browser.

### OSI Layers and Their Functions

Cisco requires that CCNAs demonstrate a basic understanding of the functions defined by each OSI layer, as well as remembering the names of the layers. You understand which layers of the OSI model most closely match the functions defined by that device or protocol.

Today, because most people happen to be much more familiar with TCP/IP functions than with OSI functions, one of the best ways to learn about the function of different OSI layers is to think about the functions in the TCP/IP model, and correlate those with the OSI model.

If you use the five-layer TCP/IP model, the bottom four layers of OSI and TCP/IP map closely together. The only difference in these bottom four layers is the name of OSI Layer 3 (network) compared to TCP/IP (Internet). The upper three layers of the OSI reference model (application, presentation, and session—Layers 7, 6, and 5) define functions that all map to the TCP/IP application layer. Table 1.4 defines the functions of the seven layers.

Table 1.5 lists most of the devices and protocols covered in the; CCNA exams and their comparable OSI layers. Note that many network devices must actually understand the protocols at multiple OSI layers, so the layer listed in Table 1.5 actually refers to the highest layer that the device normally thinks about when performing its core work. For example, routers need to think about Layer 3 concepts, but they must also support features at both Layers 1 and 2.

Besides remembering the basics of the features of each OSI layer (as in Table 1.4), and some example protocols and devices at each layer (as in Table 1.5), you should also Layer Functional Description 4 Layer 4 protocols provide a large number of services, “Fundamentals of TCP/IP Transport, Applications, and Security.” Although OSI Layers 5 through 7 focus on issues related to the application, Layer 4 focuses on issues related to data delivery to another computer (for instance, error recovery and flow control).

3 The network layer defines three main features: logical addressing, routing (forwarding), and path determination. Routing defines how devices (typically routers) forward packets to their final destination. Logical addressing defines how each device can have an address that can be used

**Table 1.4 OSI Reference Model Layer Definitions**

Laver	Functional Description
7	Layer 7 provides an interface between the communications software and any applications that need to communicate outside the computer on which the application resides. It also defines processes for user authentication.
6	This layer's main purpose is to define and negotiates data formats, such as ASCII text, EBCDIC text, binary, BCD, and JPEG. Encryption is also defined by OSI as a
5	The session layer defines how to start, control, and end conversations (called sessions). This includes the control and management of multiple bidirectional messages so that
4	Layer 4 protocols provide an l are number of services, "Fundamentals of TCP/IP Transport, Applications, and Security." Although OSI Layers 5 through 7 focus on issues
3	The network layer defines three main features: logical addressing, routing (forwarding), and path determination. Routing defines how devices (typically routers) forward
2	The data link layer defines the rules that determine when a device can send data over <i>a</i> particular medium. Data link protocols also define the format of a header and trailer that
1	This layer typically refers to standards from other organizations. These standards deal with the physical characteristics of the transmission medium, including

by the routing process. Path determination refers to the work done by routing protocols to learn all possible routes, and choose the best route.

2 The data link layer defines the rules that determine when a device can send data over a particular medium. Data link protocols also define the format of a header and trailer that allows devices attached to the medium to successfully send and receive data.

1 This layer typically refers to standards from other organizations. These standards deal with the physical characteristics of the transmission medium, including connectors, pins, use of pins, electrical currents, encoding, light modulation, and the rules for how to activate and deactivate the use of the physical medium.

Memorize the names of the layers. You can simply memorize them, but some people like to use a mnemonic phrase to make memorization easier.

**Table 1.5 OSI Reference Model—Example Devices and Protocols**

Laver Name	Protocols and	Devices
Application, presentation, session (Layers 5-7)	Telnet, HTTP, FTP, SMTP, POP3, VoIP, SNMP	Firewall, intrusion detection systems, hosts
Transport (Layer 4)	TCP, UDP	Hosts, firewalls
Network (Layer 3)	IP	Router
Data link (Layer 2)	Ethernet (IEEE 802.3), HDLC, Frame Relay, PPP	LAN switch, wireless access point, cable
Physical (Layer 1)	RJ-45, EIA/TIA- 232, V.35, Ethernet (IEEE 802.3)	LAN hub, LAN repeater, cables

In the following three phrases, the first letter of each word is the same as the first letter of an OSI layer name, in the order specified in parentheses:

- All People Seem To Need Data Processing (Layers 7 to 1)
- Please Do Not Take Sausage Pizzas Away (Layers 1 to 7)
- Pew! Dead Ninja Turtles Smell Particularly Awful (Layers 1 to 7)

### **Predict the data flow between two hosts across a network**

Determine the path between two hosts across a network

Once you create an internetwork by connecting your WANs and LANs to a router, you'll need to configure logical network addresses, such as IP addresses, to all hosts on the internetwork so that they can communicate across that internetwork.

The term routing is used for taking a packet from one device and sending it through the network to another device on a different network. Routers don't really care about hosts—they only care about networks and the best path to each network. The logical network address of the destination host is used to get packets to a network through a routed network, and then the hardware address of the host is used to deliver the packet from a router to the correct destination host.

If your network has no routers, then it should be apparent that you are not routing. Routers route traffic to all the networks in your internetwork. To be able to route packets, a router must know, at a minimum, the following:

- Destination address
- Neighbor routers from which it can learn about remote networks
- Possible routes to all remote networks
- The best route to each remote network
- How to maintain and verify routing information

The router learns about remote networks from neighbor routers or from an administrator. The router then builds a routing table (a map of the internetwork) that describes how to find the remote networks. If a network is directly connected, then the router already knows how to get to it.

If a network isn't directly connected to the router, the router must use one of two ways to learn how to get to the remote network: static routing, meaning that someone must hand-type all network locations into the routing table, or something called dynamic routing. In dynamic routing, a protocol on one router communicates with the same protocol running on neighbor routers. The routers then update each other about all the networks they know about and place this information into the routing table. If a change occurs in the network, the dynamic routing protocols automatically inform all routers about the event. If static routing is used, the administrator is responsible for updating all changes by hand into all routers. Typically, in a large network, a combination of both dynamic and static routing is used.

Figure 1.10 shows a simple two-router network. Lab A has one serial interface and three LAN interfaces.

Looking at Figure 1.10, can you see which interface Lab A will use to forward an IP datagram to a host with an IP address of 10.10.10.10?

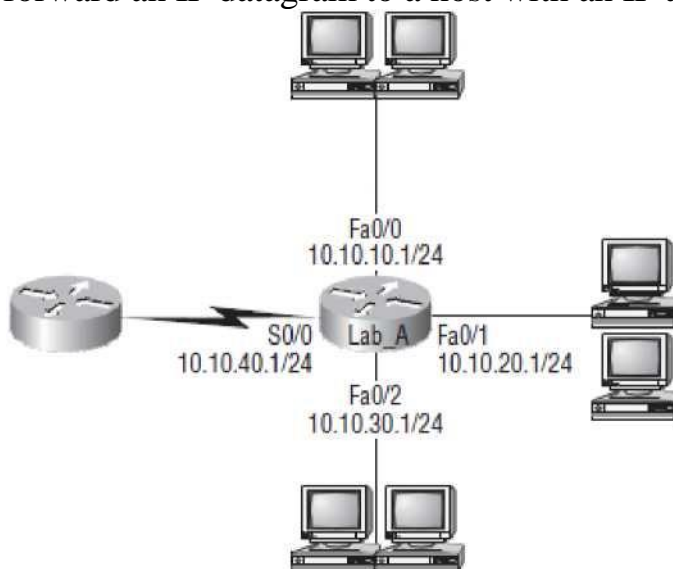


FIGURE 1.10 a simple routing example

By using the command show IP route, we can see the routing table (map of the internetwork) that Lab A uses to make forwarding decisions:

**Lab A # Show IP route [output cut]**

**Gateway of last resort is not set**

**C 10.10.10.0/24 is directly connected, FastEthernet0/0 C 10.10.20.0/24 is directly connected, FastEthernet0/1 C 10.10.30.0/24 is directly connected, FastEthernet0/2 C 10.10.40.0/24 is directly connected, Serial 0/0**

The C in the routing table output means that the networks listed are “directly connected,” and until we add a routing protocol—something like RIP, EIGRP, or the like—to the routers in our internetwork (or use static routes), we’ll have only directly connected networks in our routing table.

So let’s get back to the original question: By looking at the figure and the output of the routing table, can you tell what IP will do with a received packet that has a destination IP address of 10.10.10.10? The router will packet-switch the packet to interface Fast Ethernet 0/0, and this interface will frame the packet and then send it out on the network segment. Because we can, let’s do another example: Based on the output of the next routing table, which interface will a packet with a destination address of 10.10.10.14 be forwarded from?

**Lab A #Show IP route [output cut]**

**Gateway of last resort is not set**

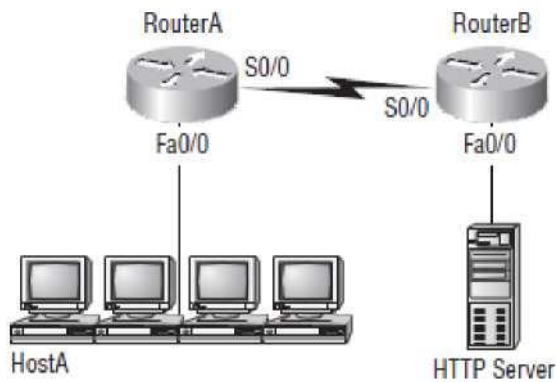
**C 10.10.10.16/28 is directly connected, FastEthernet0/0 C 10.10.10.8/29 is directly connected, FastEthernet0/1 C 10.10.10.4/30 is directly connected, FastEthernet0/2 C 10.10.10.0/30 is directly connected, Serial 0/0**

First, you can see that the network is sub-netted and each interface has a different mask. And I have to tell you—you just can’t answer this question if you can’t subnet! 10.10.10.14 would be a host in the 10.10.10.8/29 subnet connected to the FastEthernet0/1 interface.

The critical information you need to glean from this figure is exactly how IP routing will occur in this example. Okay—we’ll cheat a bit. I’ll give you the answer, but then you should go back over the figure and see if you can answer example 2 without looking at my answers.

1. The destination address of a frame, from Host A, will be the MAC address of the F0/0 interface of the Router A router.
2. The destination address of a packet will be the IP address of the network

Figure 1.11 shows a LAN connected to Router A, which is, in turn, connected via a WAN link to Router B. Router B has a LAN connected with an HTTP server attached.



**FIGURE 1.11** IP routing example 1

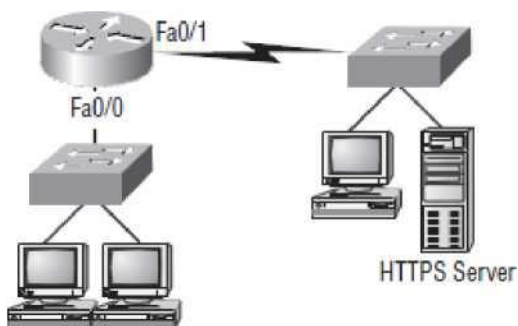
interface card (NIC) of the HTTP server.

3. The destination port number in the segment header will have a value of 80.

That example was a pretty simple one, and it was also very to the point. One thing to remember is that if multiple hosts are communicating to the server using HTTP, they must all use a different source port number. That is how the server keeps the data separated at the Transport layer.

Let's mix it up a little and add another internetworking device into the network and then see if you can find the answers. Figure 1.12 shows a network with only one router but two switches.

Router A



Host A

**FIGURE 1.12** IP routing example 2.

What you want to understand about the IP routing process here is what happens when Host A sends data to the HTTPS server:

1. The destination address of a frame, from Host A, will be the MAC address

of the F0/0 interface of the router a router.

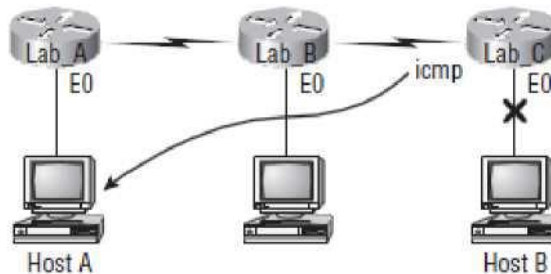
2. The destination address of a packet will be the IP address of the network interface card (NIC) of the HTTPS server.
3. The destination port number in the segment header will have a value of 443.

Notice that the switches weren't used as either a default gateway or another destination.

That's because switches have nothing to do with routing. I wonder how many of you chose the switch as the default gateway (destination) MAC address for Host A. If you did, don't feel bad— just take another look with that fact in mind. It's very important to remember that the destination MAC address will always be the router's interface—if your packets are destined for outside the LAN, as they were in these last two examples.

Before we move into some of the more advanced aspects of IP routing, let's discuss ICMP in more detail, as well as how ICMP is used in an internetwork. Take a look at the network shown in Figure 1.13. Ask yourself what will happen if the LAN interface of Lab C goes down.

Lab C will use ICMP to inform Host A that Host B can't be reached, and it will do this by sending an ICMP destination unreachable message. Lots of people think that the Lab A router would be sending this message, but they would be wrong because the router that sends the message is the one with that interface that's down is located.



*FIGURE 1.13 ICMP error example*

Let's look at another problem: Look at the output of a corporate router's routing table:

**Corp #Show IP route [output cut]**

```
R 192.168.215.0 [120/2] via 192.168.20.2, 00:00:23, Serial0/0 R
192.168.115.0 [120/1] via 192.168.20.2, 00:00:23, Serial0/0 R
192.168.30.0 [120/1] via 192.168.20.2, 00:00:23, Serial0/0 C 192.168.20.0
is directly connected, Serial0/0 C 192.168.214.0 is directly connected,
FastEthernet0/0
```

What do we see here? If I were to tell you that the corporate router received an IP packet with a source IP address of 192.168.214.20 and a destination



address of 192.168.22.3, what do you think the Corp router will do with this packet?

If you said, “The packet came in on the Fast Ethernet 0/0 interface, but since the routing table doesn’t show a route to network 192.168.22.0 (or a default route), the router will discard the packet and send an ICMP destination unreachable message back out interface Fast Ethernet 0/0,” you’re a genius! The reason it does this is because that’s the source LAN where the packet originated from.

**Identify the appropriate media, cables, ports, and connectors to connect Cisco network devices to other network devices and hosts in a LAN**

Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts

Ethernet cabling is an important discussion, especially if you are planning on taking the Cisco exams. Three types of Ethernet cables are available:

- Straight-through cable
- Crossover cable
- Rolled cable

**Straight-Through Cable**

The straight-through cable is used to connect

- Host to switch or hub
- Router to switch or hub

Four wires are used in straight-through cable to connect Ethernet devices. It is relatively simple to create this type; Figure 1.12 shows the four wires used in a straight-through Ethernet cable.



**FIGURE 1.12** *Straight-through Ethernet cable*

Notice that only pins 1, 2, 3, and 6 are used. Just connect 1 to 1, 2 to 2, 3 to 3, and 6 to 6, and you’ll be up and networking in no time. However,



remember that this would be an Ethernet-only cable and wouldn't work with voice, Token Ring, ISDN, and so on.

### Crossover Cable

The crossover cable can be used to connect

- Switch to switch
- Hub to hub
- Host to host
- Hub to switch
- Router direct to host

The same four wires are used in this cable as in the straight-through cable; we just connect different pins together. Figure 1.13 shows how the four wires are used in a crossover Ethernet cable.

Notice that instead of connecting 1 to 1, 2 to 2, and so on, here we connect pins 1 to 3 and 2 to 6 on each side of the cable.

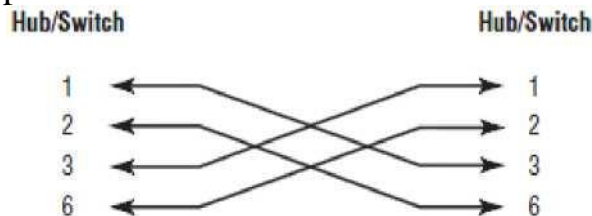


FIGURE 1.13 Crossover Ethernet cable

### Rolled Cable

Although rolled cable isn't used to connect any Ethernet connections, you can use a rolled Ethernet cable to connect a host to a router console serial communication (com) port.

If you have a Cisco router or switch, you would use this cable to connect your PC running HyperTerminal to the Cisco hardware. Eight wires are used in this cable to connect serial devices, although not all eight are used to send information, just as in Ethernet networking. Figure 1.14 shows the eight wires used in a rolled cable.

These are probably the easiest cables to make because you just cut the end off on one side of a straight-through cable, turn it over, and put it back on (with a new connector, of course).

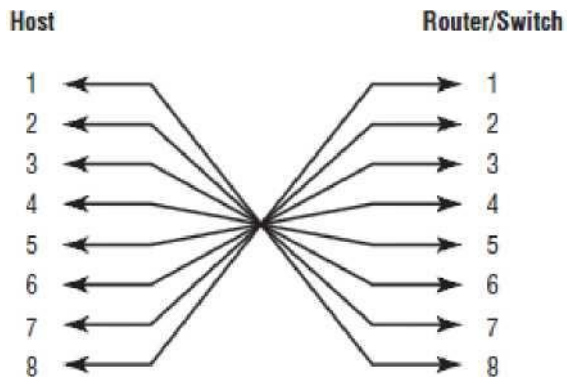
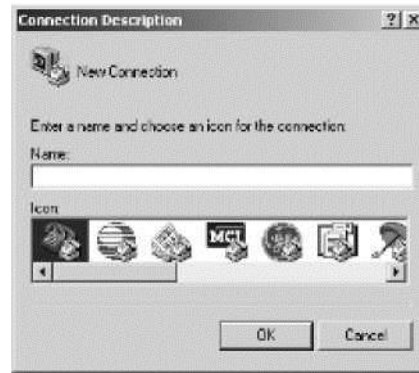


FIGURE 1.14 Rolled Ethernet cable

Once you have the correct cable connected from your PC to the Cisco router or switch, you can start HyperTerminal to create a console connection and configure the device. Set the configuration as follows:

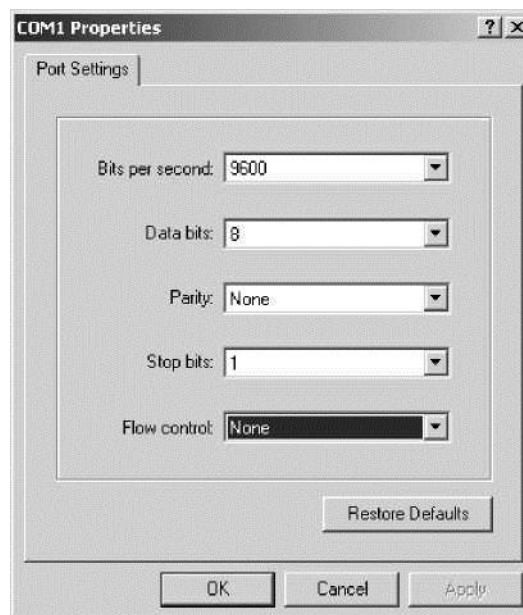
1. Open HyperTerminal and enter a name for the connection. It is irrelevant what you name it, but I always just use Cisco. Then click OK.



2. Choose the communications port—either COM1 or COM2, whichever is open on your PC.



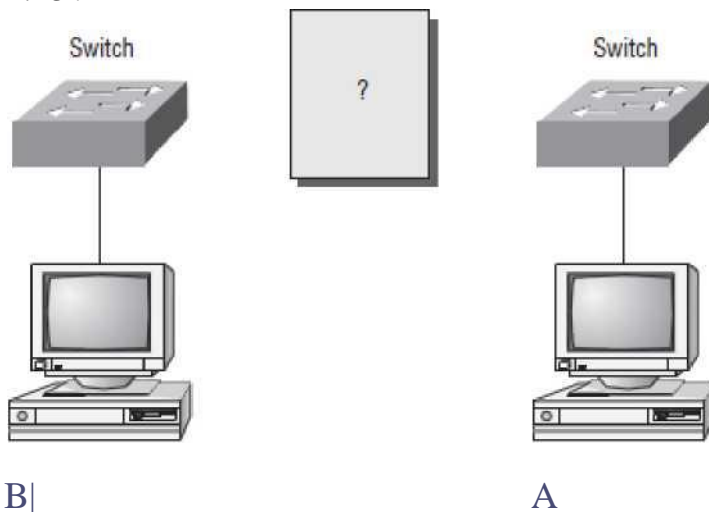
3. Now set the port settings. The default values (2400bps and no flow control hardware) will not work; you must set the port settings as shown in Figure 1.14.



### ***FIGURE 1.14 Port settings for a rolled cable connection***

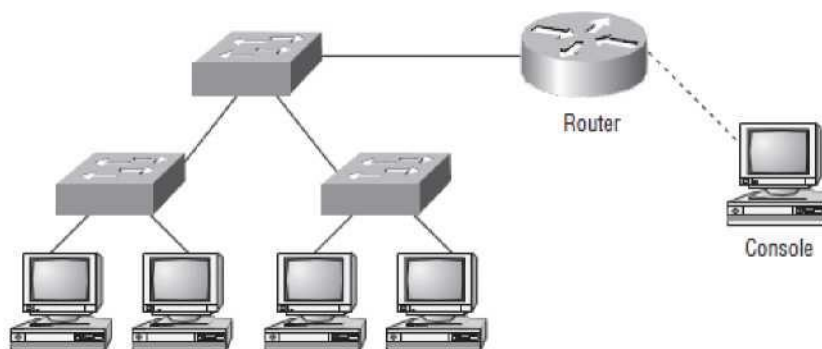
Notice that the bit rate is now set to 9600 and the flow control is set to none. At this point, you can click OK and press the Enter key and you should be connected to your Cisco device console port.

We've taken a look at the various RJ45 unshielded twisted pair (UTP) cables. Keeping this in mind, what cable is used between the switches in Figure 1.15?



**FIGURE 1.15 RJ45 cable questions #1**

In order for host A to ping host B, you need a crossover cable to connect the two switches. But what types of cables are used in the network shown in Figure 1.16?



**FIGURE 1.16 RJ45 cable questions #2**

The trouble is, we have a console connection that uses a rolled cable. Plus, the connection from the router to the switch is a straight-through cable, as is true for the hosts to the switches. Keep in mind that if we had a serial connection (which we don't); it would be a V.35 that we'd use to connect us to a WAN.

## 3.2 LAN Switching Technologies

---

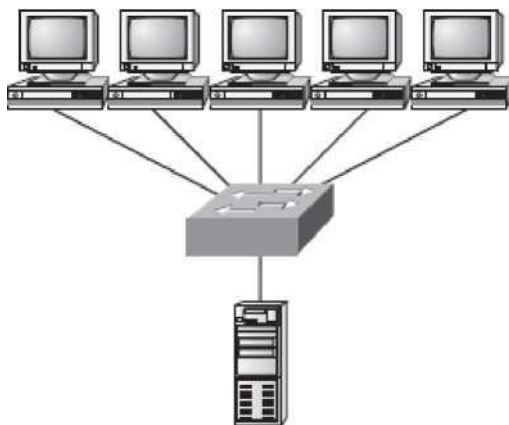
### Identify basic switching concepts and the operation of Cisco switches

Explain basic switching concepts and the operation of Cisco switches  
Unlike bridges, which use software to create and manage a filter table, switches use application-specific integrated circuits (ASICs) to build and maintain their filter tables. But it's still okay to think of a layer 2 switch as a multiport bridge because their basic reason for being is the same: to break up collision domains.

Layer 2 switches and bridges are faster than routers because they don't take up time looking at the Network layer header information. Instead, they look at the frame's hardware addresses before deciding to either forward, flood, or drop the frame.

Switches create private, dedicated collision domains and provide independent bandwidth on each port, unlike hubs. Figure 2.5 shows five hosts connected to a switch—all running 10Mbps half-duplex to the server. Unlike with a hub, each host has 10Mbps dedicated communication to the server.

10 Mbps half-duplex links



Server

FIGURE 2.5 Switches create private domains.

Layer 2 switching provides the following:  
Hardware-based bridging (ASIC)

- Wire speed
- Low latency
- Low cost

What makes layer 2 switching so efficient is that no modification to the data packet takes place. The device only reads the frame encapsulating the packet, which makes the switching process considerably faster and less error-prone than routing processes are.

And if you use layer 2 switching for both workgroup connectivity and network segmentation (breaking up collision domains), you can create a flatter network design with more network segments than you can with traditional routed networks.

Plus, layer 2 switching increases bandwidth for each user because, again, each connection (interface) into the switch is its own collision domain. This feature makes it possible for you to connect multiple devices to each interface.

I will dive deeper into the layer 2 switching technology.

#### Limitations of Layer 2 Switching

Since we commonly stick layer 2 switching into the same category as bridged networks, we also tend to think it has the same hang-ups and issues that bridged networks do. Keep in mind that bridges are good and helpful things if we design the network correctly, keeping their features as well as their limitations in mind. And to design well with bridges, these are the two most important considerations:

- We absolutely must break up the collision domains correctly.
- The right way to create a functional bridged network is to make sure that its users spend 80 percent of their time on the local segment.

Bridged networks break up collision domains, but remember, that network is still one large broadcast domain. Neither layer 2 switches nor bridges break up broadcast domains by default—something that not only limits your network's size and growth potential but also can reduce its overall performance.

Broadcasts and multicasts, along with the slow convergence time of spanning trees, can give you some major grief as your network grows. These are the big reasons that layer 2 switches and bridges cannot completely replace routers (layer 3 devices) in the internetwork.

## Bridging vs. LAN Switching

It's true—layer 2 switches really are pretty much just bridges that give us a lot more ports, but there are some important differences you should always keep in mind:

- Bridges are software based, while switches are hardware based because they use ASIC chips to help make filtering decisions.
- A switch can be viewed as a multiport bridge.
- There can be only one spanning-tree instance per bridge, while switches can have many. (I'm going to tell you all about spanning trees in a bit.)
- Switches have a higher number of ports than most bridges.
- Both bridges and switches forward layer 2 broadcasts.
- Bridges and switches learn MAC addresses by examining the source address of each frame received.
- Both bridges and switches make forwarding decisions based on layer 2 addresses.

## Three Switch Functions at Layer 2

There are three distinct functions of layer 2 switching (you need to remember these!): address learning, forward/filter decisions, and loop avoidance.

**Address learning** Layer 2 switches and bridges remember the source hardware address of each frame received on an interface, and they enter this information into a MAC database called a forward/filter table.

**Forward/filter decisions** when a frame is received on an interface, the switch looks at the destination hardware address and finds the exit interface in the MAC database. The frame is only forwarded out the specified destination port.

**Loop avoidance** if multiple connections between switches are created for redundancy purposes, network loops can occur. Spanning Tree Protocol (STP) is used to stop network loops while still permitting redundancy.

## Address Learning

When a switch is first powered on, the MAC forward/filter table is empty, as shown in Figure 2.6.

## MAC Forward/Filter Table

EO/O:

EOM:

EO/2:

EO/3:

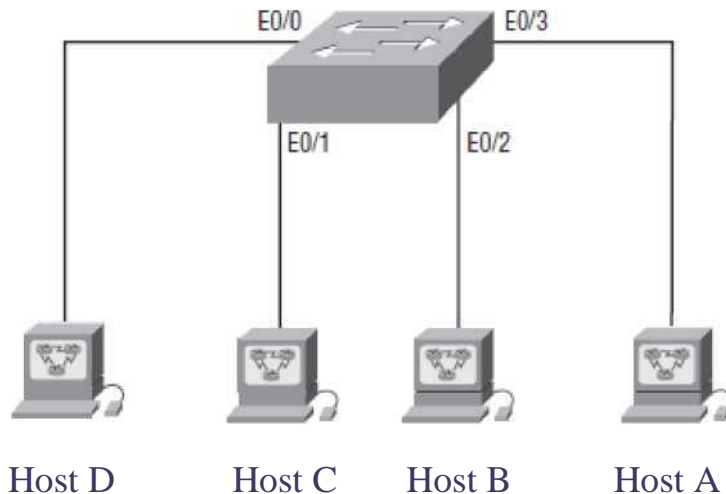


FIGURE 2.6 Empty forward/filter tables on a switch

When a device transmits and an interface receives a frame, the switch places the frame's source address in the MAC forward/filter table, allowing it to remember which interface the sending device is located on. The switch then has no choice but to flood the network with this frame out of every port except the source port because it has no idea where the destination device is actually located.

If a device answers this flooded frame and sends a frame back, then the switch will take the source address from that frame and place that MAC address in its database as well, associating this address with the interface that received the frame. Since the switch now has both of the relevant MAC addresses in its filtering table, the two devices can now make a point-to-point connection. The switch doesn't need to flood the frame as it did the first time because now the frames can and will be forwarded only between the two devices. This is exactly the thing that makes layer 2 switches better than hubs. In a hub network, all frames are forwarded out all ports every time—no matter what. Figure 2.7 shows the processes involved in building a MAC database.



## MAC Forward-Filter Table

E0/0:  
0000.8c01.  
G00A step  
2 EOT:  
0000.8c01.  
000B step  
4 E0/2:

E0/3:

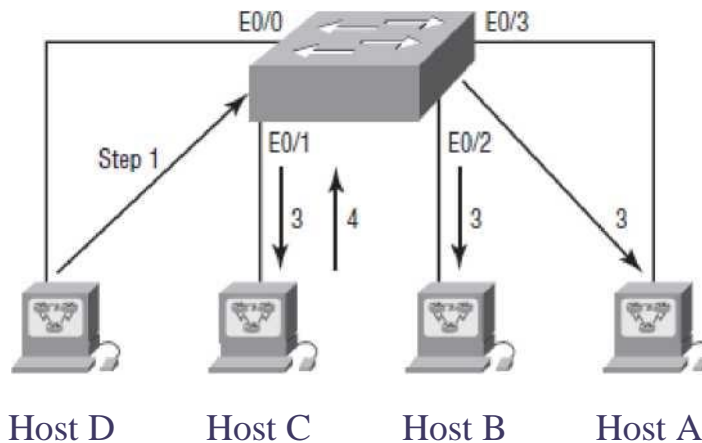


FIGURE 2.7 how switches learn hosts' locations

Let me give you an example of how a forward/filter table is populated:

1. Host A sends a frame to Host B. Host A's MAC address is 0000.8c01.000A; Host B's MAC address is 0000.8c01.000B.
2. The switch receives the frame on the E0/0 interface and places the source address in the MAC address table.
3. Since the destination address is not in the MAC database, the frame is forwarded out all interfaces—except the source port.
4. Host B receives the frame and responds to Host A. The switch receives this frame on interface E0/1 and places the source hardware address in the MAC database.
5. Host A and Host B can now make a point-to-point connection and only the two devices will receive the frames. Hosts C and D will not see the frames, nor are their MAC addresses found in the database because they haven't yet sent a frame to the switch.

If Host A and Host B don't communicate to the switch again within a certain amount of time, the switch will flush their entries from the database to keep it as current as possible.

## Forward/Filter Decisions

When a frame arrives at a switch interface, the destination hardware address is compared to the forward/filter MAC database. If the destination hardware address is known and listed in the database, the frame is only sent out the correct exit interface. The switch doesn't transmit the frame out any interface except for the destination interface. This preserves bandwidth on the other network segments and is called frame filtering.

But if the destination hardware address is not listed in the MAC database, then the frame is flooded out all active interfaces except the interface the frame was received on. If a device answers the flooded frame, the MAC database is updated with the device's location (interface).

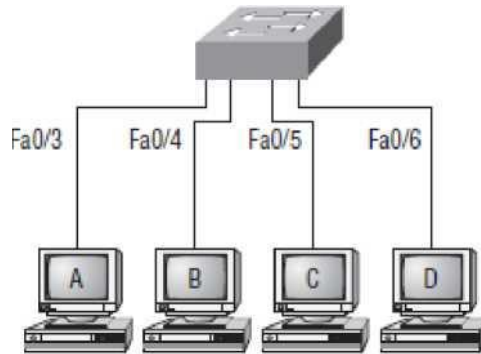


FIGURE 2.8 Forward/filter table

If a host or server sends a broadcast on the LAN, the switch will flood the frame out all active ports except the source port by default. Remember, the switch creates smaller collision domains, but it's still one large broadcast domain by default.

In Figure 2.8, Host A sends a data frame to Host D. What will the switch do when it receives the frame from Host A?

Since Host A's MAC address is not in the forward/filter table, the switch will add the source address and port to the MAC address table and then forward the frame to Host D. If Host D's MAC address was not in the forward/filter table, the switch would have flooded the frame out all ports except for port Fa0/3.

Now let's take a look at the output of a show mac address-table:

```
Switch #Show mac  
address-table  
VLAN Mac
```

## Address Type Ports

**1 0005.dccb.d74b**  
**DYNAMIC Fa0/1 1**  
**000a.f467.9e80**  
**DYNAMIC Fa0/3 1**  
**000a.f467.9e8b**  
**DYNAMIC Fa0/4 1**  
**000a.f467.9e8c**  
**DYNAMIC Fa0/3 1**  
**0010.7b7f.c2b0**  
**DYNAMIC Fa0/3 1**  
**0030.80dc.460b**  
**DYNAMIC Fa0/3 1**  
**0030.9492.a5dd**  
**DYNAMIC Fa0/1 1**  
**00d0.58ad.05f4**  
**DYNAMIC Fa0/1**

Suppose the preceding switch received a frame with the following MAC addresses:

**Source MAC: 0005.dccb.d74b Destination MAC: 000a.f467.9e8c**

**Describe how VLANs create logically separate networks and the need for routing between them.**

Describe how VLANs create logically separate networks and the need for routing between them Figure 2.12 shows how layer 2 switched networks are typically designed—as flat networks.

With this configuration, every broadcast packet transmitted is seen by every device on the network regardless of whether the device needs to receive that data or not.

By default, routers allow broadcasts to occur only within the originating network, while switches forward broadcasts to all segments. Oh, and by the way, the reason it's called a flat network is because it's one broadcast domain, not because the actual design is physically flat.

In Figure 2.12 we see Host a sending out a broadcast and all ports on all switches forwarding it—all except the port that originally received it.

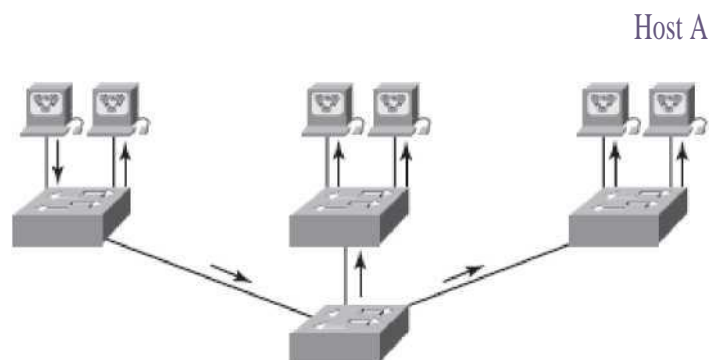


FIGURE 2.12 Flat network structure

Now check out Figure 2.13. It depicts a switched network and shows Host A sending a frame with Host D as its destination. What's important is that, as you can see, that frame is only forwarded out the port where Host D is located. This is a huge improvement over the old hub networks, unless having one collision domain by default is what you really want. (Probably not!)

Now you already know that the largest benefit you gain by having a layer 2 switched network is that it creates individual collision domain segments for each device plugged into each port on the switch. This scenario frees us

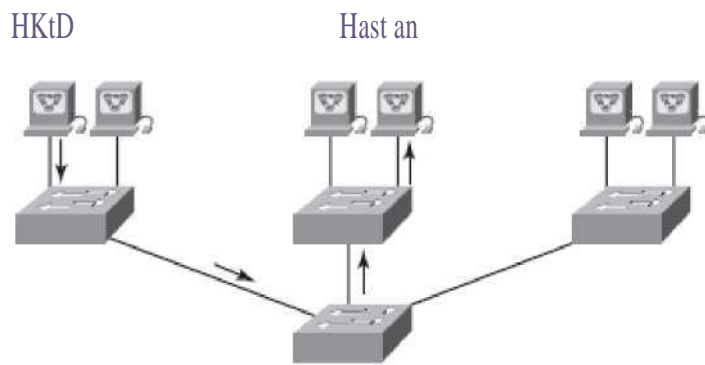


FIGURE 2.13 the benefit of a switched network

from the Ethernet distance constraints, so now larger networks can be built. But often, each new advance comes with new issues. For instance, the larger the number of users and devices, the more broadcasts and packets each switch must handle.

And here's another issue: security! This one's real trouble because within the typical layer 2 switched internetwork, all users can see all devices by default. And you can't stop devices from broadcasting, plus you can't stop users from trying to respond to broadcasts. This means your security options are dismally limited to placing passwords on your servers and other devices.

But wait—there's hope! That is, if you create a virtual LAN (VLAN). You can solve many of the problems associated with layer 2 switching with VLANs, as you'll soon see.

Here's a short list of ways VLANs simplify network management:

- Network adds, moves, and changes are achieved with ease by just configuring a port into the appropriate VLAN.
- A group of users that need an unusually high level of security can be put into its own VLAN so that users outside of the VLAN can't communicate with them.
- As a logical grouping of users by function, VLANs can be considered independent from their physical or geographic locations.
- VLANs greatly enhance network security.
- VLANs increase the number of broadcast domains while decreasing their size.

Coming up, I'm going to tell you all about switching characteristics and thoroughly describe how switches provide us with better network services than hubs can in our networks today.

## Broadcast Control

Broadcasts occur in every protocol, but how often they occur depends upon three things:

The type of protocol

The application(s) running on the internetwork how these services are used

Some older applications have been rewritten to reduce their bandwidth appetites, but there's a new generation of applications that are incredibly bandwidth greedy that will consume any and all they can find. These bandwidth gluttons are multimedia applications that use both broadcasts and multicasts extensively. And faulty equipment, inadequate segmentation, and poorly designed firewalls seriously compound the problems that these broadcast-intensive applications create. All of this has added a major new dimension to network design and presents a bunch of new challenges for an administrator. Positively making sure your network is properly segmented so that you can quickly isolate a single segment's problems to prevent them from propagating throughout your entire internetwork is imperative! And the most effective way to do that is through strategic switching and routing.

Since switches have become more affordable lately, a lot of companies are replacing their flat hub networks with pure switched network and VLAN environments. All devices within a VLAN are members of the same broadcast domain and receive all broadcasts. By default, these broadcasts are filtered from all ports on a switch that aren't members of the same VLAN. This is great because you get all the benefits you would with a switched design without getting hit with all the problems you'd have if all your users were in the same broadcast domain—sweet!

## Security

Okay, I know. There's always a catch, though right? Time to get back to those security issues. A flat internetwork's security used to be tackled by connecting hubs and switches with routers. So, it was basically the router's job to maintain security. This arrangement was pretty ineffective for several reasons. First, anyone connecting to the physical network could access the network resources located on that particular physical LAN. Second, all anyone had to do to observe any and all traffic happening in that network was to simply plug a network analyzer into the hub. And similar to that last ugly fact, users could join a workgroup by just plugging their workstations into the existing hub. That's about as secure as an open barrel of honey in a bear enclosure!

But that's exactly what makes VLANs so cool. If you build them and create multiple broadcast groups, you have total control over each port and

user! So, the days when anyone could just plug their workstation into any switch port and gain access to network resources are history because now you get to control each port, plus whatever resources that port can access. What's more, with the new 2960/3560 switches, this actually happens automatically! And it doesn't end there, my friends, because VLANs can be created in accordance with the network resources a given user requires, plus switches can be configured to inform a network management station of any unauthorized access to network resources. And if you need inter-VLAN communication, you can implement restrictions on a router to make that happen.

You can also place restrictions on hardware addresses, protocols, and applications.

Now we're talking security—the honey barrel is now sealed, shrouded in razor wire, and made of solid titanium!

## **Explain network segmentation and basic traffic management concepts**

### **Flexibility and Scalability**

If you were paying attention to what you've read so far, you know that layer 2 switches only read frames for filtering—they don't look at the Network layer protocol. And by default, switches forward all broadcasts. But if you create and implement VLANs, you're essentially creating smaller broadcast domains at layer 2.

What this means is that broadcasts sent out from a node in one VLAN won't be forwarded to ports configured to belong to a different VLAN. So, by assigning switch ports or users to VLAN groups on a switch or group of connected switches, you gain the flexibility to add only the users you want into that broadcast domain regardless of their physical location. This setup can also work to block broadcast storms caused by a faulty NIC as well as prevent an intermediate device from propagating broadcast storms throughout the entire internetwork. Those evils can still happen on the VLAN where the problem originated, but the device with the disease will be quarantined to that one ailing VLAN.

Another advantage is that when a VLAN gets too big, you can create more VLANs to keep the broadcasts from consuming too much bandwidth—the fewer users in a VLAN, the fewer users affected by broadcasts. This is all well and good, but you seriously need to keep network services in mind and understand how the users connect to these services when you create your VLAN.

It's a good move to try to keep all services, except for the email and Internet access that everyone needs, local to all users whenever possible.



To understand how a VLAN looks to a switch, it's helpful to begin by first looking at a traditional network. Figure 2.14 shows how a network was created by using hubs to connect physical LANs to a router.

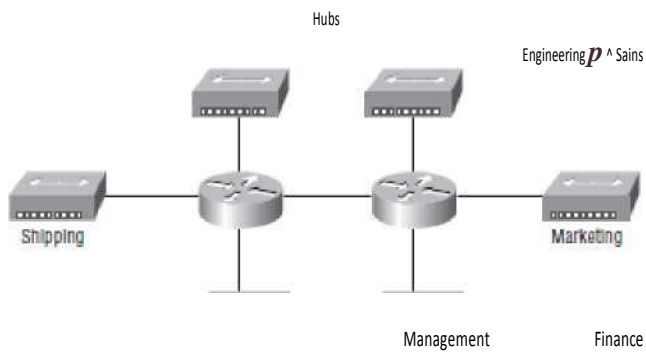


FIGURE 2.14 Physical LANs connected to a router

Here, you can see that each network is attached with a hub port to the router (each segment also has its own logical network number even though this isn't obvious from looking at the figure). Each node attached to a particular physical network has to match that network's number in order to be able to communicate on the internetwork. Notice that each department has its own LAN, so if you needed to add new users to, let's say, Sales, you would just plug them into the Sales LAN and they would automatically be part of the Sales collision and broadcast domain. This design really did work well for many years.

But there was one major flaw: What happens if the hub for Sales is full and we need to add another user to the Sales LAN? Or, what do we do if there's no more physical space where the Sales team is located for this new employee? That new Sales team member will just have to sit on the same side of the building as the Finance people, and we'll just plug the poor soul into the hub for Finance.

Doing this obviously makes the new user part of the Finance LAN, which is very bad for many reasons. First and foremost, we now have a major security issue. Because the new Sales employee is a member of the Finance broadcast domain, the newbie can see all the same servers and access all network services that the Finance folks can. Second, for this user to access the Sales network services that they need to get their job done, they would have to go through the router to log in to the Sales server—not exactly efficient!

Now let's look at what a switch accomplishes for us. Figure 2.15 demonstrates how switches come to the rescue by removing the physical boundary to solve our problem. It also shows how six VLANs (numbered 2 through 7) are used to create a broadcast domain for each department. Each switch port is then administratively assigned a VLAN membership, depending on the host and which broadcast domain it's placed in.

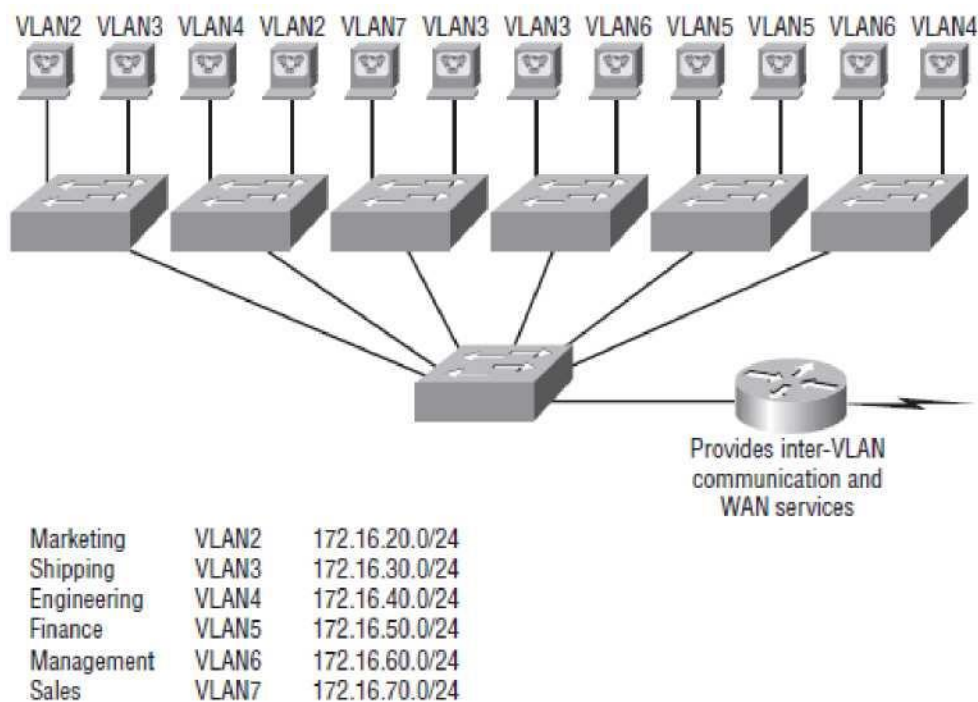


FIGURE 2.15 switches removing the physical boundary

So now, if we needed to add another user to the Sales VLAN (VLAN 7), we could just assign the port to VLAN 7 regardless of where the new Sales team member is physically located— nice! This illustrates one of the sweetest advantages to designing your network with VLANs over the old collapsed backbone design. Now, cleanly and simply, each host that needs to be in the Sales VLAN is merely assigned to VLAN 7. And by using the new switches with the predefined macros, we can just use CNA and Smart ports to configure the port to be a Desktop connection and voila! The port configuration is simply completed for us.

Notice that I started assigning VLANs with VLAN number 2. The number is irrelevant, but you might be wondering what happened to VLAN 1? Well that VLAN is an administrative VLAN, and even though it can be used for a workgroup, Cisco recommends that you use it for administrative purposes only. You can't delete or change the name of VLAN 1, and by default, all ports on a switch are members of VLAN 1 until you change them.

Since each VLAN is considered a broadcast domain, it's got to also have its own subnet number (refer again to Figure 2.15). And if you're also using IPv6, then each VLAN must also be assigned its own IPv6 network number. So you don't get confused, just keep thinking of VLANs as separate subnets or networks.

Now let's get back to that "because of switches, we don't need routers anymore" misconception. Looking at Figure 2.15, notice that there are seven VLANs, or broadcast domains, counting VLAN 1.

## Configure and verify VLANs

Configure, verify, and troubleshoot VLANs

It may come as a surprise to you, but configuring VLANs is actually pretty easy. Figuring out which users you want in each VLAN is not; it's extremely time-consuming. But once you've decided on the number of VLANs you want to create and established which users you want to belong to each one, it's time to bring your first VLAN into the world.

To configure VLANs on a Cisco Catalyst switch, use the global config `vlan` command. In the following example, I'm going to demonstrate how to configure VLANs on the S1 switch by creating three VLANs for three different departments—again, remember that VLAN 1 is the native and administrative VLAN by default:

```
S1#config t S1 (config) #vlan?
WORD ISL VLAN IDs 1-4094 internal VLAN S1(config)#vlan 2
S1(config-vlan)#name Sales S1(config-vlan)#vlan 3 S1(config-
vlan)#name Marketing S1(config-vlan)#vlan 4 S1(config-vlan)#name
Accounting S1(config-vlan)#^Z S1#
```

From the preceding, you can see that you can create VLANs from 2 to 4094. This is only mostly true. As I said, VLANs can really only be created up to 1005, and you can't use, change, rename, or delete VLANs 1 and 1002 through 1005 because they're reserved. The VLAN numbers above that are called extended VLANs and won't be saved in the database unless your switch is set to VTP transparent mode. You won't see these VLAN numbers used too often in production.

Here's an example of setting my S1 switch to VLAN 4000 when my switch is set to VTP server mode (the default VTP mode):

```
S1#config t S1 (config) #vlan 4000 S1 (config-vlan) #^Z % Failed to
create VLANs 4000
Extended VLAN(s) not allowed in current VTP mode.
%failed to commit extended VLAN(s) changes.
```

After you create the VLANs that you want, you can use the `show vlan` command to check them out. But notice that, by default, all ports on the switch are in VLAN 1. To change the VLAN associated with a port, you need to go to each interface and tell it which VLAN to be a part of.

Once the VLANs are created, verify your configuration with the `show vlan` command (`sh vlan` for short):

## **S1#sh vlan** **VLAN Name Status Ports**

- 1 default active Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Gi0/1**
- 2 Sales active**
- 3 Marketing active**
- 4 Accounting active [output cut]**

This may seem repetitive, but it's important, and I want you to remember it: You can't change, delete, or rename VLAN 1 because it's the default VLAN and you just can't change that—period. It's the native VLAN of all switches by default, and Cisco recommends that you use it as your administrative VLAN. Basically, any packets that aren't specifically assigned to a different VLAN will be sent down to the native VLAN.

In the preceding S1 output, you can see that ports Fa0/3 through Fa0/8 and the Gi0/1 uplink are all in VLAN 1, but where are ports 1 and 2? Ports one and two are trunked. Any port that is a trunk port won't show up in the VLAN database. You have to use the show interface trunk command to see your trunked ports.

## **Assigning Switch Ports to VLANs**

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries, plus the number of VLANs to which it can belong. You can configure each port on a switch to be in a specific VLAN (access port) by using the interface switchport command. You can also configure multiple ports at the same time with the interface range command.

Remember that you can configure either static memberships or dynamic memberships on a port. I'm only going to cover the static flavor. In the following example, I'll configure interface fa0/3 to VLAN 3. This is the connection from the S1 switch to the HostA device:

```
S1#config t S1 (config) #int fa0/3 S1 (config-if) #switchport?  
access Set access mode characteristics of the interface backup Set  
backup for the interface block Disable forwarding of unknown uni/multi  
cast addresses host Set port host  
Mode Set trunking mode of the interface  
Nonegotiate Device will not engage in negotiation protocol on this  
interface  
Port-security Security related command priority Set appliance 802.1p  
priority  
Protected Configure an interface to be a protected port trunk set  
trunking characteristics of the interface voice appliance attributes
```

Let's start with setting an access port on S1, which is probably the most widely used type of port on production switches that has VLANs configured:

**S1 (config-if) #switchport mode?**

**Access Set trunking mode to ACCESS unconditionally**

**Dynamic Set trunking mode to dynamically negotiate access or Trunk mode**

**Trunk Set trunking mode to TRUNK unconditionally S1 (config-if)**

**#switchport mode access S1 (config-if) #switchport access vlan 3**

By starting with the switch port mode access command, you're telling the switch that this is a layer 2 port. You can then assign a VLAN to the port with the switch port access command. Remember, you can choose many ports to configure at the same time if you use the interface range command. The dynamic and trunk commands are used for trunk ports exclusively. That's it. Well, sort of. If you plugged devices into each VLAN port, they can only talk to other devices in the same VLAN. We want to enable inter-VLAN communication, and we're going to do that, but first you need to learn a bit more about trunking.

## **Configure and verify trunking on Cisco switches**

Configure, verify, and troubleshoot trunking on Cisco switches

The 2960 switch only runs the IEEE 802.1Q encapsulation method. To configure trunking on a Fast Ethernet port, use the interface command trunk [parameter].

The following switch output shows the trunk configuration on interface fa0/8 as set to trunk on:

```
S1#config t S1 (config) #int fa0/8 S1 (config-if) #switchport mode trunk
```

The following list describes the different options available when configuring a switch interface: switch-port mode access but this puts the interface (access port) into permanent non-trunking mode and negotiates to convert the link into a non-trunk link. The interface becomes a non-trunk interface regardless of whether the neighboring interface is a trunk interface. The port would be a dedicated layer 2 port.

Switchport mode dynamic auto this mode makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode. This is now the default switchport mode for all Ethernet interfaces on all new Cisco switches.

Switchport mode dynamic desirable this one makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto

mode. I used to see this mode as the default on some older switches, but not any longer. The default is dynamic auto now.

**Switchport mode trunk** Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface isn't a trunk interface.

**Switchport nonegotiate** prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

### Trunking with the Cisco Catalyst 3560 Switch

Okay, let's take a look at one more switch—the Cisco Catalyst 3560. The configuration is pretty much the same as it is for a 2960, with the exception that the 3560 can provide layer 3 services and the 2960 can't. Plus, the 3560 can run both the ISL and the IEEE 802.1Q trunking encapsulation methods—the 2960 can only run 802.1Q. With all this in mind, let's take a quick look at the VLAN encapsulation difference regarding the 3560 switch.

The 3560 has the encapsulation command, which the 2960 switch doesn't:

**Core (config-if) #switchport trunk encapsulation? Dot1q** Interface uses only 802.1q trunking encapsulation when trunking

**Isl** Interface uses only ISL trunking encapsulation when trunking

**Negotiate** Device will negotiate trunking encapsulation with peer on interface

**Core (config-if) #switchport trunk encapsulation dot1q** Core (config-if) #switchport mode trunk

As you can see, we've got the option to add either the IEEE 802.1Q (dot1q) encapsulation or the ISL encapsulation to the 3560 switch. After you set the encapsulation, you still have to set the interface mode to trunk. Honestly, it's pretty rare that you'd continue to use the ISL encapsulation method. Cisco is moving away from ISL—its new routers don't even support it.

### Defining the Allowed VLANs on a Trunk

As I've mentioned, trunk ports send and receive information from all VLANs by default, and if a frame is untagged, it's sent to the management VLAN. This applies to the extended range VLANs as well.

But we can remove VLANs from the allowed list to prevent traffic from certain VLANs from traversing a trunked link. Here's how you'd do that:

**S1#config t S1 (config) #int f0/1**



**S1 (config-if) #switchport trunk allowed vlan?**  
**WORD** VLAN IDs of the allowed VLANs when this port is in trunking mode  
**Add** VLANs to the current list all VLANs  
**Except** all VLANs except the following none no VLANs  
**Remove** VLANs from the current list **S1 (config-if) #switchport trunk allowed vlan remove?**  
**WORD** VLAN IDs of disallowed VLANs when this port is in trunking mode **S1 (config-if) #switchport trunk allowed vlan remove 4**

The preceding command stopped the trunk link configured on S1 port f0/1, causing it to drop all traffic sent and received for VLAN 4. You can try to remove VLAN 1 on a trunk link, but it will still send and receive management like CDP, PAgP, LACP, DTP, and VTP, so what's the point? To remove a range of VLANs, just use a hyphen:

**S1 (config-if) #switchport trunk allowed vlan remove 4-8**

If by chance someone has removed some VLANs from a trunk link and you want to set the trunk back to default, just use this command:

**S1 (config-if) #switchport trunk allowed vlan all** Or this command to accomplish the same thing:  
**S1 (config-if) #no switchport trunk allowed vlan**

Next, I want to show you how to configure pruning for VLANs before we start routing between VLANs.

Changing or Modifying the Trunk Native VLAN

You really don't want to change the trunk port native VLAN from VLAN 1, but you can, and some people do it for security reasons. To change the native VLAN, use the following command:

**S1#config t** **S1 (config) #int f0/1** **S1 (config-if) #switchport trunk?**  
**Allowed** Set allowed VLAN characteristics when interface is in trunking mode  
**Native** Set trunking native characteristics when interface is in trunking mode  
**Pruning** Set pruning VLAN characteristics when interface is in trunking mode  
**S1 (config-if) #switchport trunk native?**  
**Vlan** Set native VLAN when interface is in trunking mode **S1 (config-if) #switchport trunk native vlan?**  
**<1-4094>** VLAN ID of the native VLAN when this port is in trunking mode  
**S1 (config-if) #switchport trunk native vlan 40** **S1 (config-if) #^Z**



## 3.3 IP Routing Technologies

---

### **Describe basic routing concepts**

Describe basic routing concepts (including packet forwarding, router lookup process)

Once you create an internetwork by connecting your WANs and LANs to a router, you'll need to configure logical network addresses, such as IP addresses, to all hosts on the internetwork so that they can communicate across that internetwork.

The term routing is used for taking a packet from one device and sending it through the network to another device on a different network. Routers don't really care about hosts—they only care about networks and the best path to each network. The logical network address of the destination host is used to get packets to a network through a routed network, and then the hardware address of the host is used to deliver the packet from a router to the correct destination host. If your network has no routers, then it should be apparent that you are not routing. Routers route traffic to all the networks in your internetwork. To be able to route packets, a router must know, at a minimum, the following:

- Destination address
- Neighbor routers from which it can learn about remote networks
- Possible routes to all remote networks
- The best route to each remote network
- How to maintain and verify routing information

The router learns about remote networks from neighbor routers or from an administrator.

The router then builds a routing table (a map of the internetwork) that describes how to find the remote networks. If a network is directly connected, then the router already knows how to get to it.

If a network isn't directly connected to the router, the router must use one of two ways to learn how to get to the remote network:

Static routing, meaning that someone must hand-type all network locations into the routing table, or something called dynamic routing. In dynamic routing, a protocol on one router communicates with the same protocol running on neighbor routers. The routers then update each other about all the networks they know about and place this information into the

routing table. If a change occurs in the network, the dynamic routing protocols automatically inform all routers about the event. If static routing is used, the administrator is responsible for updating all changes by hand into all routers. Typically, in a large network, a combination of both dynamic and static routing is used

## Configure and verify inter-VLAN routing (Router on a stick)

Configure, verify, and troubleshoot inter-VLAN routing

By default, only hosts that are members of the same VLAN can communicate. To change this and allow inter-VLAN communication, you need a router or a layer 3 switch. I'm going to start with the router approach.

To support ISL or 802.1Q routing on a Fast Ethernet interface, the router's interface is divided into logical interfaces—one for each VLAN. These are called sub-interfaces. From a Fast Ethernet or Gigabit interface, you can set the interface to trunk with the encapsulation command:

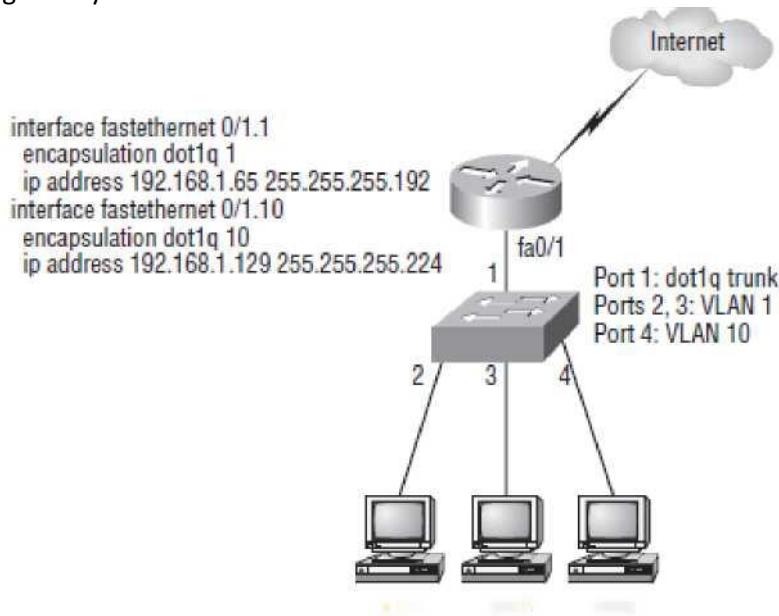
```
ISR#config t
ISR (config) #int f0/0.1
ISR (config-subif)
#encapsulation? Dot1Q
IEEE 802.1Q Virtual
LAN ISR (config-subif)
#encapsulation dot1Q?
<1-4094> IEEE 802.1Q
VLAN ID
```

Notice that my 2811 router (named ISR) only supports 802.1Q. We'd need an older-model router to run the ISL encapsulation, but why bother? The sub-interface number is only locally significant, so it doesn't matter which sub-interface numbers are configured on the router. Most of the time, I'll configure a sub-interface with the same number as the VLAN I want to route. It's easy to remember that way, since the sub-interface number is used only for administrative purposes.

It's really important that you understand that each VLAN is a separate subnet. True, I know—they don't have to be. But it really is a good idea to configure your VLANs as separate subnets, so just does that.

Now, I need to make sure you're fully prepared to configure inter-VLAN routing, as well as determine the port IP addresses of hosts connected in a switched VLAN environment. And as always, it's also a good idea to be able to fix any problems that may arise. To set you up for success, let me

You should be able to determine the IP address, masks, and default gateways of each of the hosts in the VLANs.



HostA HostB HostC FIGURE 4.9 Configuring Inter-VLAN example 1

give you few examples.

The next step after that is to figure out which subnets are being used. By looking at the router configuration in the figure, you can see that we're using 192.168.1.64/26 with VLAN 1 and 192.168.1.128/27 with VLAN 10. And by looking at the switch configuration, you can see that

ports 2 and 3 are in VLAN 1 and port 4 is in VLAN 10. This means that HostA and HostB are in VLAN 1, and HostC is in VLAN 10.

Here's what the hosts' IP addresses should be:

**HostA: 192.168.1.66, 255.255.255.192, default gateway 192.168.1.65**  
**HostB: 192.168.1.67, 255.255.255.192, default gateway 192.168.1.65**  
**HostC: 192.168.1.130, 255.255.255.224, default gateway 192.168.1.129**

The hosts could be any address in the range—I just choose the first available IP address after the default gateway address. That wasn't so hard, was it?

Now, again using Figure 4.10, let's go through the commands necessary to configure switch port 1 to establish a link with the router and provide inter-VLAN communication using the IEEE version for encapsulation. Keep in mind that the commands can vary slightly depending on what type of switch you're dealing with.

For a 2960 switch, use the following:

```
2960#config t  
2960(config) #interface fa0/1 2960(config-if) #switchport mode trunk
```

As you already know, the 2960 switch can only run the 802.1Q encapsulation, so there's no need to specify it. You can't anyway! For a 3560, it's basically the same, but since it can run ISL and 802.1Q, you have to specify the trunking protocol you're going to use.

Let's take a look at Figure 4.10 and see what we can learn from it. This figure shows three VLANs, with two hosts in each of them.

The router in Figure 4.10 is connected to the fa0/1 switch port, and VLAN 2 is configured on port f0/6. Looking at the diagram, these are the things that Cisco expects you to know: <sup>1</sup>

- 
- 1 The router is connected to the switch using sub-interfaces.
  - The switch port connecting to the router is a trunk port.

The switch ports connecting to the clients and the hub are access ports, not trunk ports.

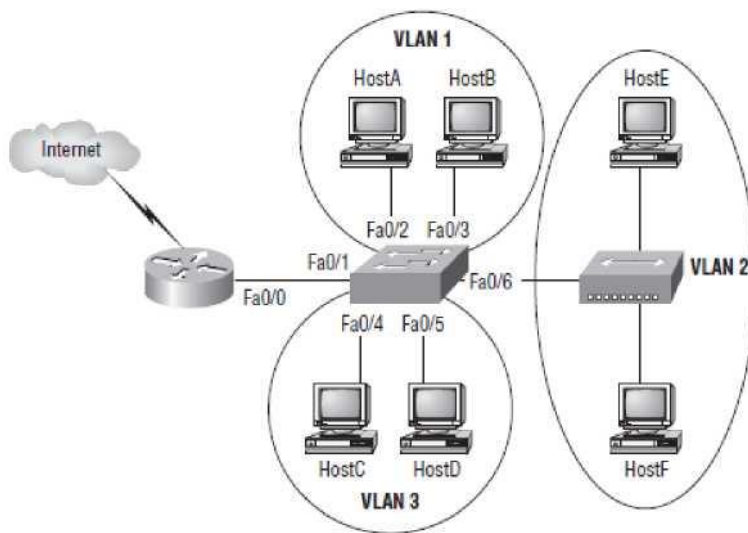


FIGURE 4.10 Inter- VLAN example 2

The configuration of the switch would look something like this:

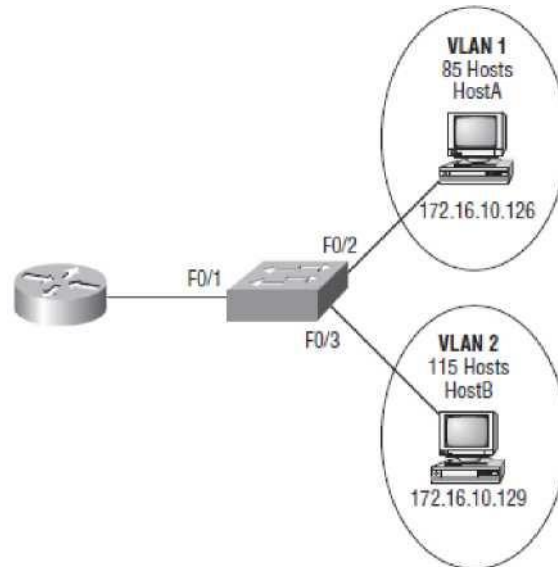
```
2960#config t 2960(config) #int f0/1
2960(config-if) #switchport mode trunk
2960(config-if) #int f0/2
2960(config-if) #switchport access vlan 1
2960(config-if) #int f0/3
2960(config-if) #switchport access vlan 1
2960(config-if) #int f0/4
2960(config-if) #switchport access vlan 3
2960(config-if) #int f0/5
2960(config-if) #switchport access vlan 3
2960(config-if) #int f0/6
2960(config-if) #switchport access vlan 2
Before we configure the router, we need to design our logical
network: VLAN 1: 192.168.10.16/28 VLAN 2: 192.168.10.32/28
VLAN 3: 192.168.10.48/28
```

The configuration of the router would then look like this:

```
ISR#config t ISR(config)#int f0/0 ISR(config-if)#no ip address
ISR(config-if)#no shutdown ISR(config-if)#int f0/0.1
ISR(config-subif)#encapsulation dot1q 1
ISR (config-subif) #ip address 192.168.10.17 255.255.255.240
ISR (config-subif) #int f0/0.2 ISR (config-subif) #encapsulation
dot1q 2
ISR (config-subif) #ip address 192.168.10.33
255.255.255.240 ISR (config-subif) #int f0/0.3 ISR
(config-subif) #encapsulation dot1q 3
ISR (config-subif) #ip address 192.168.10.49 255.255.255.240
```

The hosts in each VLAN would be assigned an address from their subnet range, and the default gateway would be the IP address assigned to the

router's sub-interface in that VLAN. Now, let's take a look at another figure and see if you can determine the switch and router configurations without looking at the answer—no cheating! Figure 4.11 shows a router connected to a 2960 switch with two VLANs. One host in each VLAN is assigned an IP address. What are your router and switch configurations based on these IP addresses?



**FIGURE 4.11** *Inter-VLAN examples 3*

Since the hosts don't list a subnet mask, you have to look for the number of hosts used in each VLAN to figure out the block size. VLAN 1 has 85 hosts and VLAN 2 has 115 hosts. Each of these will fit in a block size of 128, which is a /25 mask, or 255.255.255.128. You should know by now that the subnets are 0 and 128; the 0 subnet (VLAN 1) has a host range of 1-126, and the 128 subnet (VLAN 2) has a range of 129-254. You can almost be fooled since HostA has an IP address of 126, which makes it almost seem that HostA and B are in the same subnet. But they're not, and you're way too smart by now to be fooled by this one!

Here is the switch configuration:

```

2960#config t
2960(config)#int f0/1
2960(config-if)#switchport mode trunk
2960(config-if)#int f0/2
2960(config-if)#switchport access vlan 1
2960(config-if)#int f0/3
2960(config-if)#switchport access vlan 2
  
```

Here is the router configuration:

```

ISR#config t
ISR(config)#int f0/0
ISR(config-if)#no ip address
ISR(config-if)#no shutdown
ISR(config-if)#int f0/0.1
ISR(config-subif)#encapsulation dot1q 1
ISR(config-subif)#ip address 172.16.10.1
  
```

```
255.255.255.128 ISR (config-subif) #int f0/0.2 ISR  
(config-subif) #encapsulation dot1q 2  
ISR (config-subif) #ip address 172.16.10.254 255.255.255.128
```

I used the first address in the host range for VLAN 1 and the last address in the range for VLAN 2, but any address in the range would work. You just have to configure the host's default gateway to whatever you make the router's address.

Now, before we go on to the next example, I need to make sure that you know how to set the IP address on the switch. Since VLAN 1 is typically the administrative VLAN, we'll use an IP address from that pool of addresses. Here's how to set the IP address of the switch (I'm not nagging, but you really should already know this!):

```
2960#config t 2960(config) #int vlan 1  
2960(config-if) #ip address 172.16.10.2 255.255.255.128 2960(config-if)  
#no shutdown
```

Yes, you have to do a no shutdown on the VLAN interface. One more example, and then we'll move on to VTP—another important subject that you definitely don't want to miss! In Figure 2.26 there are two VLANs. By looking at the router configuration, what's the IP address, mask, and default gateway of HostA? Use the last IP address in the range for HostA's address:

If you really look carefully at the router configuration (the hostname in this figure is just Router), there is a simple and quick answer. Both subnets are using a /28, or 255.255.255.240 mask, which is a block size of 16. The router's address for VLAN 1 is in subnet 128. The next subnet is 144, so the broadcast address of VLAN 1 is 143 and the valid host range is 129-142. So, the host address would be this:

**IP Address: 192.168.10.142**  
**Mask: 255.255.255.240**  
**Default Gateway: 192.168.10.129**



## 3.4 Network Device Security

---

**Configure and verify network device security features such as**

### **Device Password security/enable secret vs enable**

Five passwords are used to secure your Cisco routers: console, auxiliary, Telnet (VTY), enable password, and enable secret. The enable secret and enable password are used to set the password that's used to secure privileged mode. This will prompt a user for a password when the enable command is used. The other three are used to configure a password when user mode is accessed through the console port, through the auxiliary port, or via Telnet. Let's take a look at each of these now.

### **Enable Passwords**

You set the enable passwords from global configuration mode like this:

John (config) #enable?

Last-resort Define enable action if no TACACS servers respond

Password Assign the privileged level password secret      Assign      the  
privileged level secret

Use-tacacs Use TACACS to check enable passwords

The following points describe the enable password parameters:

- Last-resort allows you to still enter the router if you set up authentication through a TACACS server and it's not available. But it isn't used if the TACACS server is working.
- Password Sets the enable password on older, pre-10.3 systems, and isn't ever used if an enable secret is set.
- Secret this is the newer, encrypted password that overrides the enable password if it's set.
- Use-tacacs this tells the router to authenticate through a TACACS server. It's convenient if you have anywhere from a dozen to multitudes of routers because, well, would you like to face the fun task of changing the password on all those routers? If you're sane, no, you

Wouldn't. So instead, just go through the TACACS server, and you only have to change the password once

If you try to set the enable secret and enable passwords the same, the router will give you a nice, polite warning to change the second password. If you don't have older legacy routers, don't even bother to use the enable password. User-mode passwords are assigned by using the line command:

```
John (config) #line?
<0-337> First Line number
Aux      Auxiliary line
Console  Primary terminalline
TTY      Terminal controller
Vty      Virtual terminal
X/y      Slot/Port for Modems
X/y/z    Slot/Subslot/Port for Modems
```

Here are the lines to be concerned with:

- Aux sets the user-mode password for the auxiliary port. It's usually used for attaching a modem to the router, but it can be used as a console as well. Console sets a console user mode password.
- Vty Sets a Telnet password on the router. If this password isn't set, then Telnet can't be used by default.

## SSH

Instead of telnet, you can use secure shell, which creates a more secure session than the Telnet application that uses an unencrypted data stream. Secure Shell (SSH) uses encrypted keys to send data so that your username and password are not sent in the clear. Here are the steps to setting up SSH:

1. Set your hostname:

```
Router (config) #hostname john
```

2. Set the domain-name. (Both the hostname and domain-name are required for the encryption keys to be generated.)

```
Todd (config) #ip domain-name johndoe.com
```

3. Generate the encryption keys for securing the session:

```
John (config) #crypto key generate rsa general-keys modulus?
```

```
<360-2048> size of the key modulus [360-2048] John (config) #crypto
key generate rsa general-keys modulus 1024 the name for the keys will
be: john.johndoe.com % the key modulus size is 1024 bits
% generating 1024 bit RSA keys, keys will be non-
Exportable... [OK]
```

```
June 24 19:25:30.035: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

4. Set the max idle timer for a SSH session:

```
John (config) #ip Ssh time-out?
```

```
<1-120> SSH time-out interval (secs)
```

```
John (config) #ip Ssh time-out 60
```

5. Set the max failed attempts for a SSH connection:

**John (config) #ip Ssh authentication-retries?**

**<0-5> Number of authentication retries John (config) #ip Ssh authentication-retries 2**

6. Connect to the vty lines of the router:

**Todd (config) #line vty 0 1180**

7. Last, configure SSH and then Telnet as access protocols.

**Todd (config-line) #transport input Ssh telnet**

If you do not use the keyword “telnet” at the end of the command string, then only SSH will work on the router. It will look like this:

**Todd (config-line) #transport input Ssh**

I am not suggesting you use either way, but just understand that SSH is more secure than Telnet.

Service Password

Several of the configuration commands used to configure passwords store the passwords in clear text in the running-config file, at least by default. In particular, the simple passwords configured on the console and vty lines, with the password command, plus the password in the username command, are all stored in clear text by default. (The enable secret command automatically hides the password value.)

To prevent password vulnerability in a printed version of the configuration file, or in a backup copy of the configuration file stored on a server, you can encrypt or encode the passwords using the service password-encryption global configuration command. The presence or absence of the service password-encryption global configuration command dictates whether the passwords are encrypted as follows: <sup>2</sup>

- If the **service password-encryption** command has already been configured, any future changes to these passwords are encrypted.
- If the **no service password-encryption** command is used later, the passwords remain encrypted, until they are changed—at which point they show up in clear text.

The following example shows this in detail:

**Switch3#show running-config | begin line vty**

**Line vty 0 4 password cisco  
login**

---

<sup>2</sup> When the **service password-encryption** command is configured, all existing console, vty, and username command passwords are immediately encrypted.

**Switch3#**configure terminal

Enter configuration commands, one per line.  
End with CNTL/Z. Switch3 (config) #**service password-encryption**

Switch3 (config) #\*Z

**Switch3#**show running-config | begin line vty

Line vty 0 4 password 7 07OC285F4DO6  
login end

**Switch3#**configure terminal

Enter configuration commands, one per line.  
End with CNTL/Z. Switch3 (config) #**no service password-encryption** Switch3 (config) #"Z

**Switch3#**show running-config | begin line vty

Line vty 0 4 password 7 07OC285F4DO6  
login end

**Switch3#**configure terminal

Enter configuration commands, one per line.  
End with CNTL/Z. Switch3 (config) #**line vty 4** Switch3 (config-line) #**password cisco** Switch3 (config-line) #\*Z

**Switch3#**show running-config | begin line vty

Line vty 0 4 password cisco login

## Configure and Verify Switch Port Security features such as

### Port Security

If the network engineer knows what devices should be cabled and connected to particular interfaces on a switch, the engineer can use port security to restrict that interface so that only the expected devices can use it. This reduces exposure to some types of attacks in which the attacker connects a laptop to the wall socket that connects to a switch port that has been configured to use port security. When that inappropriate device attempts to send frames to the switch interface, the switch can issue

informational messages, discard frames from that device, or even discard frames from all devices by effectively shutting down the interface.

Port security configuration involves several steps. Basically, you need to make the port an access port, which means that the port is not doing any VLAN trunking. You then need to enable port security and then configure the actual MAC addresses of the devices allowed to use that port. The following list outlines the steps, including the configuration commands used:

- Step 1 Make the switch interface an access interface using the switchport mode access interface subcommand.
- Step 2 Enable port security using the switchport port-security interface subcommand.
- Step 3 (Optional) Specify the maximum number of allowed MAC addresses associated with the interface using the switchport port-security maximum number interface subcommand. (Defaults to one MAC address.)
- Step 4 (Optional) Define the action to take when a frame is received from a MAC address other than the defined addresses using the switchport port-security violation {protect | restrict | shutdown} interface subcommand. (The default action is to shut down the port.)
- Step 5A Specify the MAC address (es) allowed to send frames into this interface using the switchport port-security mac-address command. Use the command multiple times to define more than one MAC address.
- Step 5B alternatively, instead of Step 5A, use the “sticky learning” process to dynamically learn and configure the MAC addresses of currently connected hosts by configuring the switchport port- security mac address sticky interface subcommand.

For example, in Figure 6.1, Server 1 and Server 2 are the only devices that should ever be connected to interfaces Fast Ethernet 0/1 and 0/2, respectively. When you configure port security on those interfaces, the switch examines the source MAC address of all frames received on those ports, allowing only frames sourced from the configured MAC addresses.

Example 6.1 shows a sample port security configuration matching Figure 9-2, with interface Fa0/1 being configured with a static MAC address, and with interface Fa0/2 using sticky learning.

#### ***Example 6.1 Using Port Security to Define Correct MAC Addresses of Particular Interfaces***

```
Fred#show running-config (Lines omitted for brevity)  
interface FastEthernet0/1 switchport mode access  
switchport port-security  
Switchport port-security mac-address 0200.1111.1111  
!  
Interface FastEthernet0/2 switchport mode access  
switchport port-security  
Switchport port-security mac-address sticky  
Fred#show port-security interface fastethernet 0/1
```

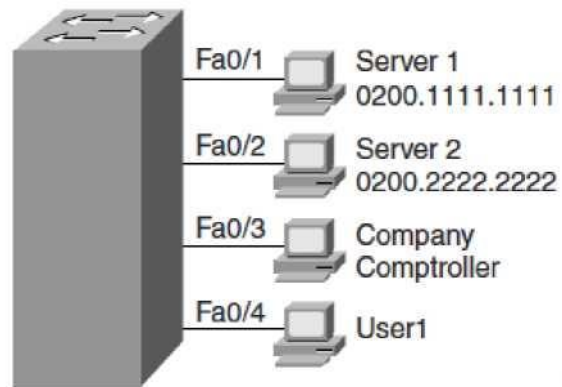


Figure 6.1 Port Security Configuration Example

```

Port Security: Enabled
Port Status: Secure-shutdown
Violation Mode: Shutdown
Aging Time: 0 mins
Aging Type: Absolute
Secure Static Address Aging: Disabled Maximum
MAC Addresses: 1 Total MAC Addresses: 1
Configured MAC Addresses: 1 Sticky MAC
Addresses: 0
Last Source Address: Vlan: 0013.197b.5004:1
Security Violation Count: 1
Fred#show port-security interface fastethernet 0/2
Port Security: Enabled
Port Status: Secure-up
Violation Mode: Shutdown
Aging Time: 0 mins
Aging Type: Absolute
Secure Static Address Aging: Disabled Maximum
MAC Addresses: 1 Total MAC Addresses: 1
Configured MAC Addresses: 1 Sticky MAC
Addresses: 1
Last Source Address: Vlan: 0200.2222.2222:1
Security Violation Count: 0
Fred#show running-config
(Lines omitted for brevity)
Interface FastEthernet0/2
Switchport mode access
Switchport port-security
Switchport port-security mac-address sticky
Switchport port-security mac-address sticky 0200.2222.2222

```

For FastEthernet 0/1, Server 1's MAC address is configured with the switchport portsecurity mac-address 0200.1111.1111 command. For port security to work, the 2960 must think that the interface is an access interface, so the switchport mode access command is required. Furthermore, the switchport port-security command is required to enable port security on the interface. Together, these three interface subcommands enable port security, and only MAC address 0200.1111.1111 is allowed to use the interface. This interface uses defaults for the other settings,



allowing only one MAC address on the interface, and causing the switch to disable the interface if the switch receives a frame whose source MAC address is not 0200.1111.1111.

Interface FastEthernet 0/2 uses a feature called sticky secure MAC addresses. The configuration still includes the switchport mode access and switchport port-security commands for the same reasons as on FastEthernet 0/1. However, the switchport portsecurity mac-address sticky command tells the switch to learn the MAC address from the first frame sent to the switch and then add the MAC address as a secure MAC to the running configuration. In other words, the first MAC address heard “sticks” to the configuration, so the engineer does not have to know the MAC address of the device connected to the interface ahead of time.

The show running-config output at the beginning of Example 9-10 shows the configuration for Fa0/2, before any sticky learning occurred. The end of the example shows the configuration after an address was sticky-learned, including the switchport port-security mac-address sticky 0200.2222.2222 interface subcommand, which the switch added to the configuration. If you wanted to save the configuration so that only 0200.2222.2222 is used on that interface from now on, you would simply need to use the copy running-config startup-config command to save the configuration.

As it turns out, a security violation has occurred on FastEthernet 0/1 in Example 9-10, but no violations have occurred on FastEthernet 0/2. The show port-security interface

FastEthernet 0/1 command shows that the interface is in a secure-shutdown state, which means that the interface has been disabled due to port security. The device connected to interface Fast Ethernet 0/1 did not use MAC address 0200.1111.1111, so the switch received a frame in Fa0/1 with a different source MAC, causing a violation.

The switch can be configured to use one of three actions when a violation occurs. All three configuration options cause the switch to discard the offending frame, but some of the configuration options include additional actions. The actions include the sending of syslog messages to the console and SNMP trap message to the network management station, as well as whether the switch should shut down (err-disable) the interface. The shutdown option actually puts the interface in an error disabled (err-disabled) state, making it unusable. An interface in err-disabled state requires that someone manually shutdown the interface and then use the no shutdown command to recover the interface.

## 3.5 LAN Switching Technologies

---

### Identify enhanced switching technologies

#### **Describe enhanced switching technologies (including: VTP, RSTP, VLAN, PVSTP, 802.1q)**

The basic goals of VLAN Trunking Protocol (VTP) are to manage all configured VLANs across a switched internetwork and to maintain consistency throughout that network. VTP allows you to add, delete, and rename VLANs—information that is then propagated to all other switches in the VTP domain.

Here's a list of some of the cool features VTP has to offer:

- Consistent VLAN configuration across all switches in the network
- VLAN trunking over mixed networks, such as Ethernet to ATM LANE or even FDDI
- Accurate tracking and monitoring of VLANs
- Dynamic reporting of added VLANs to all switches in the VTP domain
- Plug and Play VLAN adding

Very nice, but before you can get VTP to manage your VLANs across the network, you have to create a VTP server. All servers that need to share VLAN information must use the same domain name, and a switch can be in only one domain at a time. So, basically, this means that a switch can only share VTP domain information with other switches if they're configured into the same VTP domain. You can use a VTP domain if you have more than one switch connected in a network, but if you've got all your switches in only one VLAN, you just don't need to use VTP. Do keep in mind that VTP information is sent between switches only via a trunk port.

Switches advertise VTP management domain information as well as a configuration revision number and all known VLANs with any specific parameters. But there's also something called VTP transparent mode. In it, you can configure switches to forward VTP information through trunk ports but not to accept information updates or update their VTP databases.

If you've got sneaky users adding switches to your VTP domain behind your back, you can include passwords, but don't forget—every switch must be set up with the same password.

And as you can imagine, this little snag can be a real hassle administratively!



Switches detect any added VLANs within a VTP advertisement, and then prepare to send information on their trunk ports with the newly defined VLAN in tow. Updates are sent out as revision numbers that consist of the notification plus 1. Anytime a switch sees a higher revision number, it knows the information it's getting is more current, so it will overwrite the existing database with the latest information.

You should know these three requirements for VTP to communicate VLAN information between switches:

- The VTP management domain name of both switches must be set the same.
- One of the switches has to be configured as a VTP server.
- No router is necessary.

Now that you've got that down, we're going to delve deeper in the world of VTP with VTP modes and VTP pruning.

## **RSTP**

### **Rapid Spanning-Tree Protocol (RSTP) 802.1w**

How would you like to have a good STP configuration running on your switched network (regardless of the brand of switches) and have all the features built in and enabled on every switch? Absolutely—yes! Well then, welcome to the world of Rapid Spanning- Tree Protocol (RSTP).

Cisco created Port Fast, Uplink Fast, and Backbone Fast to “fix” the holes and liabilities the IEEE 802.1d standard presented. The drawbacks to these enhancements are only that they are Cisco proprietary and need additional configuration. But the new 802.1w standard (RSTP) addresses all these “issues” in one tight package—just turn on RSTP and you're good to go.

Importantly, you must make sure that all the switches in your network are running the 802.1w protocol for 802.1w to work properly! It might come as a surprise, but RSTP actually can interoperate with legacy STP protocols. Just know that the inherently fast convergence ability of 802.1w is lost when it interacts with legacy bridges.

## **PVSTP**

### **PVST**

Understand that Cisco switches run what is called Per-VLAN Spanning-Tree (PVST), which basically means that each VLAN runs its own instance of the STP protocol. If we typed `show spanning-tree`, we'd receive information for each VLAN, starting with VLAN 1. So, say we've got multiple VLANs, and we want to see what's up with VLAN 2—we'd use the command `show spanning-tree vlan 2`.

## Ether channels

### IEEE 802.1Q

Created by the IEEE as a standard method of frame tagging, IEEE 802.1Q actually inserts a field into the frame to identify the VLAN. If you're trunking between a Cisco switched link and a different brand of switch, you've got to use 802.1Q for the trunk to work.

It works like this: You first designate each port that is going to be a trunk with 802.1Q encapsulation. The ports must be assigned a specific VLAN ID, which makes them the native VLAN, in order for them to communicate. The ports that populate the same trunk create a group with this native VLAN, and each port gets tagged with an identification number reflecting that, again, the default is VLAN 1. The native VLAN allows the trunks to carry information that was received without any VLAN identification or frame tag.

The 2960s support only the IEEE 802.1Q trunking protocol, but the 3560s will support both the ISL and IEEE methods.

The basic purpose of ISL and 802.1Q frame-tagging methods is to provide inter-switch

VLAN communication. Also, remember that any ISL or 802.1Q frame tagging is removed if a frame is

Forwarded out an access link—tagging is used across trunk links only!

### **Configure and verify PVSTP operation**

#### PVST+ Operation

In a Cisco PVST+ environment, you can tune the spanning-tree parameters so that half of the VLANs forward on each uplink trunk. To easily achieve this, you configure one switch to be elected the root bridge for half of the total number of VLANs in the network and a second switch to be elected the root bridge for the other half of the VLANs. Providing different STP root switches per VLAN creates a more redundant network.

Spanning-tree operation requires that each switch has a unique BID. In the original 802.1D standard, the BID was composed of the bridge priority and the MAC address of the switch, and all VLANs were represented by a CST. Because PVST+ requires that a separate instance of spanning tree runs for each VLAN, the BID field is required to carry VID information. This is accomplished by reusing a portion of the Priority field as the extended system ID to carry a VID. Figure 8.1 shows how modifying the bridge priority offers this support.

To accommodate the extended system ID, the original 802.1D 16-bit bridge priority field is split into two fields, resulting in these components in the BID:

- Bridge priority: A 4-bit field still used to carry bridge priority. Because

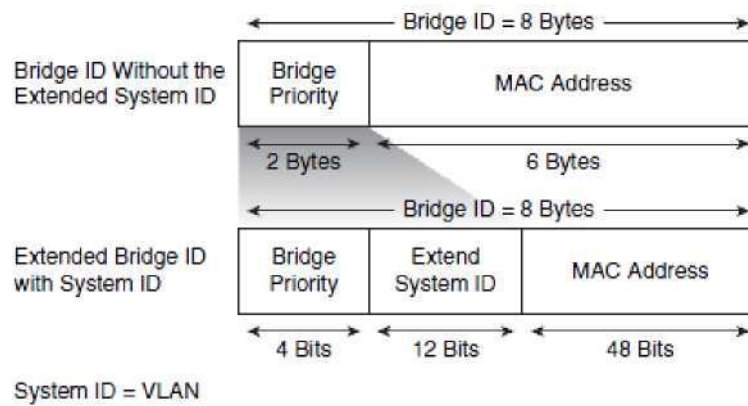


Figure 8.1 PVST+ VLAN ID

of the limited bit count, the priority is conveyed in discreet values in increments of 4096 rather than discreet values in increments of 1, as they would be if the full 16-bit field was available. The default priority, in accordance with IEEE 802.1D, is 32,768, which is the midrange value.

- Extended system ID: A 12-bit field carrying, in this case, the VID for PVST+.
- MAC address: A 6-byte field with the MAC address of a single switch.

By virtue of the MAC address, a BID is always unique. When the priority and extended system ID are prepended to the switch MAC address, each VLAN on the switch can be represented by a unique BID.

If no priority has been configured, every switch will have the same default priority, and the election of the root for each VLAN will be based on the MAC address. This method is a random means of selecting the ideal root bridge; for this reason, it is advisable to assign a lower priority to the switch that should serve as the root bridge. The root bridge should be located in the center of your network traffic flow.

## Describe root bridge election

STP performs three steps to provide a loop-free logical network topology:

1. Elects one root bridge: STP has a process to elect a root bridge. Only one bridge can act as the root bridge in a given network. On the root bridge, all ports are designated ports. Designated ports are in the forwarding state and are designated to forward traffic for a given segment. When in the forwarding state, a port can send and receive traffic.

In Figure 8.2, switch X is elected as the root bridge.

2. Selects the root port on the non-root bridge: STP establishes one root port on each non-root bridge. The root port is the lowest-cost path from the non-root bridge to the root bridge. Root ports are in the forwarding state. Spanning-tree path cost is an accumulated cost calculated on the bandwidth. In Figure 8.2, the lowest-cost path to the root bridge from switch Y is through the 100BASE-T Fast-Ethernet link.

3. Selects the designated port on each segment: On each segment, STP establishes one designated port. The designated port is selected on the bridge that has the lowest-cost path to the root bridge. Designated ports are in the forwarding state, forwarding traffic for the segment. In Figure 8.2, the designated port for both segments is on the root bridge because the root bridge is directly connected to both segments. The 10BASE-T Ethernet port on switch Y is a non-designated port because there is only one designated port per segment. Non-designated ports are normally in the blocking state to logically break the loop topology. When a port is in the blocking state, it is not forwarding data traffic but can still receive traffic.

Switches and bridges running the Spanning Tree Algorithm exchange configuration messages with other switches and bridges at regular intervals (every 2 seconds by default).

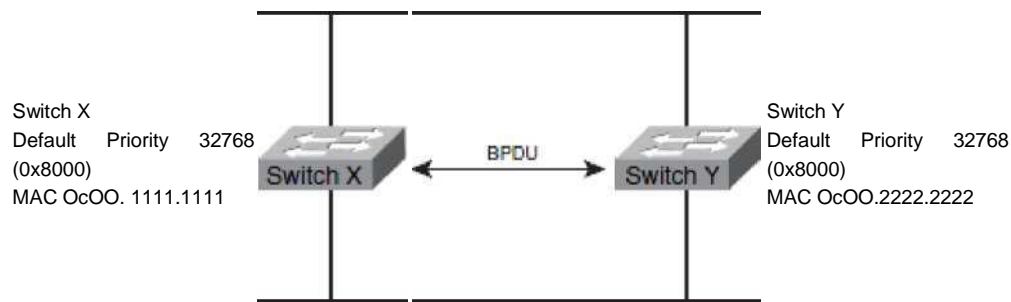
Switches and bridges exchange these messages using a multicast frame called the BPDU.

One of the pieces of information included in the BPDU is the bridge ID (BID). STP calls for each switch or bridge to be assigned a unique BID. Typically, the BID is composed of a priority value (2 bytes) and the bridge MAC address (6 bytes). The default priority, in accordance with IEEE 802.1D, is 32,768 (1000 0000 0000 0000 in binary, or 0x8000 in hex format), which is the midrange value. The root bridge is the bridge with the lowest BID.

#### **Example: Selecting the Root Bridge**

In Figure 8.1, both switches use the same default priority. The switch with the lowest

MAC address is the root bridge. In the example, switch X is the root bridge, with a BID of 0x8000 (0c00.1111.1111).  
**Figure 8.2 Root Bridge Selections**



There are five STP port states:

- Blocking
- Listening
- Learning
- Forwarding
- Disabled

When STP is enabled, every bridge in the network goes through the blocking state and the transitory states of listening and learning at power-up. If properly configured, the ports then stabilize to the forwarding or blocking state. Forwarding ports provide the lowest-cost path to the root bridge. During a topology change, a port temporarily implements the listening and learning states.

The disabled state is not strictly part of STP; a network administrator can manually disable a port, or a security or an error condition may disable it. An example of a port that is disabled would be a port that is shut down. Figure 8.3 shows the flow of spanning-tree port states.

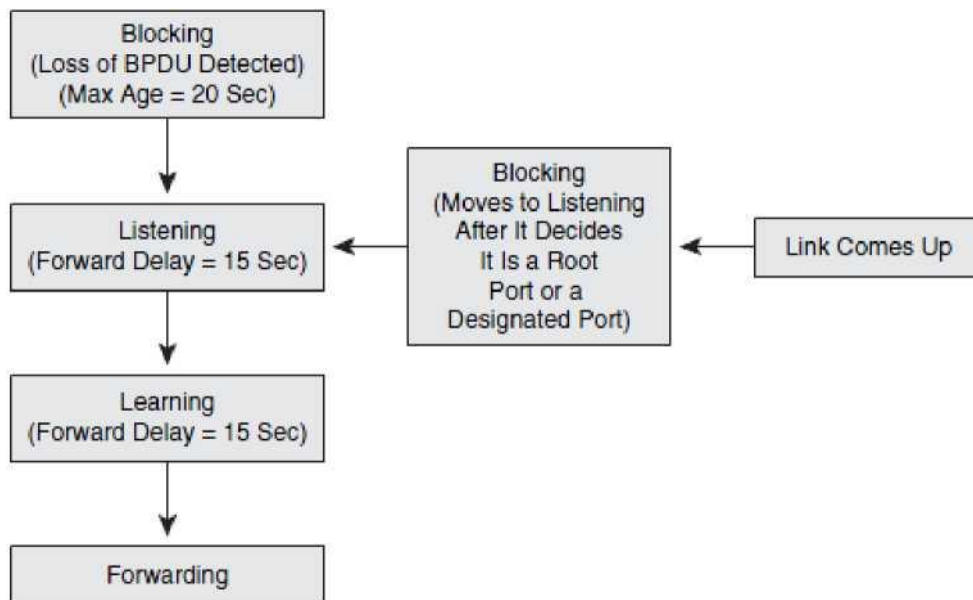


Figure 8.3 Spanning-Tree Port States

All bridge ports initially start in the blocking state, from which they listen for BPDUs.

When the bridge first boots, it functions as if it were the Root Bridge and transitions to the listening state. An absence of BPDUs for a certain period is called the maximum age (max\_age), which has a default of 20 seconds. If a port is in the blocking state and does not receive a new BPDU within the max\_age, the bridge transitions from the blocking state to the listening state. When a port is in the transitional listening state, it can send and receive BPDUs to determine the active topology. At this point, the switch is not passing user data.

During the listening state, the bridge performs these three steps:

1. Selects the root bridge
2. Selects the root ports on the non-root bridges
3. Selects the designated ports on each segment

The time that it takes for a port to transition from the listening state to the learning state or from the learning state to the forwarding state is called the forward delay. The forward delay has a default value of 15 seconds.

The learning state reduces the amount of flooding required when data forwarding begins. If a port is still a designated or root port at the end of the learning state, the port transitions to the forwarding state. In the forwarding state, a port is capable of sending and receiving user data. Ports

that are not the designated or root ports transition back to the blocking state.

A port normally transitions from the blocking state to the forwarding state in 30 to 50 seconds. You can tune the spanning-tree timers to adjust the timing, but these timers are meant to be set to the default value. The default values are put in place to give the network enough time to gather all the correct information about the network topology.

Spanning-tree PortFast causes an interface that is configured as a Layer 2 access port to transition immediately from the blocking state to the forwarding state, bypassing the listening and learning states. You can use PortFast on Layer 2 access ports that are connected to a single workstation or server to allow those devices to connect to the network immediately rather than wait for spanning tree to converge.

Figure 8.4 shows access ports connected with PortFast enabled.

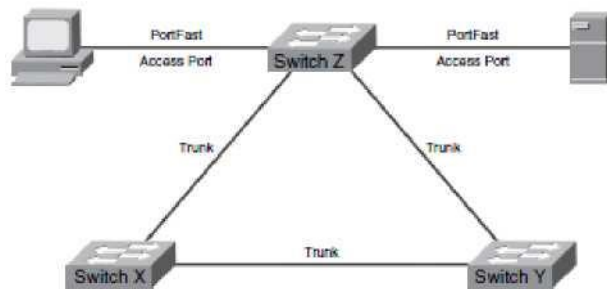


Figure 8.4 PortFast

If an interface that is configured with PortFast receives a BPDU, then spanning tree can transition the port to the blocking state. Using a feature called BPDU guard, the port can be disabled completely when it receives a BPDU to prevent any potential loops caused by PortFast.



## 3.6 IP Services

---

### VRRP

There are several ways a LAN client can determine which router should be the first hop to a particular remote destination. The client can use a dynamic process or static configuration. Examples of dynamic router discovery are as follows:

- Proxy ARP—the client uses Address Resolution Protocol (ARP) to get the destination it wants to reach, and a router will respond to the ARP request with its own MAC address.
- Routing protocol—the client listens to dynamic routing protocol updates (for example, from Routing Information Protocol [RIP]) and forms its own routing table.
- ICMP Router Discovery Protocol (IRDP) client—the client runs an Internet Control Message Protocol (ICMP) router discovery client.

The drawback to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is cut off from the rest of the network.

VRRP can solve the static configuration problem. VRRP enables a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group. VRRP is supported on Ethernet, Fast Ethernet, BVI, and Gigabit Ethernet interfaces, and on MPLS VPNs, VRF-aware MPLS VPNs, and VLANs.

### VRRP Benefits

#### Redundancy

VRRP enables you to configure multiple routers as the default gateway router, which reduces the possibility of a single point of failure in a network.

#### Load Sharing

You can configure VRRP in such a way that traffic to and from LAN clients can be shared by multiple routers, thereby sharing the traffic load more equitably among available routers.



### Multiple Virtual Routers

VRRP supports up to 255 virtual routers (VRRP groups) on a router physical interface, subject to the platform supporting multiple MAC addresses. Multiple virtual router support enables you to implement redundancy and load sharing in your LAN topology.

### Multiple IP Addresses

The virtual router can manage multiple IP addresses, including secondary IP addresses. Therefore, if you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.

### Preemption

The redundancy scheme of VRRP enables you to preempt a virtual router backup that has taken over for a failing virtual router master with a higher priority virtual router backup that has become available.

### Authentication

VRRP message digest 5 (MD5) algorithm authentications protects against VRRP-spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security.

### Advertisement Protocol

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) for VRRP advertisements. This addressing scheme minimizes the number of routers that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA assigned VRRP the IP protocol number 112.

### VRRP Object Tracking

VRRP object tracking provides a way to ensure the best VRRP router is the virtual router master for the group by altering VRRP priorities to the status of tracked objects such as the interface or IP route states.

## HSRP

Most IP hosts have an IP address of a single router configured as the default gateway. When HSRP is used, the HSRP virtual IP address is configured as the host's default gateway instead of the IP address of the router.

HSRP is useful for hosts that do not support a router discovery protocol (such as ICMP Router Discovery Protocol [IRDP]) and cannot switch to a new router when their selected router reloads or loses power. Because existing TCP sessions can survive the failover, this protocol also provides a more transparent recovery for hosts that dynamically choose a next hop for routing IP traffic.

When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among a group of routers running HSRP. The address of this HSRP group is referred to as the virtual IP address. One of these devices is selected by the protocol to be the active

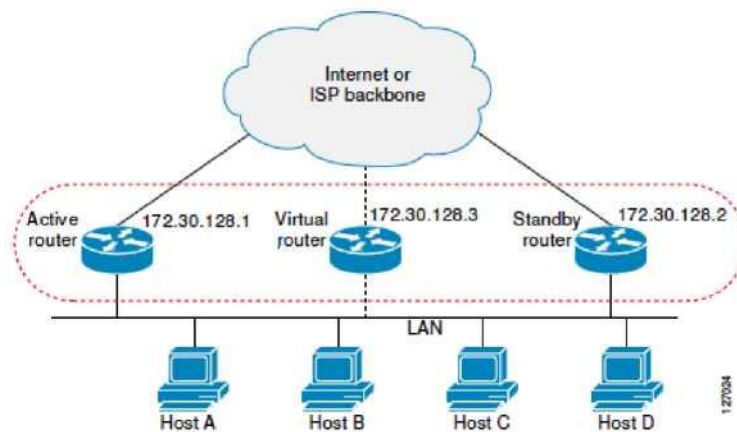
router. The active router receives and routes packets destined for the MAC address of the group. For  $n$  routers running HSRP,  $n + 1$  IP and MAC addresses are assigned.

HSRP detects when the designated active router fails, at which point a selected standby router assumes control of the MAC and IP addresses of the Hot Standby group. A new standby router is also selected at that time.

HSRP uses a priority mechanism to determine which HSRP configured router is to be the default active router. To configure a router as the active router, you assign it a priority that is higher than the priority of all the other HSRP-configured routers. The default priority is 100, so if you configure just one router to have a higher priority, that router will be the default active router. Devices that are running HSRP send and receive multicast UDP-based hello messages to detect router failure and to designate active and standby routers. When the active router fails to send a hello message within a configurable period of time, the standby router with the highest priority becomes the active router. The transition of packet forwarding functions between routers is completely transparent to all hosts on the network.

You can configure multiple Hot Standby groups on an interface, thereby making fuller use of redundant routers and load sharing.

The figure below shows a network configured for HSRP. By sharing a virtual MAC address and IP address, two or more routers can act as a single virtual router. The virtual router does not physically exist but represents the common default gateway for routers that are configured to provide backup to each other. You do not need to configure the hosts on the LAN with the IP address of the active router. Instead, you configure them with the IP address (virtual IP address) of the virtual router as their default gateway. If the active router fails to send a hello message within the configurable period of time, the standby router takes over and responds to the virtual addresses and becomes the active router, assuming the active router duties.



## GLBP

GLBP provides automatic router backup for IP hosts configured with a single default gateway on an IEEE 802.3 LAN. Multiple first-hop routers on the LAN combine to offer a single virtual first-hop IP router while sharing the IP packet forwarding load. Other routers on the LAN may act as redundant GLBP routers that will become active if any of the existing forwarding routers fail.

GLBP performs a similar function for the user as HSRP and VRRP. HSRP and VRRP allow multiple routers to participate in a virtual router group configured with a virtual IP address. One member is elected to be the active router to forward packets sent to the virtual IP address for the group. The other routers in the group are redundant until the active router fails. These standby routers have unused bandwidth that the protocol is not using. Although multiple virtual router groups can be configured for the same set of routers, the hosts must be configured for different default gateways, which result in an extra administrative burden.

The advantage of GLBP is that it additionally provides load balancing over multiple routers (gateways) using a single virtual IP address and multiple virtual MAC addresses. The forwarding load is shared among all routers in a GLBP group rather than being handled by a single router while the other routers stand idle. Each host is configured with the same virtual IP address, and all routers in the virtual router group participate in forwarding packets. GLBP members communicate between each other through hello messages sent every 3 seconds to the multicast address 224.0.0.102, UDP port 3222 (source and destination).

The Gateway Load Balancing Protocol feature provides automatic router backup for IP hosts configured with a single default gateway on an IEEE 802.3 LAN. Multiple first hop routers on the LAN combine to offer a single virtual first hop IP router while sharing the IP packet forwarding load. Other routers on the LAN may act as redundant GLBP routers that will become active if any of the existing forwarding routers fail.

GLBP performs a similar, but not identical, function for the user as the HSRP and the VRRP. HSRP and VRRP protocols allow multiple routers to participate in a virtual router group configured with a virtual IP address. One member is elected to be the active router to forward packets sent to the virtual IP address for the group. The other routers in the group are redundant until the active router fails. These standby routers have unused bandwidth that the protocol is not using. Although multiple virtual router groups can be configured for the same set of routers, the hosts must be configured for different default gateways, which results in an extra administrative burden. GLBP provides load balancing over multiple routers (gateways) using a single virtual IP address and multiple virtual MAC addresses. Each host is configured with the same virtual IP address, and all routers in the virtual router group participate in forwarding packets. GLBP members communicate between each other through hello messages sent every 3 seconds to the multicast address 224.0.0.102, User Datagram Protocol (UDP) port 3222 (source and destination).

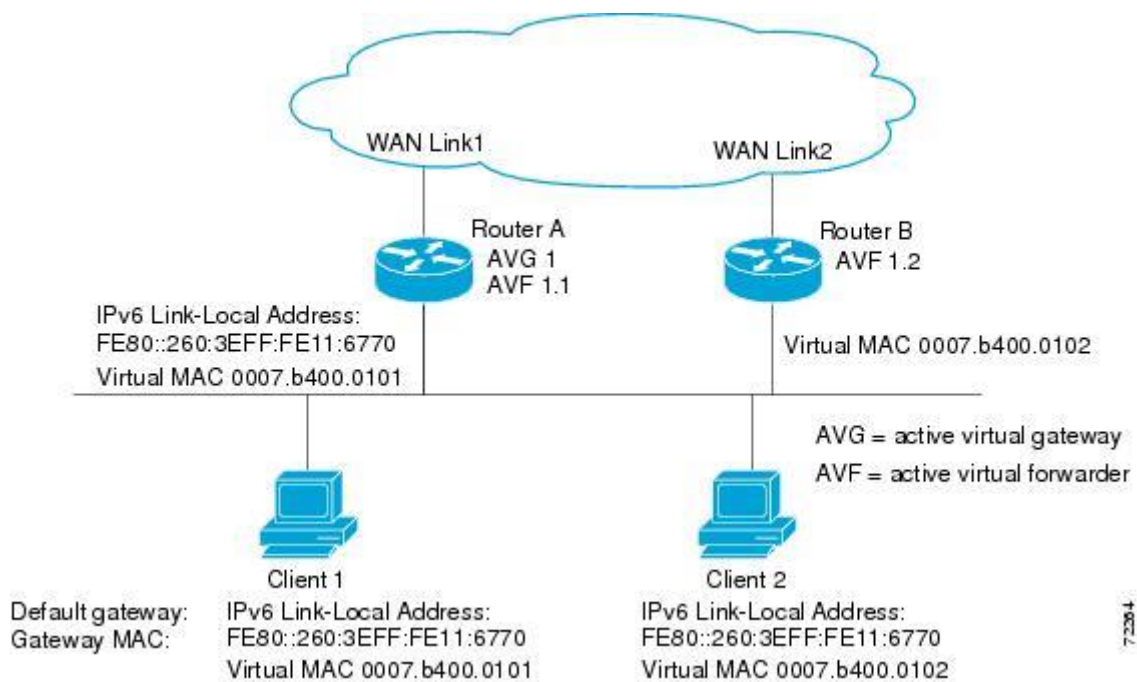
### GLBP Active Virtual Gateway

Members of a GLBP group elect one gateway to be the active virtual gateway (AVG) for that group. Other group members provide backup for the AVG in the event that the AVG becomes unavailable. The AVG assigns a virtual MAC address to each member of the GLBP group. Each gateway assumes responsibility for forwarding packets sent to the virtual MAC address assigned to it by the AVG. These gateways are known as active virtual forwarders (AVFs) for their virtual MAC address.

The AVG is responsible for answering Address Resolution Protocol (ARP) requests for the virtual IP address. Load sharing is achieved by the AVG replying to the ARP requests with different virtual MAC addresses.

In [Figure 1](#), Router A is the AVG for a GLBP group, and is responsible for the virtual IP address 10.21.8.10. Router A is also an AVF for the virtual MAC address 0007.b400.0101. Router B is a member of the same GLBP group and is designated as the AVF for the virtual MAC address 0007.b400.0102. Client 1 has a default gateway IP address of 10.21.8.10 and a gateway MAC address of 0007.b400.0101. Client 2 shares the same default gateway IP address but receives the gateway MAC address 0007.b400.0102 because Router B is sharing the traffic load with Router A.

### Figure 1 GLBP Topology



If Router A becomes unavailable, Client 1 will not lose access to the WAN because Router B will assume responsibility for forwarding packets sent to the virtual MAC address of Router A, and for responding to packets sent to its own virtual MAC address. Router B will also assume the role of the AVG for the entire GLBP group. Communication for the GLBP members continues despite the failure of a router in the GLBP group.

### GLBP Virtual MAC Address Assignment

A GLBP group allows up to four virtual MAC addresses per group. The AVG is responsible for assigning the virtual MAC addresses to each member of the group. Other group members request a virtual MAC address after they discover the AVG through hello messages. Gateways are assigned the next MAC address in sequence. A virtual forwarder that is assigned a virtual MAC address by the AVG is known as a primary virtual forwarder. Other members of the GLBP group learn the virtual MAC addresses from hello messages. A virtual forwarder that has learned the virtual MAC address is referred to as a secondary virtual forwarder.

### GLBP Virtual Gateway Redundancy

GLBP operates virtual gateway redundancy in the same way as HSRP. One gateway is elected as the AVG, another gateway is elected as the standby virtual gateway, and the remaining gateways are placed in a listen state.

If an AVG fails, the standby virtual gateway will assume responsibility for the virtual IP address. A new standby virtual gateway is then elected from the gateways in the listen state.

## GLBP Virtual Forwarder Redundancy

Virtual forwarder redundancy is similar to virtual gateway redundancy with an AVF. If the AVF fails, one of the secondary virtual forwarders in the listen state assumes responsibility for the virtual MAC address.

The new AVF is also a primary virtual forwarder for a different forwarder number. GLBP migrates hosts away from the old forwarder number using two timers that start as soon as the gateway changes to the active virtual forwarder state. GLBP uses the hello messages to communicate the current state of the timers.

The redirect time is the interval during which the AVG continues to redirect hosts to the old virtual forwarder MAC address. When the redirect time expires, the AVG stops redirecting hosts to the virtual forwarder, although the virtual forwarder will continue to forward packets that were sent to the old virtual forwarder MAC address.

The secondary hold time is the interval during which the virtual forwarder is valid. When the secondary hold time expires, the virtual forwarder is removed from all gateways in the GLBP group. The expired virtual forwarder number becomes eligible for reassignment by the AVG.

## GLBP Gateway Priority

GLBP gateway priority determines the role that each GLBP gateway plays and what happens if the AVG fails.

Priority also determines if a GLBP router functions as a backup virtual gateway and the order of ascendancy to becoming an AVG if the current AVG fails. You can configure the priority of each backup virtual gateway with a value of 1 through 255 using the **glbp priority** command.

In [Figure 1](#), if Router A, the AVG in a LAN topology, fails, an election process takes place to determine which backup virtual gateway should take over. In this example, Router B is the only other member in the group so it will automatically become the new AVG. If another router existed in the same GLBP group with a higher priority, then the router with the highest priority would be elected. If both routers have the same priority, the backup virtual gateway with the higher IP address would be elected to become the active virtual gateway.

By default, the GLBP gateway preemptive scheme is disabled. A backup virtual gateway can become the AVG only if the current AVG fails, regardless of the priorities assigned to the virtual gateways. You can enable the GLBP preemptive scheme using the **glbp preempt** command.

Preemption allows a backup virtual gateway to become the AVG, if the backup virtual gateway is assigned a higher priority than the current AVG.



## GLBP Gateway Weighting and Tracking

GLBP uses a weighting scheme to determine the forwarding capacity of each router in the GLBP group. The weighting assigned to a router in the GLBP group determines whether it will forward packets and, if so, the proportion of hosts in the LAN for which it will forward packets. Thresholds can be set to disable forwarding when the weighting falls below a certain value, and when it rises above another threshold, forwarding is automatically reenabled.

The GLBP group weighting can be automatically adjusted by tracking the state of an interface within the router. If a tracked interface goes down, the GLBP group weighting is reduced by a specified value. Different interfaces can be tracked to decrement the GLBP weighting by varying amounts.

### Types of GLBP load Balancing Mechanism.

There are **two load-balancing mechanism** that is used with GLBP. These including

1. **Round-robin:** The default one. Each AVF in turn is included in address resolution replies for the virtual IP address.
  2. **Host-dependent:** Based on the MAC address of a host where the same forwarder is always used for a particular host.
- **Weighted:** Based on weight dependent share of user between routers.

### GLBP Benefits

#### Load Sharing

You can configure GLBP in such a way that traffic from LAN clients can be shared by multiple routers, thereby sharing the traffic load more equitably among available routers.

#### Multiple Virtual Routers

GLBP supports up to 1024 virtual routers (GLBP groups) on each physical interface of a router, and up to 4 virtual forwarders per group.

#### Preemption

The redundancy scheme of GLBP enables you to preempt an active virtual gateway with a higher priority backup virtual gateway that has become available. Forwarder preemption works in a similar way, except that

forwarder preemption uses weighting instead of priority and is enabled by default.

### **Authentication**

You can use a simple text password authentication scheme between GLBP group members to detect configuration errors. A router within a GLBP group with a different authentication string than other routers will be ignored by other group members.

## 3.7 Servers

---

### **Domain controller vs. workgroup**

#### **Applies to Windows 7**

Domains and workgroups represent different methods for organizing computers in networks. The main difference among them is how the computers and other resources on the networks are managed. Computers running Windows on a network must be part of a workgroup or a domain. Computers on home networks are usually part of a workgroup and computers on workplace networks are usually part of a domain.

#### **In a workgroup:**

- All computers are peers; no computer has control over another computer.



- Each computer has a set of user accounts. To log on to any computer in the workgroup, you must have an account on that computer.
- There are typically no more than twenty computers.
- A workgroup is not protected by a password.
- All computers must be on the same local network or subnet.

### **In a domain:**

- One or more computers are servers. Network administrators use servers to control the security and permissions for all computers on the domain. This makes it easy to make changes because the changes are automatically made to all computers. Domain users must provide a password or other credentials each time they access the domain.
- If you have a user account on the domain, you can log on to any computer on the domain without needing an account on that computer.
- You probably can make only limited changes to a computer's settings because network administrators often want to ensure consistency among computers.
- There can be thousands of computers in a domain.
- The computers can be on different local networks.

### **Distributed File System (DFS):**

A distributed file system is a client/server-based application that allows clients to access and process data stored on the server as if it were on their own computer. When a user accesses a file on the server, the server sends the user a copy of the file, which is cached on the user's computer while the data is being processed and is then returned to the server. Ideally, a distributed file system organizes file and directory services of individual servers into a global directory in such a way that remote data access is not location-specific but is identical from any client. All files are accessible to all users of the global file system and organization is hierarchical and directory-based.

Since more than one client may access the same data simultaneously, the server must have a mechanism in place (such as maintaining information about the times of access) to organize updates so that the client always receives the most current version of data and that data conflicts do not arise. Distributed file systems typically use file or database replication (distributing copies of data on multiple servers) to protect against data access failures.

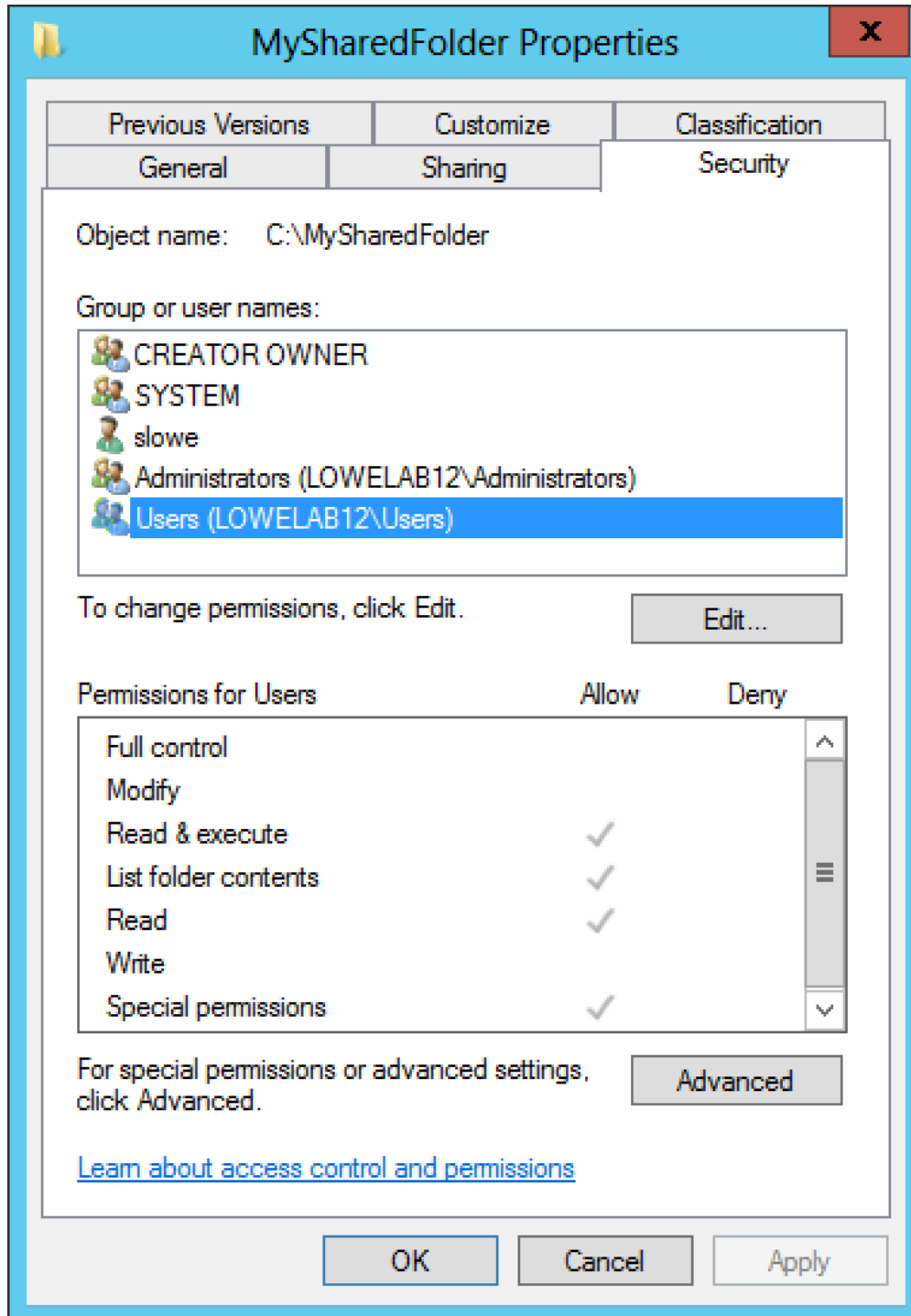
## **File Sharing and security:**

If you're an old hand when it comes to NTFS permissions, you'll find that not too much has changed with regard to permissions themselves in Windows Server 2012. However, with a new interface comes slightly different ways to accomplish familiar tasks. In this post, I'll describe the ins and outs of NTFS permissions in Windows Server 2012

If you're new to NTFS permissions, this article will be of use to you, too. You'll learn about the tricks that make NTFS permissions work the way they do.

First, let's take a look at the Security tab of a folder on my lab server. To get to this page, simply right-click a folder and, from the shortcut menu, choose Properties. Next, choose the Security tab and you will see a screen like the one shown in **Figure A**.

*Figure A*



The Security tab

On this tab, you can see that there are a number of different permissions available for the selected user. Any changes you make will apply only to the selected user. If you want to make changes to multiple users, either add the user to a group and then apply permissions to the group or individually apply permissions to individual users one by one.

## Permissions explained

I'll start with an explanation for what each permission means. Bear in mind that permissions can be set at both the folder and the file level. The table below outlines what each permission does for both folders and files.

Permission name	Description (folder)	Description (file)
Full control	The user has full control to the folder and can add, change, move and delete items. <i>The user can also add and remove permissions on the folder as well as for any subfolders.</i> The italicized sentence is very important to keep in mind. This permission level can be dangerous in the wrong hands.	The user has full control to the file and can change, move or delete it. <i>The user can also add and remove permissions on the file.</i>
Modify	A combination of Read and Write permissions. A user also has the ability to delete files within a folder that has the Modify permission. She can also view the contents of subfolders.	A user is able to modify the contents of the selected file.
Read & execute	Users are allowed to read the contents of files in the folder or execute programs inside the folder.	Users are allowed to read the contents of the file or execute the program.
List folder contents	Allows the user to view the contents of the selected folder. The user is not allowed to read a file's contents or execute a file.	This permission is not available at the file level

Read	The user can read the contents of a folder.	The user can read the contents of a file.
Write	A user can create files and folders. This does not grant a user with the ability to read any existing information.	A user can create a file.

You will note that the permissions screen has both Allow and Deny columns. You are able to allow a user a particular set of rights or deny a user access rights to a particular file or folder.

As you create groups for permissions reasons, understand that the permissions that you assign are cumulative. So, perhaps you grant a user's account rights to read/execute the contents of a folder and you grant a group to which the user belongs the ability to write to a folder. The user will get all of those permissions because NTFS rights are cumulative.

When Deny permissions are involved, they *always override Allow permissions*. It's not considered a best practice to use Deny permissions a whole lot. Doing so can create administrative nightmares that are difficult to solve. That said, Deny can be useful when group permissions have been applied to a folder, but you still want a user in that group to be denied access to the folder.

### **Security issues (file replications):**

Enables you to efficiently replicate folders (including those referred to by a DFS namespace path) across multiple servers and sites. DFS Replication uses a compression algorithm known as remote differential compression (RDC). RDC detects changes to the data in a file, and it enables DFS Replication to replicate only the changed file blocks instead of the entire file.

# Chapter 4

## System Analysis

- **Over View**
- **System Requirement**
- **USE CASE Diagram**
- **Scenario**

## 4.1 Over View

---

This chapter presents the analysis phase of the application. In this phase, the system requirements are discussed in order to fulfill the features and objectives previously mentioned in Chapter 1. These requirements are translated to users' interactions in use cases.

## 4.2 System Requirement

---

Our project needs a smart phone, which has high resources can be exploited to accomplish many of the tasks. Project represent secured communication between departments. The requirements that the system must satisfy are two types, which are the functional and non-functional requirements. Functional requirements describe what a software system should do. Non-functional requirements place constraints on how the system will do so. In the following subsections, both functional and non-functional requirements of the proposed system are listed.

### 4.2.1 Functional Requirements

In software engineering, a functional requirement defines a function of a software system or its component. A function is described as a set of inputs, the behavior, and outputs. Functional requirements may be calculations, technical details, data manipulation and processing and other specific functionality that define what a system is supposed to accomplish. Behavioral requirements describing all the cases where the system uses the functional requirements are captured in use cases.

**The following requirements were established for DUND Server:**

1. Machine must join in to domain controller.
2. Domain controller make or manage accounts for user.
3. Domain controller link between two file servers.

4. Make file distributions and file permissions on file servers.

**The following requirements were established for DUND Client:**

1. User takes account from domain controller.
2. Provide IP address for every machine
3. User login into the system.
4. User access his files with his permission.

## 4.2.2 NON-Functional Requirements

In systems engineering and [requirements engineering](#), a non-functional requirement is a [requirement](#) that specifies criteria that can be used to judge the operation of a system, rather than specific behaviors. This should be contrasted with [functional requirements](#) that define specific behavior or functions. The plan for implementing functional requirements is detailed in the [system design](#). The plan for implementing non-functional requirements is detailed in the [system architecture](#).

Broadly, functional requirements define what a system is supposed to do and non-functional requirements define how a system is supposed to be. Functional requirements are usually in the form of "system shall do requirement.

Non-functional requirements are often called qualities of a system. Other terms for non-functional requirements are "constraints", "quality attributes", "quality goals", "quality of service requirements" and "non-behavioral requirements". Informally these are sometimes called the "ilities", from attributes like stability and portability. Qualities, that are non-functional requirements, can be divided into two main categories:

1. Execution qualities, such as security and usability, which are observable at run time.
2. Evolution qualities, such as [testability](#), maintainability, extensibility and scalability, which are embodied in the static structure of the software system.

**Nonfunctional requirements that “DUND” requires:**



**Reliability:** Presents the ability of a user to perform and maintain system functions in routine circumstances, as well as unexpected circumstances.

**Accessibility:** The system should be easy to access. Enables to use the system easily and effectively.

**Availability:** The system should be in a specified operable and committable state at the start of a mission. This achieved by:-

- **DUND** is available for any one in local network.
- The system is available can be accessed easily and quickly any time with account and permission.

**Documentation:** is a set of documents provided on paper.

**Security:** The system should be able to protect the data on servers. This achieved by:-

- The system is secured by file distributions, replications and permissions.
- Clients should enter specific account and IP of server (given by server) that able only them to join domain.

**Performance:** DUND Provides high performance by load balancing on routers and link aggregations and backup for routers and switches, replications on servers.

## 4.3 USE CASE Diagram

A use case diagram at its simplest is a representation of a user's interaction with the system and depicting the specifications of a use case. A use case diagram can portray the different types of users of a system and the various ways that they interact with the system (which are a collection of actors and processes). This type of diagram is typically used in conjunction with the textual use case and will often be accompanied by other types of diagrams as well. The use case analysis is the foundation upon which the system will be built.

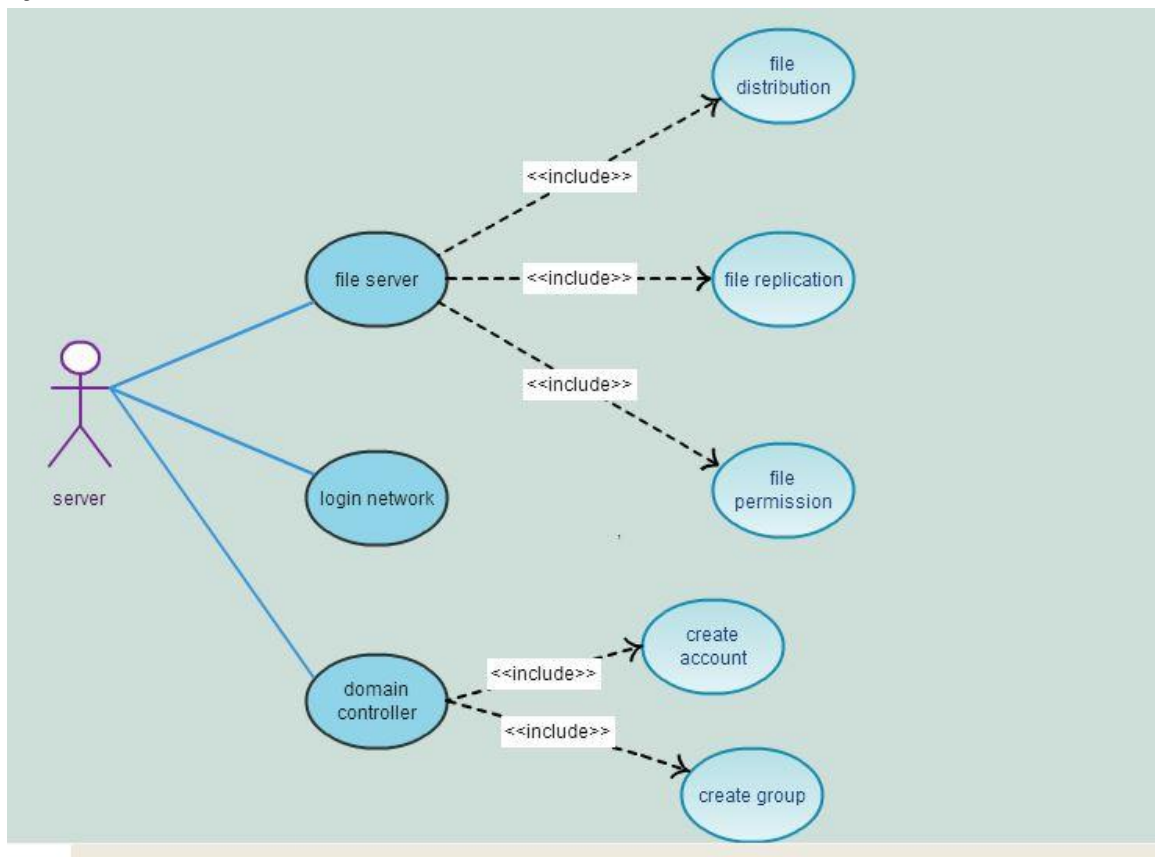


Figure 4.1

### User Server Use Cases:

**Log in to network:** This use case starts when server decides to connect with network.

**Domain controller:** This use case starts when the server manage users and accounts and can link between two file servers.

**File server:** This use case starts when the server make file replications, permissions and distributions.

Figure 4.2 presents the use case diagram of client

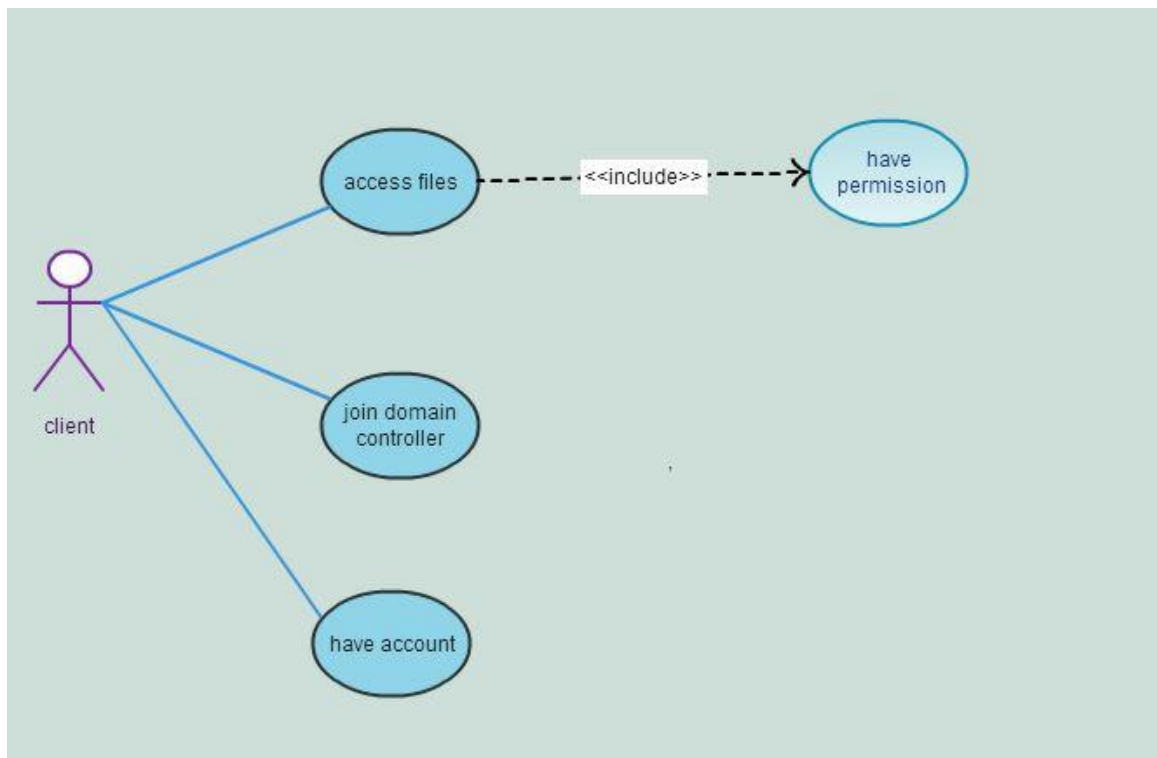


Figure 4.2

### User Client Use Cases:

**Access files:** This use case shows that client have permission on files.

**Join domain controller:** This use case that make join to domain.

**Have account:** This use case take account for each user from domain controller.

## 4.4 Scenario

---

Use Case Name:	Open System. .5	
Actor(s):	User and server	
Description	This use case describes the steps of interacting user with the system.	
Typical Course of Events:	Actor Action	System Response
	<p><u>Step1</u>: This use case initiated when the user wants to interacts with system.</p> <p><u>Step2</u>: machine must have IP address.</p> <p><u>Step3</u>: The user joins to domain.</p> <p><u>Step4</u>: The user open system with his user account.</p> <p><u>Step6</u>: The user uses files with his permission.</p>	<p><u>Step5</u>: Show files</p>
Preconditions:	User must connect to a local network.	

# Chapter 5

## System Design

- **Over View**
- **Process Modules**

## 5.1 Overview

---

After completing analysis phase, which is discussed in previous chapter, the design phase was started. Therefore, this chapter focuses on design phase. Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering.

## 5.2 Process Modeling

---

After describing the proposed system architecture and its main components, the processes of the proposed system needed to be modeled and described. In this section, a closer look to system process is provided through class diagram and sequence diagrams.

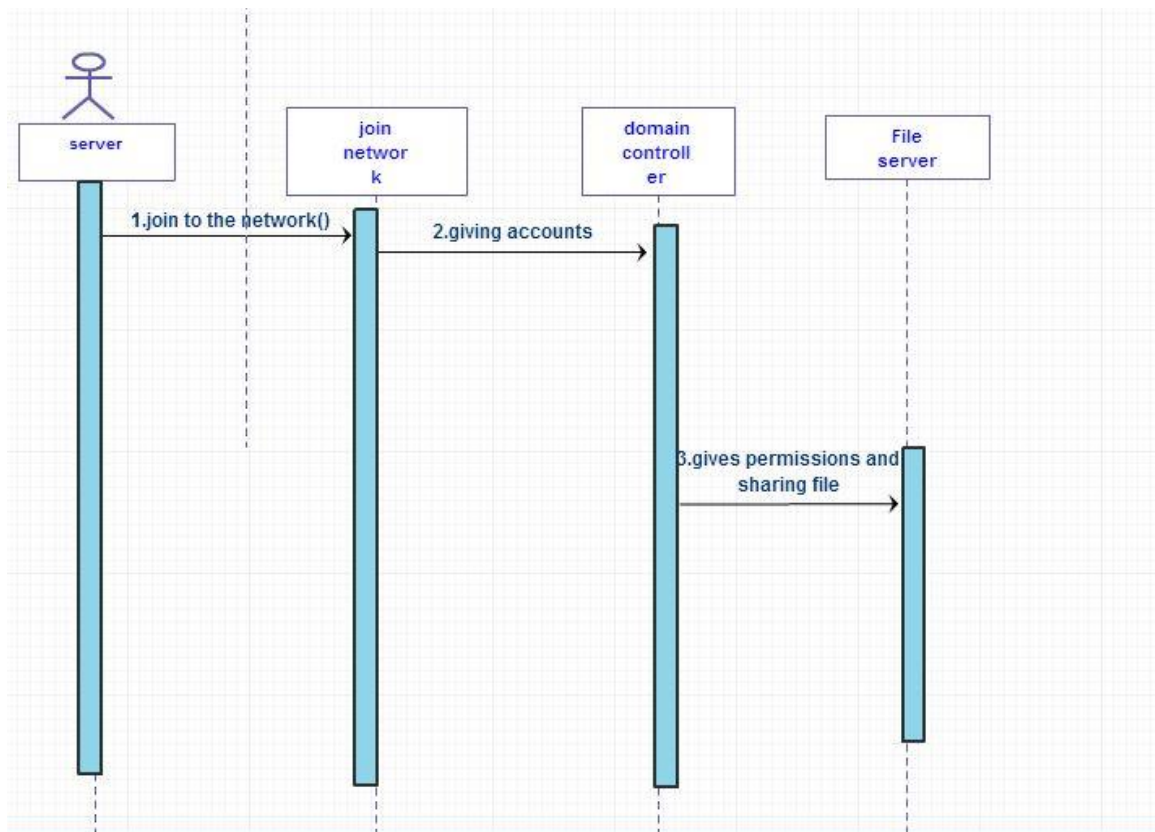
### 5.2.1 Sequence Diagram

Sequence diagram, in the context of UML, represents object collaboration and is used to define event sequences between objects for a certain outcome. A sequence diagram is also known as a timing diagram, event diagram and event scenario.

Sequence diagram is the most common kind of interaction diagram, which focuses on the message interchange between a numbers of lifelines.

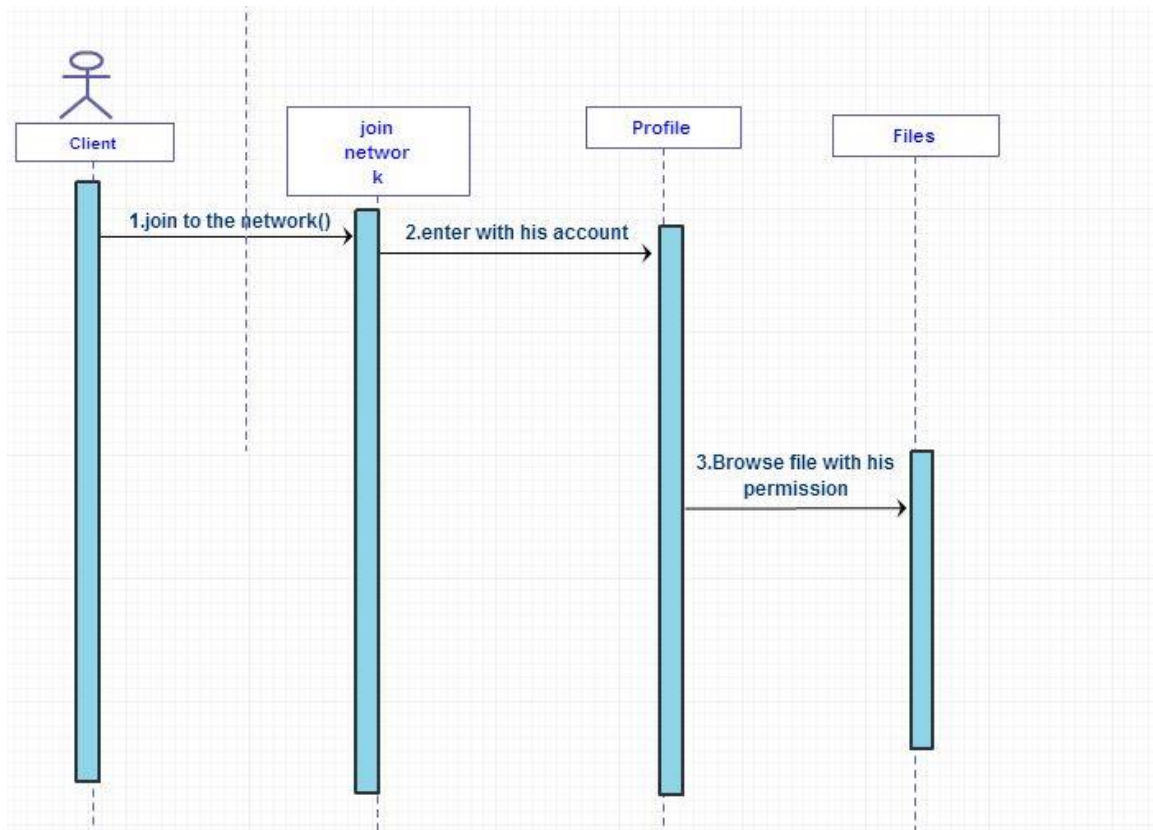
Sequence diagram describes an interaction by focusing on the sequence of messages that are exchanged, along with their corresponding occurrence specifications on the lifeline.

## Sequence diagram of Server



**Figure 5.1 Sequence Diagram**

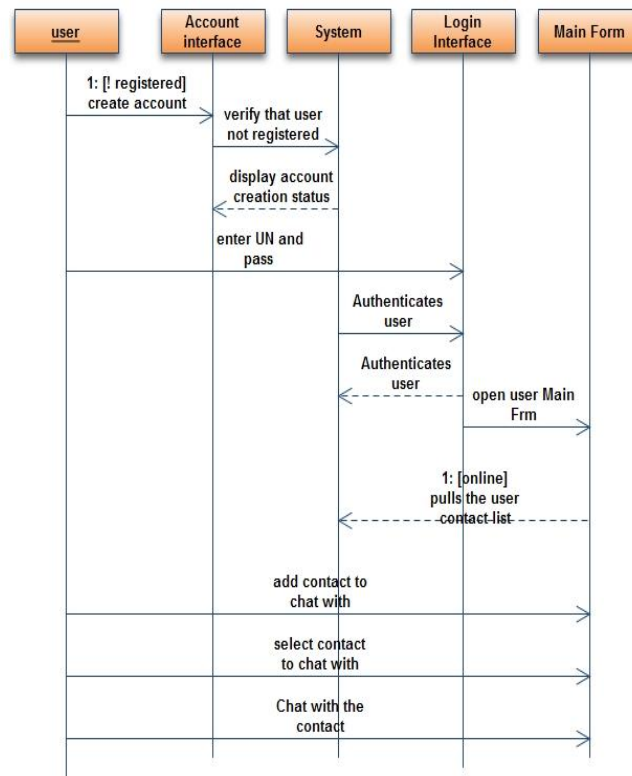
## Sequence diagram of client



**Figure 5.2 Sequence Diagram**

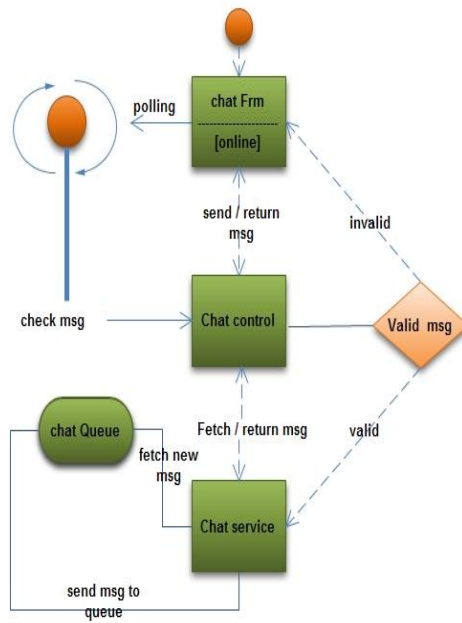


## Sequence diagram of chat



**Figure 5.3 Sequence Diagram**

## Activity Diagram of Chat



**Figure 5.4 Activity Diagram**

# Chapter 6

## Implementation

### Implementation

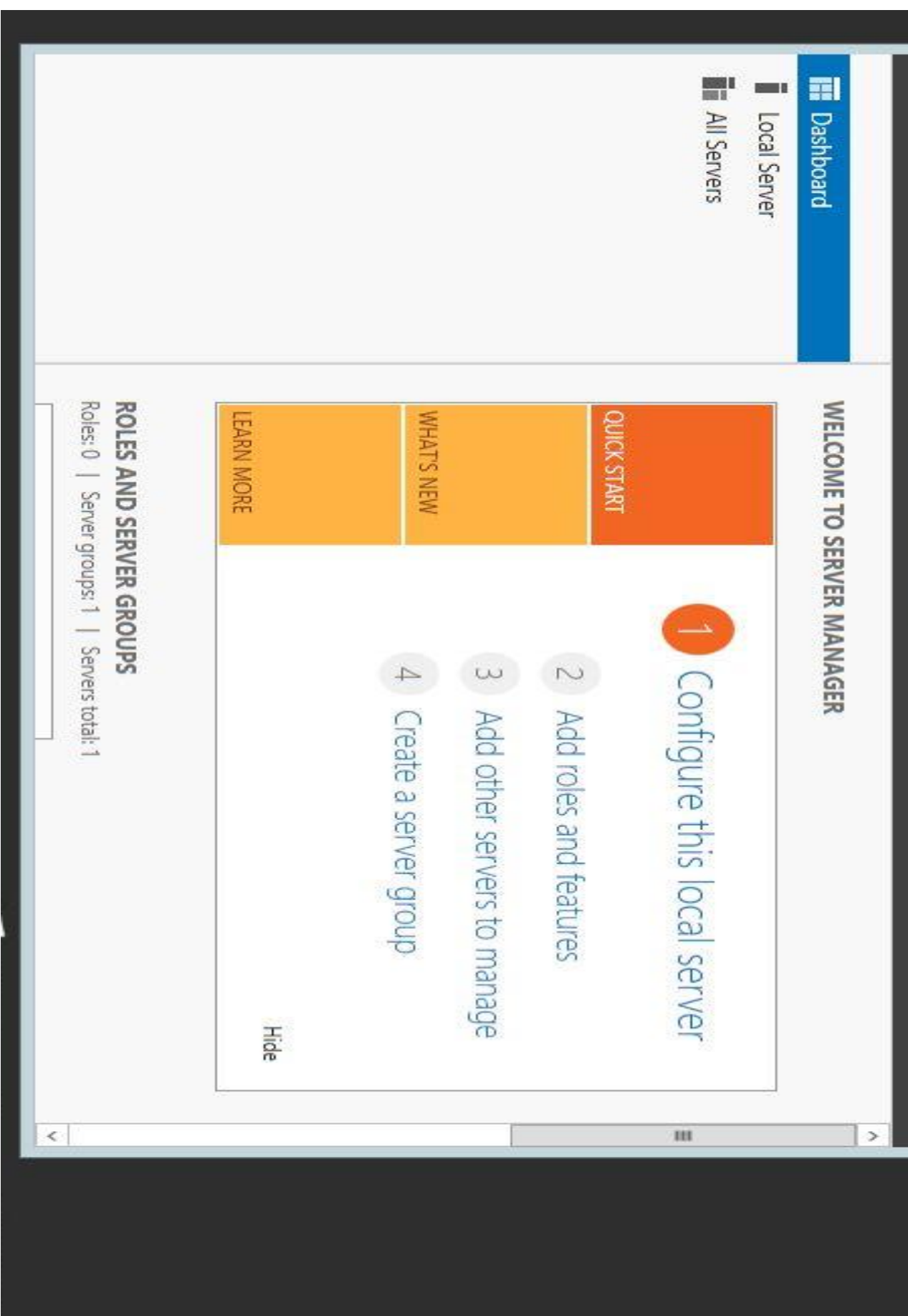
---

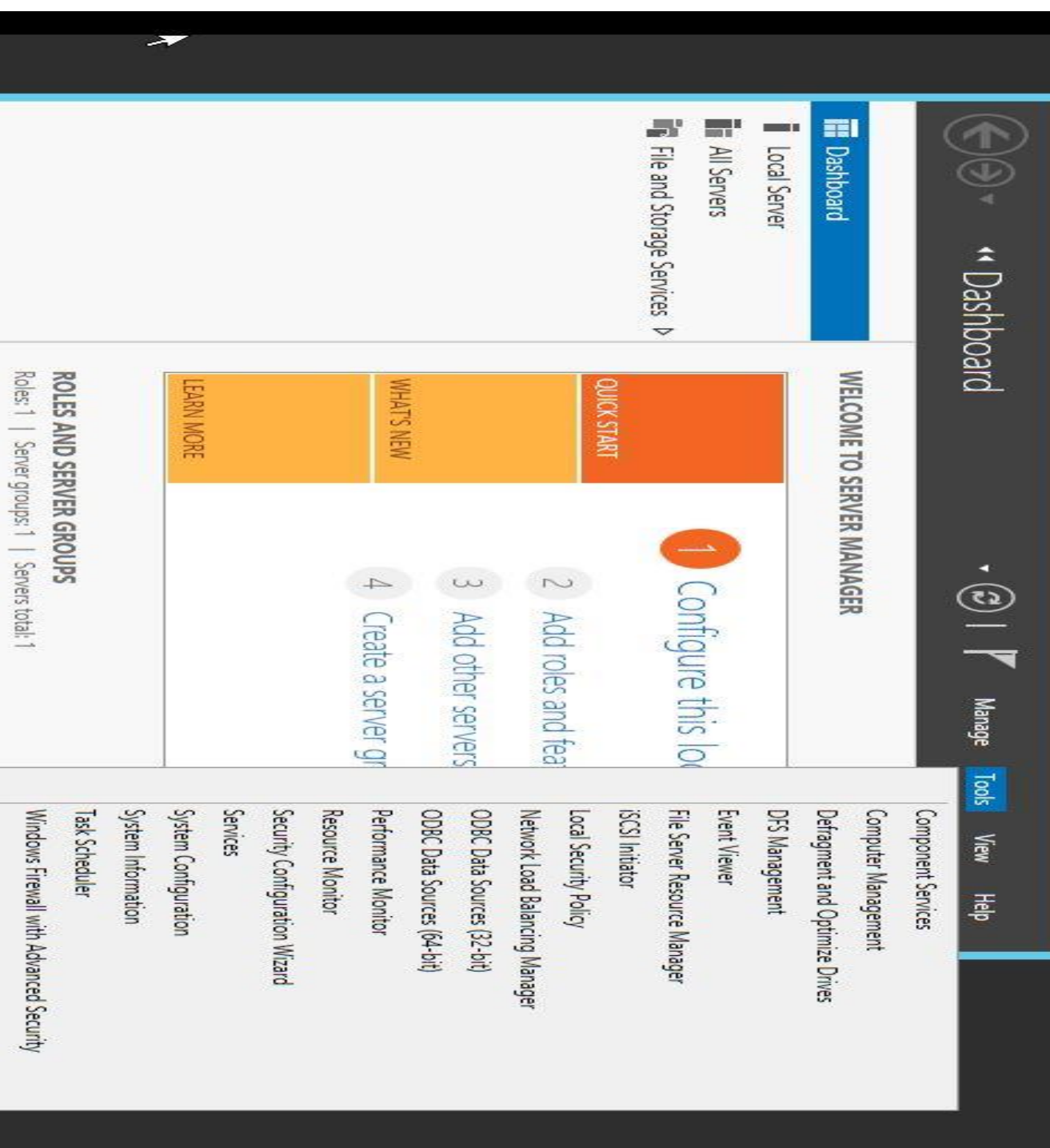
#### Overview:

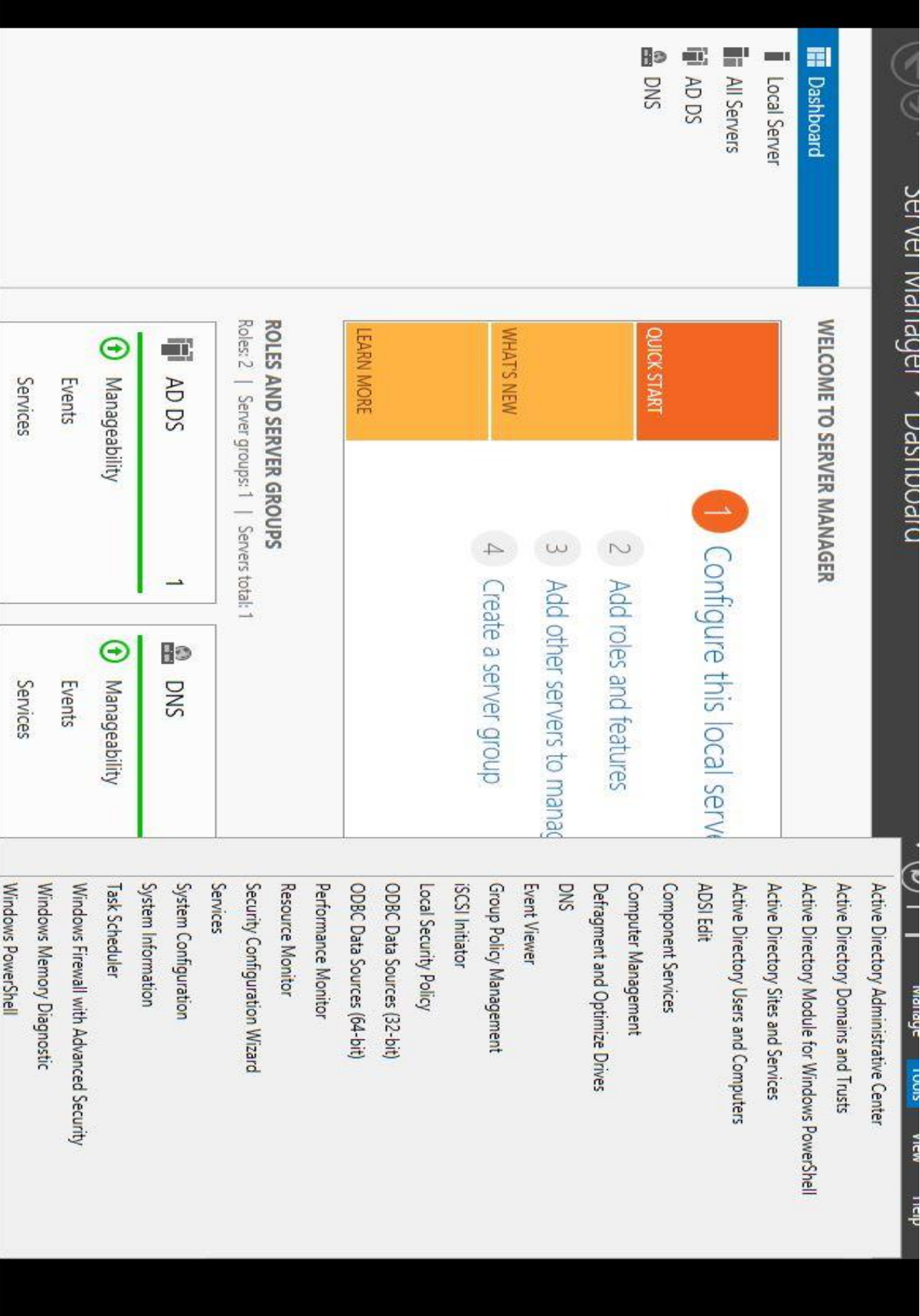
- **Overview**
- **Implementation**
  - **Server**
  - **Network**
  - **Chatting**

In computer science, an implementation is a realization of a technical specification or algorithm as a program, software component, or other computer system through computer programming and deployment. Many implementations may exist for a given specification or standard. For example, web browsers contain implementations of World Wide Web Consortium-recommended specifications, and software development tools contain implementations of programming languages.

## 1. Servers







Dashboard

Local Se

All Serv

AD DS

DNS

File and

File

Action

View

Help

Active Directory Users and Computers

-

□

X

Active Directory Users and Computers

Active Directory Users and Computers

Saved Queries

Fci.edu

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipals

Managed Service Accounts

Server-it

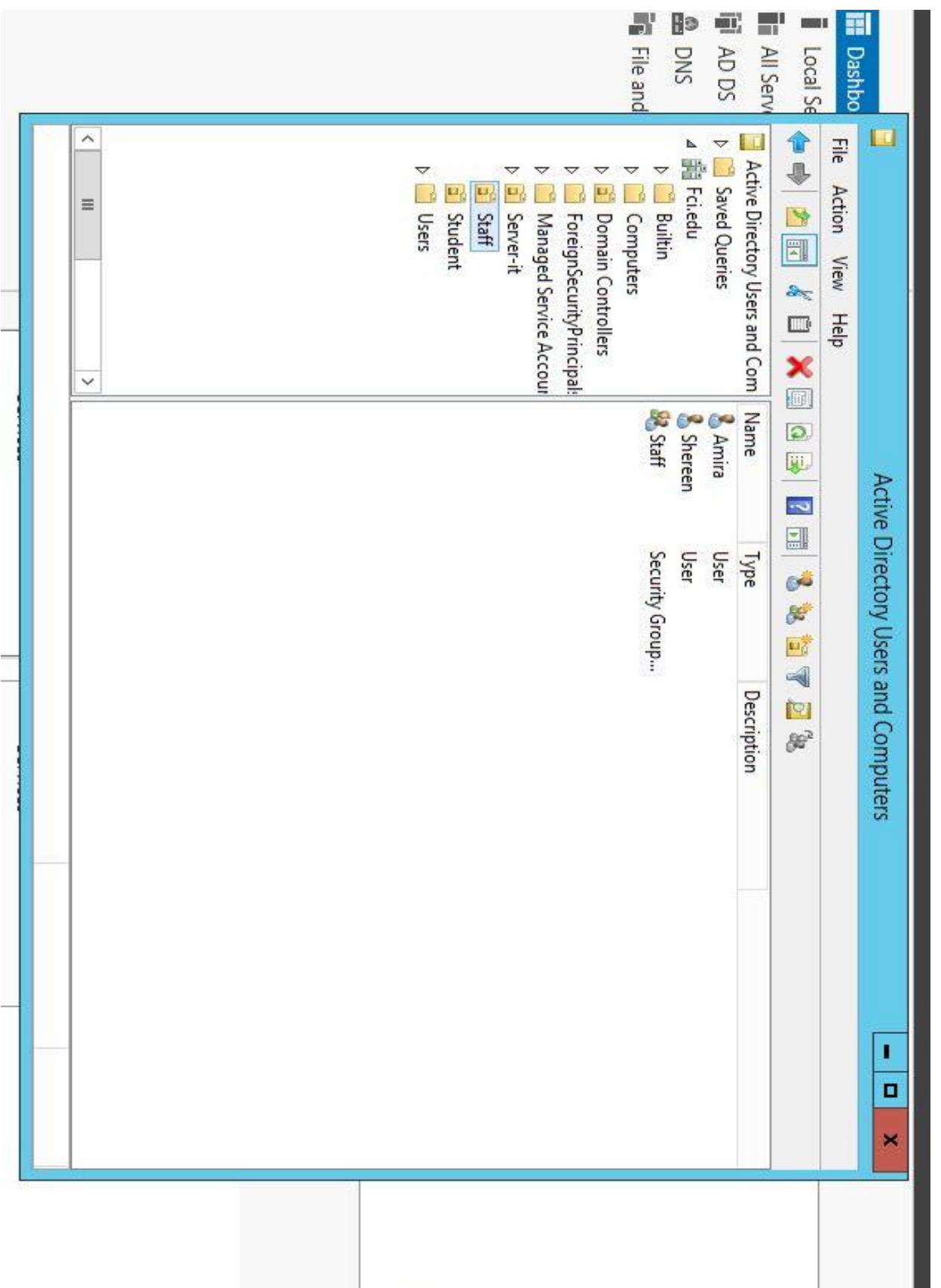
Staff

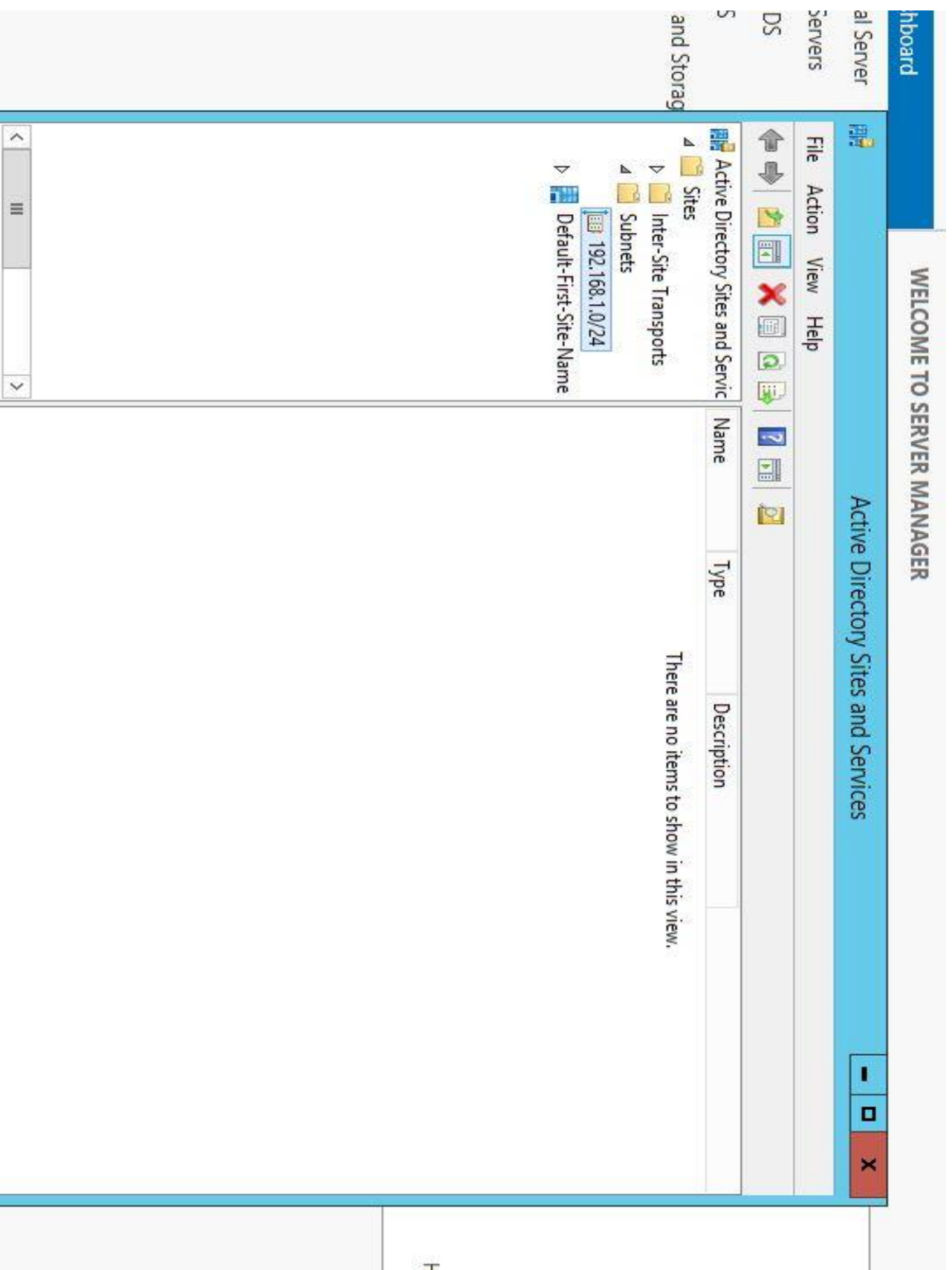
Student

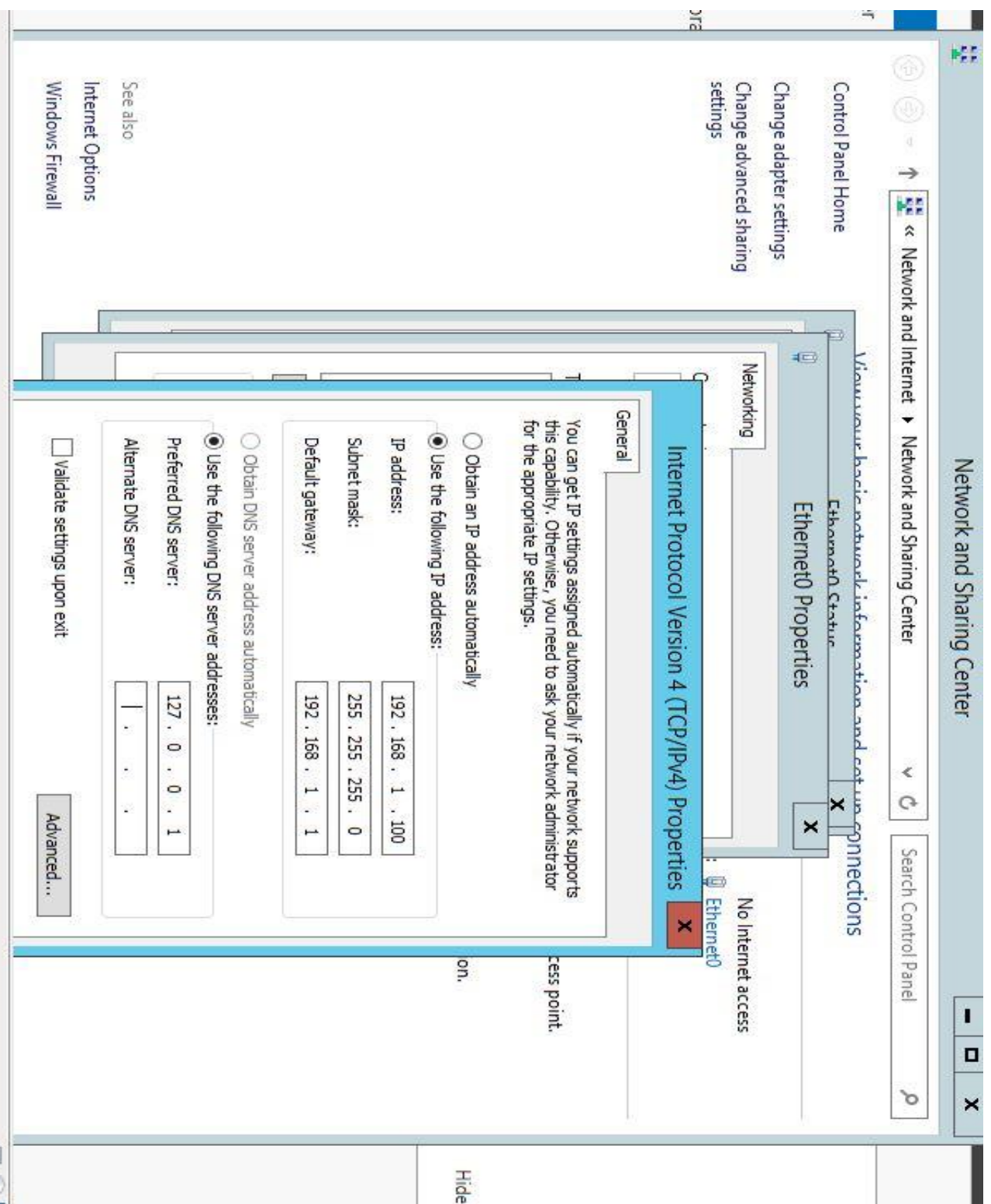
Users

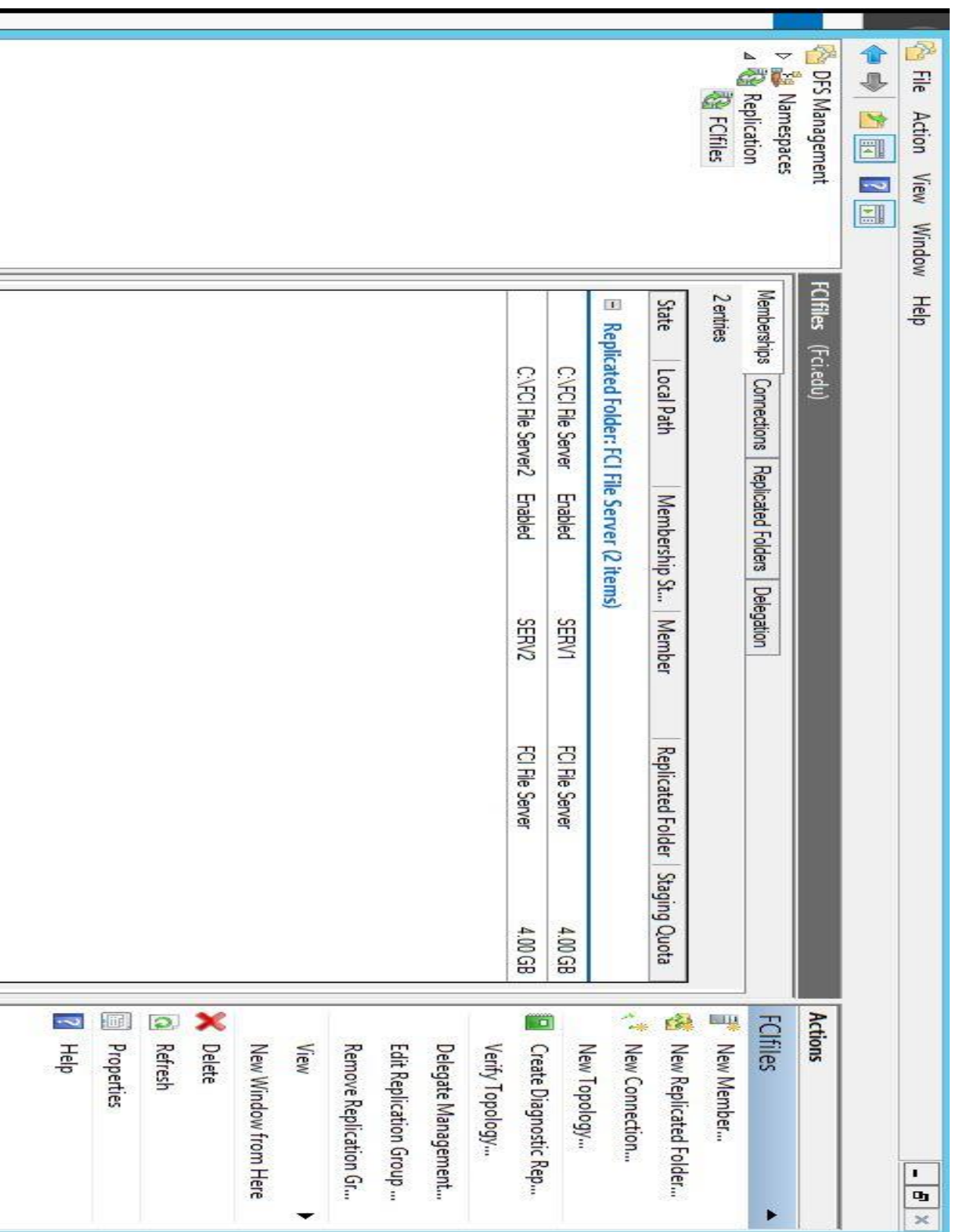
Name	Type	Description
Ahmed	User	
Mahmoud	User	
Student	Security Group...	











Dashboard

Local Server

All Servers

File and Storage Se

WELCOME TO SERVER MANAGER

FileClusterHostOptionsHelp

Network Load Balancing Manager

-

□

X

Network Load Balancing Clusters

(192.168.1.20)

SERV1(Ethernet0)

SERV2(Ethernet0)

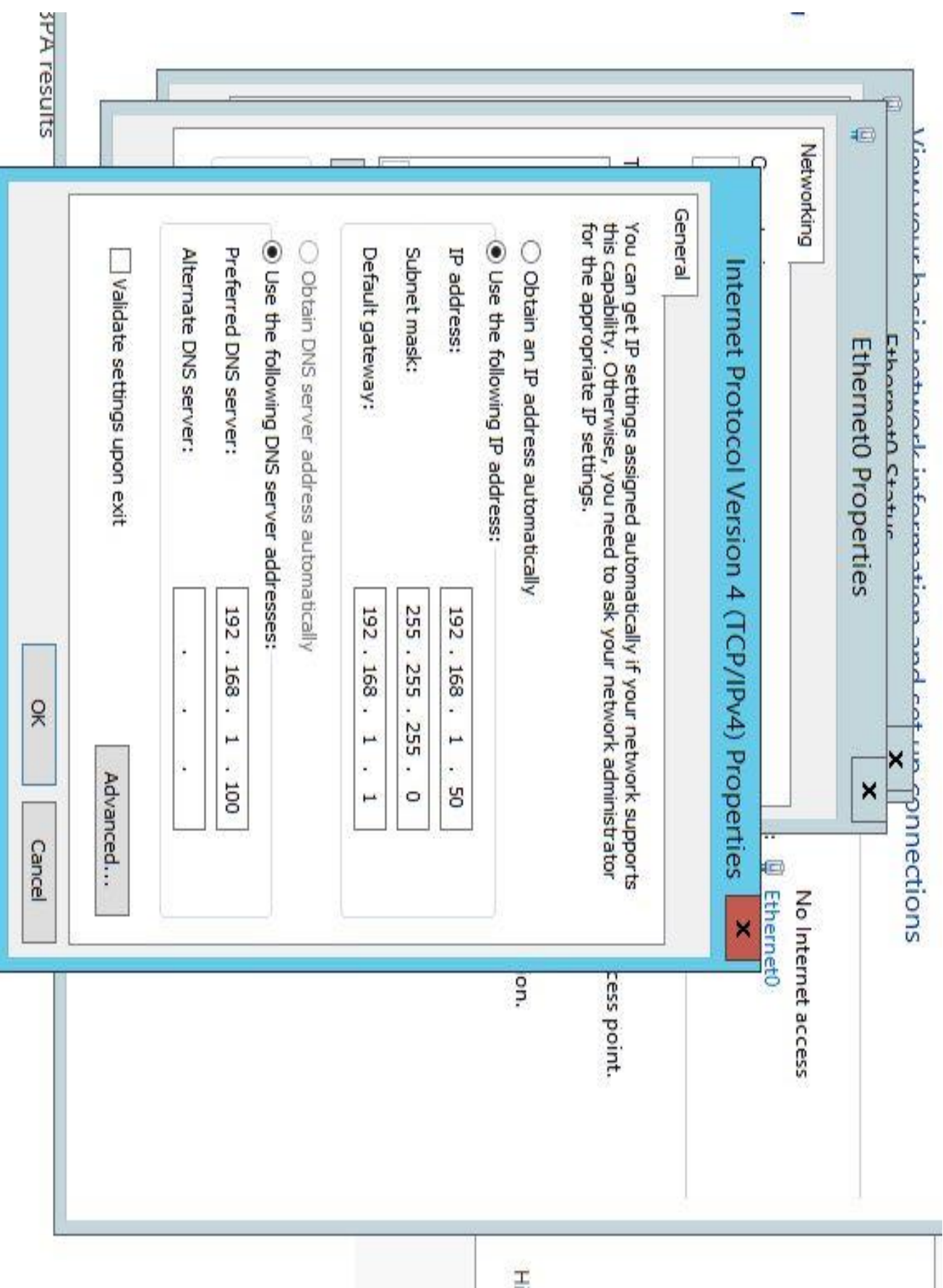
Host configuration information for hosts in cluster (192.168.1.20)

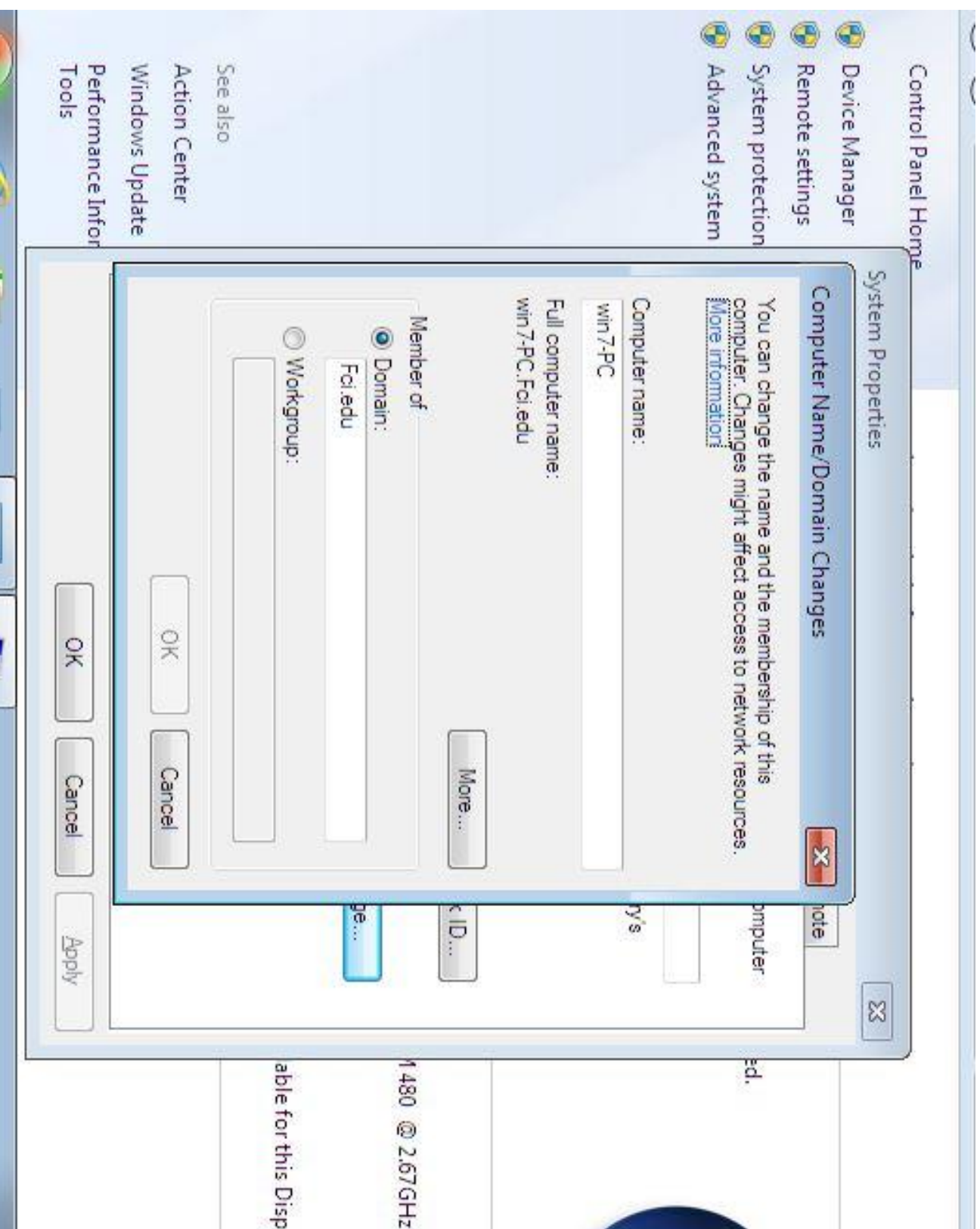
Host (Interface)	Status	Dedicated IP address	Dedicated IP subnet n
SERV1(Ethernet0)	Converged	192.168.1.50	255.255.255.0
SERV2(Ethernet0)	Converged	192.168.1.40	255.255.255.0

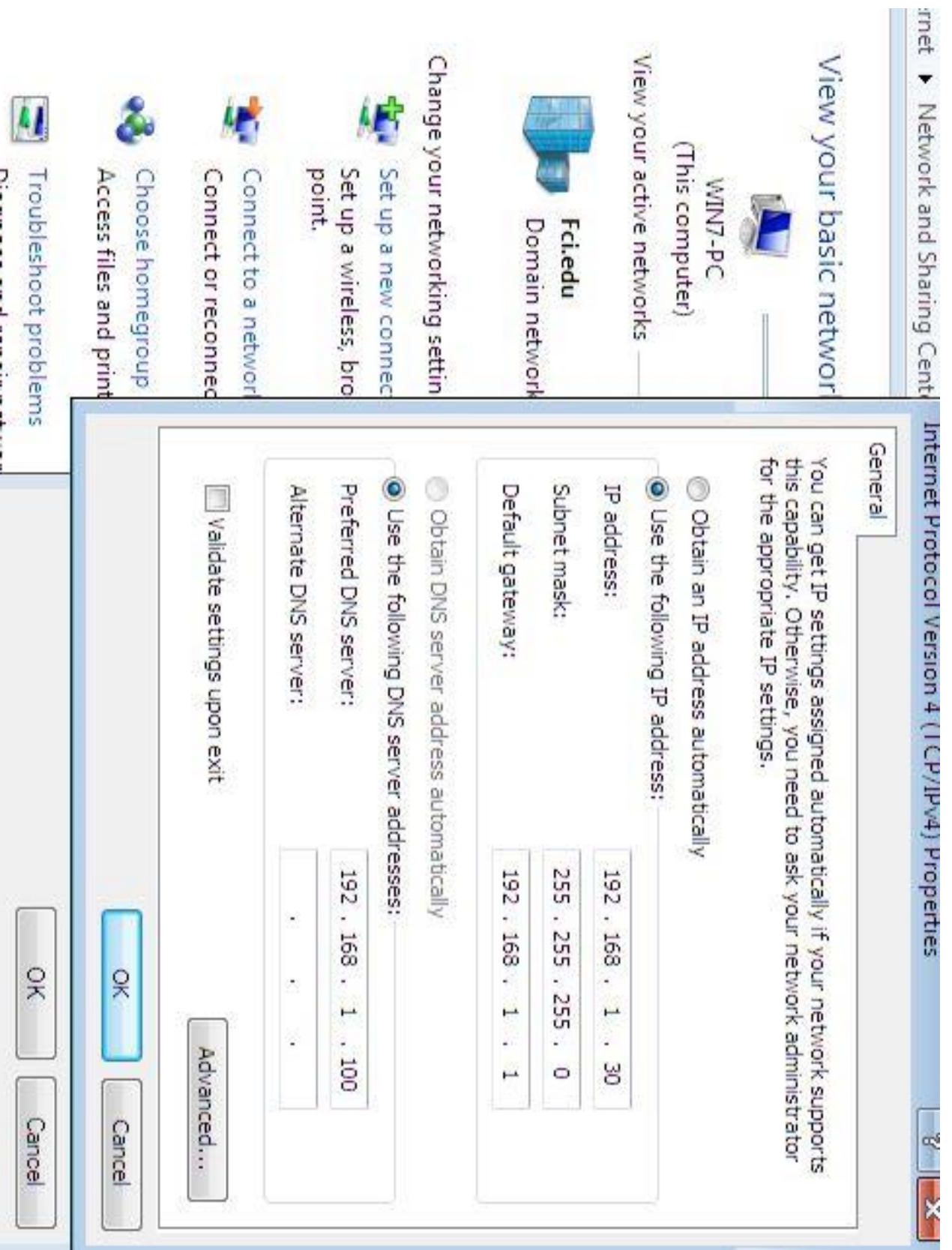
Log En...	Date	Time	Cluster	Host	Description
0001	6/24/2015	10:47:12 A...			NLB Manager session started
0002	6/24/2015	10:47:25 A...			Loading configuration information from host "serv2.Fci.edu" for clust
0003	6/24/2015	10:47:40 A...			Loading configuration information from host "serv1.Fci.edu" for clust

Hide









## 2. Network



```

!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.1.1 255.255.255.0
standby version 2
standby 2 ip 192.168.1.11
standby 2 priority 15
standby 2 preempt
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.2.1 255.255.255.0
standby version 2
standby 3 ip 192.168.2.11
standby preempt
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.3.1 255.255.255.0
standby version 2
standby 4 ip 192.168.3.11
standby 4 priority 150
standby 4 preempt
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown

```

```
interface FastEthernet0/0-30
 encapsulation dot1Q 30
 ip address 192.168.3.1 255.255.255.0
 standby version 2
 standby 4 ip 192.168.3.11
 standby 4 priority 150
 standby 4 preempt
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

VLAN Name	Status	Ports
-----	-----	-----
1 default	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
1 enet	100001	1500	-	-	-	-	-	0	0
1002 fddi	101002	1500	-	-	-	-	-	0	0
1003 tr	101003	1500	-	-	-	-	-	0	0
1004 fdnet	101004	1500	-	-	-	-	-	0	0
1005 trnet	101005	1500	-	-	-	-	-	0	0

Remote SPAN VLANs

-----

Primary	Secondary Type	Ports
-----	-----	-----

Interface	IP-Address	OK? Method Status	Protocol
FastEthernet0/0	unassigned	YES unset up	up
FastEthernet0/0.10	192.168.1.1	YES manual up	up
FastEthernet0/0.20	192.168.2.1	YES manual up	up
FastEthernet0/0.30	192.168.3.1	YES manual up	up
FastEthernet0/1	unassigned	YES unset administratively down down	
Vlan1	unassigned	YES unset administratively down down	



```
FastEthernet0/0 is up, line protocol is up (connected)
Hardware is Lance, address is 000a.f3e6.1801 (bia 000a.f3e6.1801)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0.10 is up, line protocol is up (connected)
```

```
FastEthernet0/0.10 is up, line protocol is up (connected)
Hardware is PQ1CC_FEC, address is 000a.f3e6.1801 (bia 000a.f3e6.1801)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 10
ARP type: ARPA, ARP Timeout 04:00:00,
Last clearing of "show interface" counters never
FastEthernet0/0.20 is up, line protocol is up (connected)
Hardware is PQ1CC_FEC, address is 000a.f3e6.1801 (bia 000a.f3e6.1801)
Internet address is 192.168.2.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 20
ARP type: ARPA, ARP Timeout 04:00:00,
Last clearing of "show interface" counters never
FastEthernet0/0.30 is up, line protocol is up (connected)
Hardware is PQ1CC_FEC, address is 000a.f3e6.1801 (bia 000a.f3e6.1801)
```



```

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 10
ARP type: ARPA, ARP Timeout 04:00:00,
  Last clearing of "show interface" counters never
astEthernet0/0.20 is up, line protocol is up (connected)
  Hardware is PQ1ICC_FEC, address is 000a.f3e6.1801 (bia 000a.f3e6.1801)
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 20
  ARP type: ARPA, ARP Timeout 04:00:00,
    Last clearing of "show interface" counters never
  astEthernet0/0.30 is up, line protocol is up (connected)
    Hardware is PQ1ICC_FEC, address is 000a.f3e6.1801 (bia 000a.f3e6.1801)
    Internet address is 192.168.3.1/24
    MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation 802.1Q Virtual LAN, Vlan ID 30
    ARP type: ARPA, ARP Timeout 04:00:00,
      Last clearing of "show interface" counters never
    astEthernet0/1 is administratively down, line protocol is down (disa)
      Hardware is Lance, address is 000a.f3e6.1802 (bia 000a.f3e6.1802)
      MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
        reliability 255/255, txload 1/255, rxload 1/255
        Encapsulation ARPA, loopback not set
        ARP type: ARPA, ARP Timeout 04:00:00,
          Last input 00:00:08, output 00:00:05, output hang never
          Last clearing of "show interface" counters never
          Input queue: 0/75/0 (size/max/drops); Total output drops: 0
          Queueing strategy: fifo
          Output queue :0/40 (size/max)
          5 minute input rate 0 bits/sec, 0 packets/sec
          5 minute output rate 0 bits/sec, 0 packets/sec
            0 packets input, 0 bytes, 0 no buffer
            Received 0 broadcasts, 0 runs, 0 giants, 0 throttles
            0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

```



```

Output queue : 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

Vlan1 is administratively down, line protocol is down
Hardware is CPU Interface, address is 0001.c748.4d65 (bia 0001.c748.4d65)
MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 21:40:21, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1682 packets input, 530955 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
563859 packets output, 0 bytes, 0 underruns
0 output errors, 23 interface resets
0 output buffer failures, 0 output buffers swapped out

```

```

FastEthernet0/0.10 - Group 2 (version 2)
State is Standby
    9 state changes, last state change 00:00:41
Virtual IP address is 192.168.1.11
Active virtual MAC address is 0000.0C9F.F002
    Local virtual MAC address is 0000.0C9F.F002 (v2 default)
Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.272 secs
Preemption enabled
Active router is 192.168.1.10, priority 15 (expires in 8 sec
MAC address is 0000.0C9F.F002
Standby router is local
Priority 15 (configured 15)
Group name is hrp--2 (default)
FastEthernet0/0.20 - Group 3 (version 2)
State is Active
    4 state changes, last state change 00:00:18
Virtual IP address is 192.168.2.11
Active virtual MAC address is 0000.0C9F.F003
    Local virtual MAC address is 0000.0C9F.F003 (v2 default)
Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.164 secs
Preemption disabled
Active router is local
Standby router is 192.168.2.10
Priority 100 (default 100)
Group name is hrp--3 (default)
FastEthernet0/0.30 - Group 4 (version 2)
State is Active

```



```
Standby router is 192.168.2.10
Priority 100 (default 100)
Group name is hrp--3 (default)
FastEthernet0/0.30 - Group 4 (version 2)
State is Active

 6 state changes, last state change 00:00:20
Virtual IP address is 192.168.3.11
Active virtual MAC address is 0000.0C9F.F004
Local virtual MAC address is 0000.0C9F.F004 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.228 secs
Preemption enabled
Active router is local
Standby router is 192.168.3.10, priority 150 (expires in 8 sec)
Priority 150 (configured 150)
Group name is hrp--4 (default)
```

```
Current configuration : 1640 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname sw1
!
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree portfast default
!
interface FastEthernet0/1
channel-group 4 mode active
switchport mode trunk
!
interface FastEthernet0/2
channel-group 3 mode active
switchport mode trunk
!
interface FastEthernet0/3
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 30
switchport mode access
```

---

```
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/8
 channel-group 3 mode active
 switchport mode trunk
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
 channel-group 4 mode active
 switchport mode trunk
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
```

```
.
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Port-channel 3
  switchport mode trunk
!
interface Port-channel 4
  switchport mode trunk
!
interface Vlan1
  no ip address
  shutdown
!
```



VLAN Name	Status	Ports
1 default	active	Fa0/9, Fa0/10, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10 staff	active	Fa0/7
20 student	active	Fa0/3, Fa0/4
30 management	active	Fa0/5, Fa0/6
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BridgMode	Trans1	Trans2
1 enet	100001	1500	-	-	-	-	0	0	
10 enet	100010	1500	-	-	-	-	0	0	
20 enet	100020	1500	-	-	-	-	0	0	
30 enet	100030	1500	-	-	-	-	0	0	
1002 fddi	101002	1500	-	-	-	-	0	0	
1003 tr	101003	1500	-	-	-	-	0	0	
1004 fdnet	101004	1500	-	-	-	ieee	0	0	
1005 trnet	101005	1500	-	-	-	ibm	0	0	

Remote SPAN VLANs		

Primary	Secondary	Type	Ports



Interface	IP-Address	OK? Method Status	Protocol
FastEthernet0/1	unassigned	YES manual up	up
FastEthernet0/2	unassigned	YES manual up	up
FastEthernet0/3	unassigned	YES manual up	up
FastEthernet0/4	unassigned	YES manual up	up
FastEthernet0/5	unassigned	YES manual up	up
FastEthernet0/6	unassigned	YES manual up	up
FastEthernet0/7	unassigned	YES manual up	up
FastEthernet0/8	unassigned	YES manual up	up
FastEthernet0/9	unassigned	YES manual down	down
FastEthernet0/10	unassigned	YES manual down	down
FastEthernet0/11	unassigned	YES manual up	up
FastEthernet0/12	unassigned	YES manual down	down
FastEthernet0/13	unassigned	YES manual down	down
FastEthernet0/14	unassigned	YES manual down	down
FastEthernet0/15	unassigned	YES manual down	down
FastEthernet0/16	unassigned	YES manual down	down
FastEthernet0/17	unassigned	YES manual down	down
FastEthernet0/18	unassigned	YES manual down	down
FastEthernet0/19	unassigned	YES manual down	down

FastEthernet0/20	unassigned	YES manual down	down
FastEthernet0/21	unassigned	YES manual down	down
FastEthernet0/22	unassigned	YES manual down	down
FastEthernet0/23	unassigned	YES manual down	down
FastEthernet0/24	unassigned	YES manual down	down
GigabitEthernet0/1	unassigned	YES manual down	down
GigabitEthernet0/2	unassigned	YES manual down	down
Vlan1	unassigned	YES manual administratively down	down
Port-channel 3	unassigned	YES manual up	up
Port-channel 4	unassigned	YES manual up	up

Port #

swl#show spanning-tree  
VLAN0001

Spanning tree enabled protocol rstp  
Root ID      Priority      32769  
             Address      0001.4350.943B

Cost      9  
Port      28 (Port-channel 3)  
Hello Time      2 sec      Max Age 20 sec      Forward Delay 15 sec

Bridge ID      Priority      32769      (priority 32768 sys-id-ext 1)  
             Address      00E0.8FC1.898A  
             Hello Time      2 sec      Max Age 20 sec      Forward Delay 15 sec  
             Aging Time      20

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Po4	Altn	BLK	9	128.27		Shr
Po3	Root	FWD	9	128.28		Shr

VLAN0010

Spanning tree enabled protocol rstp

Root ID      Priority      32778  
             Address      0001.4350.943B  
             Cost      9  
             Port      28 (Port-channel 3)  
             Hello Time      2 sec      Max Age 20 sec      Forward Delay 15 sec

Bridge ID      Priority      32778      (priority 32768 sys-id-ext 10)  
             Address      00E0.8FC1.898A  
             Hello Time      2 sec      Max Age 20 sec      Forward Delay 15 sec  
             Aging Time      20

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Fa0/7	Desg	FWD	19	128.7		P2p
Po4	Altn	BLK	9	128.27		Shr
Po3	Root	FWD	9	128.28		Shr

# VLAN0020

Spanning tree enabled protocol rstp

Root ID Priority 32768

Address 0001.4350.943B

Cost 9

Port 28 (Port-channel 3)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 20)

Address 00E0.8FC1.898A

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----------	------	-----	------	-------	-----	------

Fa0/3	Desg	FWD	19	128.3		P2P
-------	------	-----	----	-------	--	-----

Fa0/4	Desg	FWD	19	128.4		P2P
-------	------	-----	----	-------	--	-----

Po4	Altn	BLK	9	128.27		Shr
-----	------	-----	---	--------	--	-----

Po3	Root	FWD	9	128.28		Shr
-----	------	-----	---	--------	--	-----

# VLAN0030

Spanning tree enabled protocol rstp

Root ID Priority 32768

Address 0001.4350.943B

Cost 9

Port 28 (Port-channel 3)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 30)

Address 00E0.8FC1.898A

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----------	------	-----	------	-------	-----	------

Fa0/5	Desg	FWD	19	128.5		P2P
-------	------	-----	----	-------	--	-----

Fa0/6	Desg	FWD	19	128.6		P2P
-------	------	-----	----	-------	--	-----

Po4	Altn	BLK	9	128.27		Shr
-----	------	-----	---	--------	--	-----

Po3	Root	FWD	9	128.28		Shr
-----	------	-----	---	--------	--	-----



```
sw1#show mac-address-table
Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	0002.17de.090c	DYNAMIC	Po3
1	0060.2f4d.0701	DYNAMIC	Ea0/2
1	0060.2f4d.0703	DYNAMIC	Ea0/8
10	0002.17de.090c	DYNAMIC	Po3
20	0001.646a.9601	DYNAMIC	Po3
20	0002.17de.090c	DYNAMIC	Po3
20	000a.f3e6.1801	DYNAMIC	Po3
30	0001.646a.9601	DYNAMIC	Po3
30	0002.17de.090c	DYNAMIC	Po3
30	000a.f3e6.1801	DYNAMIC	Po3

### Channel-group listing:

-----

Group: 3

-----

Group state = L2

Ports: 2 Maxports = 16

Port-channels: 1 Max Port-channels = 16

Protocol: LACP

Group: 4

-----

Group state = L2

Ports: 2 Maxports = 16

Port-channels: 1 Max Port-channels = 16

Protocol: LACP

```

swl#show interfaces
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 000c.8561.8a01 (bia 000c.8561.8a01)
  BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue : 0/40 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
      956 packets input, 193351 bytes, 0 no buffer
      Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 watchdog, 0 multicast, 0 pause input
      0 input packets with dribble condition detected
      2357 packets output, 263570 bytes, 0 underruns
      0 output errors, 0 collisions, 10 interface resets
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier
      0 output buffer failures, 0 output buffers swapped out
FastEthernet0/2 is up, line protocol is up (connected)
  Hardware is Lance, address is 000c.8561.8a02 (bia 000c.8561.8a02)
  BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255

```



```

FastEthernet0/2 is up, line protocol is up (connected)
Hardware is Lance, address is 000c.8561.8a02 (bia 000c.8561.8a02)
  BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  956 packets input, 193351 bytes, 0 no buffer
  Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 watchdog, 0 multicast, 0 pause input
  0 input packets with dribble condition detected
  2357 packets output, 263570 bytes, 0 underruns
  0 output errors, 0 collisions, 10 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
FastEthernet0/3 is up, line protocol is up (connected)
Hardware is Lance, address is 000c.8561.8a03 (bia 000c.8561.8a03)
  BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)

```

```

Output queue : 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
0 output errors, 0 collisions, 10 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/4 is up, line protocol is up (connected)
Hardware is Lance, address is 000c.8561.8a04 (bia 000c.8561.8a04
BW 100000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drc
Queueing strategy: fifo
Output queue : 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
0 output errors, 0 collisions, 10 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

```



```
Hardware is Lance, address is 000c.8561.8a05 (bia 000c.8561.8a05)
BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue : 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
0 output errors, 0 collisions, 10 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
FastEthernet0/6 is up, line protocol is up (connected)
Hardware is Lance, address is 000c.8561.8a06 (bia 000c.8561.8a06)
BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue : 0/40 (size/max)
```

```

Output queue :0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 956 packets input, 193351 bytes, 0 no buffer
 Received 956 broadcasts, 0 runs, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 watchdog, 0 multicast, 0 pause input
 0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
 0 output errors, 0 collisions, 10 interface resets
 0 babbles, 0 late collision, 0 deferred
 0 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out

FastEthernet0/7 is up, line protocol is up (connected)
 Hardware is Lance, address is 000c.8561.8a07 (bia 000c.8561.8a07)
 BW 100000 Kbit, DLY 1000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Full-duplex, 100Mb/s
 input flow-control is off, output flow-control is off
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:08, output 00:00:05, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue :0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 956 packets input, 193351 bytes, 0 no buffer
 Received 956 broadcasts, 0 runs, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 watchdog, 0 multicast, 0 pause input
 0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
 0 output errors, 0 collisions, 10 interface resets
 0 babbles, 0 late collision, 0 deferred
 0 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out

FastEthernet0/8 is up, line protocol is up (connected)
 Hardware is Lance, address is 000c.8561.8a08 (bia 000c.8561.8a08)

```



```

Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue : 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
0 output errors, 0 collisions, 10 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
FastEthernet0/9 is down, line protocol is down (disabled)
Hardware is Lance, address is 000c.8561.8a09 (bia 000c.8561.8a09)
BW 100000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue : 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec

```

```

5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
0 output errors, 0 collisions, 10 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/10 is down, line protocol is down (disabled)
Hardware is Lance, address is 000c.8561.8a0a (bia 000c.8561.8a0a)
BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
0 output errors, 0 collisions, 10 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

FastEthernet0/11 is up, line protocol is up (connected)
Hardware is Lance, address is 000c.8561.8a0b (bia 000c.8561.8a0b)
BW 100000 Kbit, DLY 1000 usec,

```



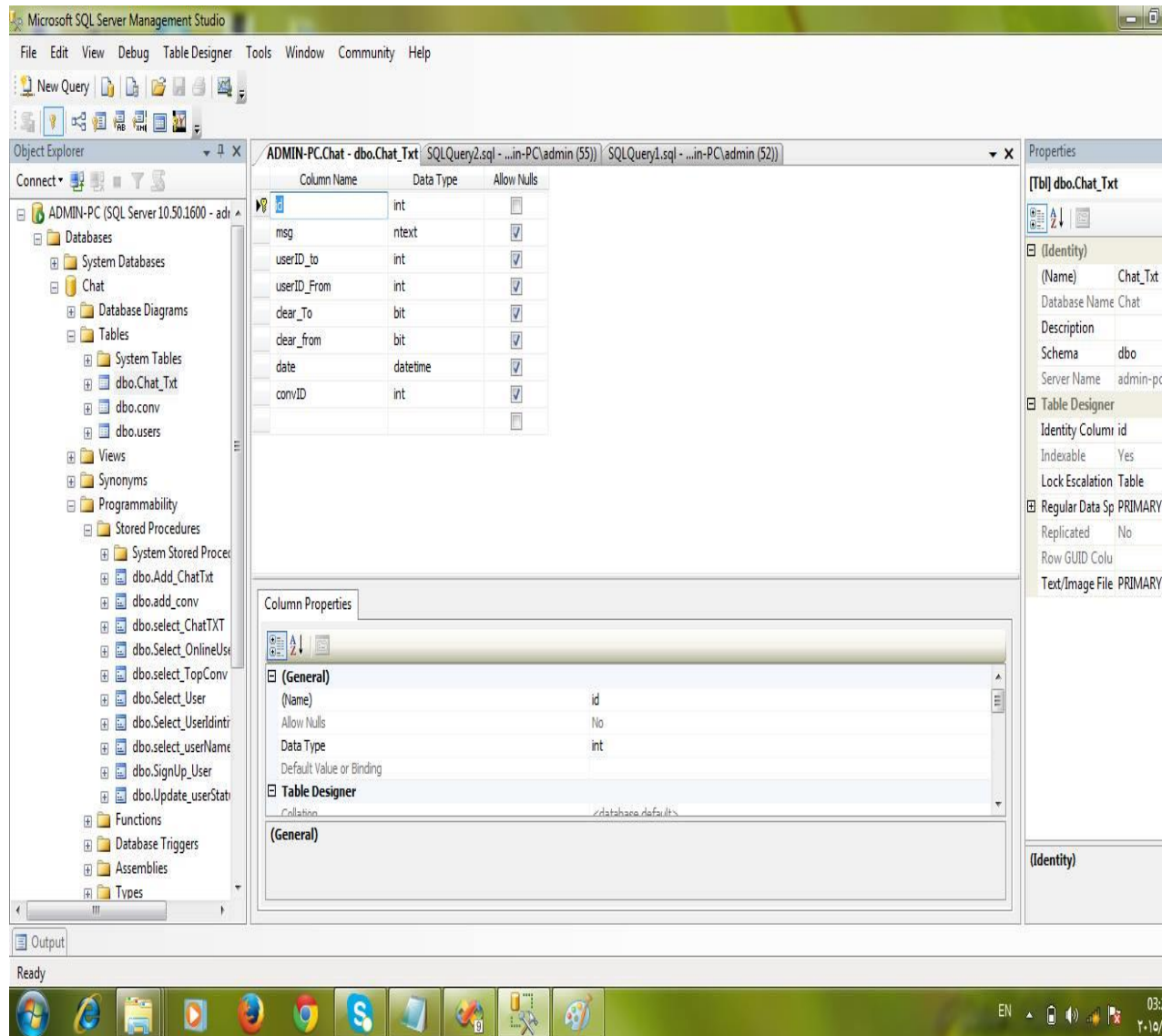
```

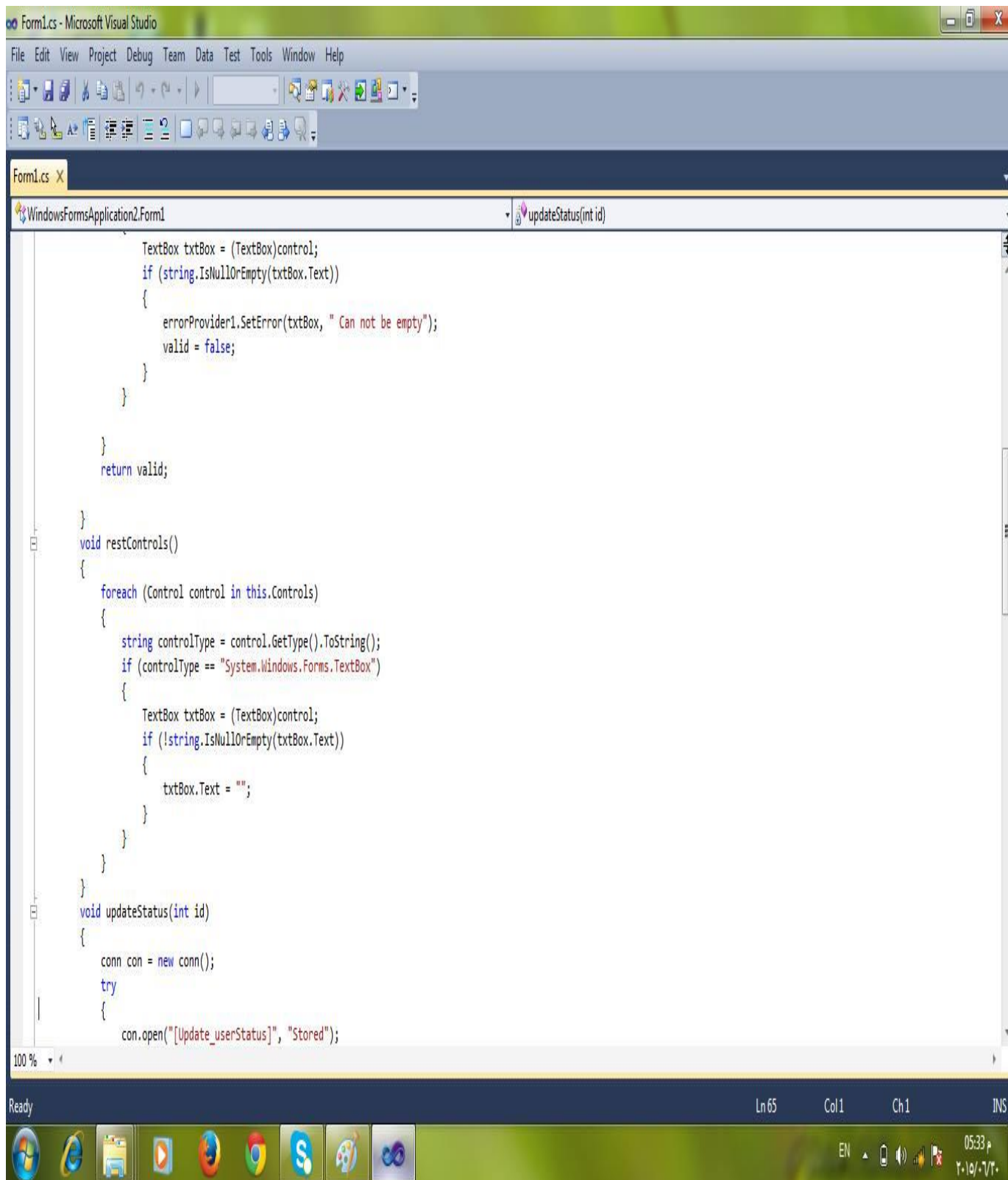
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
0 output errors, 0 collisions, 10 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
FastEthernet0/12 is down, line protocol is down (disabled)
Hardware is Lance, address is 000c.8561.8a0c (bia 000c.8561.8a0c)
BW 100000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles

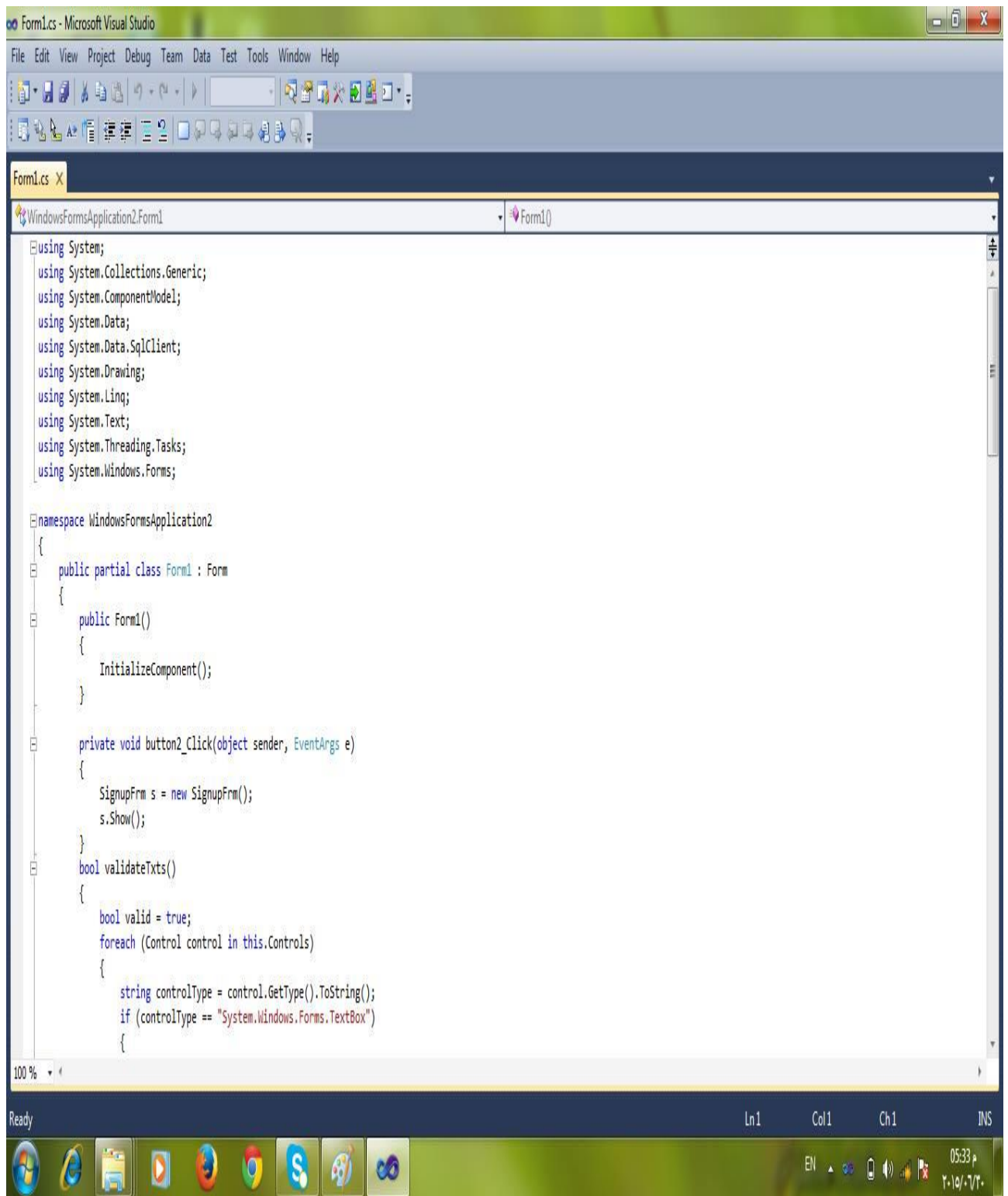
```

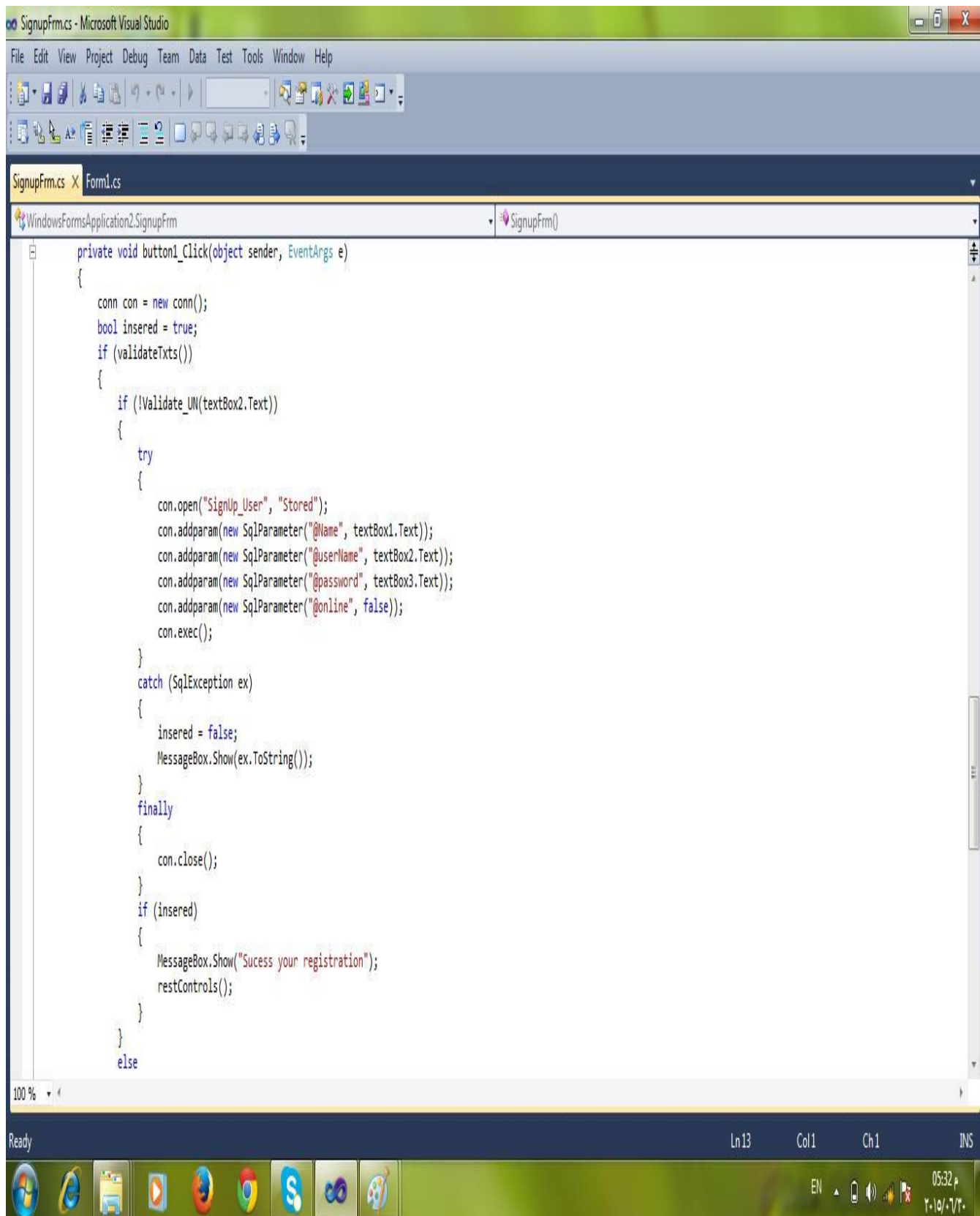


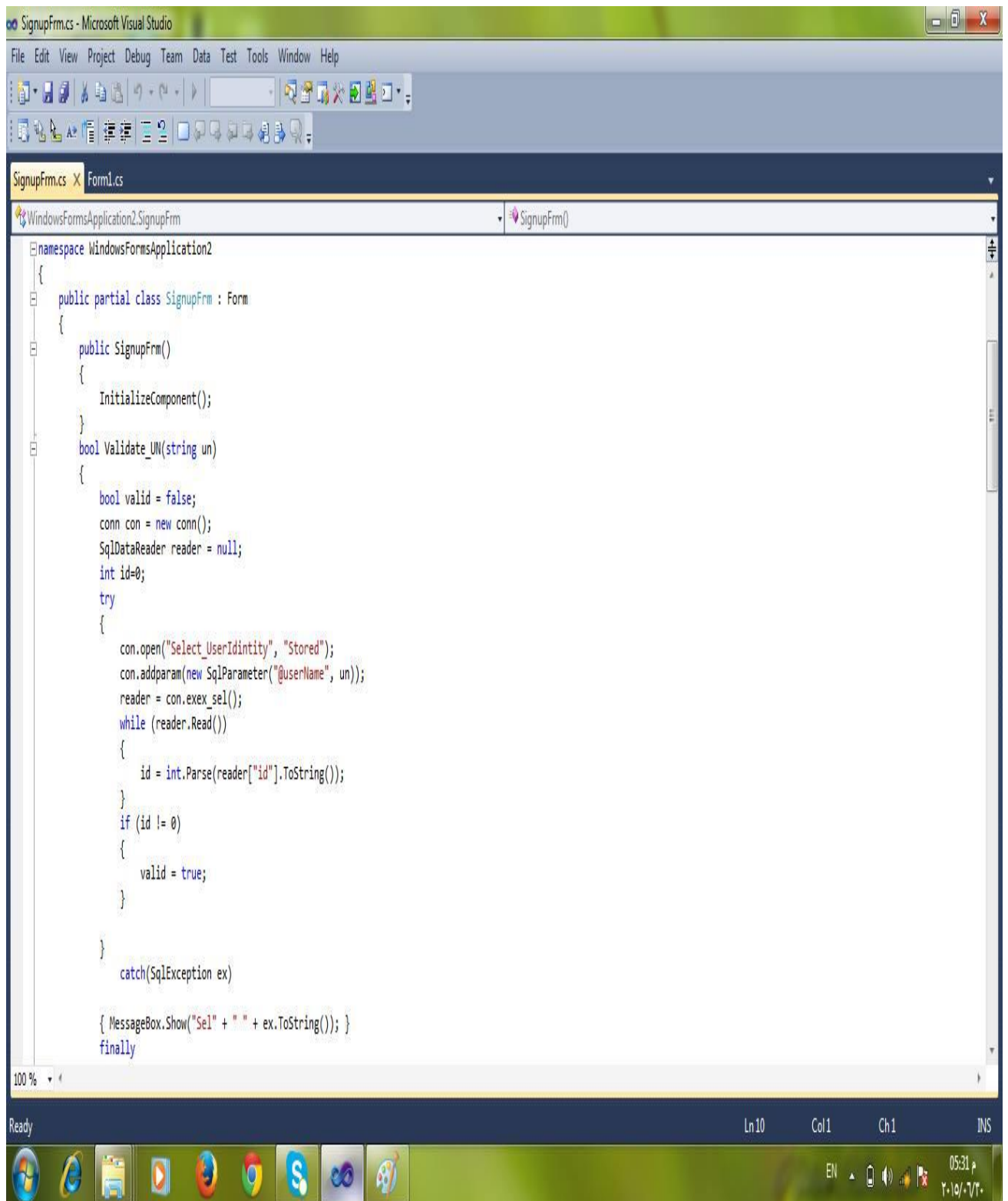
### 3. Chatting

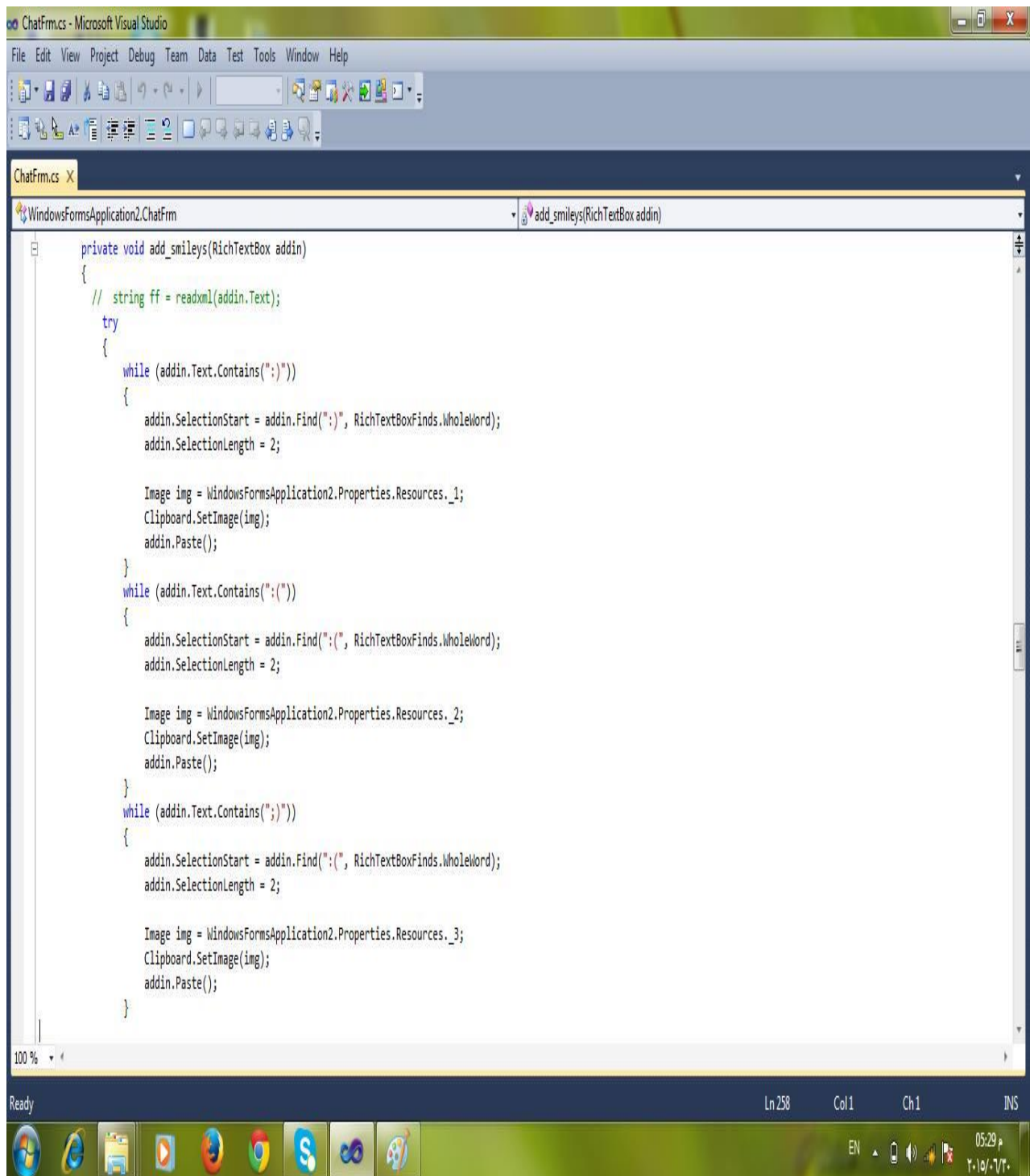




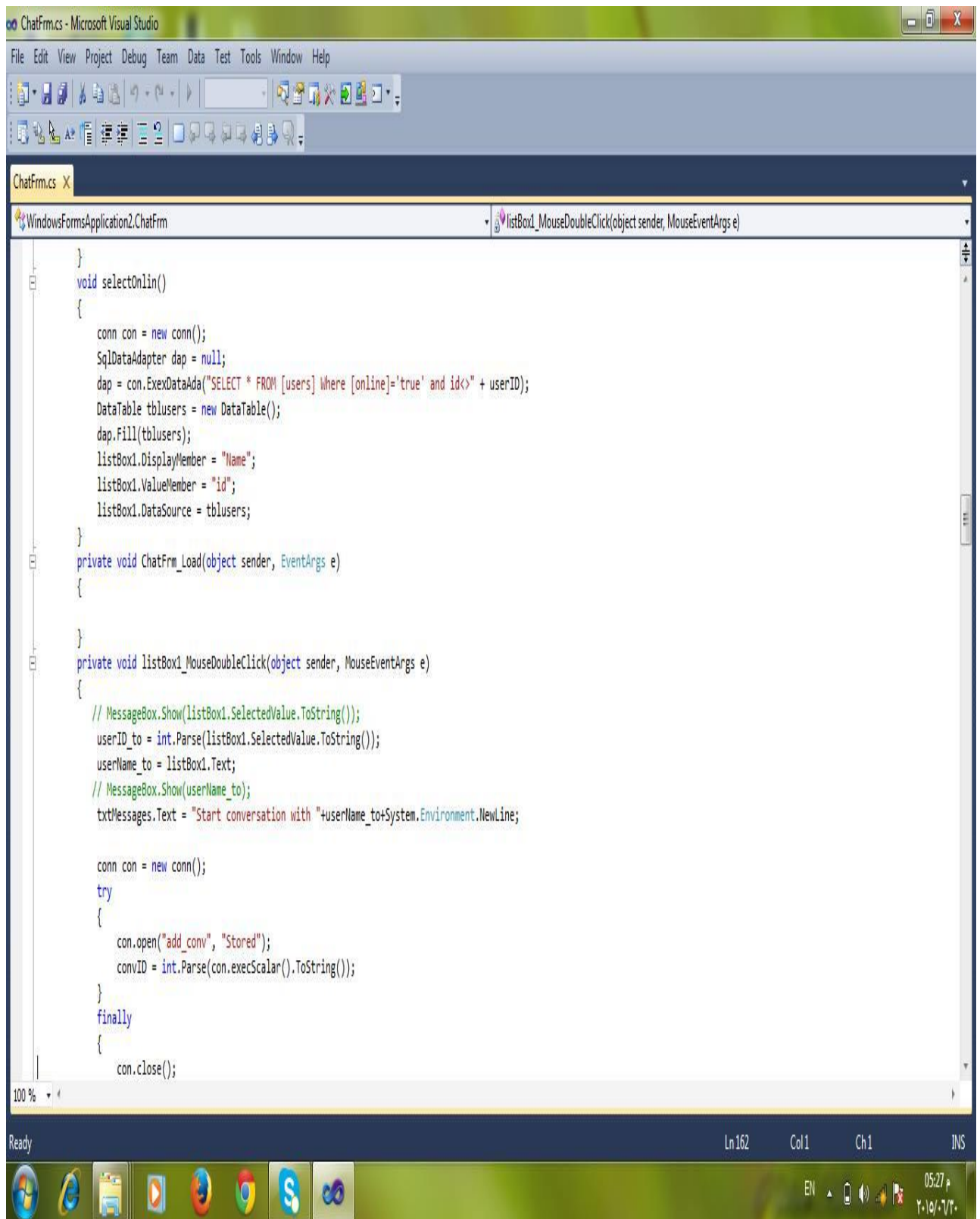


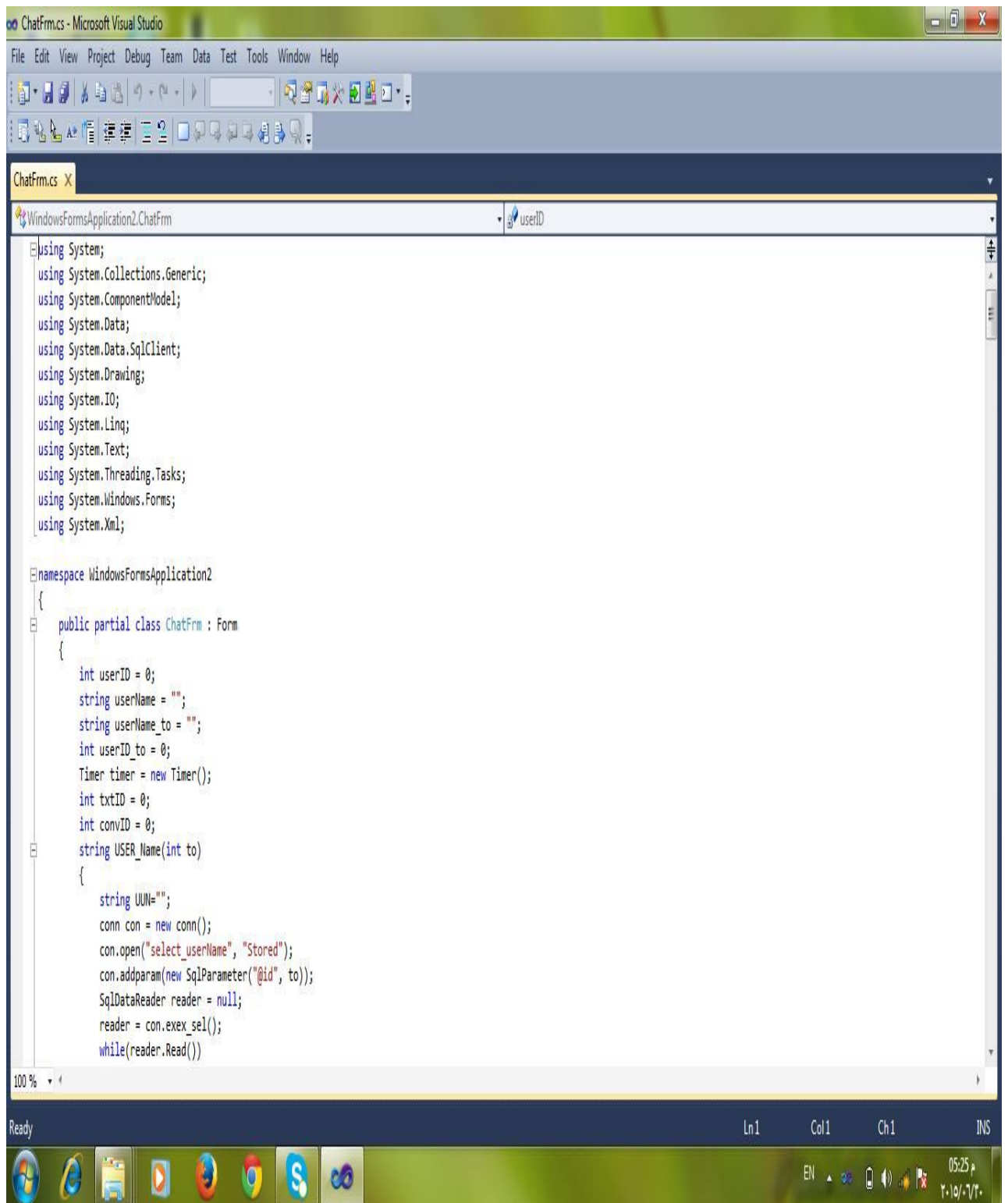


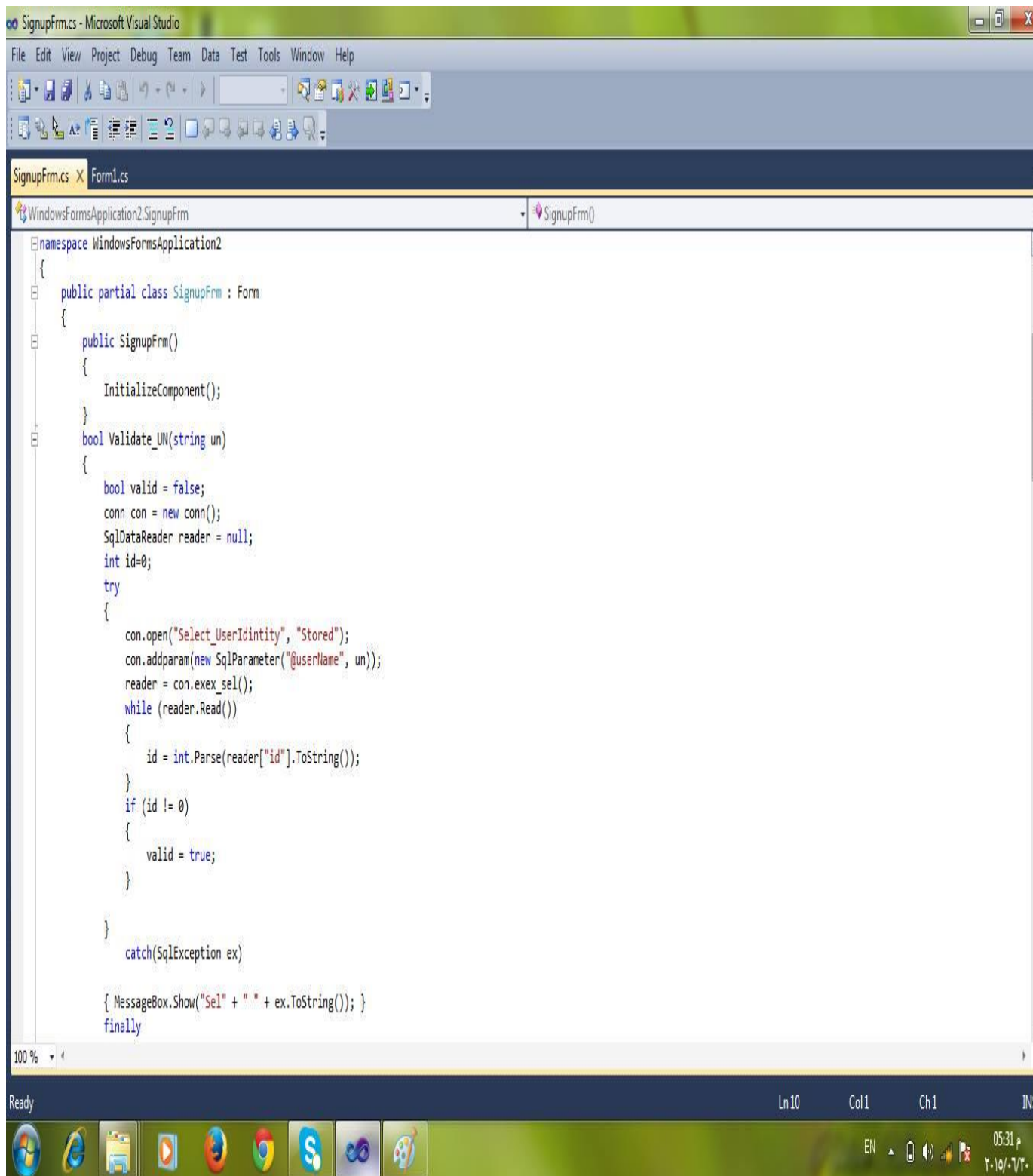












# Chapter 7

## Case Study

1-in this figure we send message from pc1 in vlan 20 to pc6 in Vlan30 (in different network).

2-the message is sent through sw1 (send broadcast message).

3-sw3 receive this message not SW2 because of SPT to avoid looping.

4-sw3 forward message to routers and sw2.

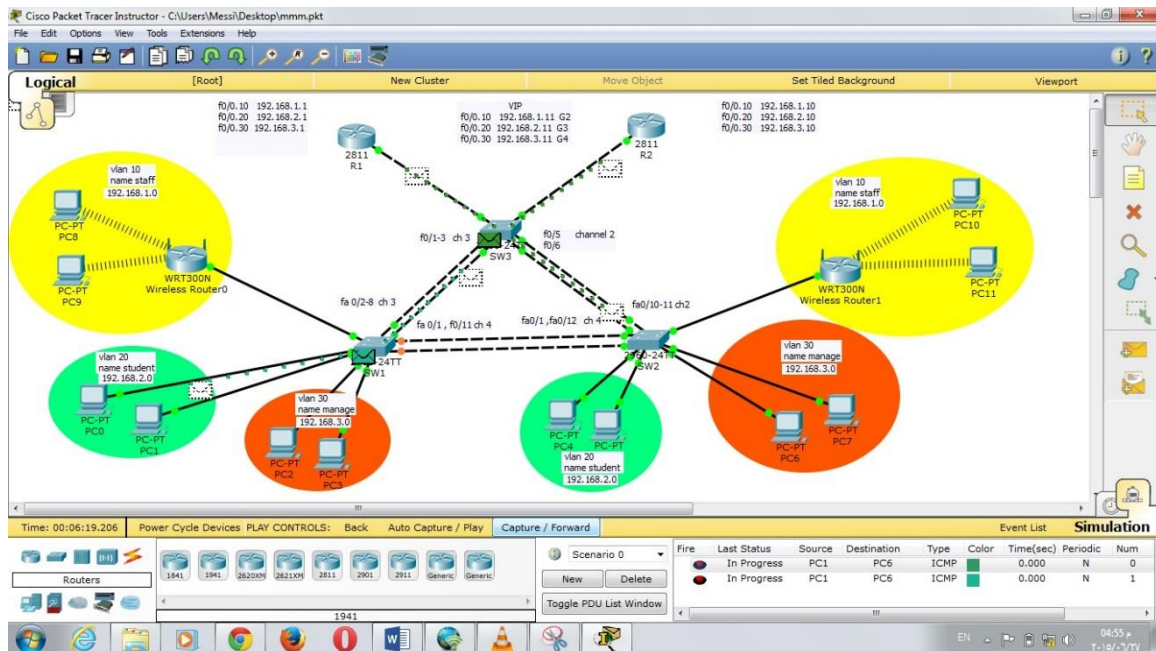


Figure 1

5-sw2 send message in broadcast to find destination

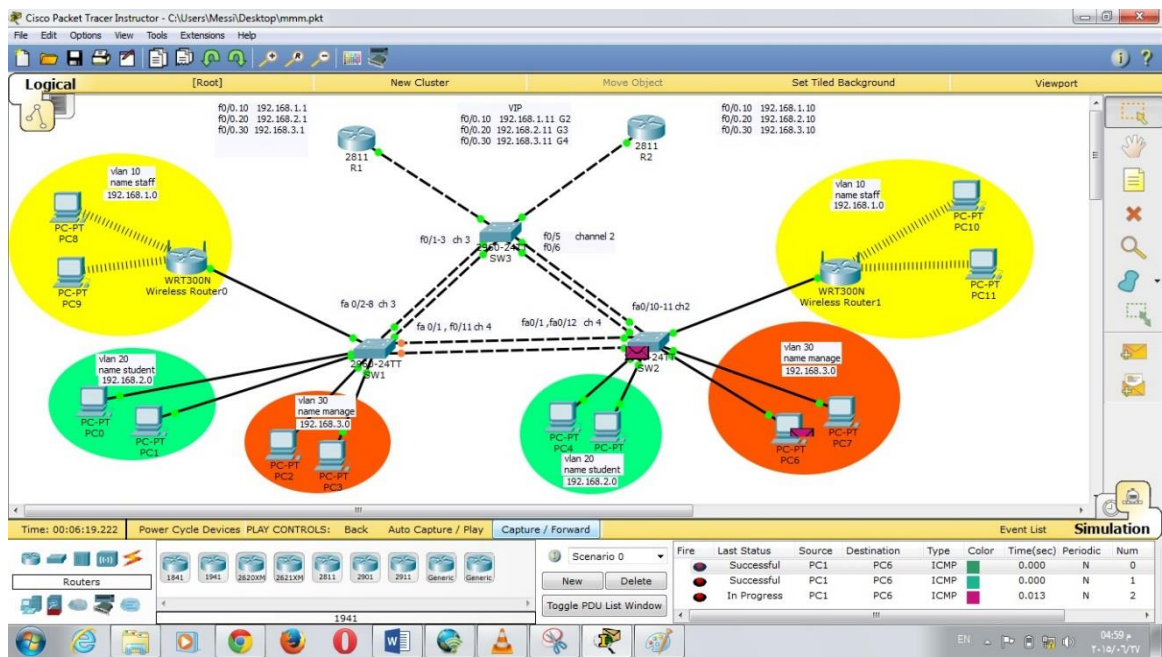


Figure2



6-same steps happened in message reply.

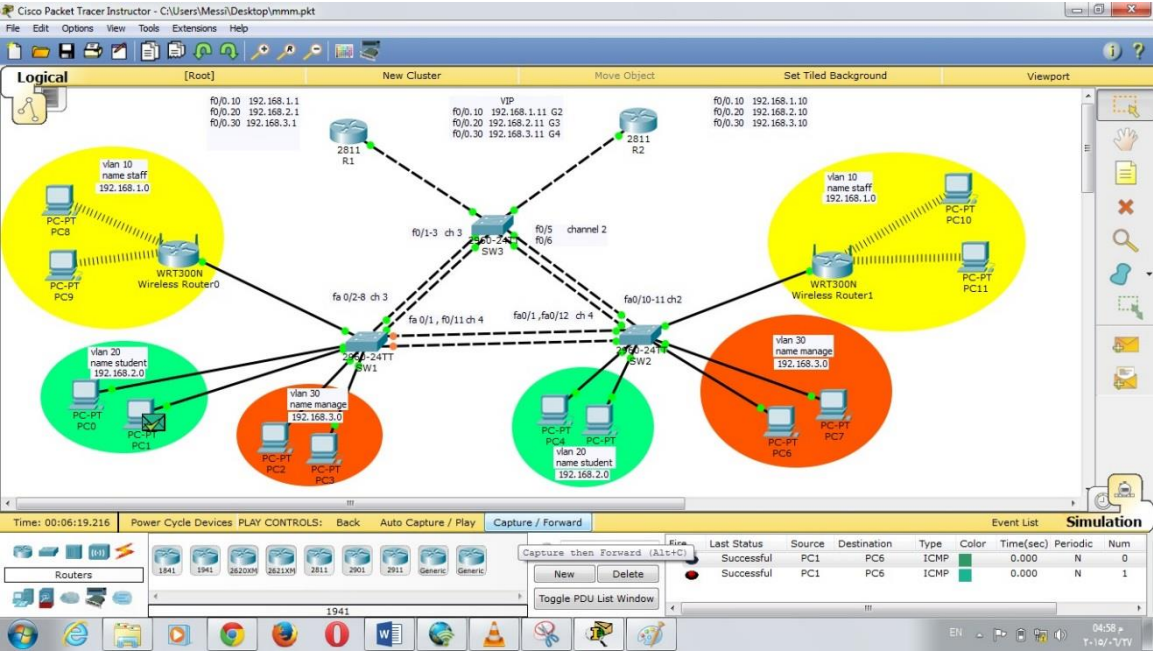
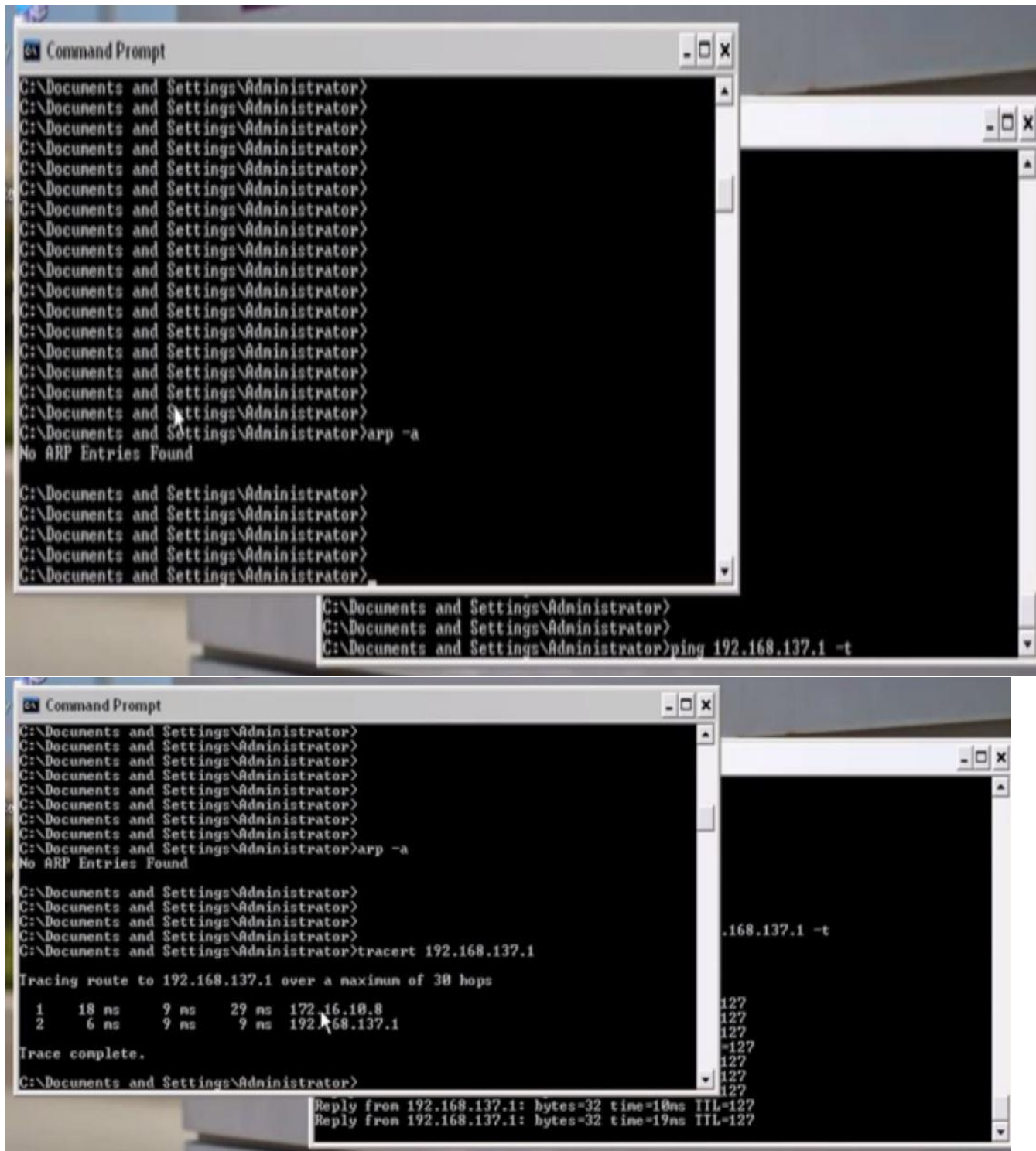


Figure3

## Trace of load balancing routers



The image consists of two screenshots of a Windows Command Prompt window, showing a series of network diagnostic commands and their outputs.

**Top Screenshot:**

```
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>arp -a
No ARP Entries Found

C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>ping 192.168.137.1 -t
```

**Bottom Screenshot:**

```
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>arp -a
No ARP Entries Found

C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>tracert 192.168.137.1

Tracing route to 192.168.137.1 over a maximum of 30 hops
  0  18 ns  9 ns  29 ns  192.168.137.1
  1   6 ns  9 ns  9 ns  192.168.137.1
Trace complete.

C:\Documents and Settings\Administrator>
Reply from 192.168.137.1: bytes=32 time=10ms TTL=127
Reply from 192.168.137.1: bytes=32 time=19ms TTL=127
```

```
Command Prompt

Tracing route to 192.168.137.1 over a maximum of 30 hops
  1  18 ns   9 ns   29 ns  172.16.10.8
  2   6 ns   9 ns   9 ns   192.168.137.1
Trace complete.

C:\Documents and Settings\Administrator>netsh interface ip delete arpccache
Ok.

C:\Documents and Settings\Administrator>arp -a
No ARP Entries Found

C:\Documents and Settings\Administrator>tracert 192.168.137.1
Tracing route to 192.168.137.1 over a maximum of 30 hops
  1  17 ns   14 ns   12 ns  172.16.10.2
  2   2 ns   19 ns   9 ns   192.168.137.1
Trace complete.

C:\Documents and Settings\Administrator>
Reply from 192.168.137.1: bytes=32 time=8ms TTL=127
Reply from 192.168.137.1: bytes=32 time=7ms TTL=127
```

```
Mark Command Prompt

No ARP Entries Found

C:\Documents and Settings\Administrator>tracert 192.168.137.1
Tracing route to 192.168.137.1 over a maximum of 30 hops
  1  17 ns   14 ns   12 ns  172.16.10.2
  2   2 ns   19 ns   9 ns   192.168.137.1
Trace complete.

C:\Documents and Settings\Administrator>netsh interface ip delete arpccache
Ok.

C:\Documents and Settings\Administrator>tracert 192.168.137.1
Tracing route to 192.168.137.1 over a maximum of 30 hops
  1  23 ns   9 ns   9 ns   172.16.10.8
  2   8 ns   9 ns   9 ns   192.168.137.1
Trace complete.

C:\Documents and Settings\Administrator>
Reply from 192.168.137.1: bytes=32 time=7ms TTL=127
Reply from 192.168.137.1: bytes=32 time=6ms TTL=127
```

```
Command Prompt

Internet Address      Physical Address      Type
172.16.10.5           00-50-56-c0-00-01    dynamic
172.16.10.10          00-07-b4-00-05-04    dynamic

C:\Documents and Settings\Administrator>netsh interface ip delete arpccache
Ok.

C:\Documents and Settings\Administrator>netsh interface ip delete arpccache
Ok.

C:\Documents and Settings\Administrator>arp -a
No ARP Entries Found

C:\Documents and Settings\Administrator>tracert 192.168.137.1
Tracing route to 192.168.137.1 over a maximum of 30 hops
  1  22 ns   9 ns   10 ns  172.16.10.8
  2  10 ns   9 ns   9 ns   192.168.137.1
Trace complete.

C:\Documents and Settings\Administrator>
Reply from 192.168.137.1: bytes=32 time=11ms TTL=127
Reply from 192.168.137.1: bytes=32 time=7ms TTL=127
```

# Chapter 8

## Gain Experiences

- **VRRP, HSRP and GLBP.**
- **Round Robin and weight Round Robin.**

Most of Universities, Faculties, Units of information technology in faculties, Units of e-learning in universities, Companies using networks, Banks and Insurance companies need networks with High performance and security with low costs to manage and secure their departments (Data).

We have developed Dynamic Uniform Network Distribution, Provide VLANs to connect each department on its VLAN to manage Group of departments on one Switch (Provide Low Costs), Build load balancing and distribution in DUND and chat Allow to departments to speak with each other.

---

## **VRRP**

There are several ways a LAN client can determine which router should be the first hop to a particular remote destination. The client can use a dynamic process or static configuration. Examples of dynamic router discovery are as follows:

- Proxy ARP—the client uses Address Resolution Protocol (ARP) to get the destination it wants to reach, and a router will respond to the ARP request with its own MAC address.
- Routing protocol—the client listens to dynamic routing protocol updates (for example, from Routing Information Protocol [RIP]) and forms its own routing table.
- ICMP Router Discovery Protocol (IRDP) client—the client runs an Internet Control Message Protocol (ICMP) router discovery client.

The drawback to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is cut off from the rest of the network.

VRRP can solve the static configuration problem. VRRP enables a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group. VRRP is supported on Ethernet, Fast Ethernet, BVI, and Gigabit Ethernet interfaces, and on MPLS VPNs, VRF-aware MPLS VPNs, and VLANs.

## **VRRP Benefits**

### **Redundancy**

VRRP enables you to configure multiple routers as the default gateway router, which reduces the possibility of a single point of failure in a network.

### **Load Sharing**

You can configure VRRP in such a way that traffic to and from LAN clients can be shared by multiple routers, thereby sharing the traffic load more equitably among available routers.

### **Multiple Virtual Routers**

VRRP supports up to 255 virtual routers (VRRP groups) on a router physical interface, subject to the platform supporting multiple MAC addresses. Multiple virtual router support enables you to implement redundancy and load sharing in your LAN topology.

### **Multiple IP Addresses**

The virtual router can manage multiple IP addresses, including secondary IP addresses. Therefore, if you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.

### **Preemption**

The redundancy scheme of VRRP enables you to preempt a virtual router backup that has taken over for a failing virtual router master with a higher priority virtual router backup that has become available.

### **Authentication**

VRRP message digest 5 (MD5) algorithm authentications protects against VRRP-spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security.

### **Advertisement Protocol**

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) for VRRP advertisements. This addressing scheme minimizes the number of routers that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA assigned VRRP the IP protocol number 112.

### **VRRP Object Tracking**

VRRP object tracking provides a way to ensure the best VRRP router is the virtual router master for the group by altering VRRP priorities to the status of tracked objects such as the interface or IP route states.

## **HSRP**

Most IP hosts have an IP address of a single router configured as the default gateway. When HSRP is used, the HSRP virtual IP address is



configured as the host's default gateway instead of the IP address of the router.

HSRP is useful for hosts that do not support a router discovery protocol (such as ICMP Router Discovery Protocol [IRDP]) and cannot switch to a new router when their selected router reloads or loses power. Because existing TCP sessions can survive the failover, this protocol also provides a more transparent recovery for hosts that dynamically choose a next hop for routing IP traffic.

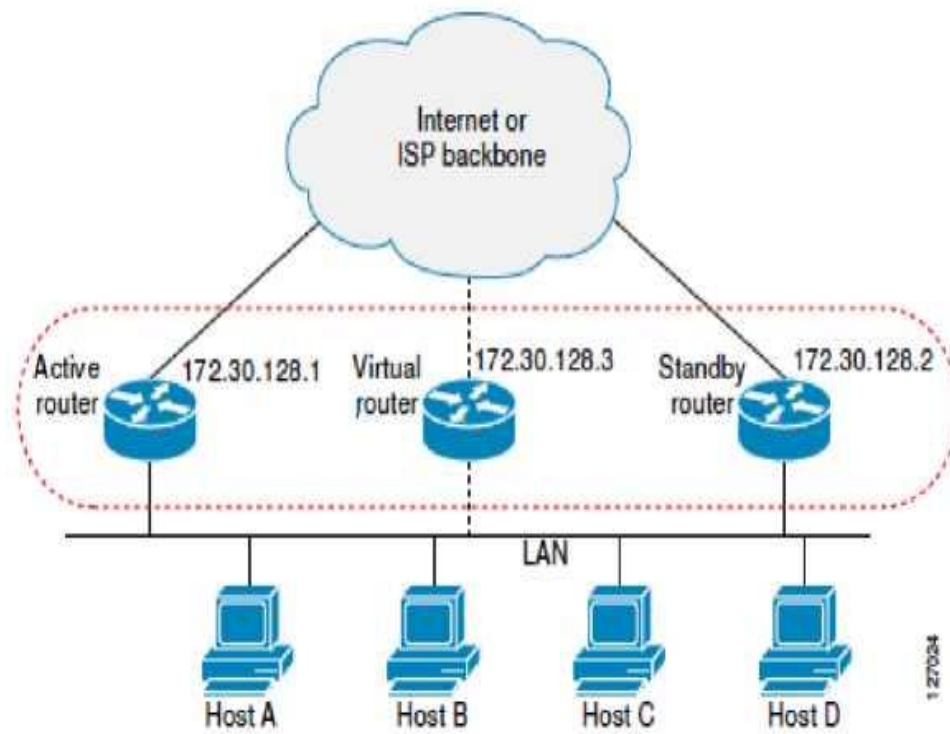
When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among a group of routers running HSRP. The address of this HSRP group is referred to as the virtual IP address. One of these devices is selected by the protocol to be the active router. The active router receives and routes packets destined for the MAC address of the group. For  $n$  routers running HSRP,  $n + 1$  IP and MAC addresses are assigned.

HSRP detects when the designated active router fails, at which point a selected standby router assumes control of the MAC and IP addresses of the Hot Standby group. A new standby router is also selected at that time.

HSRP uses a priority mechanism to determine which HSRP configured router is to be the default active router. To configure a router as the active router, you assign it a priority that is higher than the priority of all the other HSRP-configured routers. The default priority is 100, so if you configure just one router to have a higher priority, that router will be the default active router. Devices that are running HSRP send and receive multicast UDP-based hello messages to detect router failure and to designate active and standby routers. When the active router fails to send a hello message within a configurable period of time, the standby router with the highest priority becomes the active router. The transition of packet forwarding functions between routers is completely transparent to all hosts on the network.

You can configure multiple Hot Standby groups on an interface, thereby making fuller use of redundant routers and load sharing.

The figure below shows a network configured for HSRP. By sharing a virtual MAC address and IP address, two or more routers can act as a single virtual router. The virtual router does not physically exist but represents the common default gateway for routers that are configured to provide backup to each other. You do not need to configure the hosts on the LAN with the IP address of the active router. Instead, you configure them with the IP address (virtual IP address) of the virtual router as their default gateway. If the active router fails to send a hello message within the configurable period of time, the standby router takes over and responds to the virtual addresses and becomes the active router, assuming the active router duties.



1 27034

## **GLBP**

GLBP provides automatic router backup for IP hosts configured with a single default gateway on an IEEE 802.3 LAN. Multiple first-hop routers on the LAN combine to offer a single virtual first-hop IP router while sharing the IP packet forwarding load. Other routers on the LAN may act as redundant GLBP routers that will become active if any of the existing forwarding routers fail.

GLBP performs a similar function for the user as HSRP and VRRP. HSRP and VRRP allow multiple routers to participate in a virtual router group configured with a virtual IP address. One member is elected to be the active router to forward packets sent to the virtual IP address for the group. The other routers in the group are redundant until the active router fails. These standby routers have unused bandwidth that the protocol is not using. Although multiple virtual router groups can be configured for the same set of routers, the hosts must be configured for different default gateways, which result in an extra administrative burden.

The advantage of GLBP is that it additionally provides load balancing over multiple routers (gateways) using a single virtual IP address and multiple virtual MAC addresses. The forwarding load is shared among all routers in a GLBP group rather than being handled by a single router while the other routers stand idle. Each host is configured with the same virtual IP address, and all routers in the virtual router group participate in forwarding packets. GLBP members communicate between each other through hello messages sent every 3 seconds to the multicast address 224.0.0.102, UDP port 3222 (source and destination).

The Gateway Load Balancing Protocol feature provides automatic router backup for IP hosts configured with a single default gateway on an IEEE 802.3 LAN. Multiple first hop routers on the LAN combine to offer a single virtual first hop IP router while sharing the IP packet forwarding load. Other

routers on the LAN may act as redundant GLBP routers that will become active if any of the existing forwarding routers fail.

GLBP performs a similar, but not identical, function for the user as the HSRP and the VRRP. HSRP and VRRP protocols allow multiple routers to participate in a virtual router group configured with a virtual IP address. One member is elected to be the active router to forward packets sent to the virtual IP address for the group. The other routers in the group are redundant until the active router fails. These standby routers have unused bandwidth that the protocol is not using. Although multiple virtual router groups can be configured for the same set of routers, the hosts must be configured for different default gateways, which results in an extra administrative burden. GLBP provides load balancing over multiple routers (gateways) using a single virtual IP address and multiple virtual MAC addresses. Each host is configured with the same virtual IP address, and all routers in the virtual router group participate in forwarding packets. GLBP members communicate between each other through hello messages sent every 3 seconds to the multicast address 224.0.0.102, User Datagram Protocol (UDP) port 3222 (source and destination).

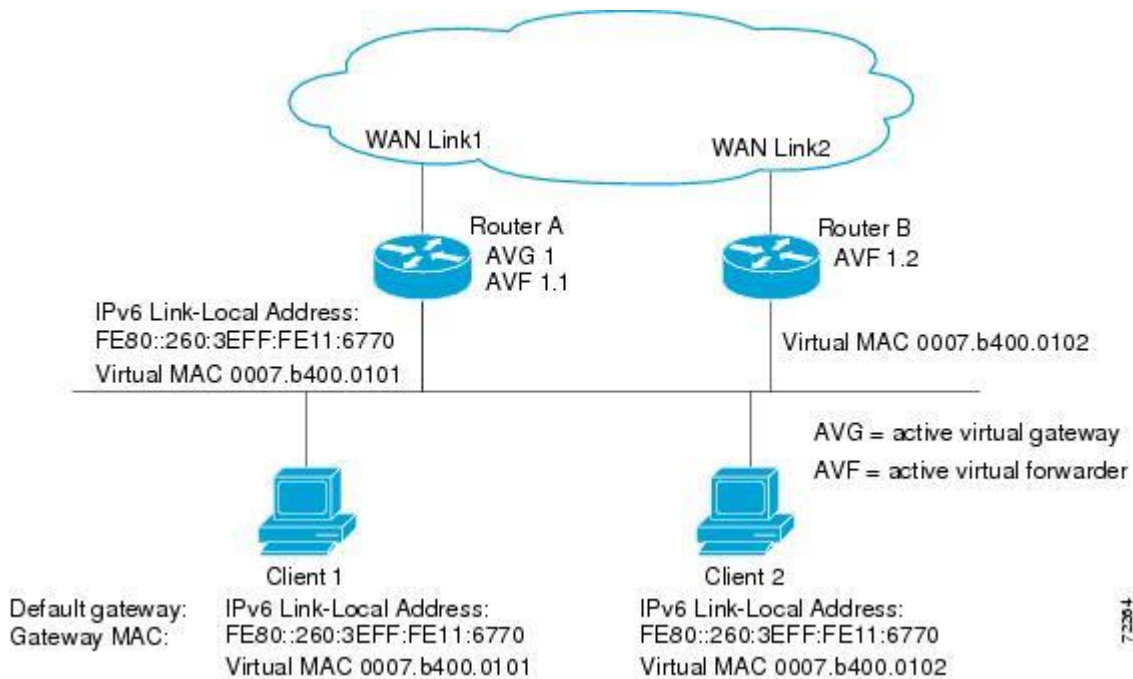
### GLBP Active Virtual Gateway

Members of a GLBP group elect one gateway to be the active virtual gateway (AVG) for that group. Other group members provide backup for the AVG in the event that the AVG becomes unavailable. The AVG assigns a virtual MAC address to each member of the GLBP group. Each gateway assumes responsibility for forwarding packets sent to the virtual MAC address assigned to it by the AVG. These gateways are known as active virtual forwarders (AVFs) for their virtual MAC address.

The AVG is responsible for answering Address Resolution Protocol (ARP) requests for the virtual IP address. Load sharing is achieved by the AVG replying to the ARP requests with different virtual MAC addresses.

In [Figure 1](#), Router A is the AVG for a GLBP group, and is responsible for the virtual IP address 10.21.8.10. Router A is also an AVF for the virtual MAC address 0007.b400.0101. Router B is a member of the same GLBP group and is designated as the AVF for the virtual MAC address 0007.b400.0102. Client 1 has a default gateway IP address of 10.21.8.10 and a gateway MAC address of 0007.b400.0101. Client 2 shares the same default gateway IP address but receives the gateway MAC address 0007.b400.0102 because Router B is sharing the traffic load with Router A.

**Figure 1 GLBP Topology**



If Router A becomes unavailable, Client 1 will not lose access to the WAN because Router B will assume responsibility for forwarding packets sent to the virtual MAC address of Router A, and for responding to packets sent to its own virtual MAC address. Router B will also assume the role of the AVG for the entire GLBP group. Communication for the GLBP members continues despite the failure of a router in the GLBP group.

### GLBP Virtual MAC Address Assignment

A GLBP group allows up to four virtual MAC addresses per group. The AVG is responsible for assigning the virtual MAC addresses to each member of the group. Other group members request a virtual MAC address after they discover the AVG through hello messages. Gateways are assigned the next MAC address in sequence. A virtual forwarder that is assigned a virtual MAC address by the AVG is known as a primary virtual forwarder. Other members of the GLBP group learn the virtual MAC addresses from hello messages. A virtual forwarder that has learned the virtual MAC address is referred to as a secondary virtual forwarder.

### GLBP Virtual Gateway Redundancy

GLBP operates virtual gateway redundancy in the same way as HSRP. One gateway is elected as the AVG, another gateway is elected as the

standby virtual gateway, and the remaining gateways are placed in a listen state.

If an AVG fails, the standby virtual gateway will assume responsibility for the virtual IP address. A new standby virtual gateway is then elected from the gateways in the listen state.

### GLBP Virtual Forwarder Redundancy

Virtual forwarder redundancy is similar to virtual gateway redundancy with an AVF. If the AVF fails, one of the secondary virtual forwarders in the listen state assumes responsibility for the virtual MAC address.

The new AVF is also a primary virtual forwarder for a different forwarder number. GLBP migrates hosts away from the old forwarder number using two timers that start as soon as the gateway changes to the active virtual forwarder state. GLBP uses the hello messages to communicate the current state of the timers.

The redirect time is the interval during which the AVG continues to redirect hosts to the old virtual forwarder MAC address. When the redirect time expires, the AVG stops redirecting hosts to the virtual forwarder, although the virtual forwarder will continue to forward packets that were sent to the old virtual forwarder MAC address.

The secondary hold time is the interval during which the virtual forwarder is valid. When the secondary hold time expires, the virtual forwarder is removed from all gateways in the GLBP group. The expired virtual forwarder number becomes eligible for reassignment by the AVG.

### GLBP Gateway Priority

GLBP gateway priority determines the role that each GLBP gateway plays and what happens if the AVG fails.

Priority also determines if a GLBP router functions as a backup virtual gateway and the order of ascendancy to becoming an AVG if the current AVG fails. You can configure the priority of each backup virtual gateway with a value of 1 through 255 using the **glbp priority** command.

In [Figure 1](#), if Router A, the AVG in a LAN topology, fails, an election process takes place to determine which backup virtual gateway should take over. In this example, Router B is the only other member in the group so it will automatically become the new AVG. If another router existed in the same GLBP group with a higher priority, then the router with the highest priority would be elected. If both routers have the same priority, the backup



virtual gateway with the higher IP address would be elected to become the active virtual gateway.

By default, the GLBP gateway preemptive scheme is disabled. A backup virtual gateway can become the AVG only if the current AVG fails, regardless of the priorities assigned to the virtual gateways. You can enable the GLBP preemptive scheme using the **glbp preempt** command.

Preemption allows a backup virtual gateway to become the AVG, if the backup virtual gateway is assigned a higher priority than the current AVG.

### GLBP Gateway Weighting and Tracking

GLBP uses a weighting scheme to determine the forwarding capacity of each router in the GLBP group. The weighting assigned to a router in the GLBP group determines whether it will forward packets and, if so, the proportion of hosts in the LAN for which it will forward packets. Thresholds can be set to disable forwarding when the weighting falls below a certain value, and when it rises above another threshold, forwarding is automatically reenabled.

The GLBP group weighting can be automatically adjusted by tracking the state of an interface within the router. If a tracked interface goes down, the GLBP group weighting is reduced by a specified value. Different interfaces can be tracked to decrement the GLBP weighting by varying amounts.

## Types of GLBP load Balancing Mechanism.

There are **two load-balancing mechanism** that is used with GLBP. These including

1. **Round-robin:** The default one. Each AVF in turn is included in address resolution replies for the virtual IP address.

2. **Host-dependent:** Based on the MAC address of a host where the same forwarder is always used for a particular host.

- **Weighted:** Based on weight dependent share of user between routers.

We choose GLBP Because:

### Load Sharing

You can configure GLBP in such a way that traffic from LAN clients can be shared by multiple routers, thereby sharing the traffic load more equitably among available routers.

### Multiple Virtual Routers

GLBP supports up to 1024 virtual routers (GLBP groups) on each physical interface of a router, and up to 4 virtual forwarders per group.

### Preemption

The redundancy scheme of GLBP enables you to preempt an active virtual gateway with a higher priority backup virtual gateway that has become available. Forwarder preemption works in a similar way, except that forwarder preemption uses weighting instead of priority and is enabled by default.

### Authentication

You can use a simple text password authentication scheme between GLBP group members to detect configuration errors. A router within a GLBP group with a different authentication string than other routers will be ignored by other group members.

## **WEIGHTED:**

This is the ability GLBP to place a weight on each device when calculating the amount of load sharing that will occur through MAC assignment. Each GLBP router in the group will advertise its weighting and assignment; the AVG will act based on that value. For example, if there are two routers in a group and router A has double the forwarding capacity of router B, the weighting value of router A should be configured to be double the amount of router B.

## **ROUND ROBIN**

With Round Robin each VF MAC address is used sequentially in ARP replies for the virtual IP address Round Robin load balancing is suitable for any number of end hosts.

And we choose Round Robin Because  
Our Project have Two Routers with the same quality

# References

## References helped us:

[1] CCNA Study Guide 200-120.

[http://www.mediafire.com/download/9uzuny66o74x30y/CCNAX%2520200-120%2520BY%2520ENG\\_ELDEEB.rar](http://www.mediafire.com/download/9uzuny66o74x30y/CCNAX%2520200-120%2520BY%2520ENG_ELDEEB.rar)

[2] Wikipedia. Waterfall model.

[http://en.wikipedia.org/wiki/Waterfall\\_model](http://en.wikipedia.org/wiki/Waterfall_model)

[3] Wikipedia. Implementation.

<http://en.wikipedia.org/wiki/Implementation>

[4] GLBP Load Balancing.

[http://www.cisco.com/en/US/docs/ios/12\\_2t/12\\_2t15/feature/guide/ft\\_glb.html](http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glb.html)

<http://orbit-computer-solutions.com/CCNA%3A-Redundancy-Protocol---Understanding-GLBP.php>

[4] Network.

[http://www.tcpipguide.com/free/t\\_WhatIsNetworking.htm](http://www.tcpipguide.com/free/t_WhatIsNetworking.htm)

[5] Permissions in win server 2012.

<http://www.techrepublic.com/blog/data-center/setting-basic-ntfs-permissions-in-windows-server-2012/>

[6] Domain and Workgroup.

<http://windows.microsoft.com/en-us/windows7/what-is-the-difference-between-a-domain-a-workgroup-and-a-homegroup>

[7] Distributed File System DFS

<http://searchwindowsserver.techtarget.com/definition/distributed-file-system-DFS>

**[8] DFS Replication**

<https://technet.microsoft.com/en-us/library/jj127250.aspx>

**[9] Wikipedia. SDLC.**

<http://en.wikipedia.org/wiki/SDLC>

**[10] Wikipedia. System Analysis.**

[http://en.wikipedia.org/wiki/System\\_analysis](http://en.wikipedia.org/wiki/System_analysis)

**[11] Wikipedia. System Design.**

[http://en.wikipedia.org/wiki/System\\_design](http://en.wikipedia.org/wiki/System_design)