Deploying, Managing, and Monitoring System and Network Infrastructure

A Graduation Project Report Submitted to

the Faculty of Computers and Information at Zagazig University

in Partial Fulfillment of the Requirements for the

Degree of

Bachelor of Computer Science in Information Technology

Supervised By:

Dr. Ehab Rushdy

Faculty of Computers and Information, Zagazig University

Zagazig, Egypt

July 2015

Team Members:

- ➔ **Mohamed Ahmed Hassan Waly**

- ➔ **Mohamed Eid Mohamed Hashim**

- ➔ **Mohamed Said Ahmed Aly**

- ➔ **Osama Ahmed Fathi El-Ghayesh**

Table of Contents

Acknowledgments

We acknowledge:

- ✓ The great support that we got from Dr. Ehab Rushdy.
- ✓ Microsoft TechNet.
- ✓ Cisco Official Documentation.

Abstract

A recent international study on the capacity of information technology (IT) of hundreds of companies shows that IT is critical to their growth because it provides them with scalability, the ability to successfully manage the increase in the complexity of the organization and its processes and business model. Academics and professionals struggle to understand the way in which IT affects the performance of the companies (or if this influence really exists). There are those who think that it has become an omnipresent factor, like electricity, which provides a minimum competitive advantage to companies that use it. Others claim that the use of IT is essential; however, they could not find a systematic correlation between investment in IT and the company's performance. Some believe that the use of IT is important but base their arguments on a few examples of exceptional companies, like Dell and FedEx (who have used IT for many years) to highlight the difference in their market sectors. Can a company benefit from intensive IT implementation to differentiate themselves from the competition and reach important business objectives? This seems to be the crucial question.

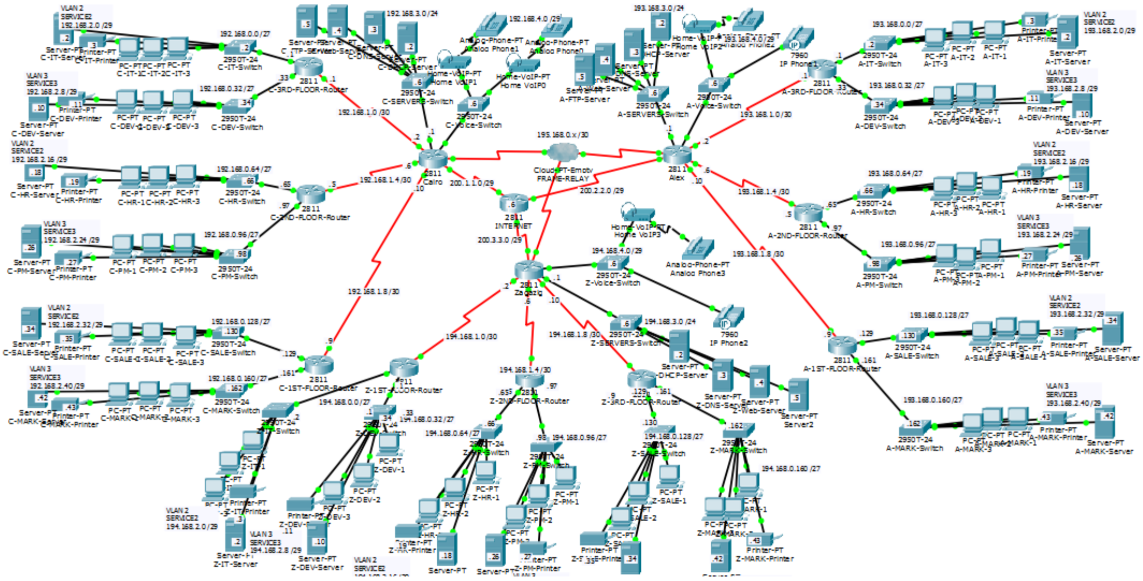
According to recent studies, the answer is yes, although it cannot be simply measured by the amount of money invested in IT. Expenditure in the organizations' IT is a poor indicator of the functionality of it and its business impact. It is possible to use vast economic resources in technology without significant improvements in the operational capacity of the company.

The capacity of IT contributes to the growth of enterprises. Several studies of international medium-sized companies show that the capacity of IT has a close correlation with the growth of the cost-effectiveness of the organizations. Data obtained from these studies indicate that IT accelerates the growth of businesses because it provides them with scalability, the ability to successfully manage the increase in the complexity of the organization and its processes and business model. Companies with business processes scalability are better placed to overcome obstacles to growth, differentiate themselves from the competition and quickly seize the business opportunities that arise. In summary, the use of IT is relevant and is an essential ingredient for the success of companies' long term. IT is not simply a component whose influence on the prosperity of the company is nothing to be lowered. IT promotes the growth of organizations.

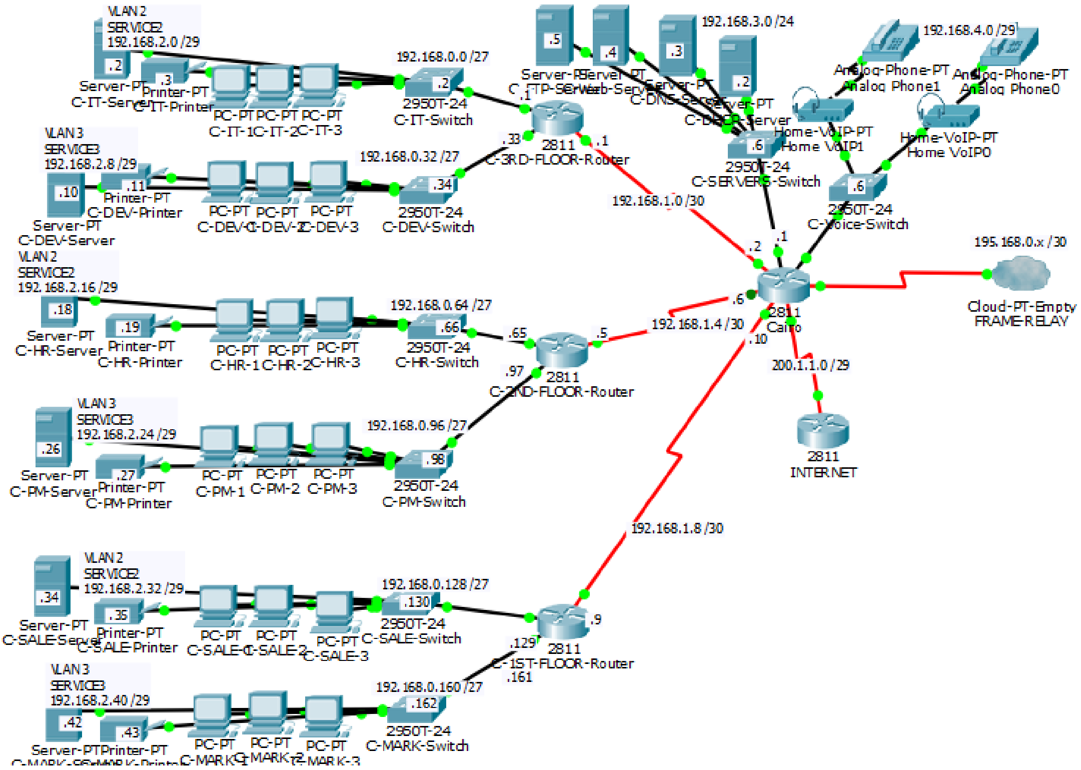
Part I

Chapter 1: Introduction

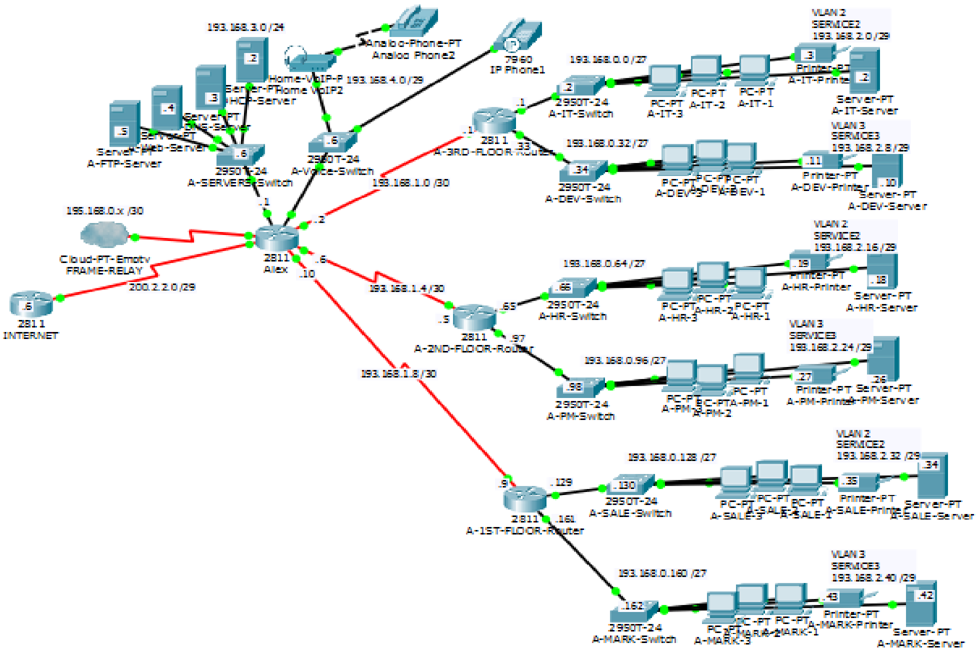
General View



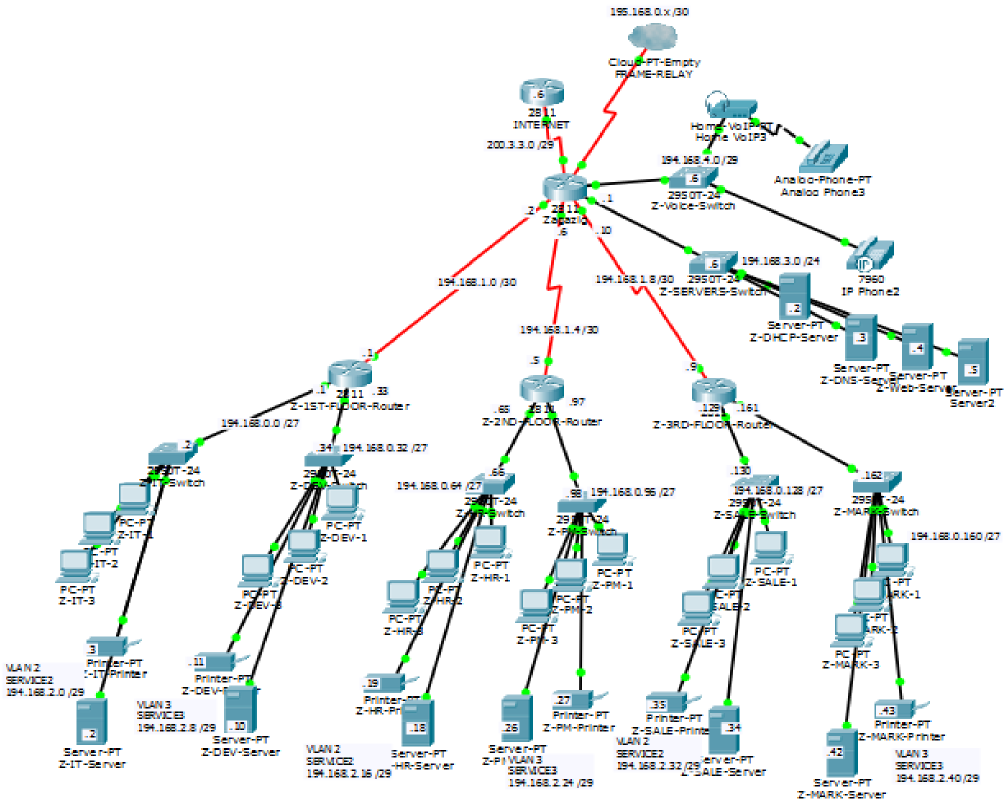
Cairo Branch



Alex Branch



Zagazig Branch



IT-Solution Company has three branches:

- Cairo Branch
- Alex Branch
- Zagazig Branch

Every branch has its own network infrastructure:

- Routers
- Switches
- Cables
- Servers
- Phones
- PCs
- Home VoIP

Every branch has three floors and two departments at each floor:

- 1st-Floor

- Information Technology Department
- Development Department

- 2nd-Floor

- Human Resource Department
- Project Management Department

- 3rd-Floor

- Sales Department
- Marketing Department

Every floor has its own:

- Router
- Switches
- PCs
- Server
- Printer

Every branch has four servers connected by a switch:

- DHCP Server
- DNS Server
- Web Server
- FTP Server
- VoIP Server

Every branch has two phones connected by a switch

- Analog Phone
- IP Phone

Every branch has a main router that connects:

- Floors
- Servers
- Phones
- Frame Relay
- Internet
- Other Branches

About the Tools/Technologies used in our Project:

- Routing & switching: used for connecting hosts, routers, switches, servers, and other devices.

- Network Security: used for securing the connection between the connected hosts, routers, switches, servers, and other devices.

- VoIP: stands for Voice over Internet Protocol. Sometimes it is referred to as Voice over Networks or (VoN), Voice over Broadband (VoB) and sometimes Internet Telephony. VoIP allows you to make free, or very low cost, telephone calls over the Internet. You can call any telephone in the world and any telephone can call you - regardless of what equipment or network the person you are calling uses.

Chapter 2: Building the network infrastructure

In this chapter, we will walkthrough what we have done in the network infrastructure including routing & switching techniques.

Here are the steps we have gone through during building our project. Moreover, we describe the tools/protocols/techniques used in order to perform our project.

1- Media, Cables, Ports, and Connectors:

- PCs, Server and Printer of every department are connected to Fast-Ethernet (100Mbps) Switch Ports by a straight-through UTP (Unshielded Twisted Pair) cable and RJ-45 connector. Switch is connected to Router's Fast-Ethernet Interface using also straight-through UTP cable and RJ-45 connector.

- DHCP, DNS, Web, and FTP Servers are connected to Fast-Ethernet Switch ports by straight-through UTP cable and RJ-45 connector, and this switch is connected to Main Router's Fast-Ethernet Interface by using straight-through UTP cable and RJ-45 connector too.

- Phones are connected to Fast-Ethernet Switch ports by straight-through UTP cable and RJ-45 connector, and this switch is connected to Main Router's Fast-Ethernet Interface by using straight-through UTP cable and RJ-45 connector too.

- Floor Router is connected to Main Router's Serial (1.544Mbps) Interface using serial cable and RS-232 connector.

- Main Router is connected to Frame-Relay cloud and Internet serial interface by using serial cable and RS-232 connector.

2- IP Addressing

- An IP address is an address used in order to uniquely identify a device on an IP network and to deliver packets from one host to another.

3- VLSM (Variable Length Subnet Mask):

- Divides an IP address space into a hierarchy of subnets of different sizes, making it possible to create subnets with very different host counts without wasting large numbers of addresses.

4- VLAN (Private Local Area Network):

- Breaks up broadcast domain without using a router.
- Provides more security to devices, which separate them from others.
- Native VLAN: traffic is carried untagged. It's better to tag the native VLAN in order to prevent against security vulnerability in your network environment.
- The logical grouping of network nodes.
- Switch that supports VLANs allows the administrator to select which ports will participate in the VLAN. These ports are then grouped to become one VLAN, and any broadcasts or information passed among these ports will not be seen by the remaining ports on the switch.

- The server and printer located in every department are separated in a VLAN named SERVICES to make a specific task and to provide a more secure environment for them. /29 subnet mask is used in this VLAN to provide only 8 addresses.

5- Dynamic Routing: EIGRP (Enhanced Interior Gateway Routing Protocol):

- Network protocol that lets routers exchange information more efficiently.
- When a routing table entry changes in one of the routers, it notifies its neighbors of the change only.
- Router keeps a copy of its neighbor's routing tables. If it can't find a route to a destination in one of these tables, it queries its neighbors for a route and they in turn query their neighbors until a route is found.
- Encrypts and Authenticates routing information sent to other routers.
- Using no-auto summary command to enable using classless subnet mask used by VLSM and prevent conflicts.
- Configured EIGRP routing protocol numbered 100 on Cairo, Alex, and Zagazig Routers to let them communicate with each other and to let network devices communicate with each other too, reduce the time for administration, maintain the change, and match the growing in network.
- Every router has its own routing table stores connected networks and the networks that other routers notified with.

6- ACL (Access Control List):

Standard access-list

- Creates filters based on source addresses and are used for server based filtering.
- Address based access lists distinguish routes on a network you want to control by using network address number (IP).
- Address-based access lists consist of a list of addresses or address ranges and a statement as to whether access to or from that address is permitted or denied.
- Denies or Permits all services from a single host.
- Uses an assigned number from 1 to 99.
- Can be named or numbered.

Extended access lists

- Creates filters based on source addresses, destination addresses, protocol, port number and other features and are used for packet based filtering for packets that traverse the network.
- Made up of one or more access control entries, used to control network access or to specify traffic for many features to act upon.
- Much more complex, variety of fields in the packet can be compared for matching by extended access lists.

- The list is searched sequentially; the first statement matched stops the search through the list and defines the action to be taken.
- Uses an assigned number from 100 to 199.
- Can be named or numbered.
- Configured extended access-list named sl-def-acl on Cairo, Alex, and Zagazig main routers, and floor routers to disable telnet remote access to hosts which is configured by default (vty 0 4), because telnet is not very secure, it doesn't encrypt sent packets and send packets as clear text.

7- Switching

STP (Spanning Tree Protocol):

- Configured on switches to let them communicate with each other and other network devices.
- Ensures a loop-free topology for any bridged Ethernet local area network.
- Switches exchange BPDU (Bridge Protocol Data Unit) information about every connected switch in network like MAC Address Table, Priority, and Root Switch.
- Every network has only one rooted switch.
- Blocking, Listening, Learning, Forwarding and Disabled States.
- Enabled by default on switches.

- Can be disabled using port-fast command which takes the port and tell spanning tree not to implement STP on that port.
- Configured on Cairo, Alex, and Zagazig Switches BPDU guard, and root guard to prevent man-in-the-middle attack that may forward the network traffic to their host instead of switch.

RSTP (Rapid Spanning Tree Protocol):

- Provides significantly faster spanning tree convergence after a topology change.
- Introduces new high convergence behaviors and bridge port roles.
- Add an alternative port and a backup port compared to STP. These ports are allowed to immediately enter the forwarding state rather than passively wait for the network to converge.
- Activates a redundant path if the main path goes down.
- Configured on Cairo, Alex, and Zagazig switches to enable a rapid communication between them, and to reduce the time that switches goes from off state to on state.

PVSTP (Per VLAN Spanning Protocol):

- Allows a switch to have multiple spanning trees, interoperate with switches that are running a single spanning tree.
- Creates one spanning tree topology for each VLAN.
- Enabled by default on VLAN ports of switch.

RPVSTP (Rapid Per VLAN Spanning Protocol):

- Converges more quickly than PVST+ to a new spanning tree after a topology change.
- Configured on Cairo, Alex, and Zagazig switches to enable a rapid communication between them, and to reduce the time that VLANs of switches goes from off state to on state.

VTP (Virtual Trunking Protocol):

- Reduces administration in a switched network
- When configuring a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain.
- Carries VLAN information to all the switches in a VTP domain.
- Reduces the need to configure the same VLAN everywhere.
- Helps simplify management of the VLAN database across multiple switches.

DTP (Dynamic Trunking Protocol):

- Used to negotiate forming a trunk between two devices to determine if the interface should become and access port or trunk. DTP causes increased traffic.
- Access Port: takes the packets it receives and retags them, usually reserved for end-devices like hosts or servers, configured to only accept a finite number of MAC addresses in order to prevent attacks.

- Trunk Port: allows pre-tagged packets to pass through without changing the tag, generally points to either another switch or a router.

- Auto Negotiation: two connected devices choose common transmission parameters, such as speed, duplex mode, and flow control.

- Enabled by default on switches.

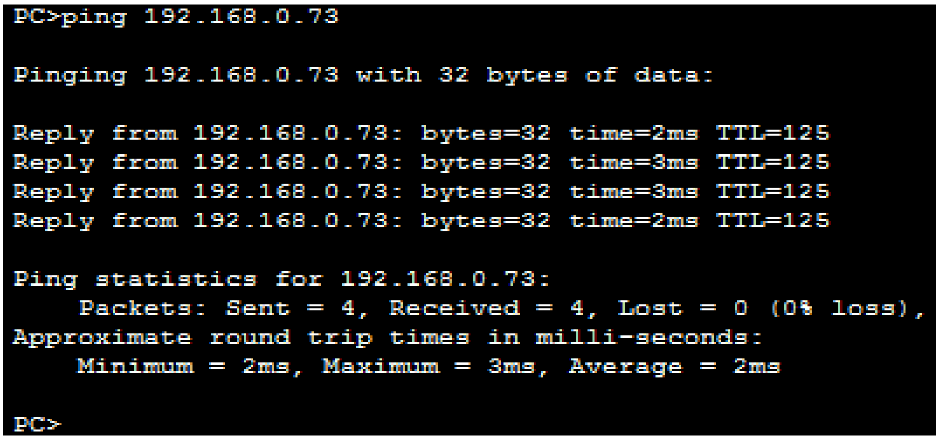
- Configured on Cairo, Alex, and Zagazig switches trunk port that connects a router port to carry traffic to or from it. Non-negotiate command to disable negotiation on this trunk port, and to prevent man-in-the-middle attack that may masquerade as a switch device, make their device as a root switch, take the traffic to them and hack the network.

8- PING

- The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response.

- It uses ICMP (Internet Change Message Protocol) echo using TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) Transport Layer Protocols on port number 7.

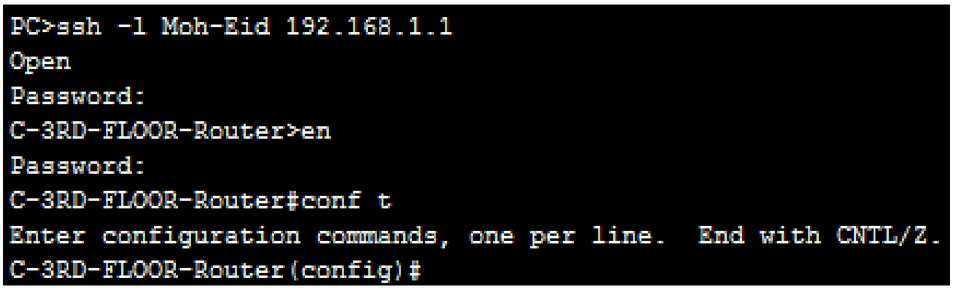
- Used between networks and branches of Cairo, Alex, and Zagazig to test connectivity and ensure that there's a communication between devices located in different networks.



```
PC>ping 192.168.0.73

Pinging 192.168.0.73 with 32 bytes of data:

Reply from 192.168.0.73: bytes=32 time=2ms TTL=125
Reply from 192.168.0.73: bytes=32 time=3ms TTL=125
Reply from 192.168.0.73: bytes=32 time=3ms TTL=125
Reply from 192.168.0.73: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.0.73:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

PC>
```

9- SSH (Secure Shell):

- Secure protocol that encrypts all data sent between the client computer and the computer it is connecting to.
- Allows a user to run commands on a machine's command prompt without them being physically present near the machine.
- Uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user.
- It uses TCP Transport Layer Protocol on port number 22.
- Configured on Cairo, Alex, and Zagazig routers and switches to enable remote and secure access to them from anywhere inside or outside the network. Set execution timeout which will close the connected session after a specific period of time (30 Minutes) to increase the security of connection and not to waste the network bandwidth.



```
PC>ssh -l Moh-Eid 192.168.1.1
Open
Password:
C-3RD-FLOOR-Router>en
Password:
C-3RD-FLOOR-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
C-3RD-FLOOR-Router(config)#
```

10- DHCP (Dynamic Host Configuration Protocol):

- Used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
- It uses UDP Transport Layer Protocol on port number 67.
- Configured on Cairo, Alex, and Zagazig floor routers and DHCP Server to enable dynamic distribution of IP Addresses to connected hosts in the network rather than configuring IP Addresses statically. Enable DHCP Snooping on switch ports that connect host that get their IP Addresses from Router DHCP.

11- NAT (Network Address Translation):

- Remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
- Remapping from Private (non-routable) IP Address to Public or Real (routable) IP Address or reverse to enable LAN or WAN communication.

  Static NAT:

  - Private IP address is mapped to a public IP address, where the public address is always the same IP address
  - This allows an internal host, such as a Web server, to have an unregistered (private) IP address and still be reachable over the Internet.
  - One-to-one mapping from one IP subnet to another IP subnet.

Dynamic Nat:

- Private IP address is mapped to a public IP address drawing from a pool of registered (public) IP addresses.
- The NAT router in a network will keep a table of registered IP addresses, and when a private IP address requests access to the Internet, the router chooses an IP address from the table that is not at the time being used by another private IP address.

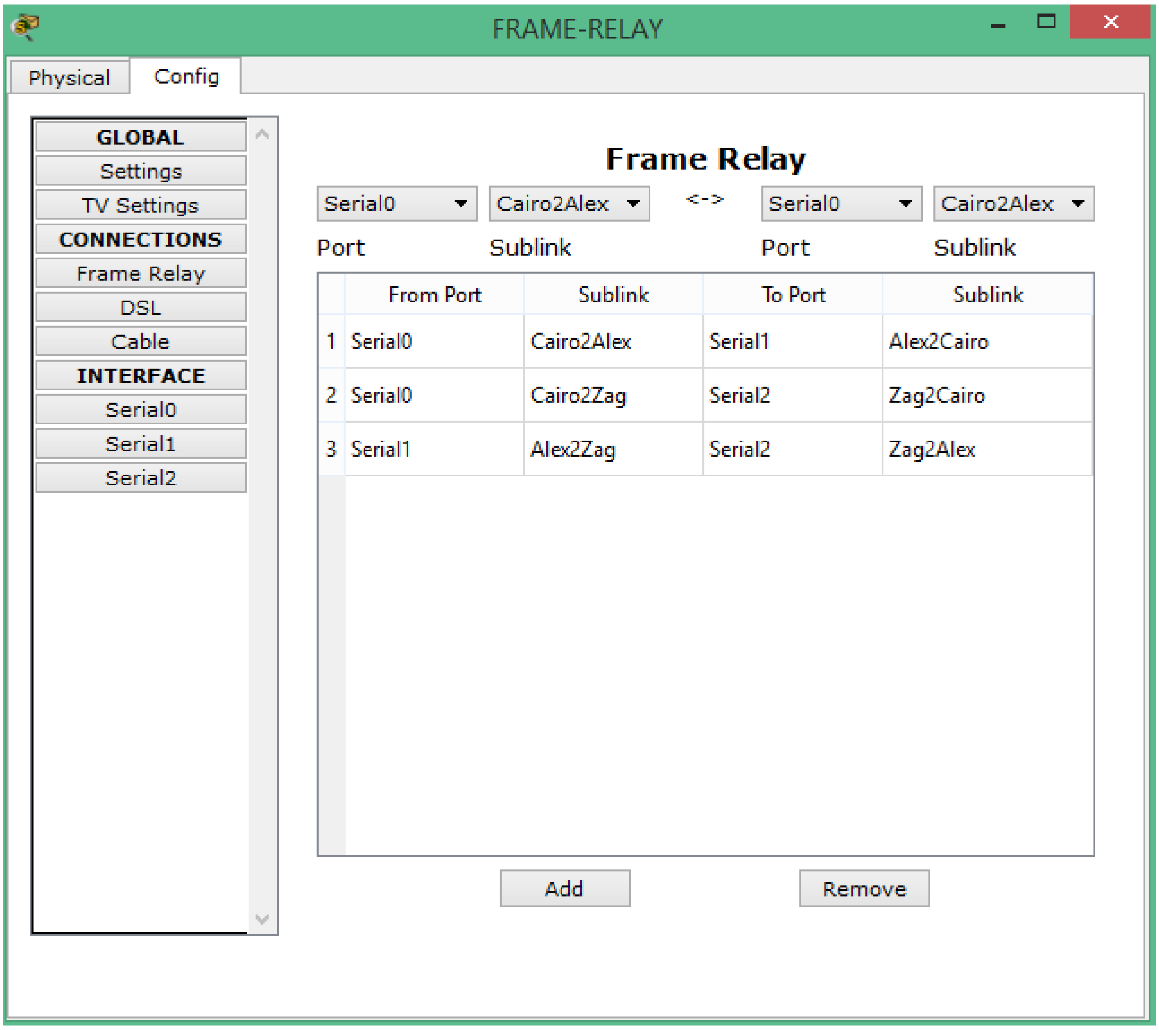
PAT (Port address translation):

- Only one public IP address assigned to the network, and so all devices inside this network would share this one public IP Address when using the internet.
- The NAT device will use the PAT method to look up the port information which maps to the internal computer requesting it.
- Configured on Cairo, Alex, and Zagazig main router to enable internal device go to internet and communicate with other devices from internet or from other company branches. Access Control List is configured to permit internal devices use NAT Technology.

12- Frame-Relay:

- Frame Relay is an industry-standard, switched data link layer protocol that handles multiple virtual circuits using High-Level Data Link Control (HDLC) encapsulation between connected devices.

- Each virtual circuit is identified by a Data Link Connection Identifier (DLCI), which is simply a number between 0 and 1023.
- Frame Relay provides greater bandwidth, reliability, and resiliency than private or leased lines. Cost Effectiveness, and Flexibility.
- Mapping router’s interfaces IP Addresses into DLCI Numbers.
- DTE (Data Terminal Equipment): device that ends a communication line, source device, destination device, device that creates data for communication with others, end devices, PCs, Servers or portable devices.
- DCE (Data Communications Equipment): provides a path for communication, interconnecting devices, routers, switches or bridges.
- Configured a Point to multi-point Frame-Relay between the three branches, Cairo, Alex, and Zagazig branches. Assign DLCI numbers to different connections between these branches:
- DLCI 101: Connection from Cairo Branch to Alex Branch.
- DLCI 102: Connection from Cairo Branch to Zagazig Branch.
- DLCI 201: Connection from Alex Branch to Cairo Branch.
- DLCI 202: Connection from Alex Branch to Zagazig Branch.
- DLCI 301: Connection from Zagazig Branch to Cairo Branch.
- DLCI 302: Connection from Zagazig Branch to Alex Branch.



Frame Relay

Port: Serial0 | Sublink: Cairo2Alex <-> Port: Serial0 | Sublink: Cairo2Alex

	From Port	Sublink	To Port	Sublink
1	Serial0	Cairo2Alex	Serial1	Alex2Cairo
2	Serial0	Cairo2Zag	Serial2	Zag2Cairo
3	Serial1	Alex2Zag	Serial2	Zag2Alex

13- VPN (Virtual Private Network):

- Network allows connectivity between two devices. Those two devices could be computers on the same local-area network or could be connected over a wide area network.

- Each user could connect to his local side and communicate with each other over the dedicated link.

- Security, Reliability, Scalability, Improve productivity.

- IPsec: implements security of IP packets at Layer 3 of the OSI model, and can be used for site-to-site VPNs and remote-access VPNs. Works at the network layer, protecting and authenticating IP packets. It is a framework of open standards which is algorithm-independent. It provides data confidentiality, data integrity, and origin authentication. Compatible with all IP-based applications, Key Length from 56 to 256 bits, Two-Way authentication using shared secrets or digital certificates, and only specific devices with specific configurations can connect.

- ➢ Authentication: the assurance to one entity that another entity is who they claim to be. Using HMAC-SHA-1.
- ➢ Integrity: the assurance to an entity that data has not been altered between sender and receiver. Using SHA.
- ➢ Confidentiality: the assurance to an entity that no one can read particular piece of data except the receiver. Using AES (Advanced Encryption Standard).

Remote-access VPN:

- ➢ VPN remote connection from individual computer to inside company devices.
- ➢ Can use IPsec or SSL technologies for their VPN.
- ➢ Called a Virtual Private Dial-up Network (VPDN), this is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations.
- ➢ Typically, a corporation that wishes to set up a large remote-access VPN provides some form of Internet dial-up account to their users using an Internet service provider (ISP).

- Configured on the three branches to enable secure connection from a remote host outside these branches that can access inside branch hosts. It can be initiated from a PC, Laptop, or any portable device.

Site-to-site VPN:

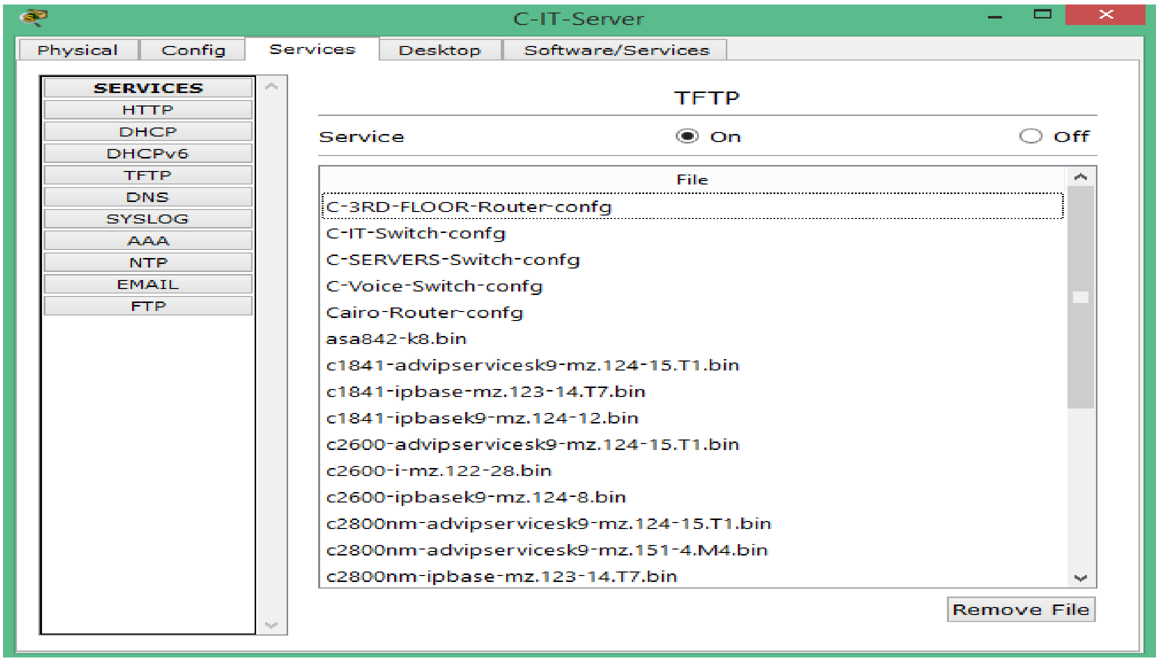
- VPN implementation by companies that may have two or more sites that they want to connect securely together (likely using the Internet) so that each site can communicate with the other site or sites.
- Uses a collection of VPN technologies called IPsec.
- Each site needs only a local connection to the same public network, thereby saving money on long private leased-lines.
- Configured between Cairo, Alex, and Zagazig to provide a secure connection between them with the help of ISP (Internet Service Provider) equipment.
- ISAKMP (Internet Security Association and Key Management Protocol): is a protocol used for establishing Security Associations (SA) and cryptographic keys in an Internet environment. Only provides a framework for authentication and key exchange and is designed to be key exchange independent. ISAKMP defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques. ISAKMP defines procedures and packet formats to establish, negotiate, modify and delete Security Associations.
- Encryption: Using AES 128-bits.

- Hash: HMAC-SHA-1 160-bits.
- Authentication: Pre-Shared key.
- Group 5: Diffie-Hellman 1536-bits.

14- Cisco IOS Files:

- FLASH Memory: This is where the IOS is stored. When a router is powered down, the contents of Flash memory are not lost.
- NVRAM: Non-Volatile Random Access Memory (NVRAM) is used as the storage location for the router's startup configuration file. This is where the configuration is saved when you type copy run start. After the router loads its IOS image, the settings found in the startup configuration are applied.
- RAM: Random Access Memory (RAM) represents the non-permanent or volatile working area of memory on a Cisco router.
- ROM: stands for Read Only Memory. Used to store the IOS software. ROM is used as the memory area from which a Cisco router begins the boot process, and is made up of a number of elements. When a valid IOS image cannot be found in Flash or on a TFTP server.
- Configured on Cairo, Alex, and Zagazig routers and switches to protect IOS Images, Boot Images, Running Configurations, and Basic Configurations from being lost. Using Write Memory Command stores the running configurations in the NVRAM to prevent them from being lost. Using the TFTP (Trivial File Transfer Protocol) Server located in every department to take a copy from the running configurations as a Backup to use it when there’s a loss in any device IOS.

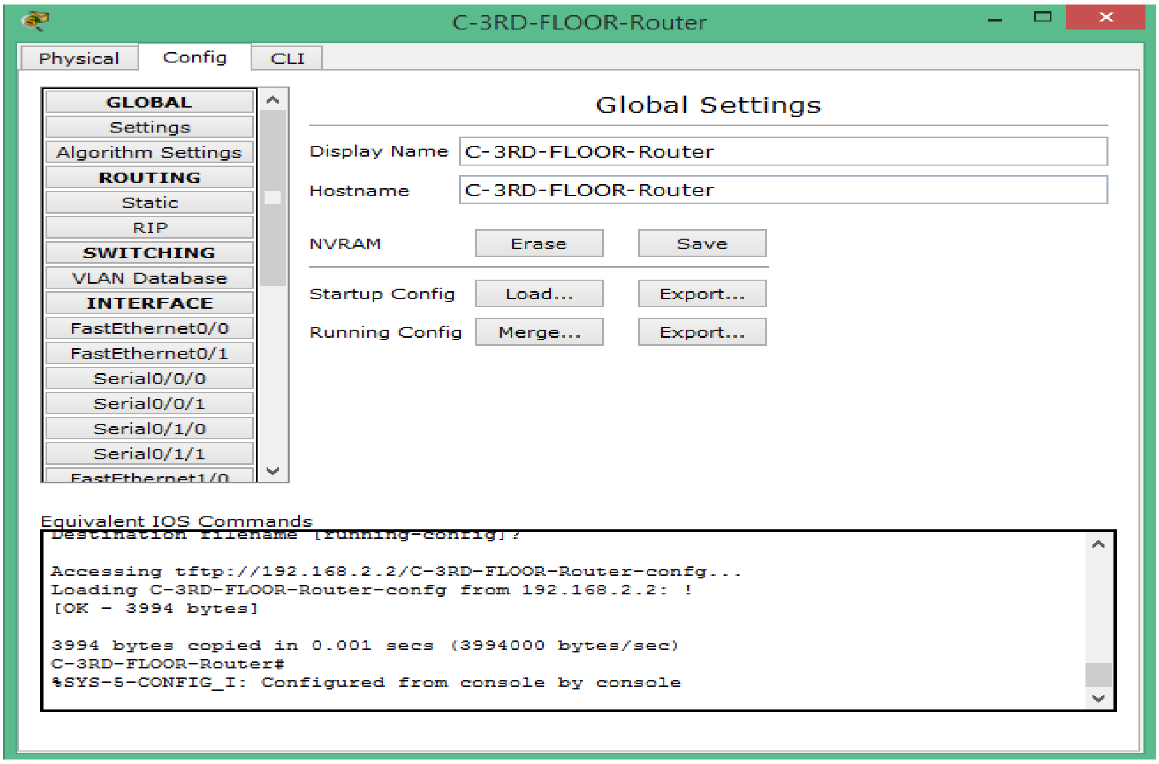
The TFTP server located in IT department which is used to save and take a backup of the running configurations of routers and switches.



Service ● On ○ Off

File
C-3RD-FLOOR-Router-confg
C-IT-Switch-confg
C-SERVERS-Switch-confg
C-Voice-Switch-confg
Cairo-Router-confg
asa842-k8.bin
c1841-advipservicesk9-mz.124-15.T1.bin
c1841-ipbase-mz.123-14.T7.bin
c1841-ipbasek9-mz.124-12.bin
c2600-advipservicesk9-mz.124-15.T1.bin
c2600-i-mz.122-28.bin
c2600-ipbasek9-mz.124-8.bin
c2800nm-advipservicesk9-mz.124-15.T1.bin
c2800nm-advipservicesk9-mz.151-4.M4.bin
c2800nm-ipbase-mz.123-14.T7.bin

Some options that can be done on the router to do a specific action related to NVRAM, Startup Configurations, or The Running Configurations.



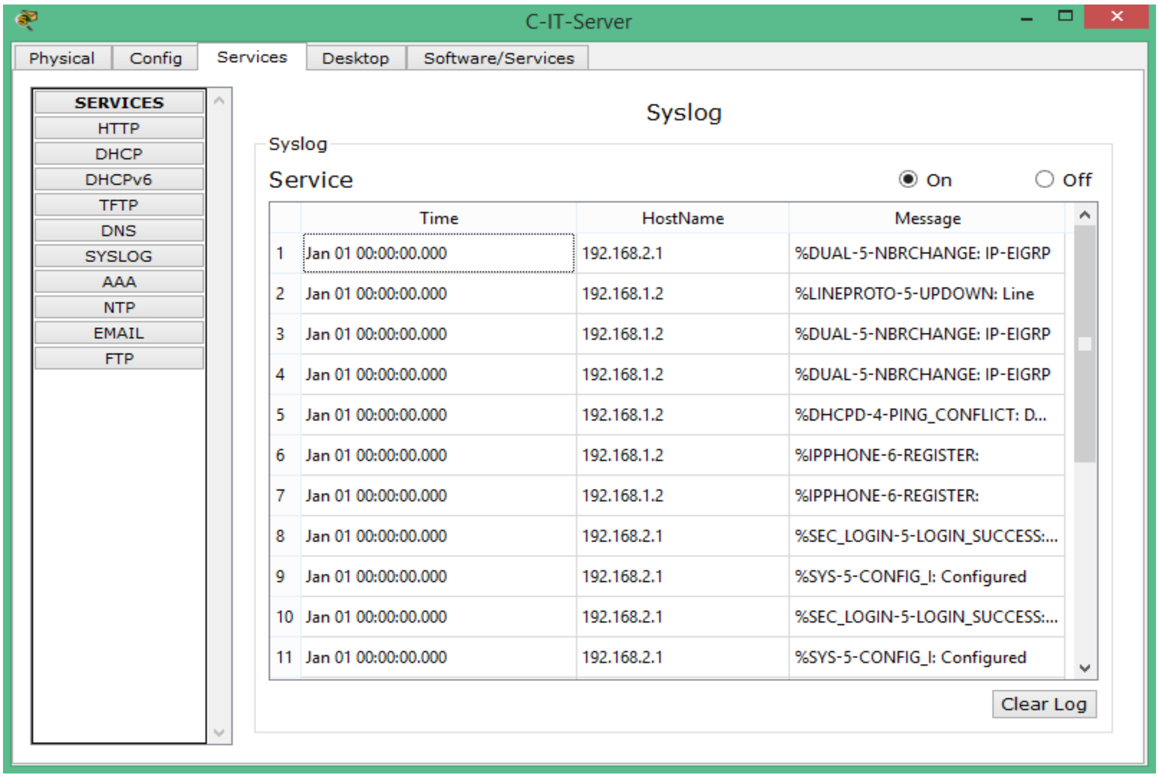
Display Name: C-3RD-FLOOR-Router

Hostname: C-3RD-FLOOR-Router

```
Destination filename [running-config]?

Accessing tftp://192.168.2.2/C-3RD-FLOOR-Router-confg...
Loading C-3RD-FLOOR-Router-confg from 192.168.2.2: !
[OK - 3994 bytes]

3994 bytes copied in 0.001 secs (3994000 bytes/sec)
C-3RD-FLOOR-Router#
%SYS-5-CONFIG_I: Configured from console by console
```

15-SYSLOG:

- Used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them.
- Used for system management and security auditing as well as general informational, analysis, and debugging messages.
- Can be enabled locally on router, switch, or a centralized server that stores these log messages generated from any device and some actions.
- Configured on Cairo, Alex, and Zagazig routers and switches to log every actions executed by these device. Let Admin determine what happened by observing log server and by checking the IP Address of the host that made this change, time, date, and the action. Every department has its own SYSLOG Server that stores logs from connected switch and router. The IT department SYSLOG Server stores logs from Main Router, Servers Switch, and Voice Switch.



Syslog

Syslog

Service ● On ○ Off

	Time	HostName	Message
1	Jan 01 00:00:00.000	192.168.2.1	%DUAL-5-NBRCHANGE: IP-EIGRP
2	Jan 01 00:00:00.000	192.168.1.2	%LINEPROTO-5-UPDOWN: Line
3	Jan 01 00:00:00.000	192.168.1.2	%DUAL-5-NBRCHANGE: IP-EIGRP
4	Jan 01 00:00:00.000	192.168.1.2	%DUAL-5-NBRCHANGE: IP-EIGRP
5	Jan 01 00:00:00.000	192.168.1.2	%DHCPD-4-PING_CONFLICT: D...
6	Jan 01 00:00:00.000	192.168.1.2	%IPPHONE-6-REGISTER:
7	Jan 01 00:00:00.000	192.168.1.2	%IPPHONE-6-REGISTER:
8	Jan 01 00:00:00.000	192.168.2.1	%SEC_LOGIN-5-LOGIN_SUCCESS:...
9	Jan 01 00:00:00.000	192.168.2.1	%SYS-5-CONFIG_I: Configured
10	Jan 01 00:00:00.000	192.168.2.1	%SEC_LOGIN-5-LOGIN_SUCCESS:...
11	Jan 01 00:00:00.000	192.168.2.1	%SYS-5-CONFIG_I: Configured

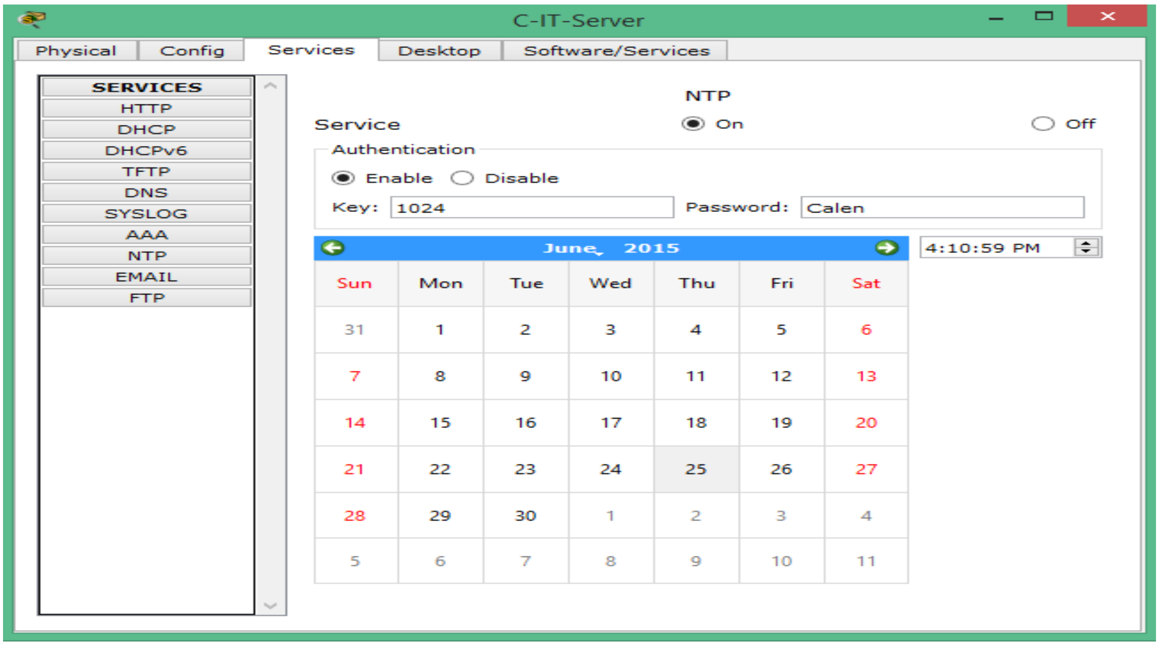
16- NTP (Network Time Protocol):

- Networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

- NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).

- Fault-tolerant protocol that will automatically select the best of several available time sources to synchronize to.

- Configured on Cairo, Alex, and Zagazig routers and switches to set the date and the time. Used to complement the SYSLOG Server so that the Administrator can know the exact date and time of a specific action executed by the router or the switch. It’s configured on a specific server located in every department. The main router, the servers switch, and the voice switch use IT Server NTP to set date and time. Every floor router and department switch uses its connected NTP Server to set date and time. Using 1024-Bits authentication key, MD5 Algorithm to increase the security between devices and to ensure that there’s a secure connection between the device and the server which ensure Integrity.



NTP

Service ● On ○ Off

Authentication

● Enable ○ Disable

Key: 1024 Password: Calen

June 2015 4:10:59 PM

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

17- SNMP (Simple Network Management Protocol):

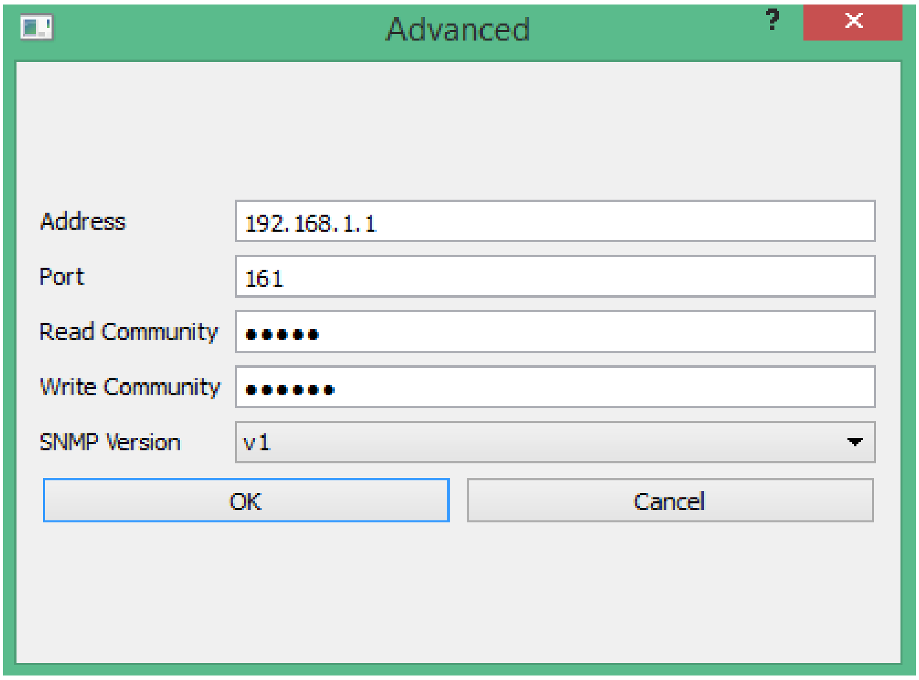
- Internet-standard protocol for managing devices on IP networks.

- Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.

- The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP.

- The SNMP agent is the software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems.

- Configured on Cairo, Alex, and Zagazig routers and switches to enable Administrator of the network manage this network and troubleshoot it from a host using MIB Browser that accept some parameters like The IP Address of router or switch, The Port Number, The Read Community Word which enable read operations like the device up-time, and The Write Community Word which enable Read & Write operations like device name.



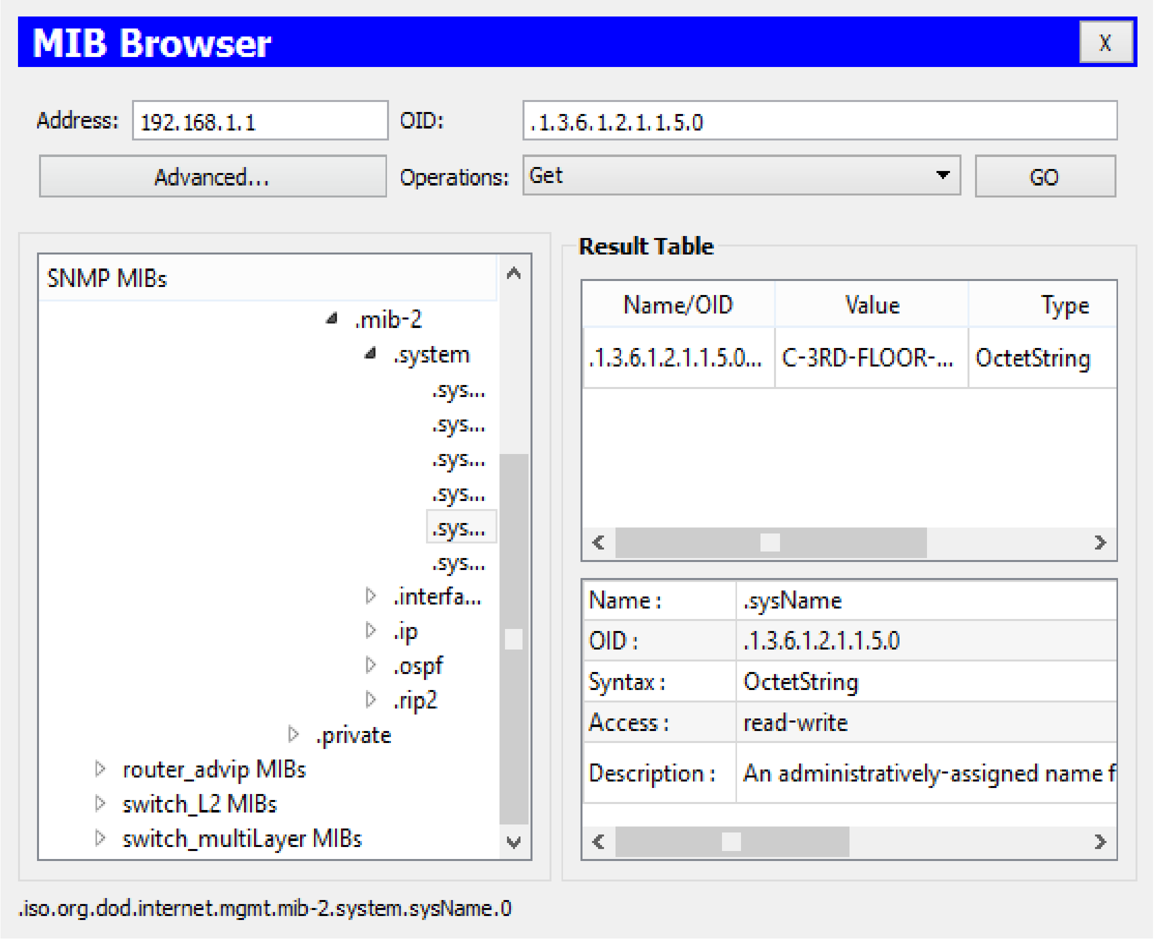
Address: 192.168.1.1

Port: 161

Read Community: •••••

Write Community: ••••••

SNMP Version: v1



Address: 192.168.1.1

OID: .1.3.6.1.2.1.1.5.0

Operations: Get

Result Table

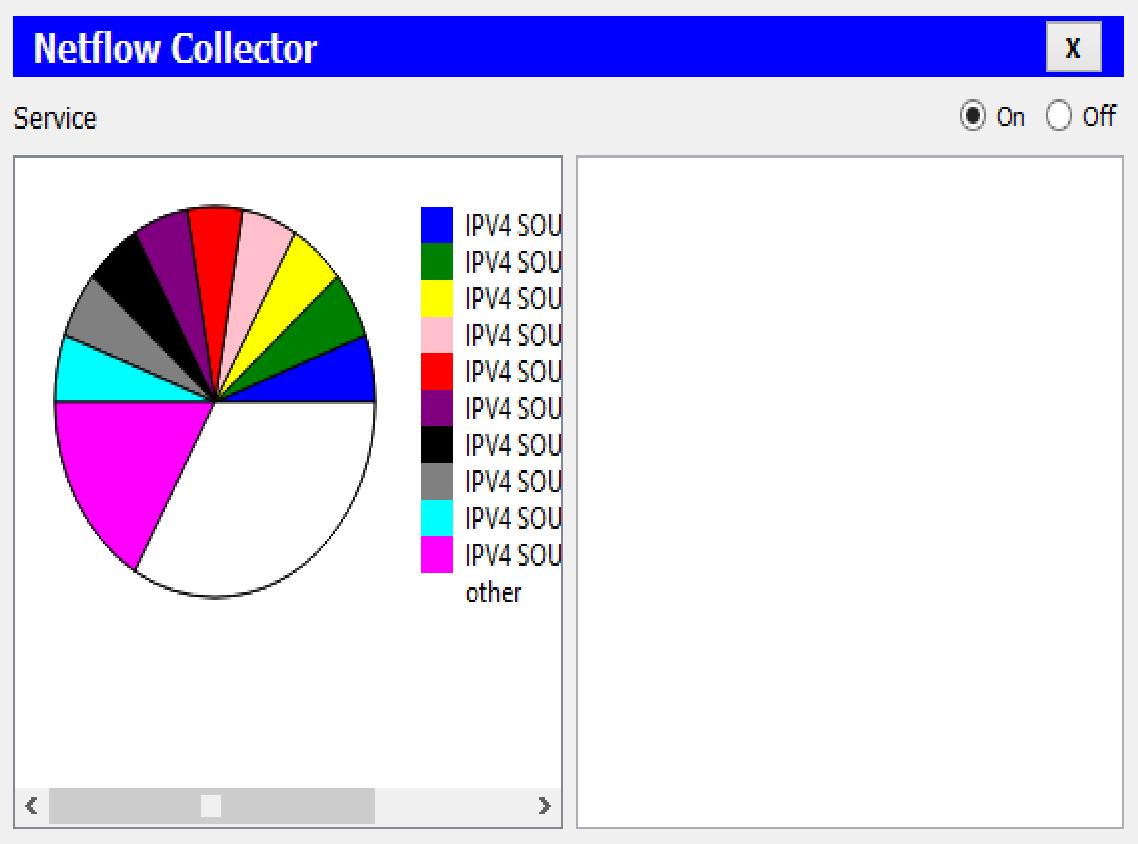
Name/OID	Value	Type
.1.3.6.1.2.1.1.5.0...	C-3RD-FLOOR-...	OctetString

Name :	.sysName
OID :	.1.3.6.1.2.1.1.5.0
Syntax :	OctetString
Access :	read-write
Description :	An administratively-assigned name f

.iso.org.dod.internet.mgmt.mib-2.system.sysName.0

18- Net-Flow:

- Embedded instrumentation within Cisco IOS Software to characterize network operation.
- Provides the ability to collect IP network traffic as it enters or exits an interface.
- Flow exporter: aggregates packets into flows and exports flow records towards one or more flow collectors.
- Flow collector: responsible for reception, storage and pre-processing of flow data received from a flow exporter.
- Analysis application: analyzes received flow data in the context of intrusion detection or traffic profiling, for example.
- Net-Flow records are traditionally exported using User Datagram Protocol (UDP) and collected using a Net-Flow collector.
- Configured on Cairo, Alex, and Zagazig routers and switches to inform the Administrator of the network about the traffic that devices do, utilize the bandwidth of the network, observe the network well to detect outside attack like denial of service or flood attack which break down the network. Every server located in specific department is responsible for collecting information about the traffic entering and leaving this department. IT Department Server collects information about the traffic coming from or going to Main Router, Server Switch, and The Voice Switch.



Netflow Collector

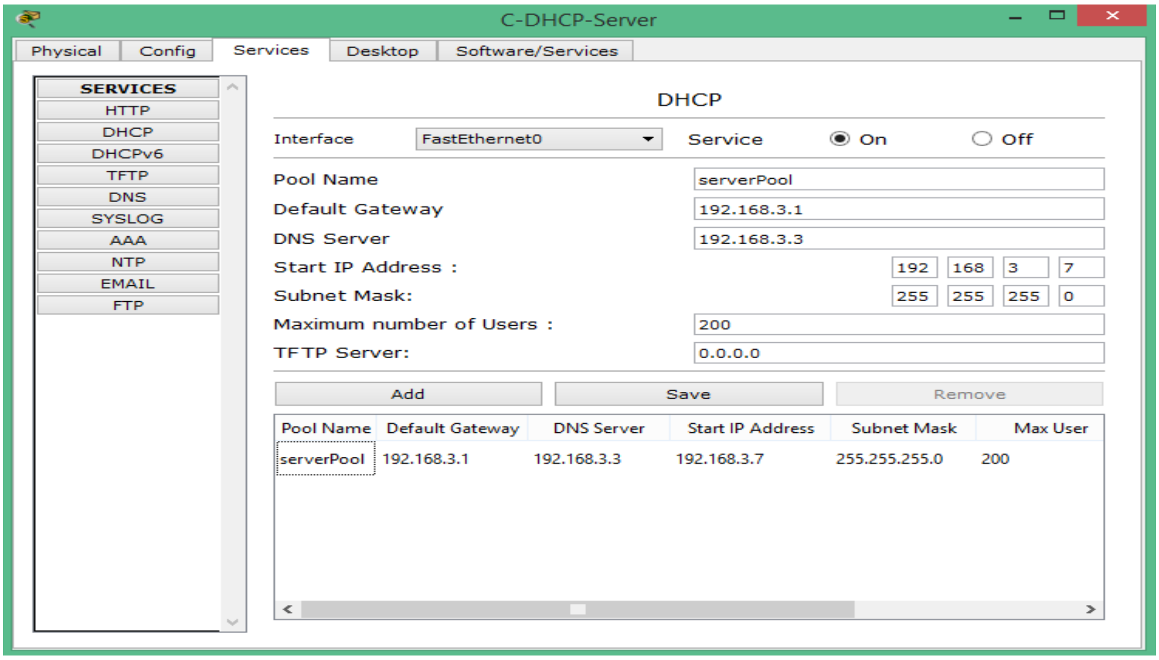
Service ● On ○ Off

19- HDLC (High-Level Data Link Control):

- Transmission protocol used at the data link layer (layer 2) of the OSI seven layer model for data communications. Switched and non-switched protocol.
- Configured by default on cisco devices to enable communication between them. It's a point to point protocol. It's used in WAN Technologies for data exchange between inside LANs cisco devices.
- HDLC are also used for the public networks that use the communications protocol and for frame relay, a protocol used in both and wide area network, public and private.

20- DHCP Server:

- Automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
- Configured on Cairo, Alex, and Zagazig branches and connected to Servers switch to assign IPs to connected hosts.

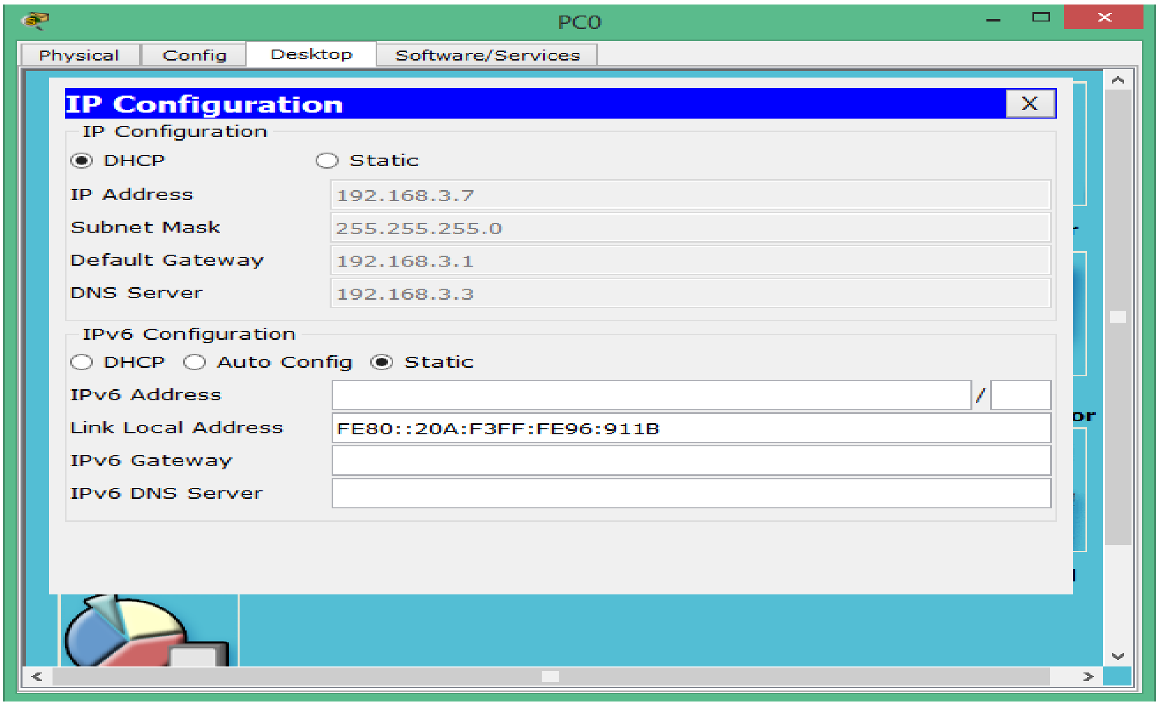


DHCP

Interface: FastEthernet0 — Service: ● On ○ Off

Pool Name	serverPool
Default Gateway	192.168.3.1
DNS Server	192.168.3.3
Start IP Address :	192 168 3 7
Subnet Mask:	255 255 255 0
Maximum number of Users :	200
TFTP Server:	0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User
serverPool	192.168.3.1	192.168.3.3	192.168.3.7	255.255.255.0	200



IP Configuration

● DHCP ○ Static

IP Address	192.168.3.7
Subnet Mask	255.255.255.0
Default Gateway	192.168.3.1
DNS Server	192.168.3.3

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

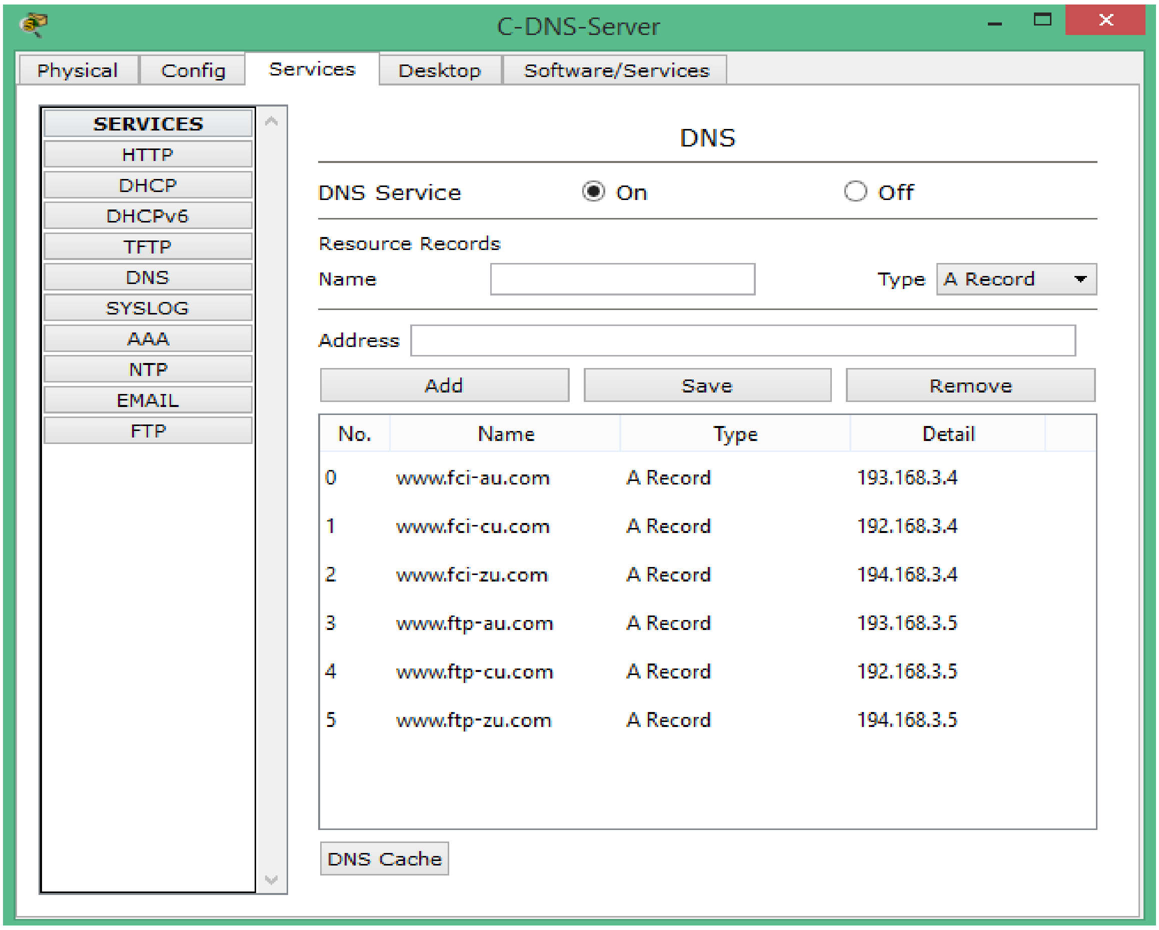
IPv6 Address	/
Link Local Address	FE80::20A:F3FF:FE96:911B
IPv6 Gateway	
IPv6 DNS Server	

21- Domain Name System (DNS) Server:

- Computer hardware or software server that implements a network service for providing responses to queries against a directory service.

- It translates an often humanly-meaningful, text-based identifier to a system-internal, often numeric identification or addressing component.

- Configured on Cairo, Alex, and Zagazig DNS Servers to provide resolution of branches web sites by writing a name in the using URL instead of using IP Addresses that may be forgettable.



DNS Service ● On ○ Off

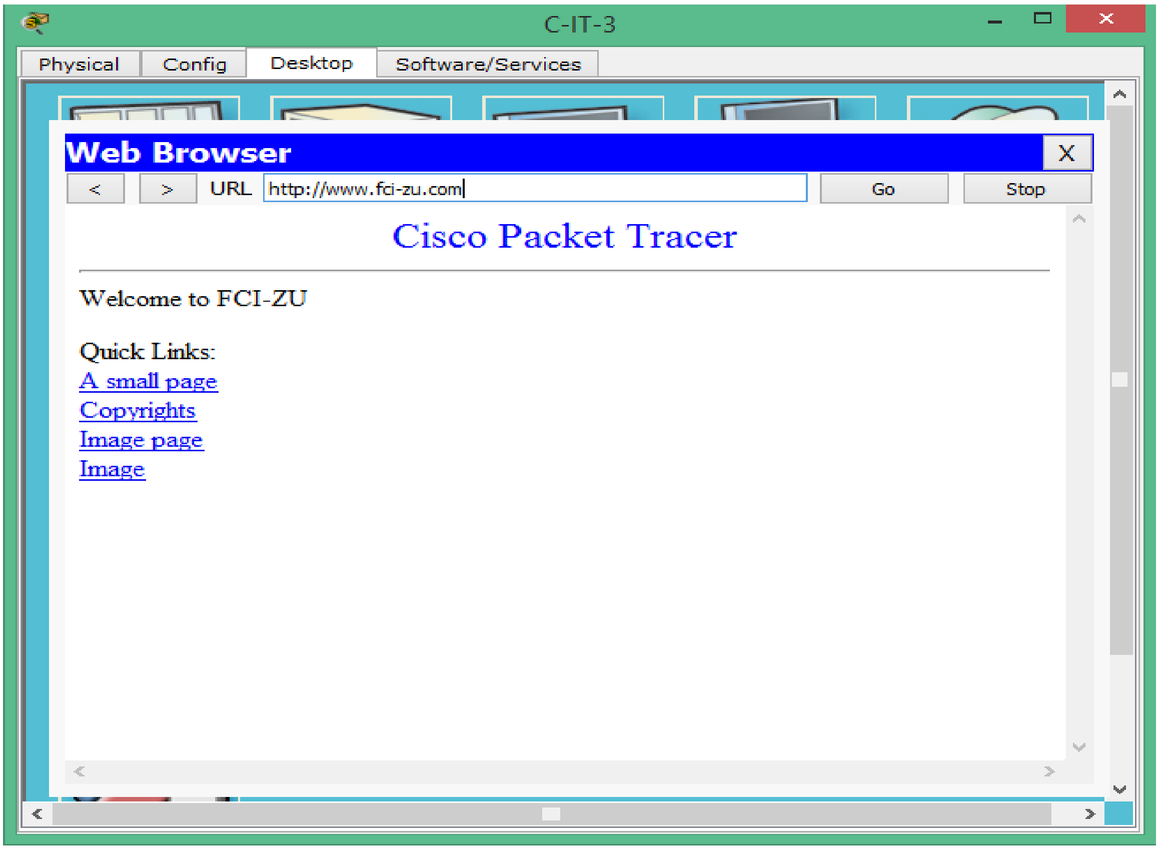
Resource Records

Name

Type A Record

Address

No.	Name	Type	Detail
0	www.fci-au.com	A Record	193.168.3.4
1	www.fci-cu.com	A Record	192.168.3.4
2	www.fci-zu.com	A Record	194.168.3.4
3	www.ftp-au.com	A Record	193.168.3.5
4	www.ftp-cu.com	A Record	192.168.3.5
5	www.ftp-zu.com	A Record	194.168.3.5

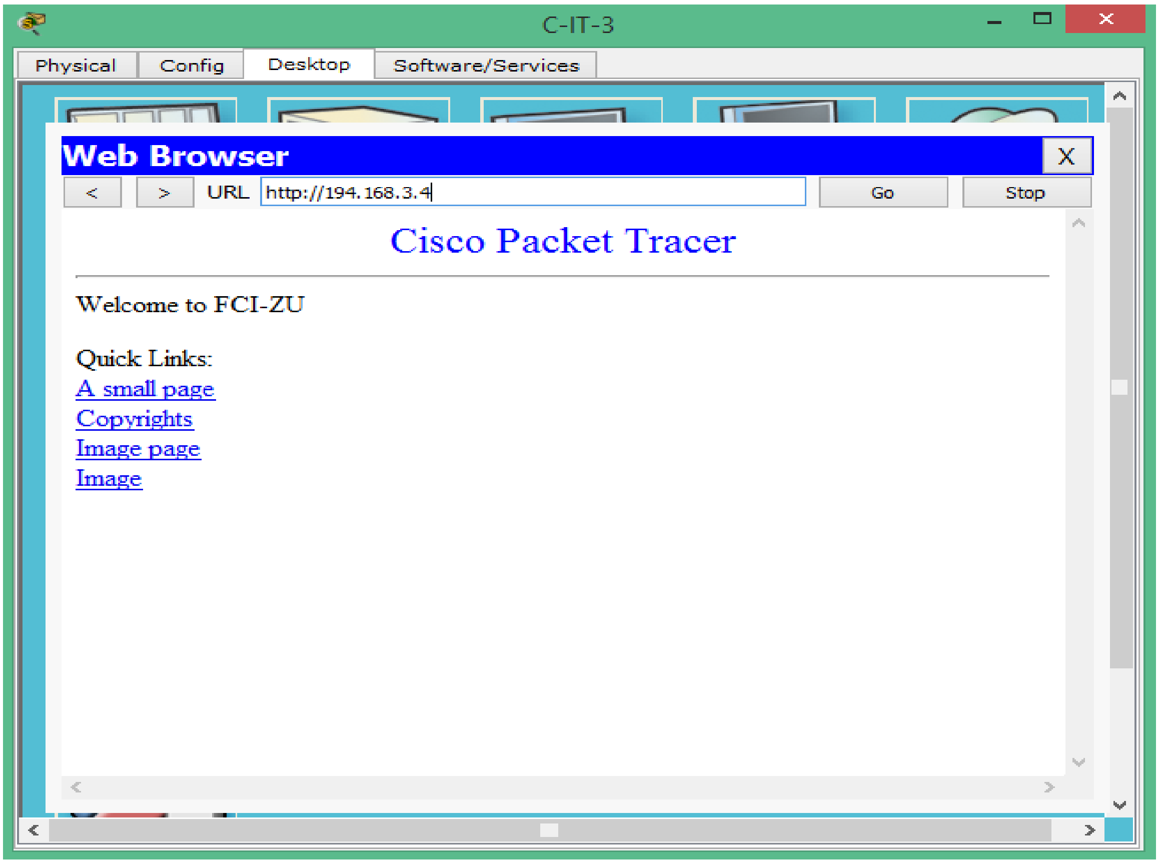


http://www.fci-zu.com

Cisco Packet Tracer

Welcome to FCI-ZU

Quick Links:
A small page
Copyrights
Image page
Image



http://194.168.3.4

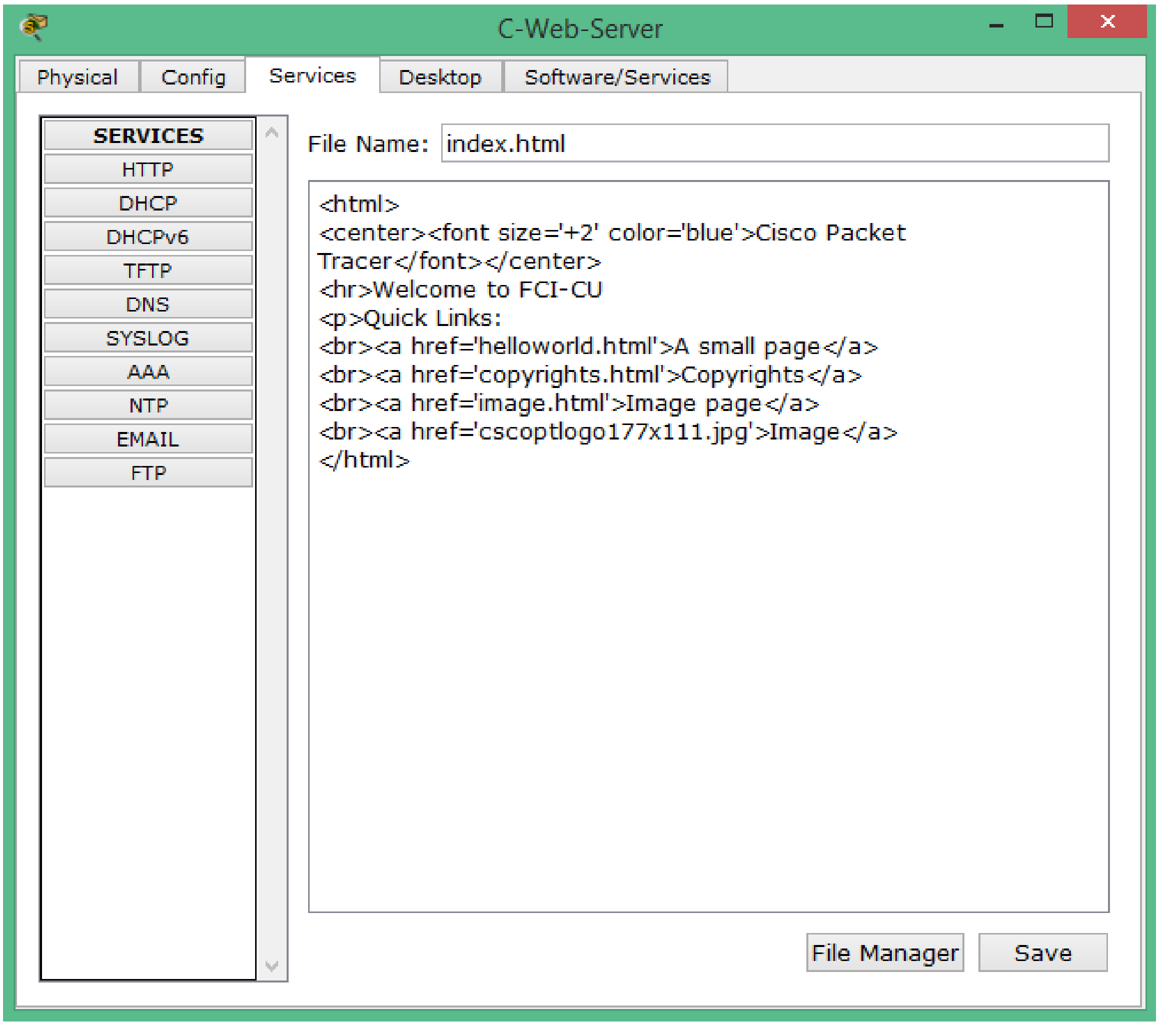
Cisco Packet Tracer

Welcome to FCI-ZU

Quick Links:
A small page
Copyrights
Image page
Image

22- Web Server:

- Information Technology that processes requests via HTTP, the basic network protocol used to distribute information on the World Wide Web.
- The primary function of a web server is to store, process and deliver web pages to clients.
- The communication between client and server takes place using the Hypertext Transfer Protocol (HTTP).
- Pages delivered are most frequently HTML documents, which may include images, style sheets and scripts in addition to text content.



File Name: index.html

```
<html>
<center><font size='+2' color='blue'>Cisco Packet
Tracer</font></center>
<hr>Welcome to FCI-CU
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

23- E-mail Server:

- Application that receives incoming e-mail from local users (people within the same domain) and remote senders and forwards outgoing e-mail for delivery.
- A mail server usually consists of a storage area where e-mail is stored for local users.
- Every email that is sent passes through a series of mail servers along its way to its intended recipient.

- **Simple Mail Transfer Protocol (SMTP)**:

  - TCP/IP protocol used in sending and receiving e-mail.

  - SMTP usually is implemented to operate over Internet port 25.

  - Handles outgoing e-mail, and is used in conjunction with a POP3 incoming e-mail server.

- **Post Office Protocol 3 (POP 3)**:

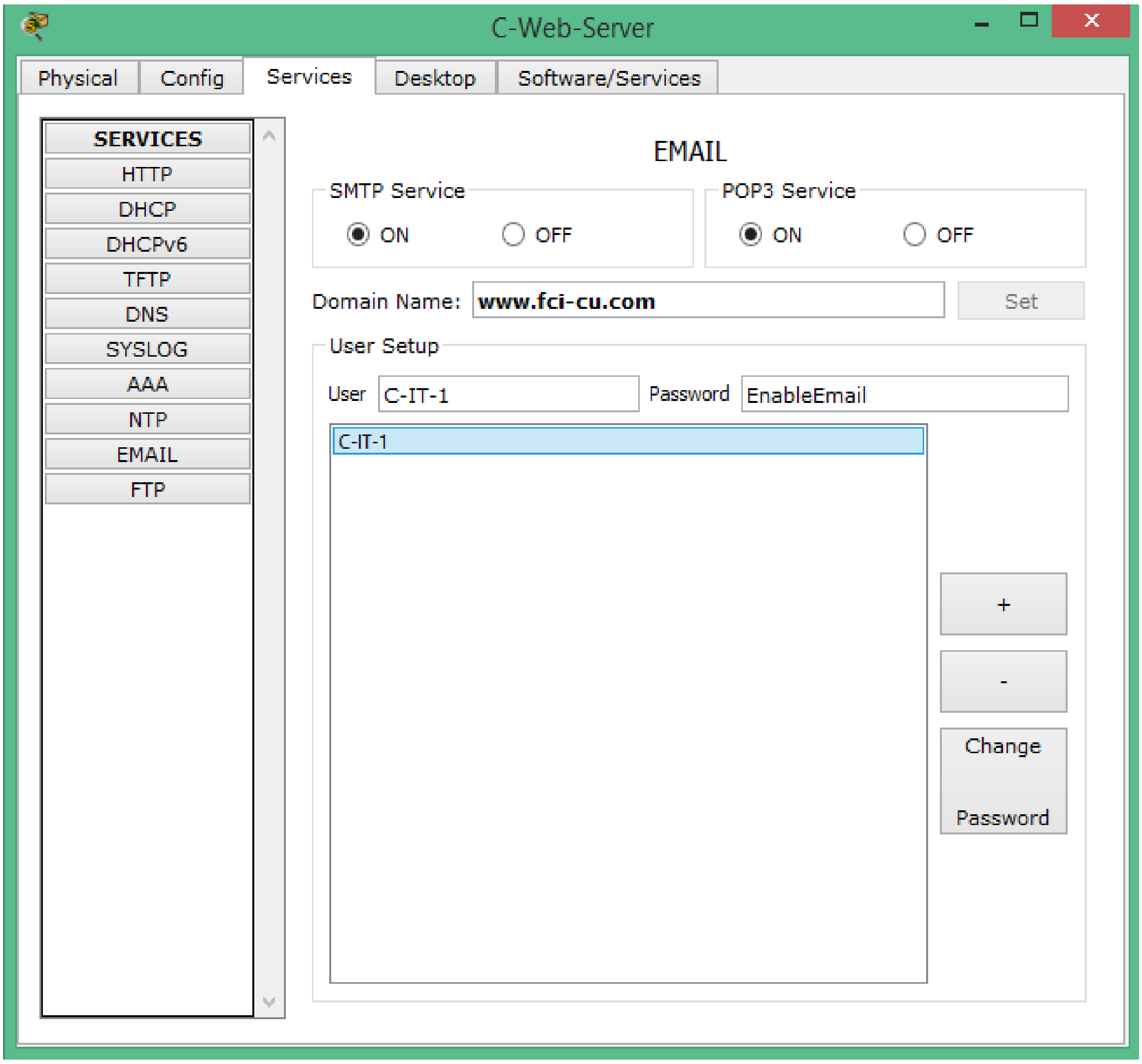
  - It is a client/server protocol in which e-mail is received and held for you by your Internet server.

  - Holds incoming e-mail messages until you check your e-mail, at which point they're transferred to your computer.

  - It is the most common account type for personal e-mail.

  - It is usually implemented to operate over Internet port 110.

- Configured on Cairo, Alex, and Zagazig Mail Servers to enable mail exchange between hosts inside and outside branches using specific username, password, and domain name. SMTP and POP3 are used for email exchange between these hosts.



EMAIL

SMTP Service: ● ON ○ OFF

POP3 Service: ● ON ○ OFF

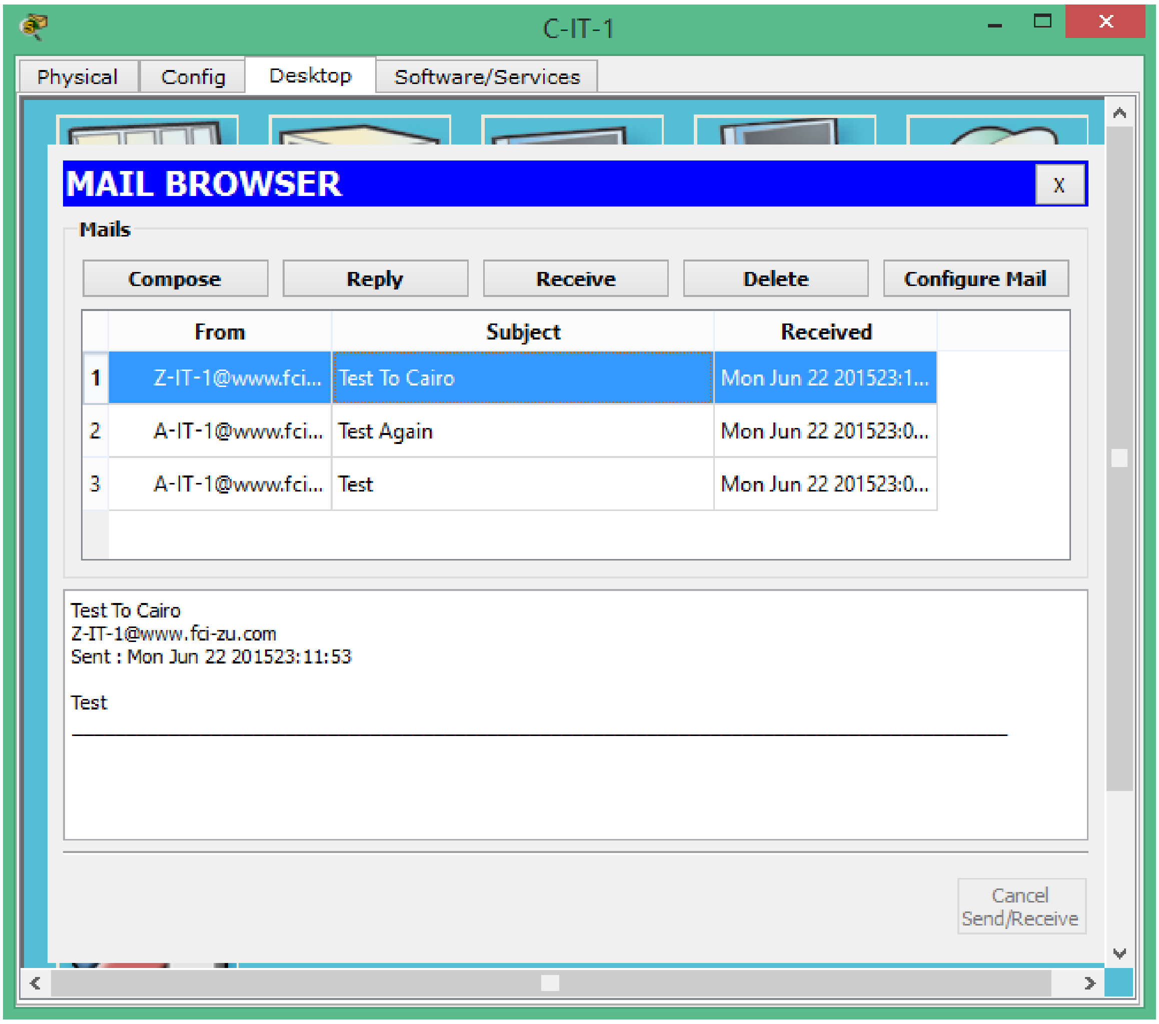
Domain Name: www.fci-cu.com

User Setup

User C-IT-1 Password EnableEmail

C-IT-1

- Email Application on Cairo Branch Host that allows transmitting and receiving emails from different hosts in the other branches Alex, and Zagazig.



	From	Subject	Received
1	Z-IT-1@www.fci...	Test To Cairo	Mon Jun 22 201523:1...
2	A-IT-1@www.fci...	Test Again	Mon Jun 22 201523:0...
3	A-IT-1@www.fci...	Test	Mon Jun 22 201523:0...

Test To Cairo
Z-IT-1@www.fci-zu.com
Sent : Mon Jun 22 201523:11:53

Test

24- File Transfer Protocol (FTP) Server:

- Standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet.

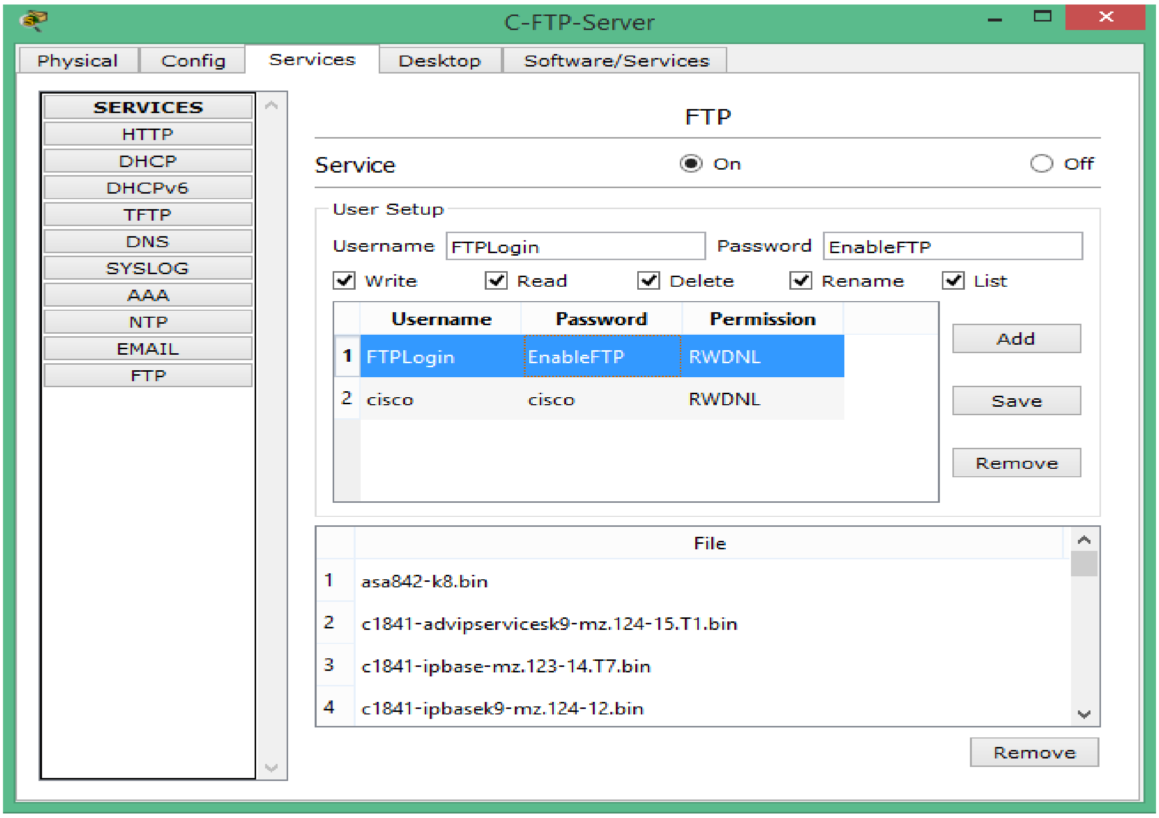
- It is built on a client-server architecture and uses separate control and data connections between the client and the server.

- Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as Web page editors.

- It uses TCP or UDP port 20 for data transfer, and TCP port 21 for control.

- FTP login utilizes a normal username and password scheme for granting access. The username is sent to the server using the USER command, and the password is sent using the PASS command.

- Configured on Cairo, Alex, and Zagazig FTP Servers to enable data exchange between hosts inside and outside branches. FTP Server has a database which stores usernames, passwords, permissions (Write, Read, Delete, Rename, or List), and Files that can be accessed from a specific host with the help of The DNS Server which resolves a specific name to the corresponding IP Address of the FTP Server inside the different branches.



Service ● On ○ Off

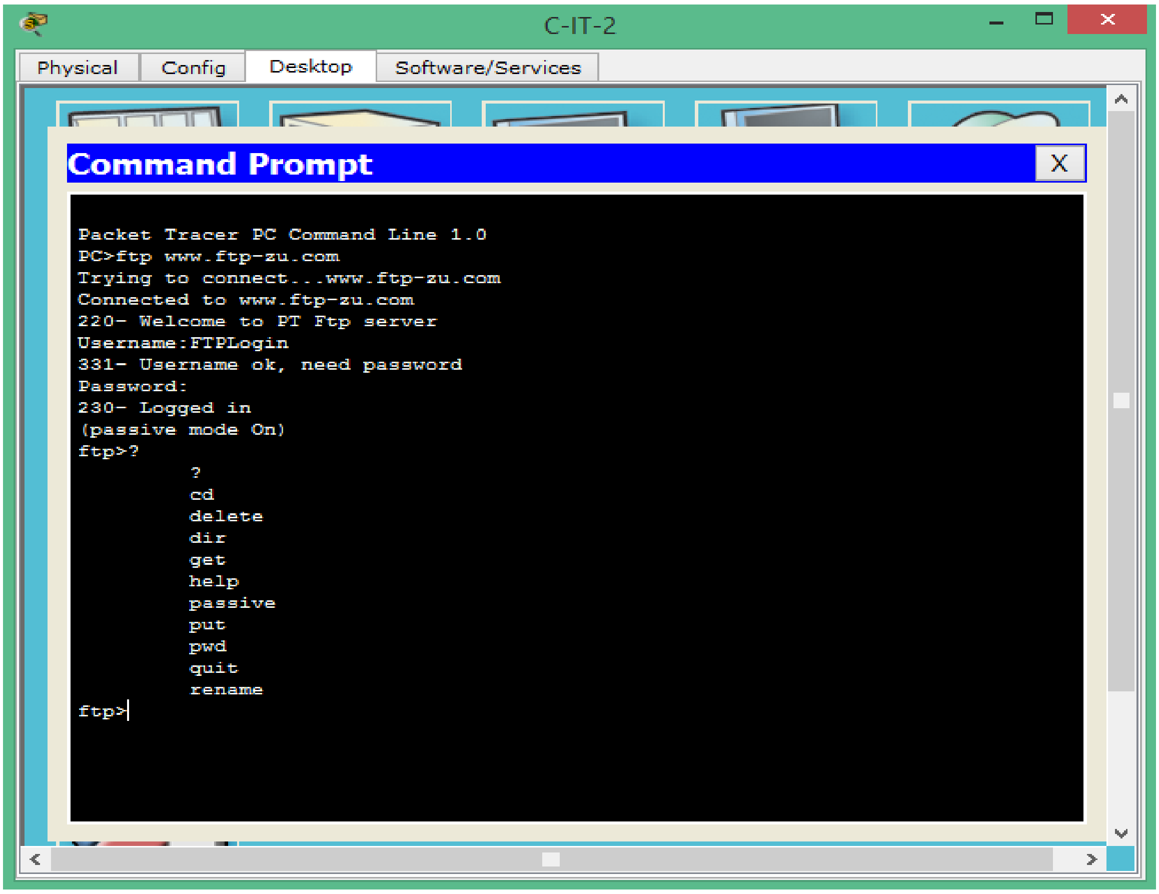
User Setup

Username FTPLogin Password EnableFTP

☑ Write ☑ Read ☑ Delete ☑ Rename ☑ List

	Username	Password	Permission
1	FTPLogin	EnableFTP	RWDNL
2	cisco	cisco	RWDNL

	File
1	asa842-k8.bin
2	c1841-advipservicesk9-mz.124-15.T1.bin
3	c1841-ipbase-mz.123-14.T7.bin
4	c1841-ipbasek9-mz.124-12.bin



```
Packet Tracer PC Command Line 1.0
PC>ftp www.ftp-zu.com
Trying to connect...www.ftp-zu.com
Connected to www.ftp-zu.com
220- Welcome to PT Ftp server
Username:FTPLogin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>?
         ?
         cd
         delete
         dir
         get
         help
         passive
         put
         pwd
         quit
         rename
ftp>
```

Chapter 3: Configuring Voice and Network Security

After configuring our environment, performing routing, and switching, we will use Cisco VoIP and Cisco Security in order to make our environment much more reliable and consistent in the collaboration and security.

VoIP Server:

- The VoIP Server is the piece of software that the client connects to when it wants to make a call or when receives one. Without a server, a lot of services would not be possible.

- First of all, a server takes care of routing. It finds the paths between two endpoints along which pieces of information will pass from one to the other. There are different algorithms for determining that, varying from the shortest path to the most secure or the fastest. This is done automatically, so there is no need for human intervention.

- The VoIP server can also be used to make communication possible through a lot of types of protocols. Modules that implement different protocols can be added. But what happens if the caller knows a protocol and the other one doesn’t know it. It is just like two different people are trying to talk to each other, but they speak different languages. In this case, the role of the translator can be taken by the server.

VoIP Client

- a computer
- a tablet PC
- a smart phone
- a VoIP telephone
- a traditional IP phone
- a call center

IP phone:

is a telephone set designed specifically for use in a voice over IP (VoIP) system by converting standard telephone audio into a digital format that can be transmitted over the Internet, and by converting incoming digital phone signals from the Internet to standard telephone audio.

VoIP software:

used to conduct telephone like voice conversations across Internet Protocol (IP) based networks. For residential markets, VoIP phone service is often cheaper than traditional public switched telephone network (PSTN) service and can remove geographic restrictions to telephone numbers

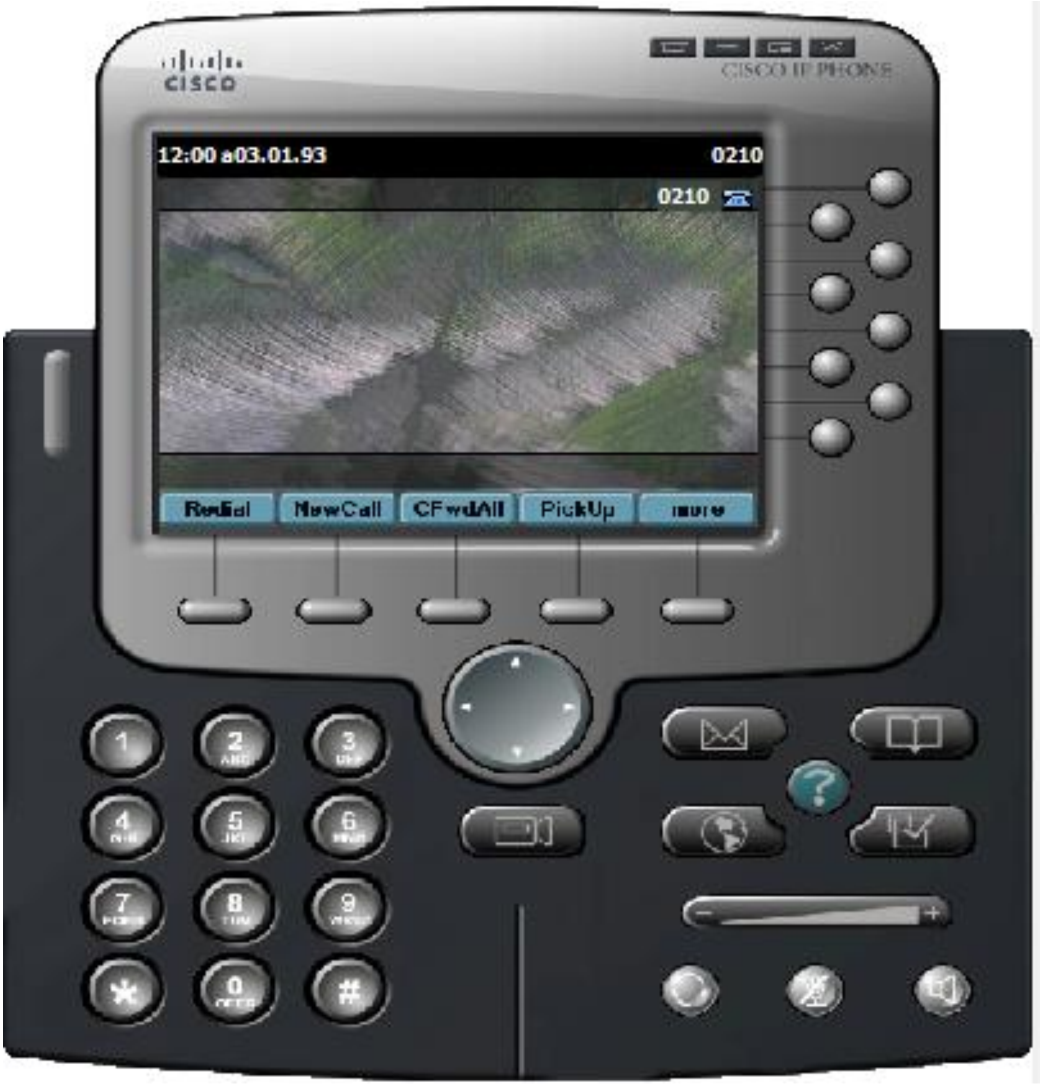
Softphones: are client devices for making and receiving voice and video calls over the IP network with the standard functionality of most "original" telephones and usually allow integration with IP phones and USB phones instead of utilizing a computer's microphone and speakers. Most softphone clients run on the open Session Initiation Protocol (SIP).

General Softphone clients:

- Avaya Application Server 5300Soft Client
- Audio Codes Mobility PLUS
- Blink
- Cisco IP Communicator

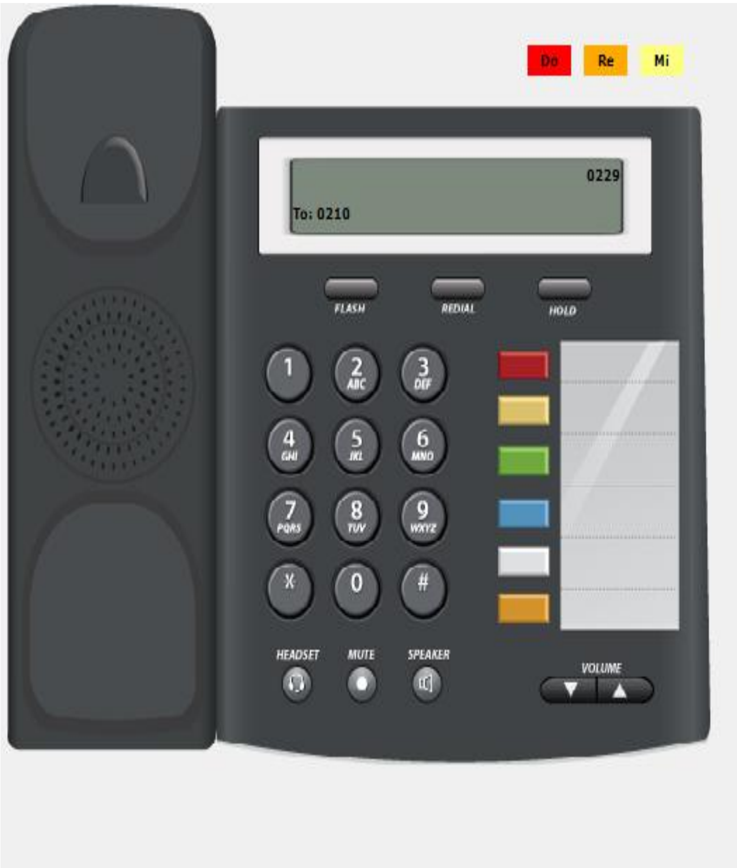
After configuring the VoIP server of each branch, such as Cairo branch:

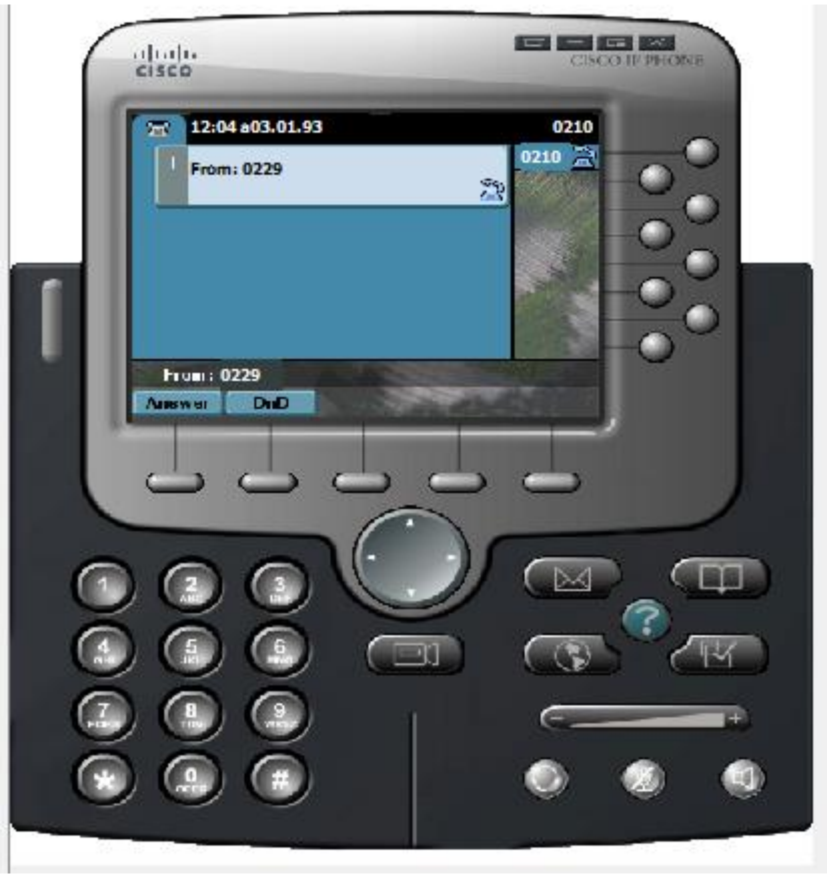
We find that the phones have been configured from DHCP server and have phone numbers.



We see that the phone number starts with “02” the key of Cairo branch.

After configuring Cairo Branch Phones we made a call inside the branch.





We made these configuration on the other branches, and gave same results as results on Cairo Branch:

- **Alex Branch:** same results but the phone number starts with “03” the key of Alex
- **Zagazig Branch:** same results but the phone number starts with “05” the key of Zagazig

Now we want to connect each branch with each other using dial peer.

<u>Dial peer:</u>

When a call is placed, an edge device generates dialed digits as a way of signaling where the call should terminate. When these digits enter a router voice port, the router must have a way to decide whether the call can be routed, and where the call can be sent. The router does this by looking through a list of dial peers. A dial peer is an addressable call endpoint. The address is called a destination pattern and is configured in every dial peer. Destination patterns can point to one telephone number only or to a range of telephone numbers. Destination patterns use both explicit digits and wildcard variables to define a telephone number or range of numbers. The router uses dial peers to establish logical connections. These logical connections, known as call legs, are established in either an inbound or outbound direction.

VoIP dial peers:

- Connect over a packet network. VoIP dial peers perform these functions:
- Provide a destination address (telephone number or range of numbers) for the edge device that is located in the network.
- Associate the destination address with the next-hop router or destination router, depending on the technology used.

Configuring VoIP Dial Peers:

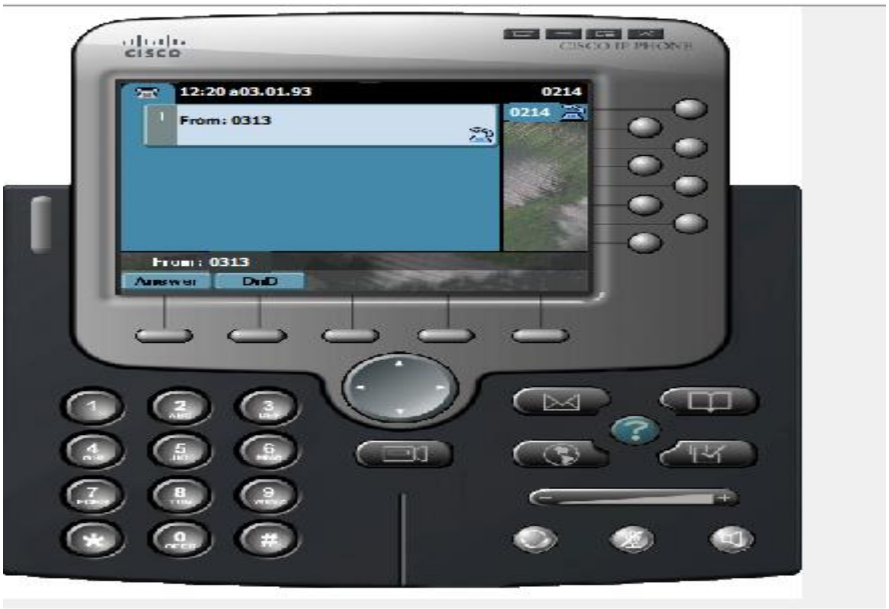
The administrator must know how to identify the far-end voice-enabled device that will terminate the call. In a small network environment, the device may be the IP address of the remote device. In a large environment, identifying the device may mean pointing to a Cisco Call Manager or gatekeeper for address resolution and Call Admission Control (CAC) to complete the call.

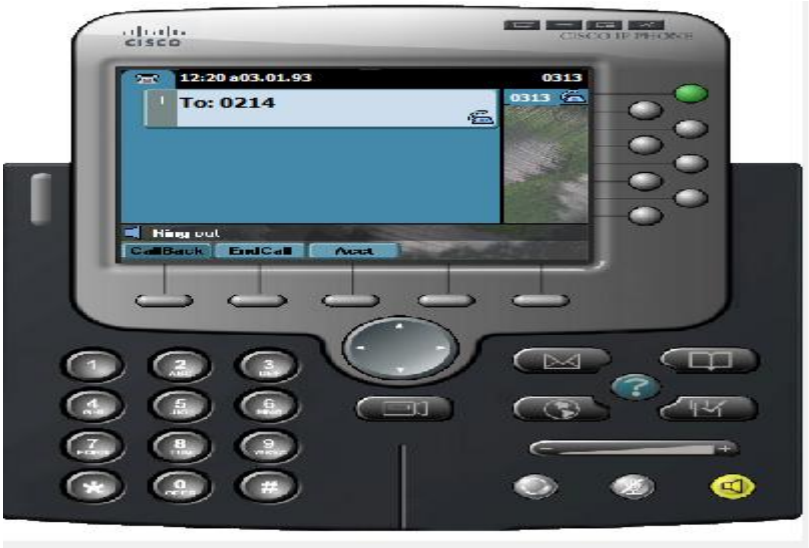
You must follow these steps to configure VoIP dial peers:

Step	**Action**
1.	Configure the path across the network for voice data.
2.	Specify the dial peer as a VoIP dial peer.
3.	Use the destination-pattern command to configure a range of numbers reachable by the remote router or gateway.
4.	Use the session target command to specify an IP address of the terminating router or gateway.
5.	Use the remote device loopback address as the IP address.

The dial peer is specified as a VoIP dial peer, which alerts the router that it must process a call according to the various parameters that are specified in the dial peer. The dial peer must then package it as an IP packet for transport across the network. Specified parameters may include the codec used for compression (VAD, for example), or marking the packet for priority service.

After configuring dial peer we can make a call from one branch to the other.





We see that two branches are connected to each other.

Network Security:

- Steps that are taken to ensure the confidentiality, integrity, and availability of data or resources.
- Confidentiality: prevent the disclosure of sensitive information from unauthorized people, resources, and processes.
- Integrity: the protection of system information or processes from intentional or accidental modification.
- Availability: the assurance that systems and data are accessible by authorized users when needed.
- Risk Management: the process of assessing and quantifying risk and establishing an acceptable level of risk for the organization.
- Risk Assessment: involves determining the likelihood that the vulnerability is a risk to the organization. Each vulnerability can be ranked by the scale.
- Network Threat: potential danger to information or a system. The ability to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network.
- Vulnerability: is a weakness in a system, technology, product or policy. Each vulnerability is given an ID and can be reviewed by network security professionals over the Internet.
- Vulnerability Appraisal: is a snapshot of the current security of the organization as it now stands.

Types of Attacks:

- Structured attack: comes from hackers who are more highly motivated and technically competent.
- Unstructured attack: consists of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers.
- External attacks: Initiated by individuals or groups working outside of a company. They do not have authorized access to the computer systems or network.
- Internal attacks: more common and dangerous. Internal attacks are initiated by someone who has authorized access to network.
- Passive Attack:

  - Listen to system passwords.
  - Release of message content.
  - Traffic analysis.
  - Data capturing.

- Active Attack:

  - Attempt to log into someone else's account.
  - Wire taps.
  - Denial of services.
  - Message modifications.

Network Security can be done using these steps:

1-Security Administration:

- Policy: document that states how an organization plans to protect its tangible and intangible information assets.
- All users must have a unique user ID and password that conforms to the company password standard.
- Users must not share their password with anyone regardless of title or position.
- Passwords must not be stored in written or any readable form.
- If a compromise is suspected, it must be reported to the help desk and a new password must be requested.
- Standards: criteria of passwords.

  -Minimum of 8 upper- and lowercase alphanumeric characters.

  - Must include a special character.

  - Must be changed every 30 days.

2- Securing the Management Plane:

- Authentication, Authorization, and Accounting (AAA).
- Network Time Protocol (NTP).
- Secure Shell (SSH).
- Simple Network Management Protocol (SNMP).
- Protected Syslog.

3- Securing the Control Plane:

- Routing: Static & EIGRP.
- Security Zoning (Inside, Outside, and DMZ).

4- Securing the Data Plane:

- Access Control List (ACL).
- Virtual Local Area Networks (VLANS).
- Spanning-Tree Protocol (STP) Guards.
- Virtual Private Network (VPN).
- Internetworking Operating System Intrusion Prevention System IOS IPS.

5- Areas of Security:

- Physical Security:

  - Place router in a secured, locked room.

  - Install an uninterruptible power supply.

- Operating System Security:

  -Use the latest stable version that meets network requirements.

  -Keep a copy of the O/S and configuration file as a backup.

- Router Hardening:

  - Secure administrative control.

  - Disable unused ports and interfaces.

  - Disable unnecessary services.

Some kinds of attacks that can be mitigated:

- MAC Address Spoofing Attack: technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device.

  - Countermeasures: Port Security.

- MAC Address Table Overflow Attack: technique employed to compromise the security of network switches.

  - Countermeasures: Port Security.

- STP Manipulation Attack: changes the topology of a network—the attacking host appears to be the root bridge.

  - Countermeasures: Spanning-Tree Port Fast, BPDU Guard, Root Guard.

- LAN Storm Attack: Broadcast, multicast, or unicast packets are flooded on all ports in the same VLAN. These storms can increase the CPU utilization on a switch to 100%, reducing the performance of the network.

  - Countermeasures: Port Security.

- VLAN Hopping Attack: can be launched by spoofing DTP Messages from the attacking host to cause the switch to enter trunking mode.

  - Countermeasures: Port Security.

- ACLs can be used to:

  - Mitigate IP address spoofing—inbound/outbound.

  - Mitigate Denial of service (DoS) TCP synchronizes (SYN) attacks blocking external attacks.

- Mitigate DoS TCP SYN attacks using TCP intercept.

- Mitigate DoS smurf attacks.

- Filter Internet Control Message Protocol (ICMP) messages inbound.

- Filter ICMP messages outbound.

- Filter traceroute.

6- Firewall: system that enforces an access control policy between networks.

- Resistant to attacks.
- Enforces the access control policy.
- Prevents exposing sensitive hosts and applications to untrusted users.
- Prevents the exploitation of protocol flaws by sanitizing the protocol flow.
- Prevents malicious data from being sent to servers and clients.
- Are based on simple permit or deny rule set.
- Have a low impact on network performance.
- Afford an initial degree of security at a low network layer.

7- Security Zoning:

- Standard baseline security requirements that will lead to consistency in implementation of network security.

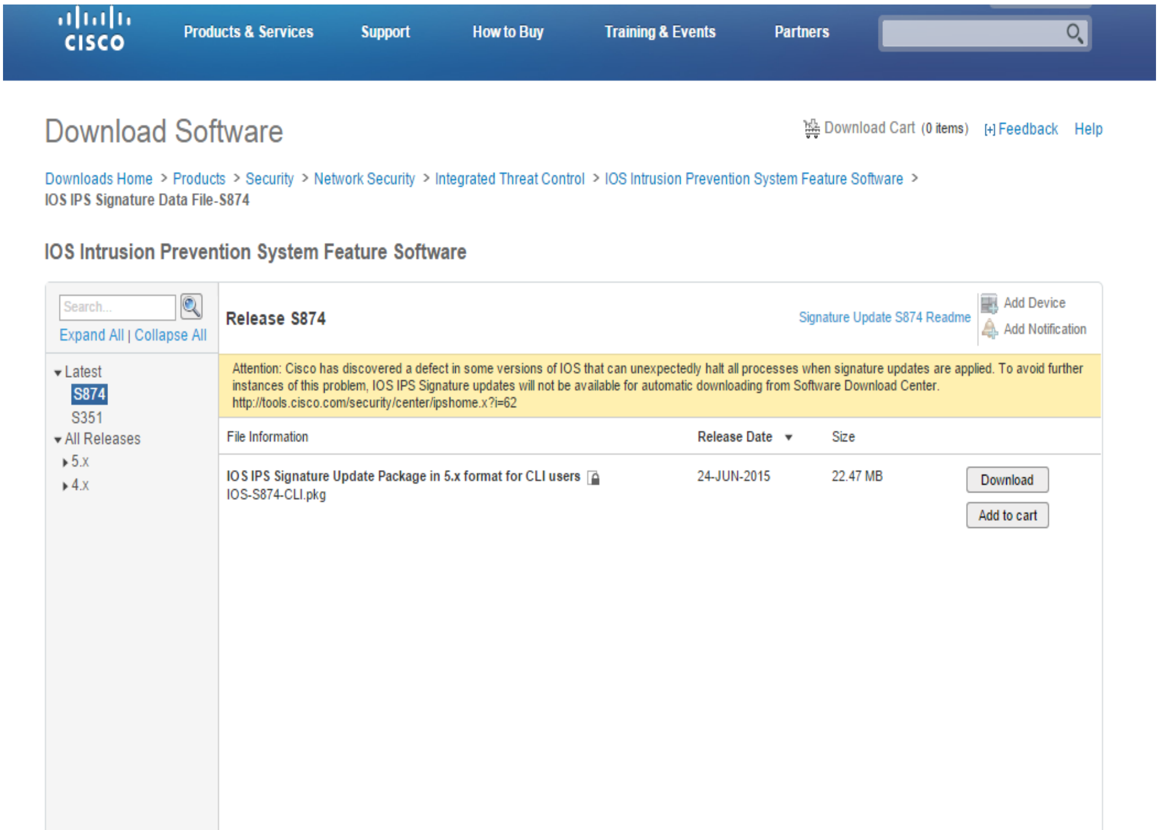
- Used to mitigate the risk of an open network by segmenting infrastructure services into logical groupings that have the same communication security policies and security requirements.
- Every zone contains one or more separate, routable networks.
- Inside Zone: trusted LAN that connects local hosts and every branch devices that employees use to communicate with each other.
- Outside Zone: external network node only has direct access to equipment in the DMZ, rather than any other part of the network. Has a limit access to inside zone.
- Demilitarized Zone (DMZ): physical or logical subnetwork that contains and exposes an organization's external-facing services or servers to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN). Have no access to inside zone.
- Configured on Cairo, Alex, and Zagazig main routers to limit the traffic coming in to DMZ or to Inside Zone.
- Define Inside Zone for trusted connected hosts inside LAN of every branch, Outside Zone for untrusted hosts in the internet, and DMZ for company servers that provide services to internet host and enable connection to them with a limitation.

8- IOS IPS: Prevents and Drops the untrusted packets.

- An attack is launched on a network that has a sensor deployed in IPS mode (inline mode).

- The IPS sensor analyzes the packets as they enter the IPS sensor interface. The IPS sensor matches the malicious traffic to a signature and the attack is stopped immediately.
- The IPS sensor can also send an alarm to a management console for logging and other management purposes.
- Traffic in violation of policy can be dropped by an IPS sensor.
- Configured on Cairo, Alex, and Zagazig main routers to prevent the untrusted traffic or packets coming from the internet to the inside zone.

- IOS IPS Signature Update Files can be downloaded from Cisco Web Site to ensure an up-to-date signature file on routers.



Download Software

Downloads Home > Products > Security > Network Security > Integrated Threat Control > IOS Intrusion Prevention System Feature Software > IOS IPS Signature Data File-S874

IOS Intrusion Prevention System Feature Software

Release S874

Attention: Cisco has discovered a defect in some versions of IOS that can unexpectedly halt all processes when signature updates are applied. To avoid further instances of this problem, IOS IPS Signature updates will not be available for automatic downloading from Software Download Center. http://tools.cisco.com/security/center/ipshome.x?i=62

File Information	Release Date	Size
IOS IPS Signature Update Package in 5.x format for CLI users IOS-S874-CLI.pkg	24-JUN-2015	22.47 MB

This downloaded signature file that contains the crypto public key can be copied from notepad to the router console window:

9- Port Security:

- Used to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port.
- STATIC: the entry (MAC address) is permanently mapped to a specific port.
- DYNAMIC: the entry is created from the incoming frames by reading the source MAC address field in the Ethernet header.
- Sticky MAC Address: Persistent MAC learning, also known as sticky MAC, is a port security feature that allows retention of dynamically learned MAC addresses on an interface across restarts of the switch.
- Protect: when the port receives the traffic from the MAC addresses which are not configured as secure, it silently drops those transmissions. There is NO notification logged about the violation occurring on a port.
- Restrict - when the port receives the traffic from the MAC addresses which are not configured as secure, it silently drops those transmissions. There is a notification logged about the violation occurring on a port.
- Shutdown (default) - the port will transition to err-disable upon detecting the violation.
- Shut down all unused ports to prevent unsecure access to switches or routers or to prevent the unsecure connection to one of these ports.
- Configured on Cairo, Alex, and Zagazig switches to increase the security of network and connected devices. Enable Restrict Violation on switch ports to prevent unsecure traffic from being transferred and Log the violations so that the Administrator can know what happened inside the network and the threats that may counter this network.

10- Device Security:

- Disabling unused services.
- Set a secret (Encrypted) to the enable mode. And define a number of users that are able to login to this device with a specific privileges.
- Set passwords for remote, console, and auxiliary connection to device.
- Physical Security: security measures that are designed to deny unauthorized access to facilities, equipment and resources. Locate devices in places that are not reachable by every employee at the company and determine this access to a specific number of employees such as ADMIN, HELPDESK, and MANAGER.
- Determine a specific number of tries when connecting to a device to prevent denial of service attack or brute-force attack. Log these attempts to login.
- Create a local database for users who are accepted to login to router or switch, encrypt this database using RSA Algorithm, put it inside a domain, and apply it to VTY remote connection or logic to this device.

11- AAA (Authentication Authorization Accounting) Server:

- Allows you to verify the identity of, grant access to, and track the actions of users managing a device.
- Based on the user ID and password combination that you provide.
- A pre-shared secret key provides security for communication between the Cisco device and AAA servers.

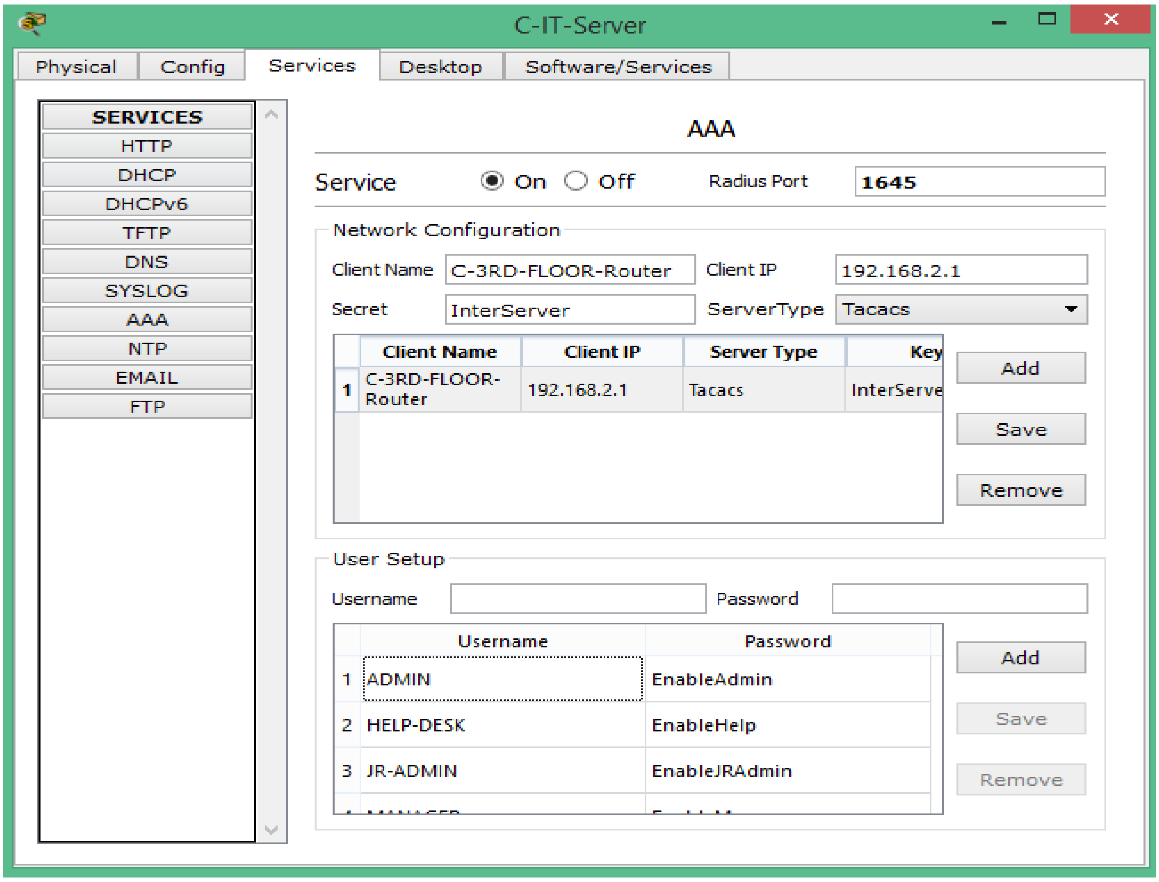
- Authentication: provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption. It is the way a user is identified prior to being allowed access to the network and network services.

- Authorization: provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server.

- Accounting: enables tracking the services users are accessing as well as the amount of network resources they are consuming. The network access server reports user activity to the RADIUS or TACACS+ security server in the form of accounting records.

- TACACS (Terminal Access Controller Access-Control System) refers to a family of related protocols handling remote authentication and related services for networked access control through a centralized server.

- Configured on Cairo, Alex, and Zagazig floor routers to determine who has permission to access these routers. Servers located in IT, HR, and Sales Departments has AAA technology which store a database about users who has the ability to access floor routers by their usernames and passwords. There’s a secret key shared between floor router and AAA Server to enable secure connection between them and prevent attacks. TACACS protocol is used for this AAA Server using its IP Address and a specific port number for a successful connection between this server and floor router.



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name C-3RD-FLOOR-Router Client IP 192.168.2.1

Secret InterServer ServerType Tacacs

	Client Name	Client IP	Server Type	Key
1	C-3RD-FLOOR-Router	192.168.2.1	Tacacs	InterServe

User Setup

Username Password

	Username	Password
1	ADMIN	EnableAdmin
2	HELP-DESK	EnableHelp
3	JR-ADMIN	EnableJRAdmin

The impact on the company of implementing this solution:

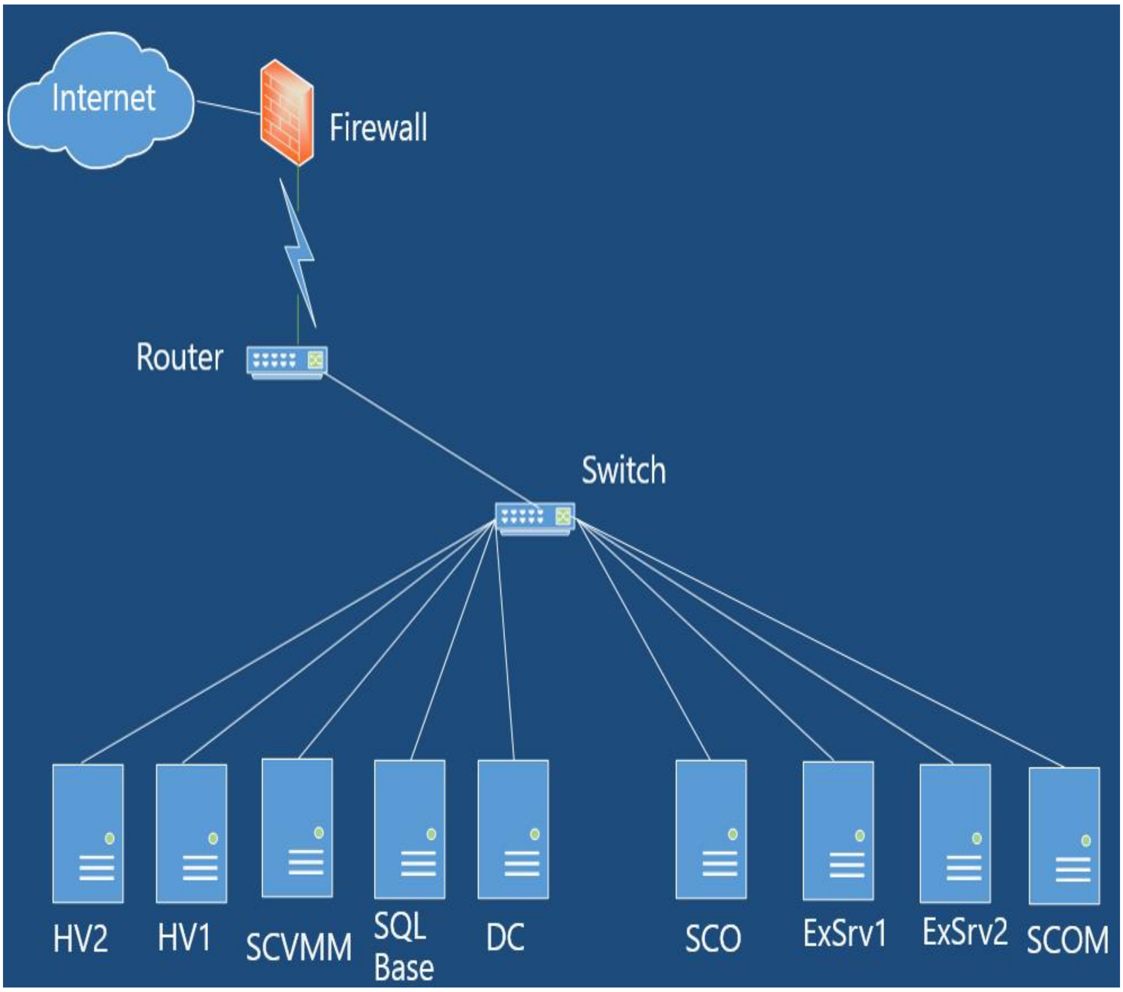
- ➢ Optimizing the utilization of the built infrastructure by using every component inside every branch that makes a specific task.
- ➢ Lower costs by implementing a good solution that connects three branches of a single company together.
- ➢ Increase the security inside every branch by using security zoning, IOS IPS, firewall, VPN, and frame-relay techniques.
- ➢ Scalability to meet the growth of users, or services.
- ➢ Multi-Service company that offers a combination of related and non-related services to meet the requirements of the user.

- Fault-Tolerance between branches by using frame-relay, VPN, or the internet to exchange data to ensure that services are always available.
- Enable backup using TFTP to easy recover a specific device if it’s dropped.
- Administration that ensure service availability and continuity.
- Ease of contact between the user and company using phones or web.
- Quick recovery and solutions of problems, errors, or any fault.
- Giving a valuable, secure, and good service to users.
- Implementing CIA (Confidentiality, Integrity, and Availability).
- Using up-to-date services & devices to enable a good services.

Part II

Chapter 4: Introduction

In this project we aim to create a scalable, flexible, automated, agile, and Self-Serviced IT environment. Here is the design of the environment:



- Figure 4.1

Each server of the servers illustrated in the design has a certain role or multiple roles to perform.

1. DC: perform the role of domain controller plus some other roles such as (DNS+ File Server + Storage Spaces).
2. SQL Base: is a SQL Server, which is used to store the database of the products used in this project.

3. SCVMM: this server contains the System Center Virtual Machine Manager (Management Server + the Console) and we use it to create our Private Cloud.

4. HV1: a virtualization host in which we create virtual machines that is managed by SCVMM.

5. HV2: another virtualization host in which we create virtual machines that is managed by SCVMM.

6. SCO: this server contains all the System Center Orchestrator components including (Management Server – Rub Book Server – Run Book Designer – Deployment Manager – Orchestration Console and Web Service).

7. ExSrv1: is an exchange server that provide the mail services to the users in our environment.

8. ExSrv2: another exchange server that is used to failover the first exchange server in case of failure.

9. SCOM: is a System Center Operations Manager server that is used to monitor and fix the errors in our system.

About the Products/Technologies used in our Project:

- ✓ **Windows Server 2012 R2**: At the heart of the Microsoft Cloud Platform vision, Windows Server 2012 R2 brings Microsoft's experience delivering global-scale cloud services into your infrastructure with new features and enhancements in virtualization, management, storage, networking, virtual desktop infrastructure, access and information protection, the web and application platform, and more. We are using it as our main server platform in the project.

- ✓ **SQL Server 2012 SP1**: Microsoft SQL Server 2012 is a relational database management system (RDBMS) designed for the enterprise environment. SQL Server 2012 comprises a set of programming extensions to enhance the Structured Query Language (SQL), a standard interactive and programming language for getting information from and updating a database, and we are using it in this project as our main database.

- ✓ **Exchange Server 2013**: is a reliable messaging platform that reduces costs, increases productivity, and improves communications. enables small and medium-sized companies to achieve greater reliability and improved performance by simplifying administration tasks such as calendaring, creating distribution lists, sending email messages, automatically performing voicemail transcriptions, providing messaging delivery reports, and archiving mail boxes, and we are using it in the project as a mail server.

- ✓ **System Center Virtual Machine Manager 2012 R2:** It enables you to manage physical and virtual infrastructure. Data centers have evolved from physical to virtual to IaaS. Customers are using different services across datacenters on premises and in public cloud and managing these services costs a lot to organizations. It provides tools to manage cloud and datacenter applications and services. Virtual Machine Manager 2012 R2 supports Citrix, VMWare and Hyper-V infrastructure. We can pool key components like compute, network and storage resources into private cloud fabric resources and dynamically allocate, by enabling a service catalog-based self-service experience for our business. Quotas can be applied to define the level of granularity on a Shared basis or on per-user basis.

- ✓ **System Center Operations Manager 2012 R2:** is a cross-platform datacenter management system for operating systems and hypervisors. It uses a single interface that shows state, health and performance information of computer systems. It also provides alerts generated according to some availability, performance, configuration or security situation being identified. It works with Microsoft Windows Server and Unix-based hosts.

- ✓ **System Center Orchestrator 2012 R2:** is a workflow management solution for the data center. Orchestrator lets you automate the creation, monitoring, and deployment of resources in your environment. Orchestrator is a complete solution that goes beyond basic automation. You can configure Orchestrator runbooks to be triggered according to event logs or, more usefully, Microsoft Systems Center Operations Manager alerts. Rather than waiting for an end user to notice that a service has become unavailable or having a member of the support team raise a job according to an Ops Manager alert, you can automate the process entirely through the use of an Orchestrator runbook that is triggered by an alert, raises a job in the job-tracking system, runs a complex operation to resolve the issue that triggered the alert, adds information to the job in the job-tracking system, and then closes that job. The alert is resolved, the job is logged and closed, and everything is completed without direct human intervention.

- ✓ **Virtualization Technology:** In computing, virtualization means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments. Even something as simple as partitioning a hard drive is considered virtualization because you take one drive and partition it to create two separate hard drives. Devices, applications and human users are able to interact with the virtual resource as if it were a real single logical resource.

- ✓ **Cloud Computing:** A model for delivering information technology services in which resources are retrieved from the internet through web-based tools and applications, rather than a direct connection to a server. Data and software packages are stored in servers. However, cloud computing structure allows access to information as long as an electronic device has access to the web. This type of system allows employees to work remotely.

Chapter 5: Building the System Platform

In this chapter, we will illustrate what is the system platforms we have built and how it is going on within it.

As said before, we are using Windows Server 2012 R2 as our server platform, so the first thing we have done was to build our DC in order to control the whole IT environment and assign the policies we want according to the organization needs.

Here is a description we have installed in our first server:

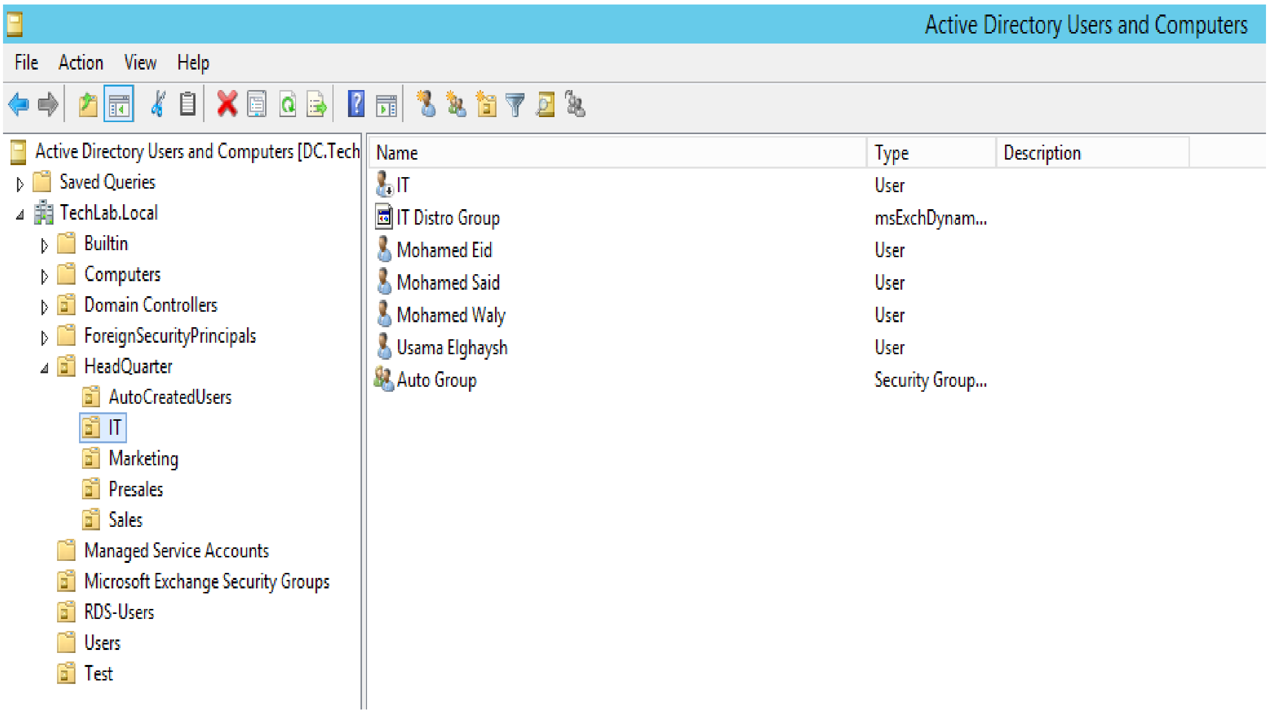
Role	Description
Active Directory Domain Services	AD DS provides a distributed database that stores and manages information about network resources and application-specific data from directory-enabled applications. Administrators can use AD DS to organize elements of a network, such as users, computers, and other devices, into a hierarchical containment structure.
DNS	Network resources are identified by numeric IP addresses, but these IP addresses are difficult for network users to remember. The DNS database contains records that map user-friendly alphanumeric names for network resources to the IP address used by those resources for communication. In this way, DNS acts as a

	mnemonic device, making network resources easier to remember for network users.
File and Storage Services	File and Storage Services includes technologies that help you set up and manage one or more file servers, which are servers that provide central locations on your network where you can store files and share them with users. If your users need access to the same files and applications, or if centralized backup and file management are important to your organization, you should set up one or more servers as a file server by installing the File and Storage Services role and the appropriate role services.

- Table: 4.1

Building Active Directory Domain services enabled us to organize our environment by building organizational units in which we can store our users according to their departments/locations/projects…etc.

In our use case we have made an organizational unit for the headquarters of the organization, and some sub-organizational units according to the department of the user. You can check that from the following screenshot.



- Active Directory Users and Computers [DC.Tech
  - Saved Queries
  - TechLab.Local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - HeadQuarter
      - AutoCreatedUsers
      - IT
      - Marketing
      - Presales
      - Sales
    - Managed Service Accounts
    - Microsoft Exchange Security Groups
    - RDS-Users
    - Users
    - Test

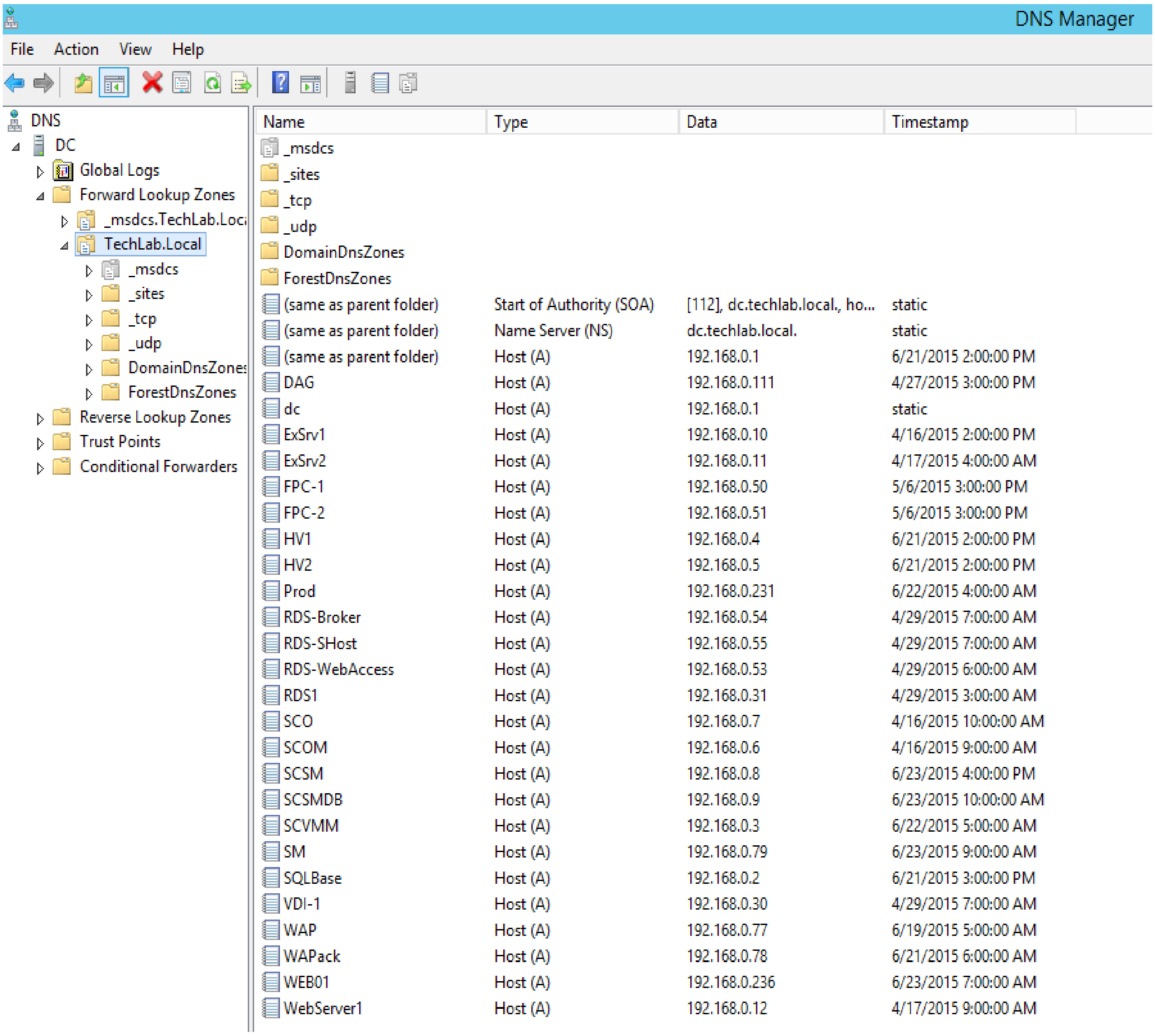
Name	Type	Description
IT	User	
IT Distro Group	msExchDynam...	
Mohamed Eid	User	
Mohamed Said	User	
Mohamed Waly	User	
Usama Elghaysh	User	
Auto Group	Security Group...	

- Figure 5.1

We also have DNS that is used to resolve the names of the websites or devices or even computers locally and externally.

For Example: Computer "A" cannot contact with Computer "B" if there is no DNS in our environment. Also we cannot access any external websites or devices from inside our IT environment if we don't have DNS.

Here is a screenshot for some DNS records from within our IT environment:

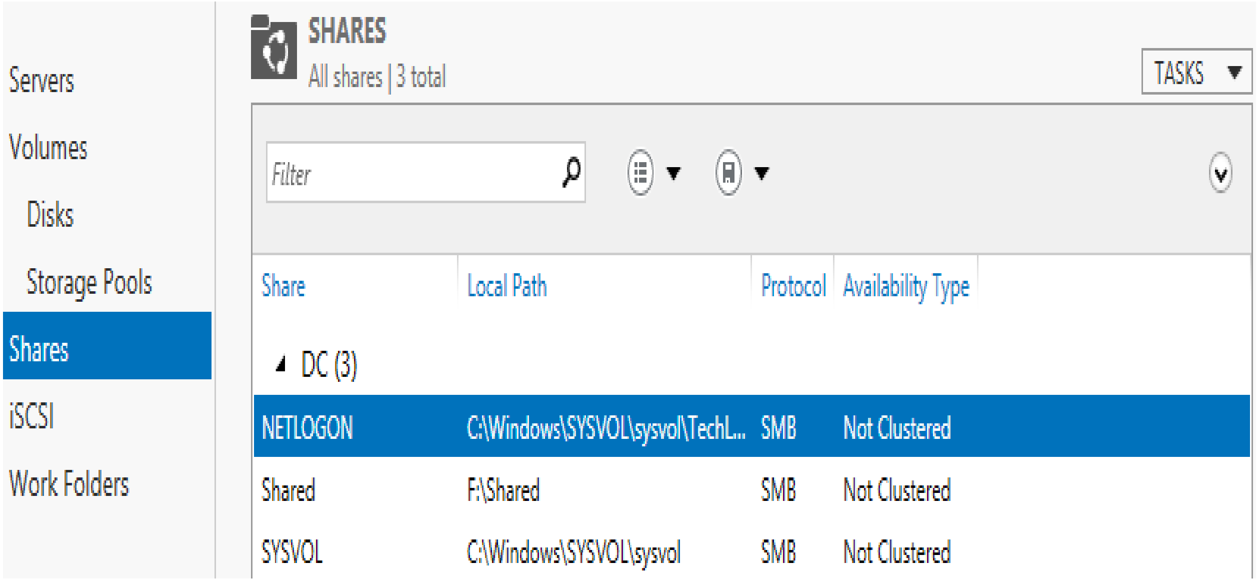


Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[112], dc.techlab.local., ho...	static
(same as parent folder)	Name Server (NS)	dc.techlab.local.	static
(same as parent folder)	Host (A)	192.168.0.1	6/21/2015 2:00:00 PM
DAG	Host (A)	192.168.0.111	4/27/2015 3:00:00 PM
dc	Host (A)	192.168.0.1	static
ExSrv1	Host (A)	192.168.0.10	4/16/2015 2:00:00 PM
ExSrv2	Host (A)	192.168.0.11	4/17/2015 4:00:00 AM
FPC-1	Host (A)	192.168.0.50	5/6/2015 3:00:00 PM
FPC-2	Host (A)	192.168.0.51	5/6/2015 3:00:00 PM
HV1	Host (A)	192.168.0.4	6/21/2015 2:00:00 PM
HV2	Host (A)	192.168.0.5	6/21/2015 2:00:00 PM
Prod	Host (A)	192.168.0.231	6/22/2015 4:00:00 AM
RDS-Broker	Host (A)	192.168.0.54	4/29/2015 7:00:00 AM
RDS-SHost	Host (A)	192.168.0.55	4/29/2015 7:00:00 AM
RDS-WebAccess	Host (A)	192.168.0.53	4/29/2015 6:00:00 AM
RDS1	Host (A)	192.168.0.31	4/29/2015 3:00:00 AM
SCO	Host (A)	192.168.0.7	4/16/2015 10:00:00 AM
SCOM	Host (A)	192.168.0.6	4/16/2015 9:00:00 AM
SCSM	Host (A)	192.168.0.8	6/23/2015 4:00:00 PM
SCSMDB	Host (A)	192.168.0.9	6/23/2015 10:00:00 AM
SCVMM	Host (A)	192.168.0.3	6/22/2015 5:00:00 AM
SM	Host (A)	192.168.0.79	6/23/2015 9:00:00 AM
SQLBase	Host (A)	192.168.0.2	6/21/2015 3:00:00 PM
VDI-1	Host (A)	192.168.0.30	4/29/2015 7:00:00 AM
WAP	Host (A)	192.168.0.77	6/19/2015 5:00:00 AM
WAPack	Host (A)	192.168.0.78	6/21/2015 6:00:00 AM
WEB01	Host (A)	192.168.0.236	6/23/2015 7:00:00 AM
WebServer1	Host (A)	192.168.0.12	4/17/2015 9:00:00 AM

- Figure 5.2

Moreover, the last role of the server is "File and Storage Services" that helps us to create file shares and LUNs that are used to store the virtual machines data since System Center Virtual Machine Manager is using this server as a virtual SAN, and we will talk about it in more details later.

Here are some screenshots that illustrates the file shares and LUNs created using this service.

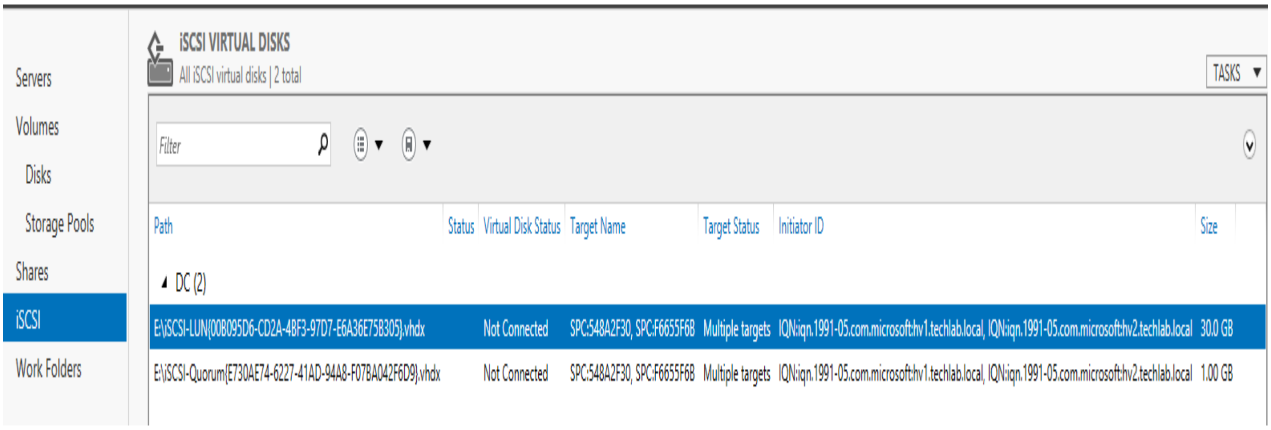


SHARES

All shares | 3 total

Share	Local Path	Protocol	Availability Type
DC (3)			
NETLOGON	C:\Windows\SYSVOL\sysvol\TechL...	SMB	Not Clustered
Shared	F:\Shared	SMB	Not Clustered
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered

- Figure 5.3



iSCSI VIRTUAL DISKS

All iSCSI virtual disks | 2 total

Path	Status	Virtual Disk Status	Target Name	Target Status	Initiator ID	Size
DC (2)						
E:\iSCSI-LUN{00B095D6-CD2A-4BF3-97D7-E6A36E75B305}.vhdx		Not Connected	SPC:548A2F30, SPC:F6655F6B	Multiple targets	IQN:iqn.1991-05.com.microsoft:hv1.techlab.local, IQN:iqn.1991-05.com.microsoft:hv2.techlab.local	30.0 GB
E:\iSCSI-Quorum{E730AE74-6227-41AD-94A8-F07BA042F6D9}.vhdx		Not Connected	SPC:548A2F30, SPC:F6655F6B	Multiple targets	IQN:iqn.1991-05.com.microsoft:hv1.techlab.local, IQN:iqn.1991-05.com.microsoft:hv2.techlab.local	1.00 GB

- Figure 5.4

The second server we have used in our System Infrastructure is SQL Server.

Here are the features we have installed on our SQL Server.

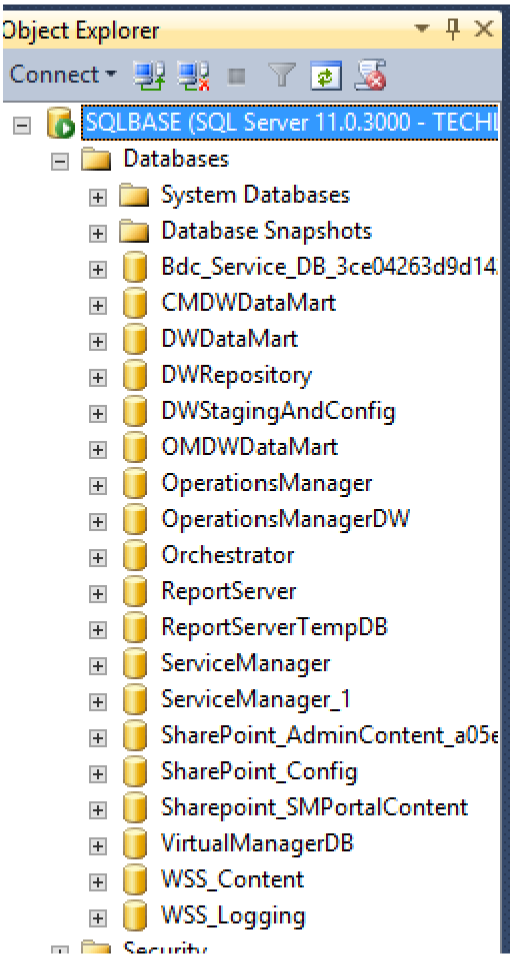
Feature	Description
Database Engine Services	Includes the Database Engine, the core service for storing, processing and securing data. The Database Engine provides controlled access and rapid

	transaction processing and also provides rich support for sustaining high availability. The Database Engine also provides support for the utility control point in the SQL Server Utility. Only Database Engine Services and Analysis Services can be clustered.
Full-text and Semantic Extractions for Search	Includes the Search engine that supports Full-Text Extraction for fast text search as well as Semantic Extraction for key phrases (likely tags) and similarity search on content stored in SQL Server.
Reporting Services - Native	Includes Reporting Services, a server-based application for creating, managing, and delivering reports to email, multiple file formats, and interactive Web-based formats. The Native mode server provides all processing and management functionality through Reporting Services components. Reporting Services cannot be clustered.
Management Tools - Basic	Includes Management Studio support for the Database Engine and SQL Server Express, SQL Server command-line utility (SQLCMD), SQL Server PowerShell provider, and Distributed Replay Administration Tool.
Management Tools - Complete	Adds the following components to the basic management tools installation: Management Studio support for Reporting Services, Analysis Services, and Integration Services technologies, SQL Server Profiler, Database Tuning Advisor, and SQL Server Utility management.

- Table 5.2

This server as said before is used to store the databases of the applications that we will talk about in the next chapter.

Here are the databases created in SQL Server for the applications such as (System Center Virtual Machine Manager, System Center Orchestrator, System Center Operations Manager,…etc.).



- SQLBASE (SQL Server 11.0.3000 - TECHI
  - Databases
    - System Databases
    - Database Snapshots
    - Bdc_Service_DB_3ce04263d9d14
    - CMDWDataMart
    - DWDataMart
    - DWRepository
    - DWStagingAndConfig
    - OMDWDataMart
    - OperationsManager
    - OperationsManagerDW
    - Orchestrator
    - ReportServer
    - ReportServerTempDB
    - ServiceManager
    - ServiceManager_1
    - SharePoint_AdminContent_a05e
    - SharePoint_Config
    - Sharepoint_SMPortalContent
    - VirtualManagerDB
    - WSS_Content
    - WSS_Logging
  - Security

- Figure 5.5

Last, but not least we have two Hyper-V Servers deployed as Virtualization hosts, and they are used to build our virtual machines and construct the cloud.

Chapter 6: Building and Integrating the System Applications

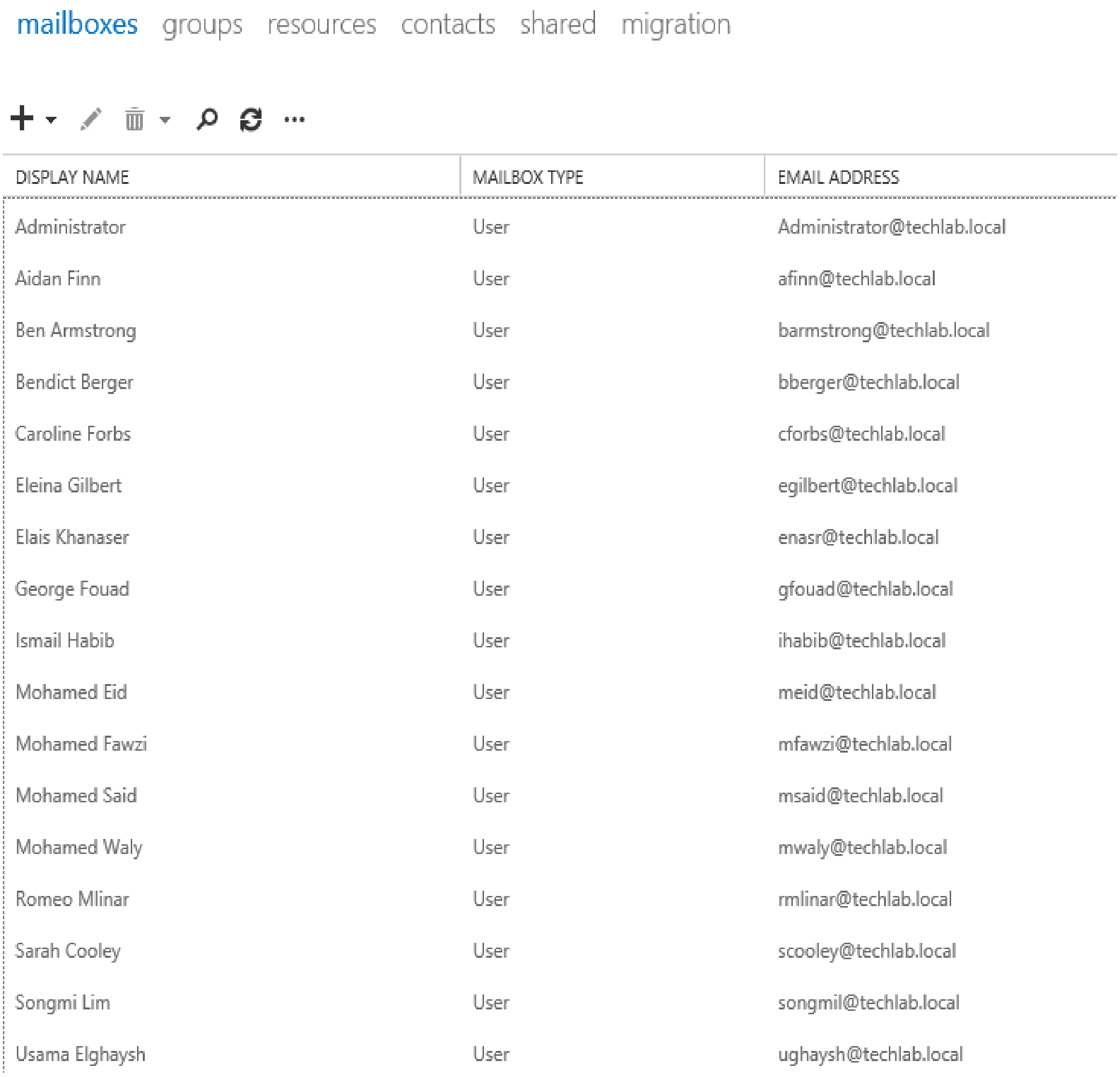
As said in the introduction, we have multiple applications that forms our IT environment. Here are the applications that we have deployed.

1. Exchange Server
2. System Center Virtual Machine Manager
3. System Center Orchestrator
4. System Center Operations Manager

6.1 Exchange Server:

We use Exchange Server to send messages to and receive messages from inside or outside our IT environment. However, there some features that are available in Exchange Server that we have used to make it much more reliable and consistent.

Starting with the mailboxes. Every user in the domain has an e-mail as shown in the following screenshot:

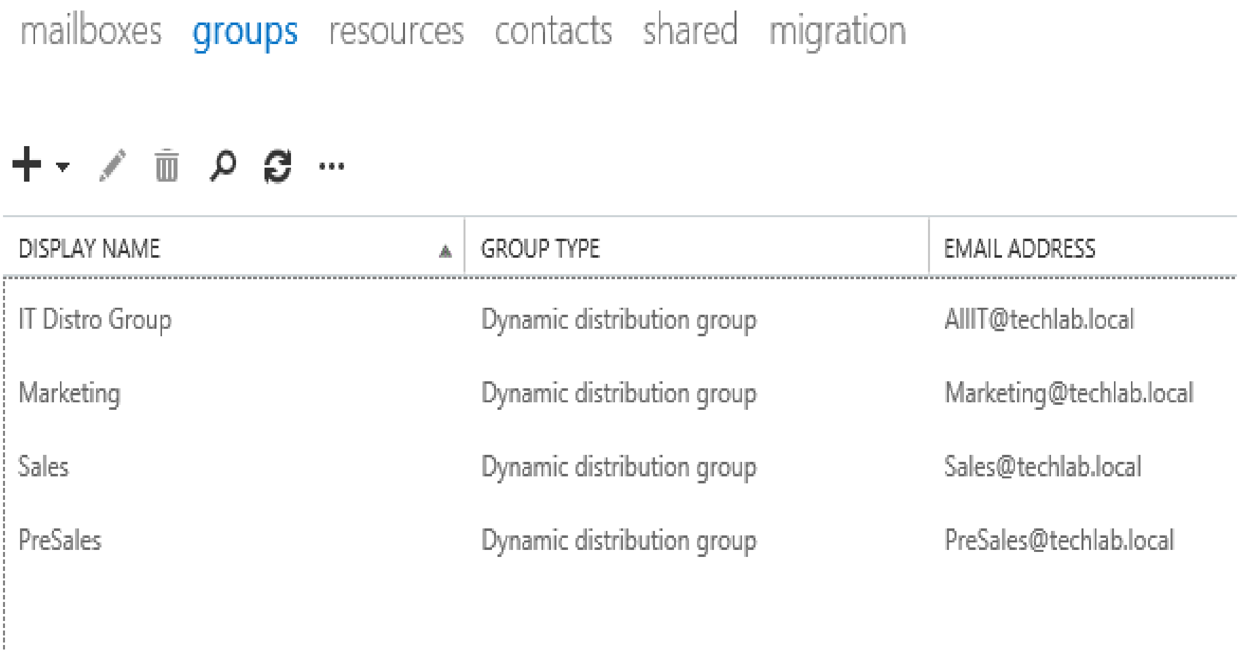


DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
Administrator	User	Administrator@techlab.local
Aidan Finn	User	afinn@techlab.local
Ben Armstrong	User	barmstrong@techlab.local
Bendict Berger	User	bberger@techlab.local
Caroline Forbs	User	cforbs@techlab.local
Eleina Gilbert	User	egilbert@techlab.local
Elais Khanaser	User	enasr@techlab.local
George Fouad	User	gfouad@techlab.local
Ismail Habib	User	ihabib@techlab.local
Mohamed Eid	User	meid@techlab.local
Mohamed Fawzi	User	mfawzi@techlab.local
Mohamed Said	User	msaid@techlab.local
Mohamed Waly	User	mwaly@techlab.local
Romeo Mlinar	User	rmlinar@techlab.local
Sarah Cooley	User	scooley@techlab.local
Songmi Lim	User	songmil@techlab.local
Usama Elghaysh	User	ughaysh@techlab.local

✓ Figure 6.1

We also have made some dynamic groups so that any new member who joins the IT Department will be automatically join that group, so later on , when anyone in the organization wants to send a mail to all IT Department members, he doesn't have to send to every single member, he can just send it to the group mail and all the members of the IT Department will receive it.

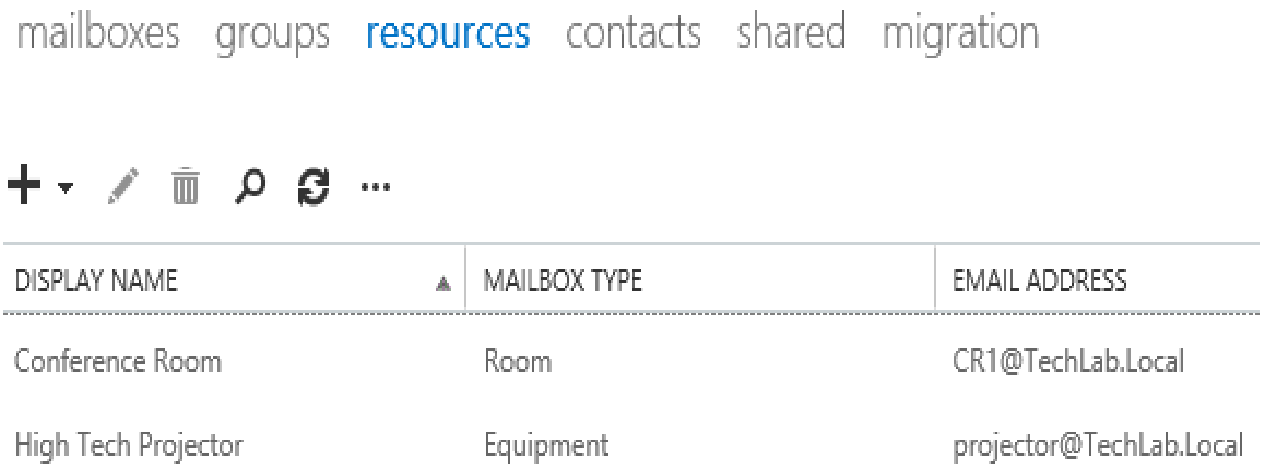
Here is an example of a group for the IT Department:



DISPLAY NAME ▲	GROUP TYPE	EMAIL ADDRESS
IT Distro Group	Dynamic distribution group	AllIT@techlab.local
Marketing	Dynamic distribution group	Marketing@techlab.local
Sales	Dynamic distribution group	Sales@techlab.local
PreSales	Dynamic distribution group	PreSales@techlab.local

✓ Figure 6.2

Since we need some resources to reserve in our environment for examples (Rooms & Projectors) we have to made mailboxes for them, so they can be reserved as shown in the following screenshot:

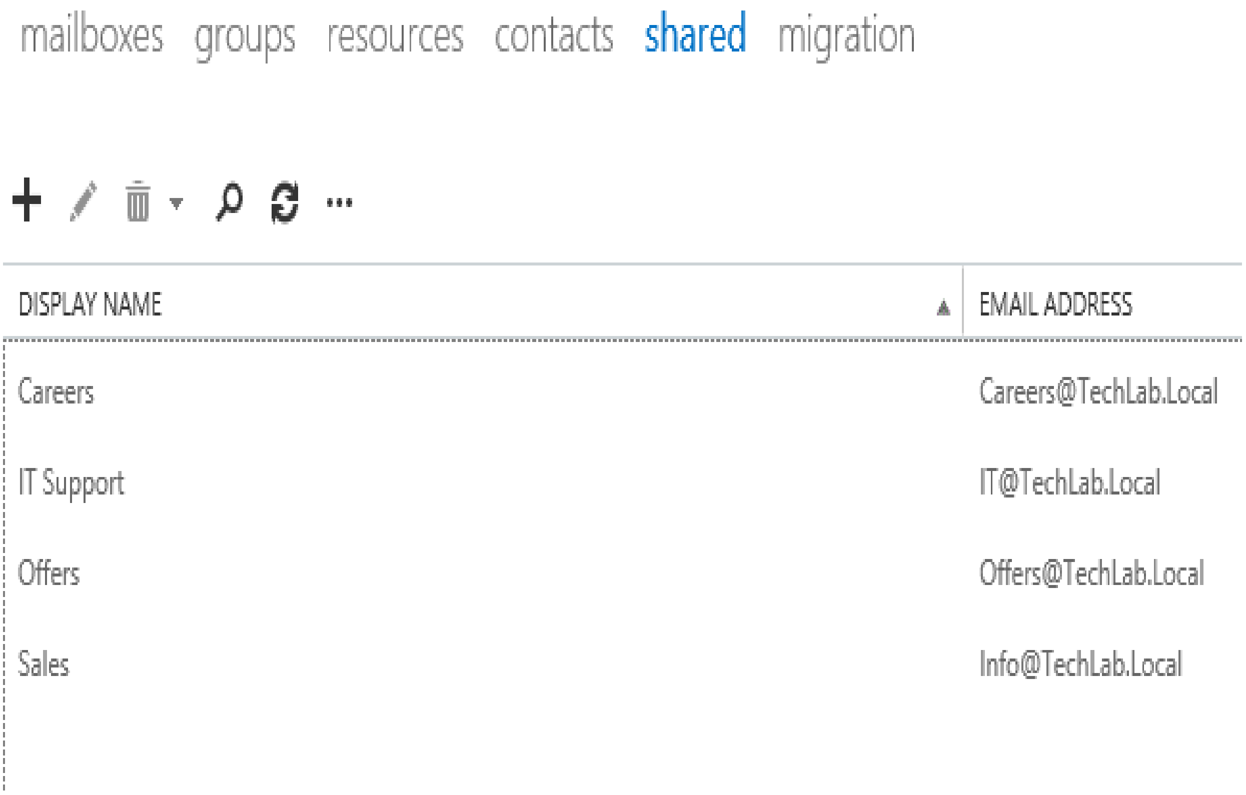


DISPLAY NAME ▲	MAILBOX TYPE	EMAIL ADDRESS
Conference Room	Room	CR1@TechLab.Local
High Tech Projector	Equipment	projector@TechLab.Local

✓ Figure 6.3

Moreover, we need to have some shared mailboxes so they can be used in case of support or job recruitment, so the responsible people about IT Support in the IT team will be the only persons who receive a mail about the issues of the end users in the IT environment.

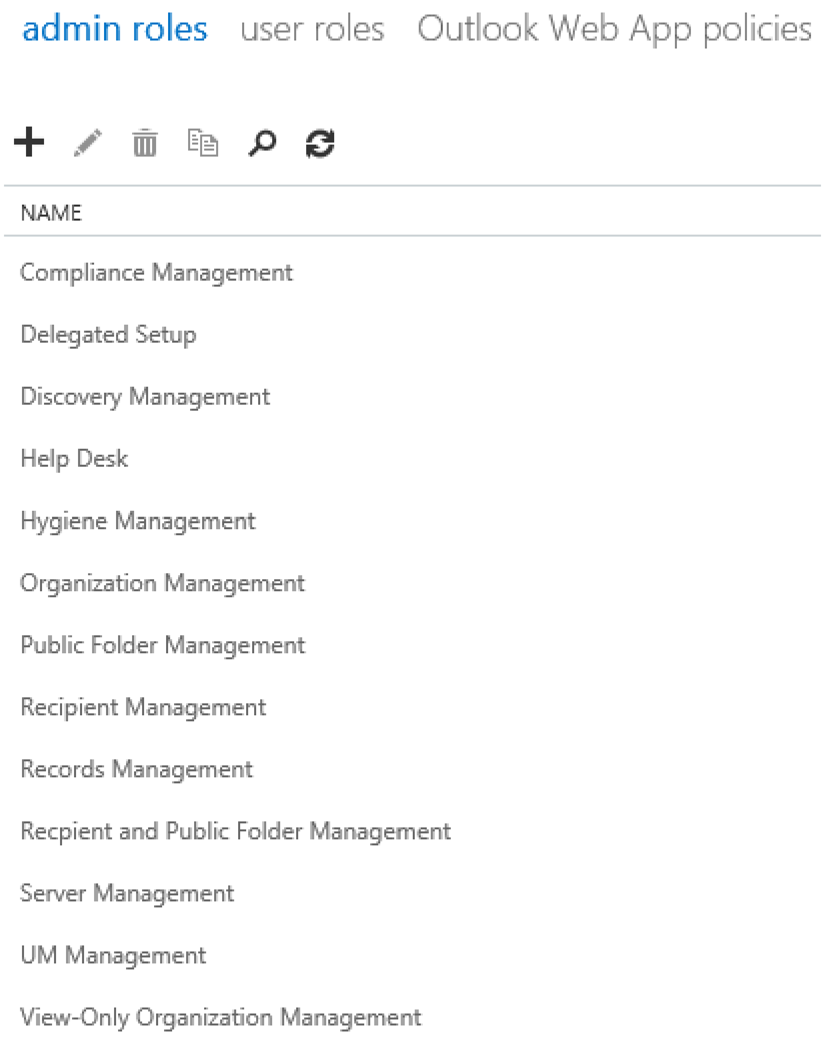
Here are the shared mailboxes in our environment:



DISPLAY NAME	EMAIL ADDRESS
Careers	Careers@TechLab.Local
IT Support	IT@TechLab.Local
Offers	Offers@TechLab.Local
Sales	Info@TechLab.Local

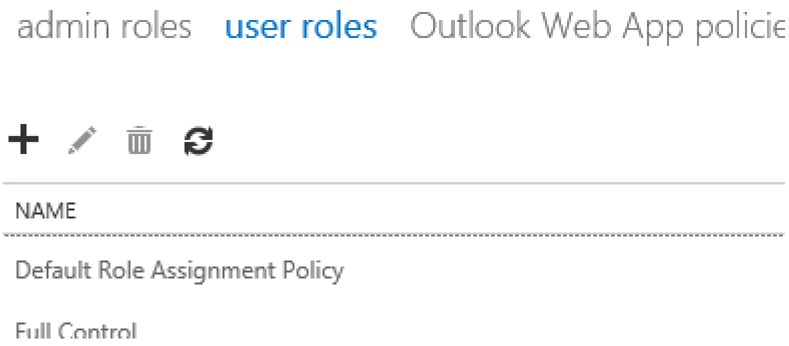
- ✓ Figure 6.4

One of the most important things in every IT environment is the permissions, in order to ensure that everyone who is accessing anything in the environment is eligible, so we have made so permissions for admins roles and user roles, as show in the following screenshot:



NAME
Compliance Management
Delegated Setup
Discovery Management
Help Desk
Hygiene Management
Organization Management
Public Folder Management
Recipient Management
Records Management
Recpient and Public Folder Management
Server Management
UM Management
View-Only Organization Management

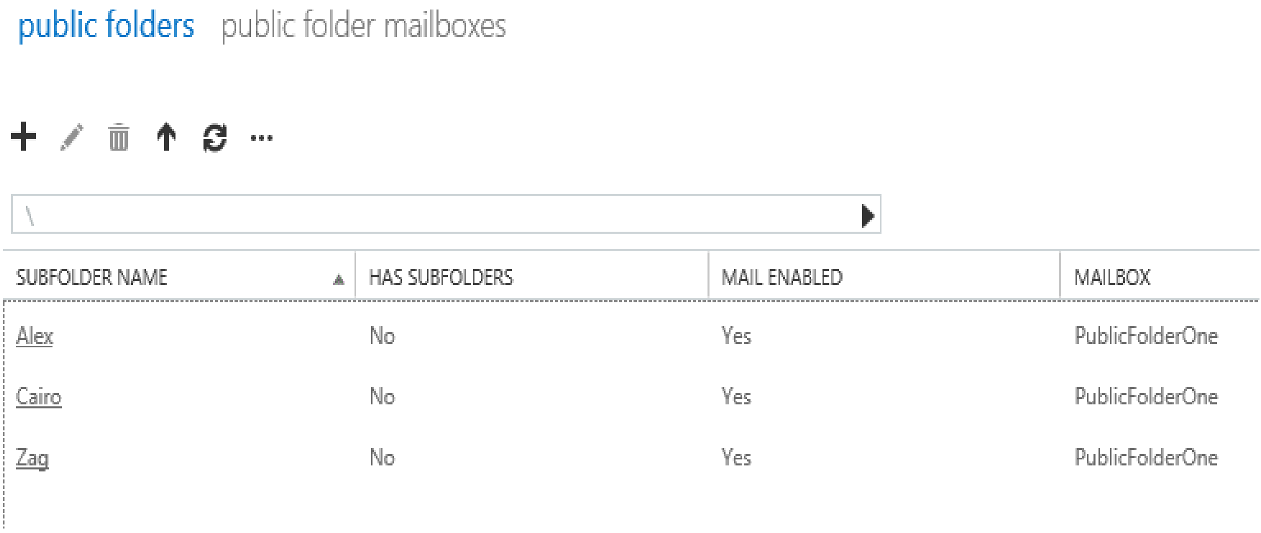
✓ Figure 6.5



NAME
Default Role Assignment Policy
Full Control

✓ Figure 6.6

Public folders are designed for shared access and provide an easy and effective way to collect, organize, and share information with other people in your workgroup or organization. Public folders help organize content in a deep hierarchy that is easy to browse. Users will see the full hierarchy in Outlook, which makes it easy for them to browse for the content they are interested in. That is why we have made some public folders based on the location of the user as shown in the following screenshot:

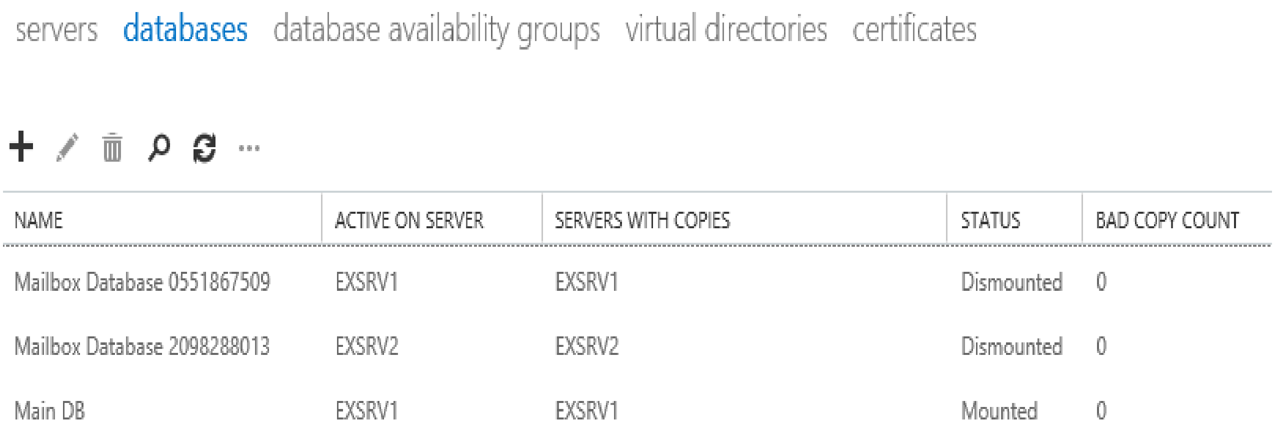


SUBFOLDER NAME	HAS SUBFOLDERS	MAIL ENABLED	MAILBOX
Alex	No	Yes	PublicFolderOne
Cairo	No	Yes	PublicFolderOne
Zag	No	Yes	PublicFolderOne

- ✓ Figure 6.7

As said, before we have mailboxes for every user and that mean they send and receive data locally and externally, and that mean we need a database to store the mailboxes.

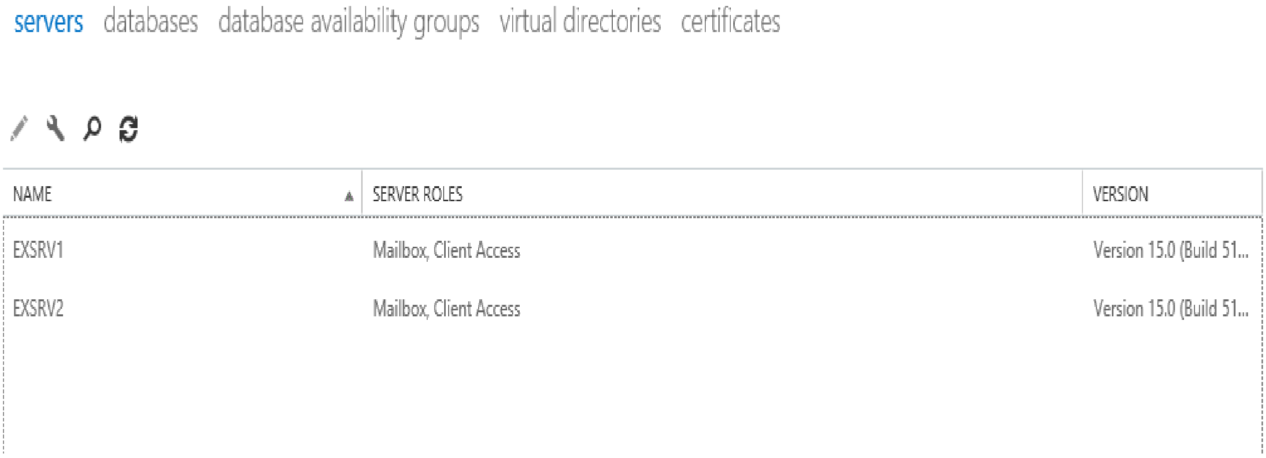
Here are the databases of the system:



NAME	ACTIVE ON SERVER	SERVERS WITH COPIES	STATUS	BAD COPY COUNT
Mailbox Database 0551867509	EXSRV1	EXSRV1	Dismounted	0
Mailbox Database 2098288013	EXSRV2	EXSRV2	Dismounted	0
Main DB	EXSRV1	EXSRV1	Mounted	0

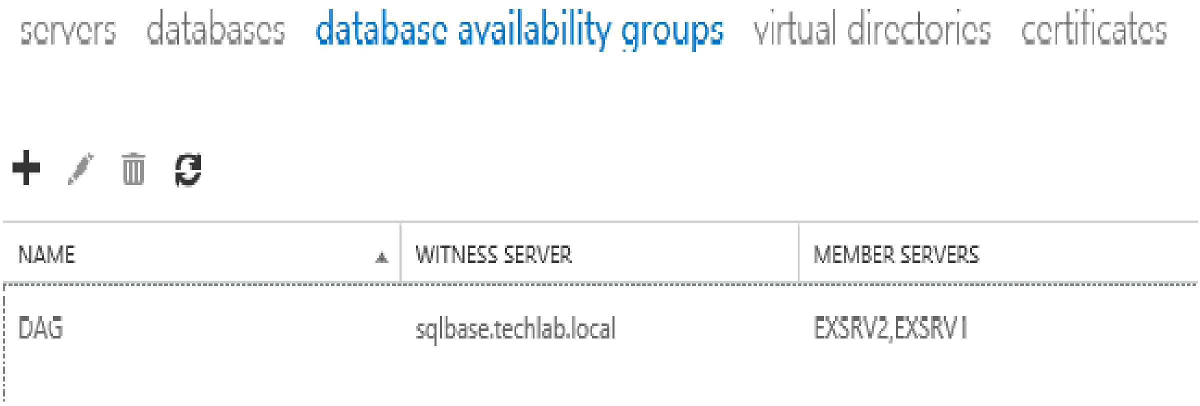
✓ Figure 6.8

To avoid the disasters that may happen and the failure that might happens to the exchange server, we have built another server so if one of them failed it will failover to the other one, so we have clustered the two servers as shown in the following screenshot:



NAME	SERVER ROLES	VERSION
EXSRV1	Mailbox, Client Access	Version 15.0 (Build 51...
EXSRV2	Mailbox, Client Access	Version 15.0 (Build 51...

✓ Figure 6.9



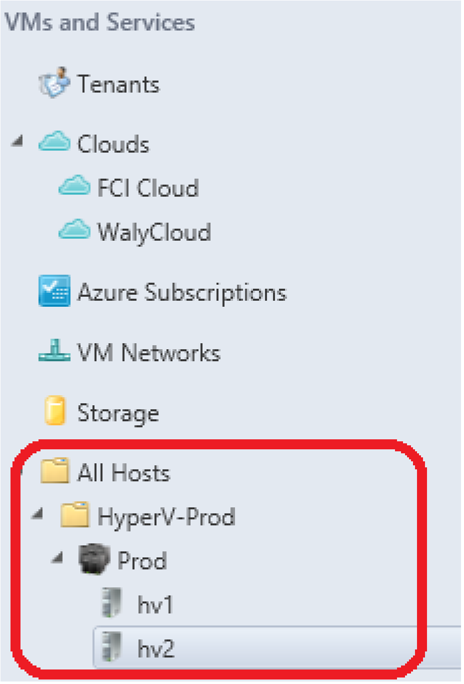
NAME	WITNESS SERVER	MEMBER SERVERS
DAG	sqlbase.techlab.local	EXSRV2,EXSRV1

- ✓ Figure 6.10

6.2 System Center Virtual Machine Manager:

This is the application we use to build our cloud and manage our virtual environment.

To build the cloud we needed to have a virtual environment first, so we have added to virtual hosts (HV1 & HV2) to be managed by SCVMM, and to ensure that everything is up and running the whole time, we made a cluster for our virtual environment, as shown in the following screenshot:



VMs and Services

Tenants

Clouds

FCI Cloud

WalyCloud

Azure Subscriptions

VM Networks

Storage

All Hosts

HyperV-Prod

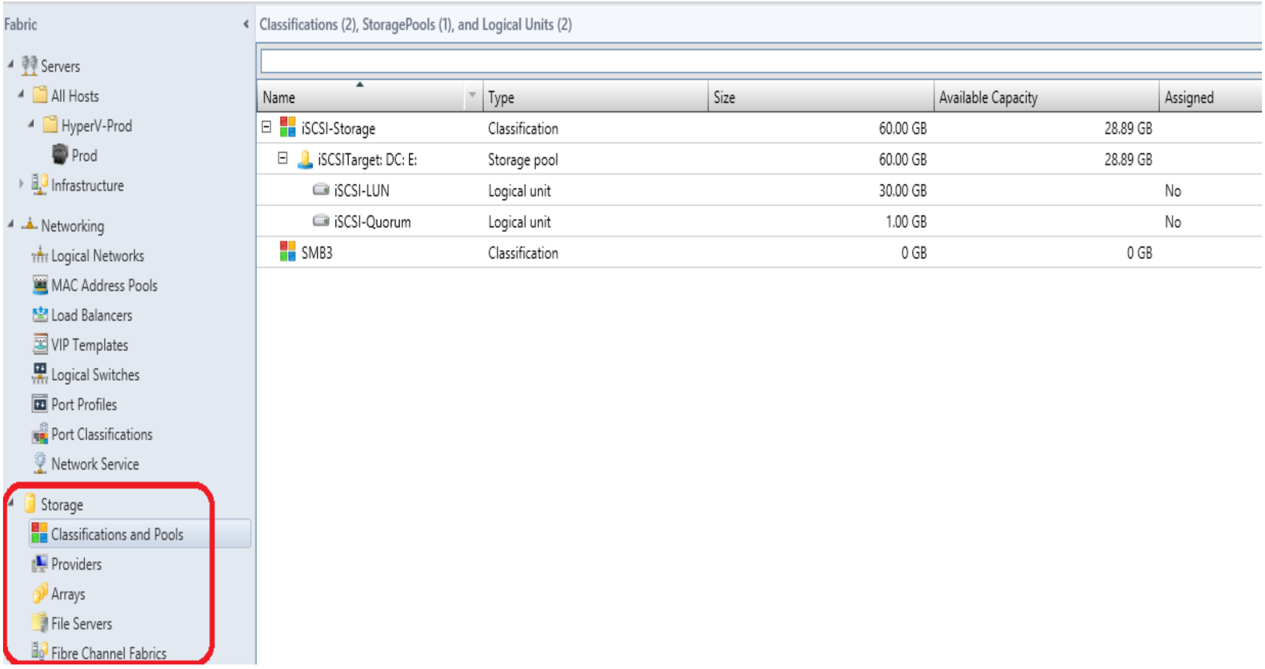
Prod

hv1

hv2

✓ Figure 6.11

As it is a needed component in the cloud environment to store the virtual machines and their data, the Storage comes to play a very important role and since we do not have enough budget to buy a SAN, so we used virtual SAN as described in the previous chapter and then we connected it to our virtual environment using SCVMM as shown in the following screenshot:

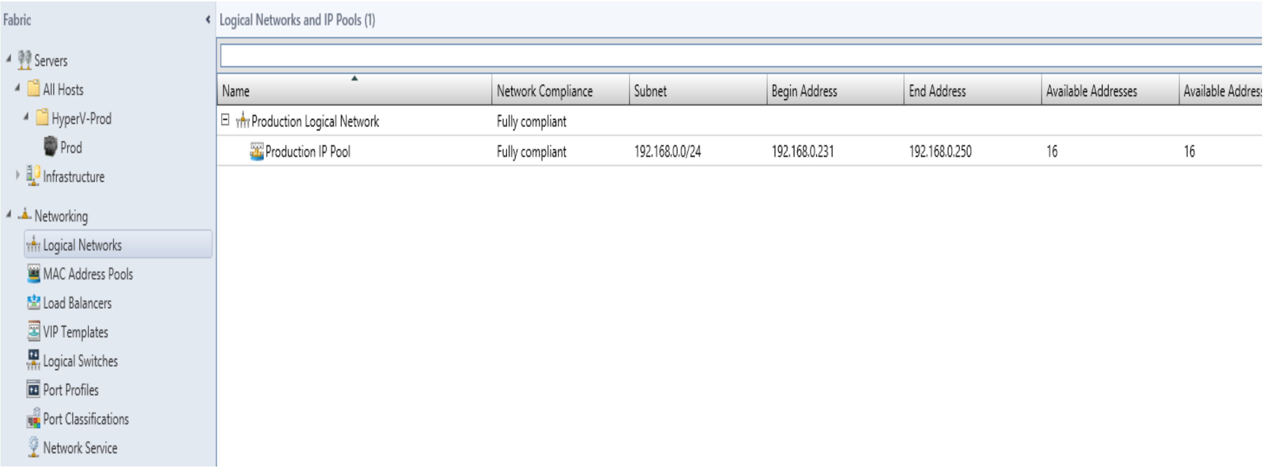


Classifications (2), StoragePools (1), and Logical Units (2)

Name	Type	Size	Available Capacity	Assigned
⊟ iSCSI-Storage	Classification	60.00 GB	28.89 GB	
⊟ iSCSITarget: DC: E:	Storage pool	60.00 GB	28.89 GB	
iSCSI-LUN	Logical unit	30.00 GB		No
iSCSI-Quorum	Logical unit	1.00 GB		No
SMB3	Classification	0 GB	0 GB	

- ✓ Figure 6.12

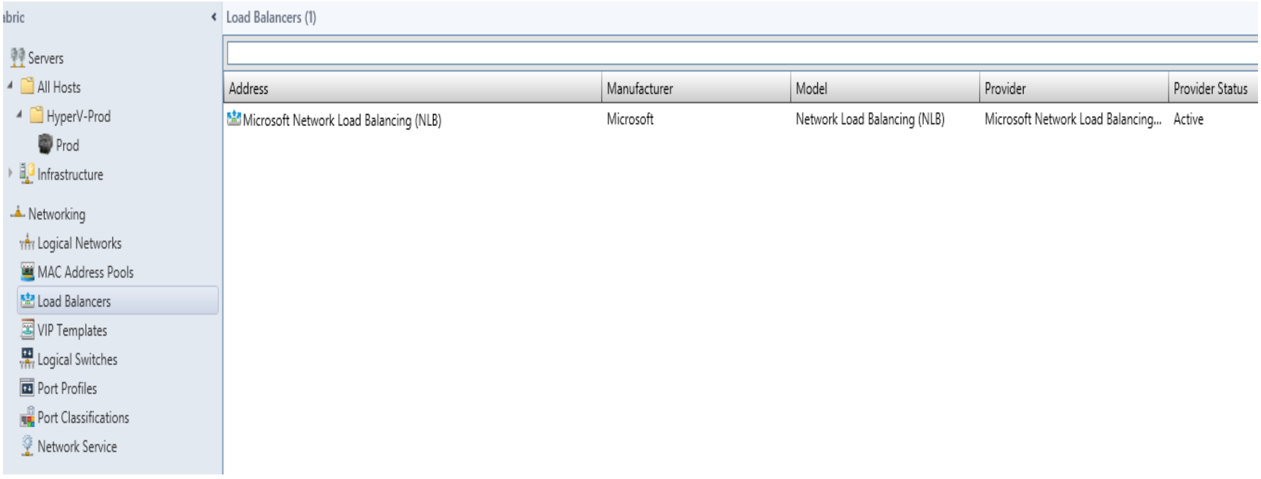
Another important part that would allow the virtual machines to communicate in the cloud is the networking so we have to create Logical Networks, Load Balancers, VIP Templates…etc., as shown in the following screenshots:



Logical Networks and IP Pools (1)

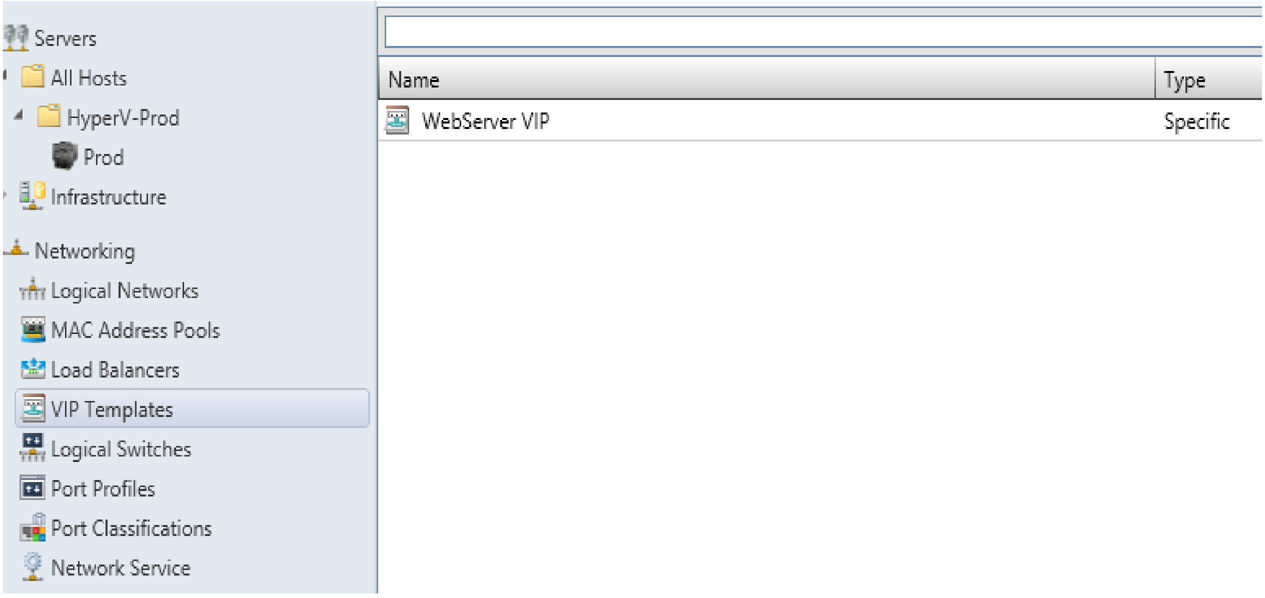
Name	Network Compliance	Subnet	Begin Address	End Address	Available Addresses	Available Addres
⊟ Production Logical Network	Fully compliant					
Production IP Pool	Fully compliant	192.168.0.0/24	192.168.0.231	192.168.0.250	16	16

- ✓ Figure 6.13



Address	Manufacturer	Model	Provider	Provider Status
Microsoft Network Load Balancing (NLB)	Microsoft	Network Load Balancing (NLB)	Microsoft Network Load Balancing...	Active

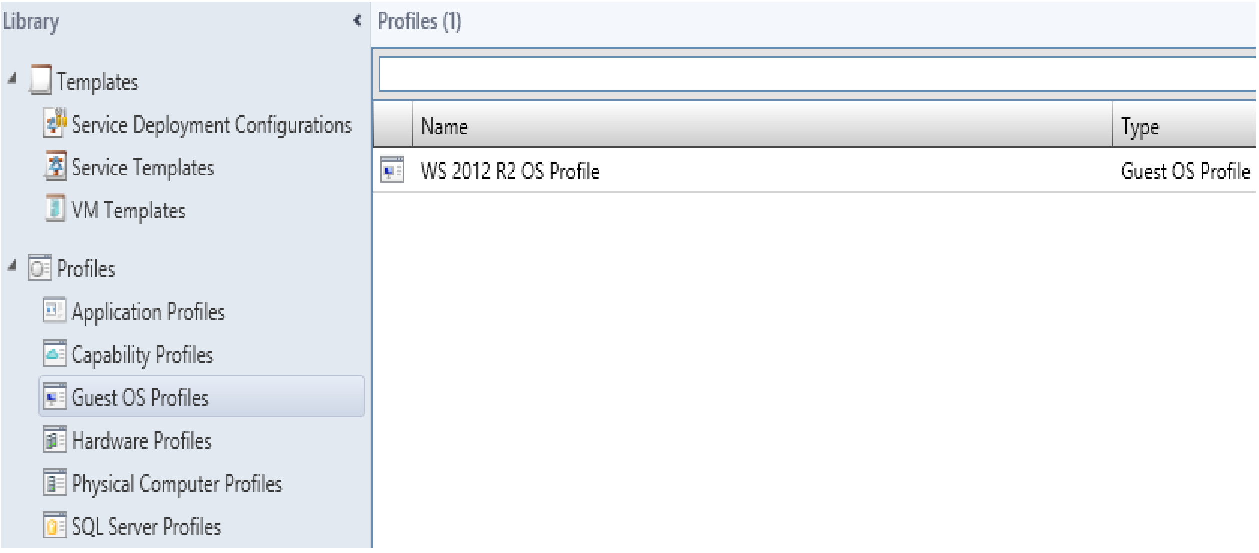
✓ Figure 6.14



Name	Type
WebServer VIP	Specific

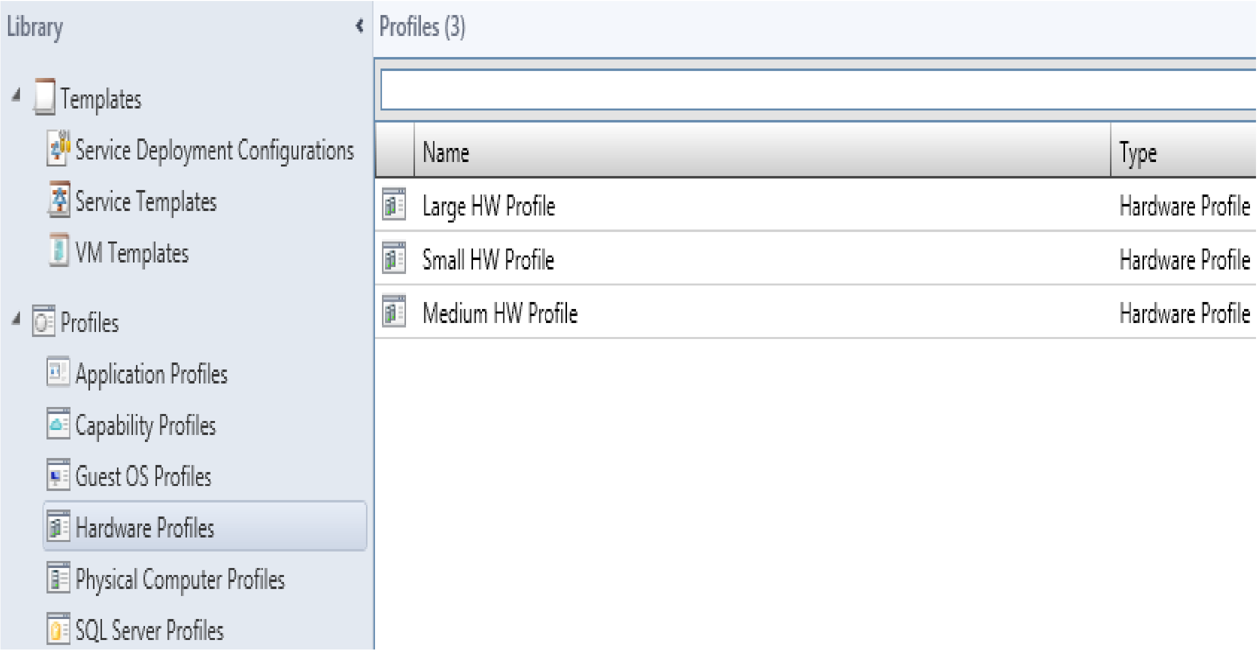
✓ Figure 6.15

In order to make it easy for Admins who want to create VMs in the cloud we have made some Guest OS Profiles and Hardware Profiles, as shown in the following screenshots:



Name	Type
WS 2012 R2 OS Profile	Guest OS Profile

✓ Figure 6.16

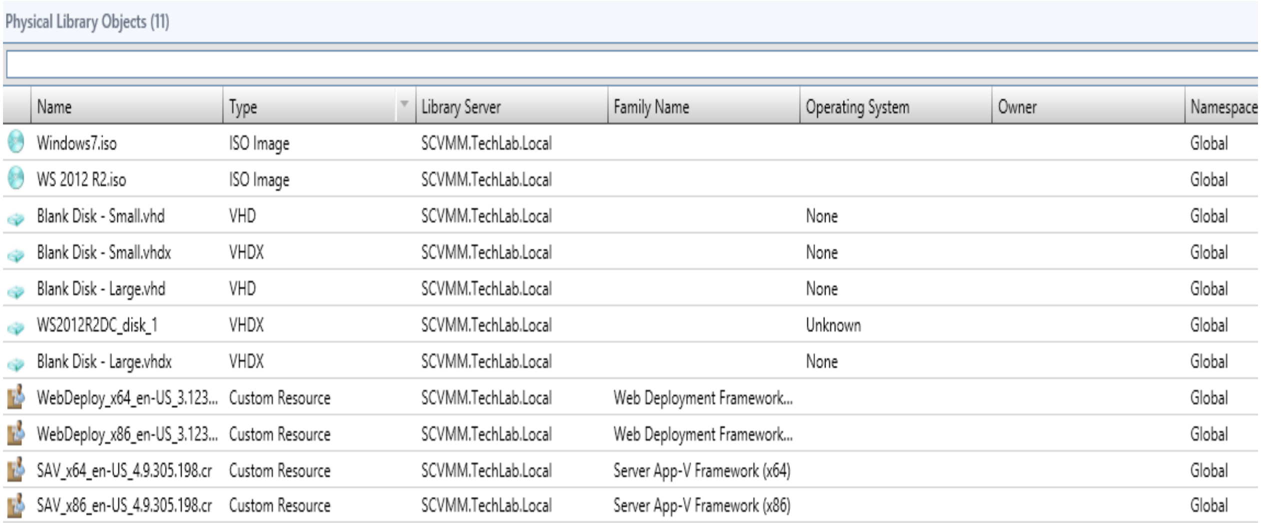


Name	Type
Large HW Profile	Hardware Profile
Small HW Profile	Hardware Profile
Medium HW Profile	Hardware Profile

✓ Figure 6.17

In addition, we have added some objects such as (ISOs, VHDs…etc.) to the library, which is part of the SCVMM, so we can use these objects when we create VMs.

Here are the objects added in our project.

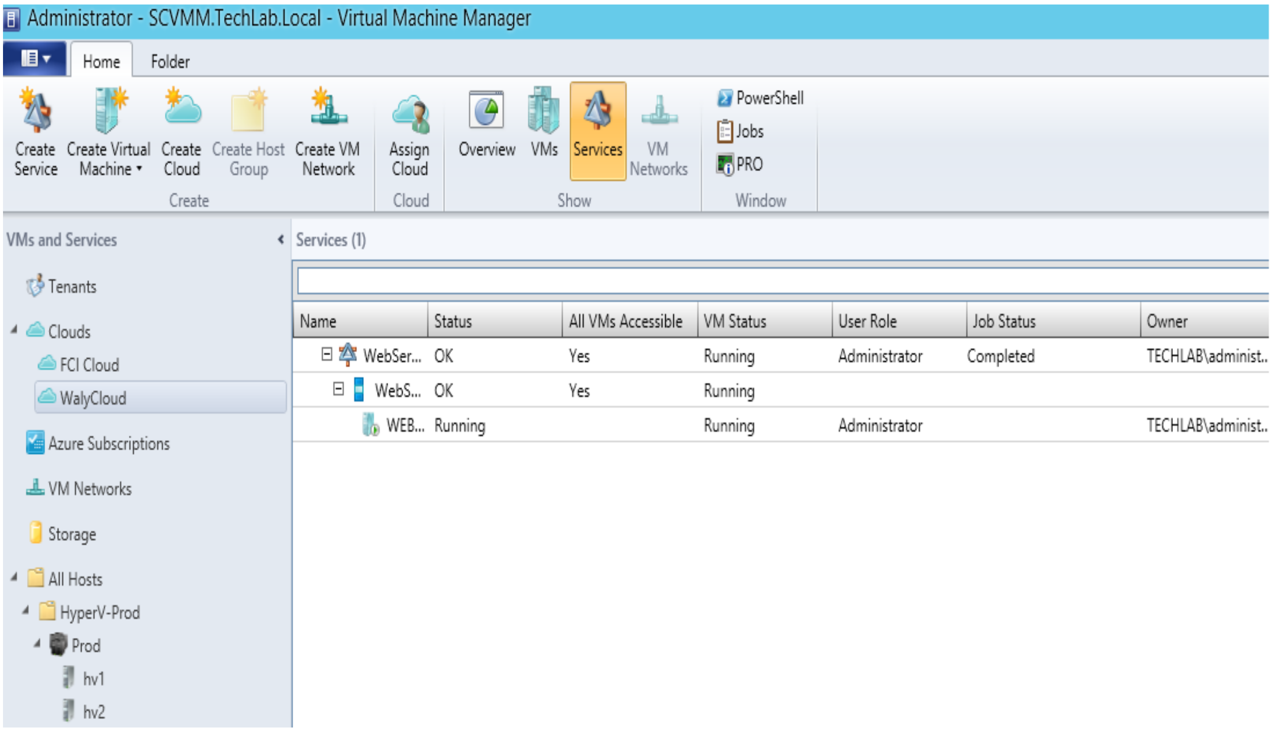


Physical Library Objects (11)

Name	Type	Library Server	Family Name	Operating System	Owner	Namespace
Windows7.iso	ISO Image	SCVMM.TechLab.Local				Global
WS 2012 R2.iso	ISO Image	SCVMM.TechLab.Local				Global
Blank Disk - Small.vhd	VHD	SCVMM.TechLab.Local		None		Global
Blank Disk - Small.vhdx	VHDX	SCVMM.TechLab.Local		None		Global
Blank Disk - Large.vhd	VHD	SCVMM.TechLab.Local		None		Global
WS2012R2DC_disk_1	VHDX	SCVMM.TechLab.Local		Unknown		Global
Blank Disk - Large.vhdx	VHDX	SCVMM.TechLab.Local		None		Global
WebDeploy_x64_en-US_3.123...	Custom Resource	SCVMM.TechLab.Local	Web Deployment Framework...			Global
WebDeploy_x86_en-US_3.123...	Custom Resource	SCVMM.TechLab.Local	Web Deployment Framework...			Global
SAV_x64_en-US_4.9.305.198.cr	Custom Resource	SCVMM.TechLab.Local	Server App-V Framework (x64)			Global
SAV_x86_en-US_4.9.305.198.cr	Custom Resource	SCVMM.TechLab.Local	Server App-V Framework (x86)			Global

✓ Figure 6.18

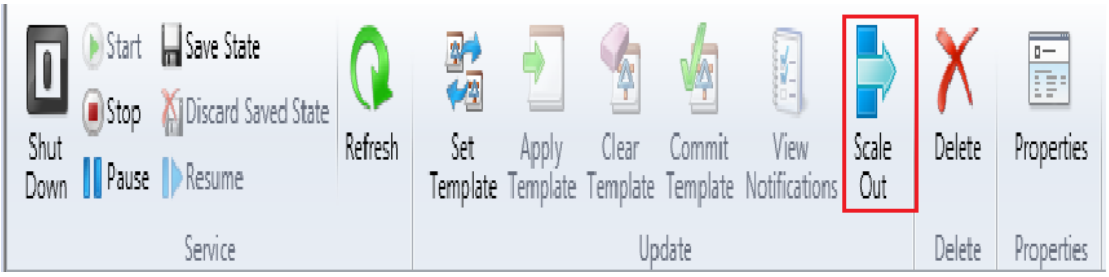
In our Project, we have two clouds one is called "FCI Cloud" and the other one is called "FCI Cloud". We have deployed a webserver, which the developers use to publish the organization website. This service can be scaled at any time as shown in the following screenshots:



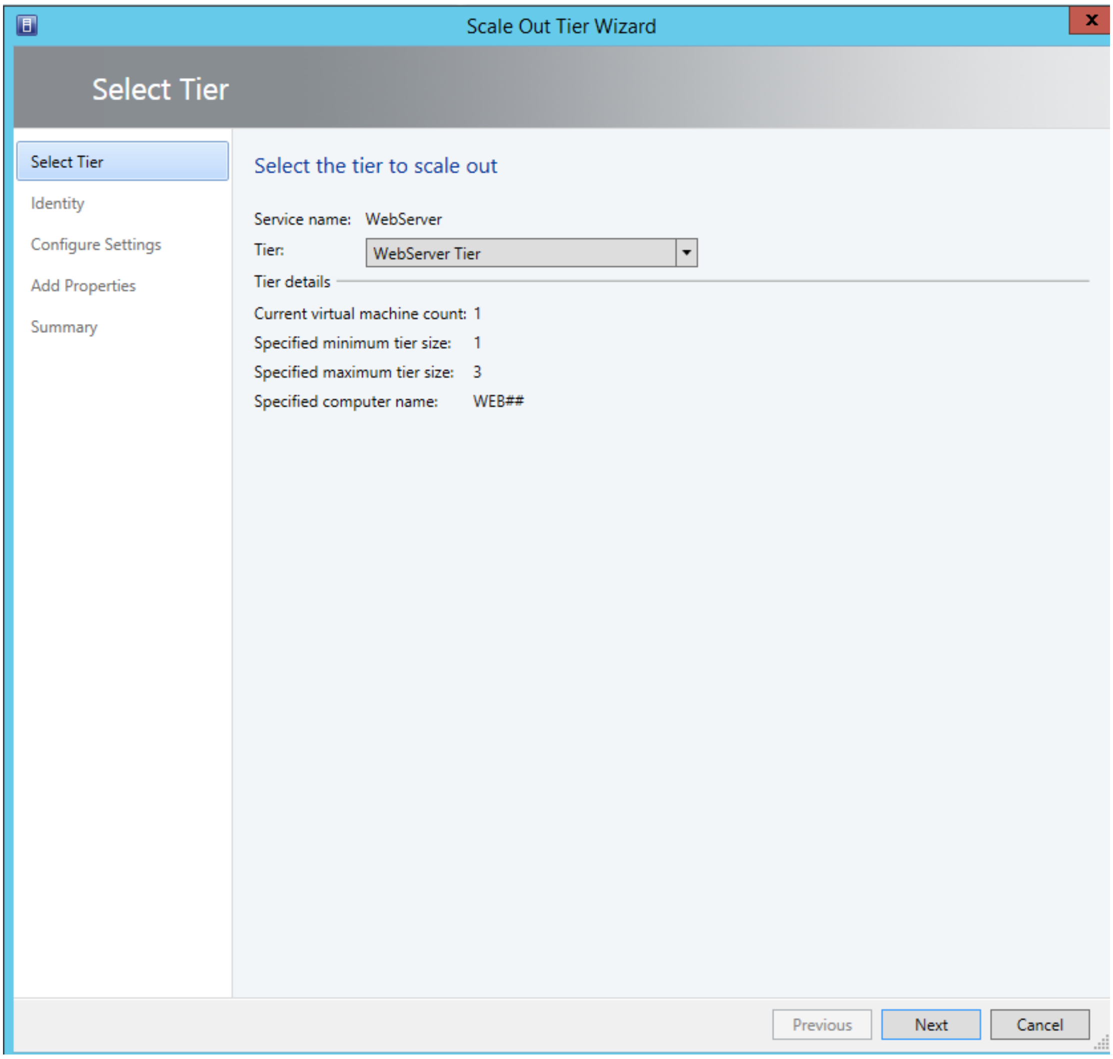
Services (1)

Name	Status	All VMs Accessible	VM Status	User Role	Job Status	Owner
WebSer...	OK	Yes	Running	Administrator	Completed	TECHLAB\administ...
WebS...	OK	Yes	Running			
WEB...	Running		Running	Administrator		TECHLAB\administ...

✓ Figure 6.19



- ✓ Figure 6.20



Select the tier to scale out

Service name: WebServer

Tier: WebServer Tier

Tier details

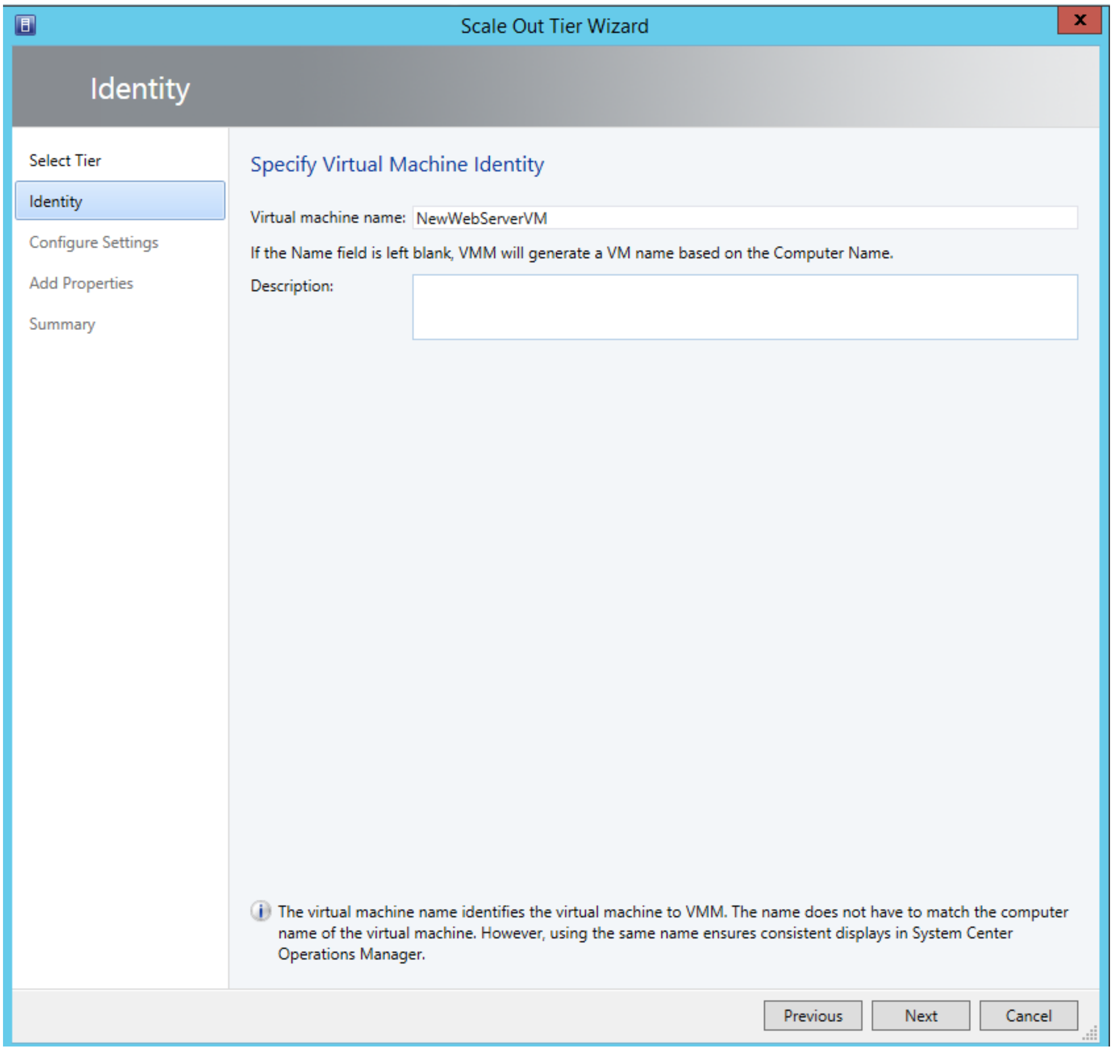
Current virtual machine count: 1

Specified minimum tier size: 1

Specified maximum tier size: 3

Specified computer name: WEB##

- ✓ Figure 6.21



Specify Virtual Machine Identity

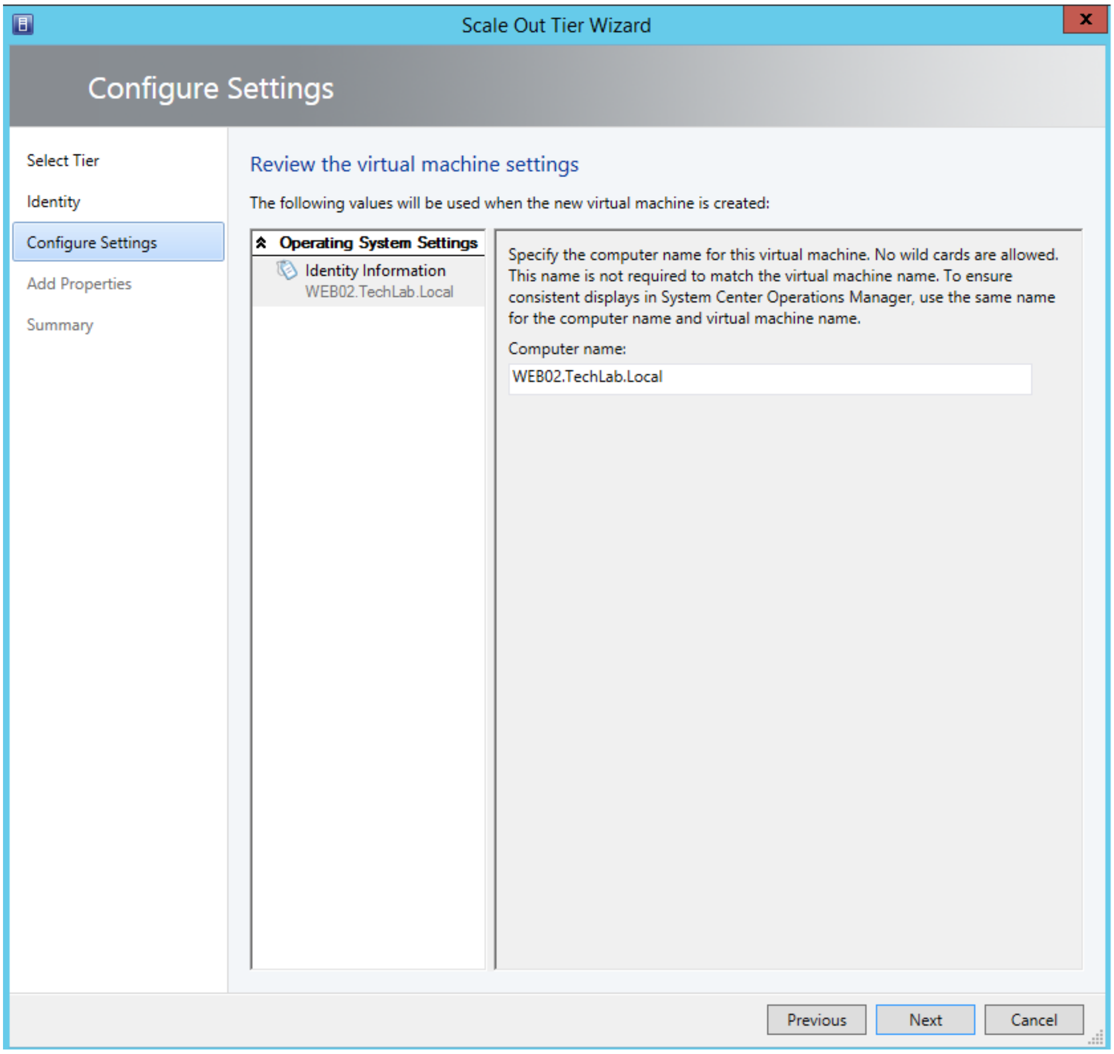
Virtual machine name: NewWebServerVM

If the Name field is left blank, VMM will generate a VM name based on the Computer Name.

Description:

The virtual machine name identifies the virtual machine to VMM. The name does not have to match the computer name of the virtual machine. However, using the same name ensures consistent displays in System Center Operations Manager.

- ✓ Figure 6.22



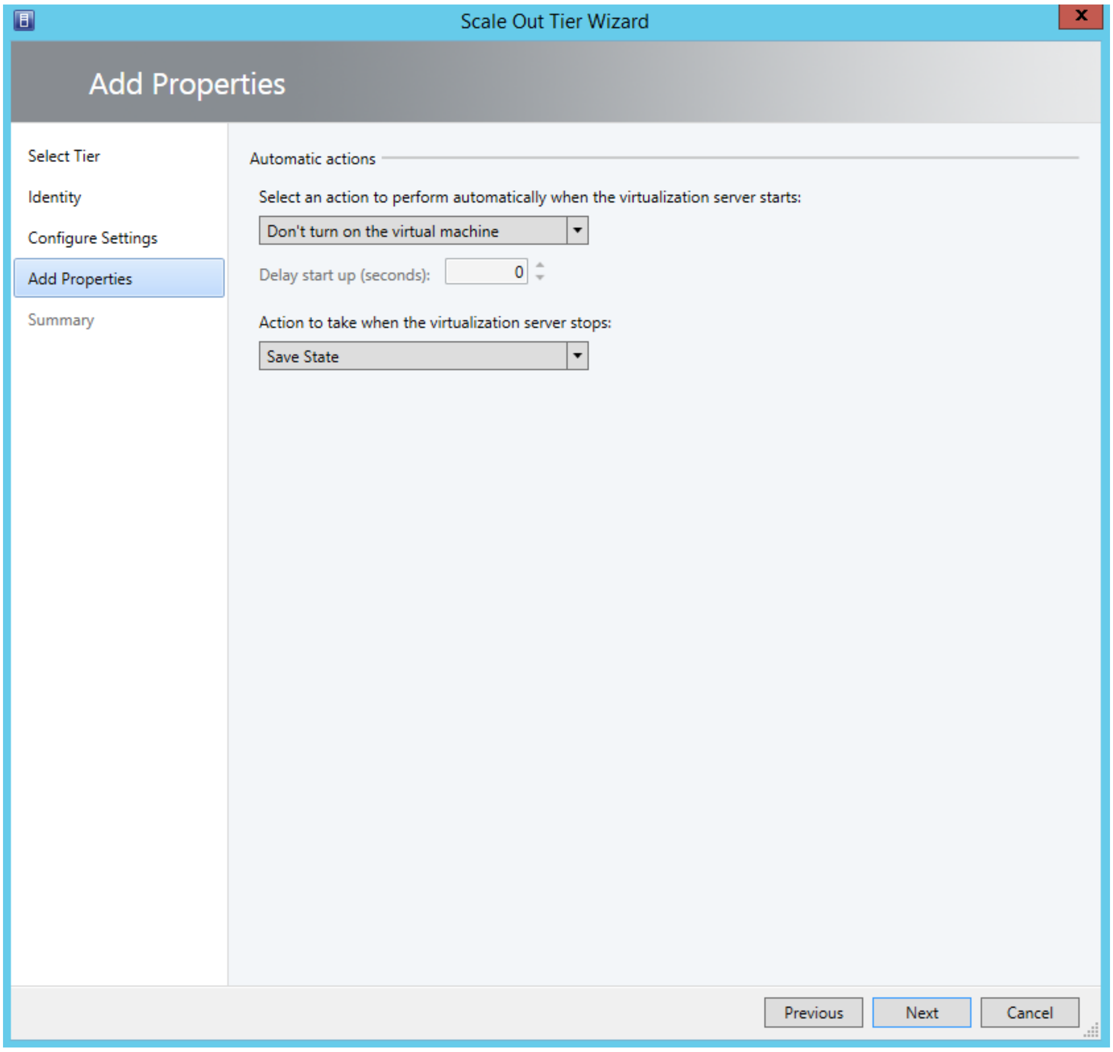
Review the virtual machine settings

The following values will be used when the new virtual machine is created:

Specify the computer name for this virtual machine. No wild cards are allowed. This name is not required to match the virtual machine name. To ensure consistent displays in System Center Operations Manager, use the same name for the computer name and virtual machine name.

Computer name: WEB02.TechLab.Local

- ✓ Figure 6.23



Automatic actions

Select an action to perform automatically when the virtualization server starts:

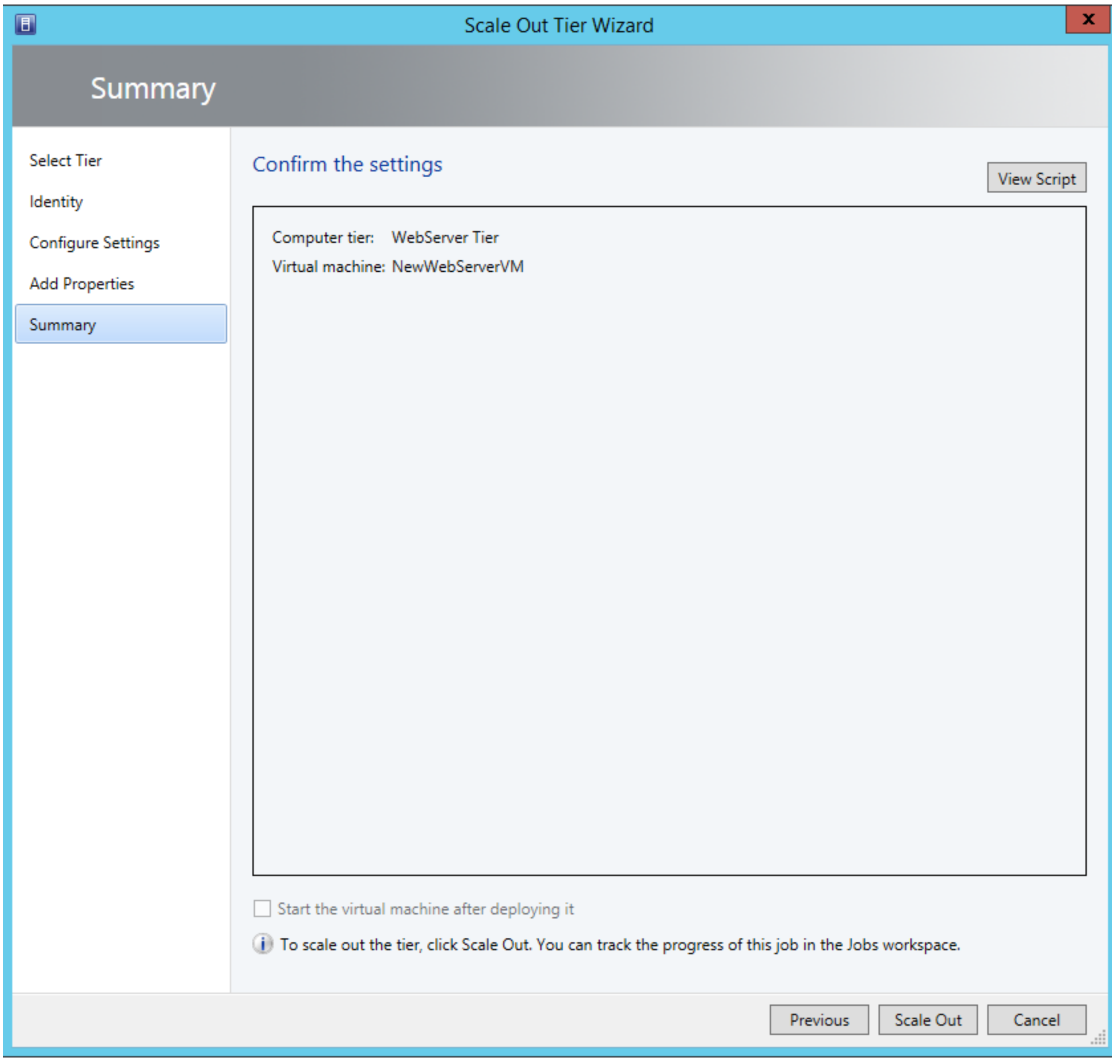
Don't turn on the virtual machine

Delay start up (seconds): 0

Action to take when the virtualization server stops:

Save State

- ✓ Figure 6.24

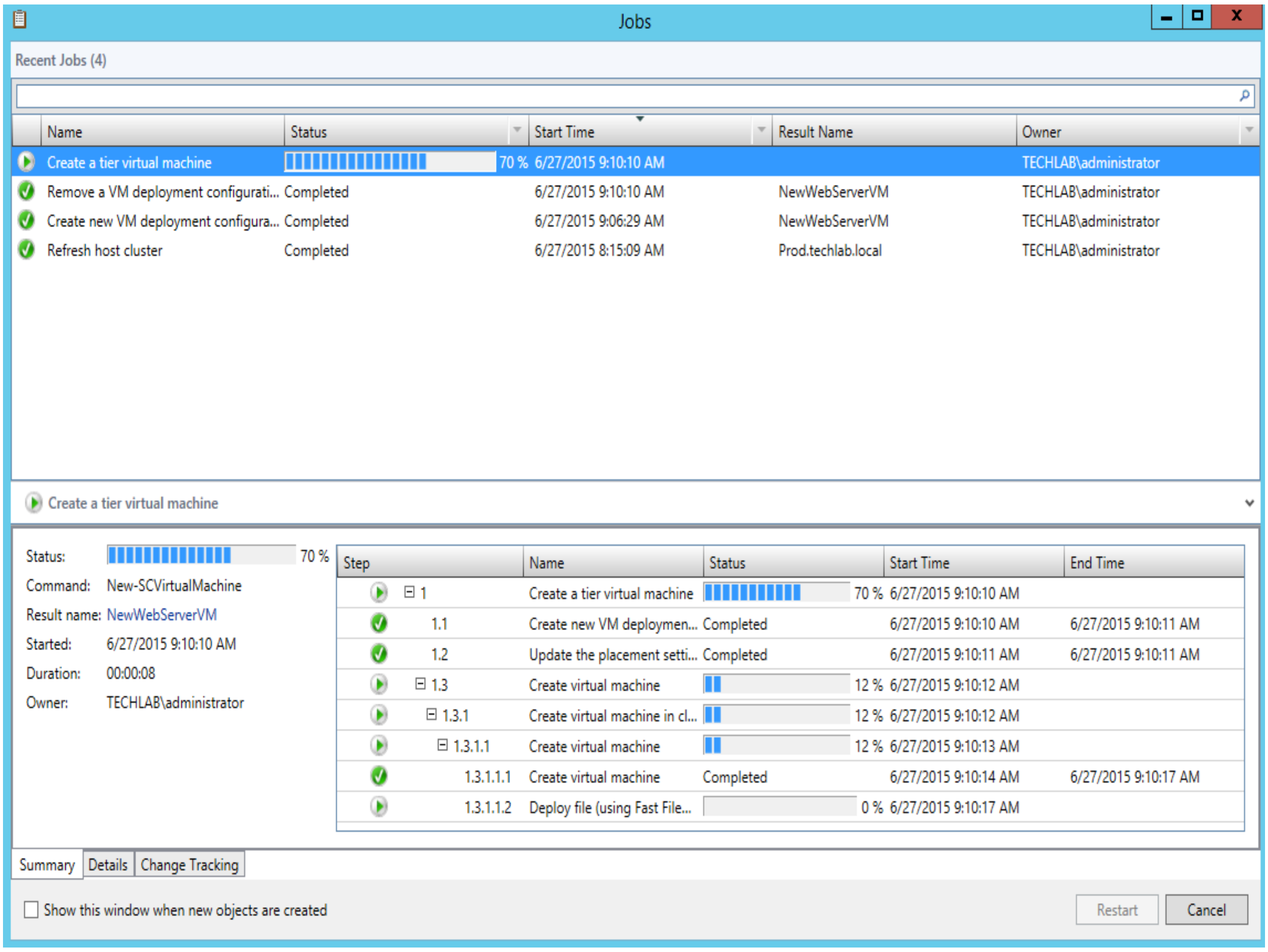


Computer tier: WebServer Tier
Virtual machine: NewWebServerVM

☐ Start the virtual machine after deploying it

To scale out the tier, click Scale Out. You can track the progress of this job in the Jobs workspace.

✓ Figure 6.25



Jobs

Recent Jobs (4)

Name	Status	Start Time	Result Name	Owner
Create a tier virtual machine	70 %	6/27/2015 9:10:10 AM		TECHLAB\administrator
Remove a VM deployment configurati...	Completed	6/27/2015 9:10:10 AM	NewWebServerVM	TECHLAB\administrator
Create new VM deployment configura...	Completed	6/27/2015 9:06:29 AM	NewWebServerVM	TECHLAB\administrator
Refresh host cluster	Completed	6/27/2015 8:15:09 AM	Prod.techlab.local	TECHLAB\administrator

Create a tier virtual machine

Status:	70 %
Command:	New-SCVirtualMachine
Result name:	NewWebServerVM
Started:	6/27/2015 9:10:10 AM
Duration:	00:00:08
Owner:	TECHLAB\administrator

Step	Name	Status	Start Time	End Time
⊟ 1	Create a tier virtual machine	70 %	6/27/2015 9:10:10 AM	
1.1	Create new VM deploymen...	Completed	6/27/2015 9:10:10 AM	6/27/2015 9:10:11 AM
1.2	Update the placement setti...	Completed	6/27/2015 9:10:11 AM	6/27/2015 9:10:11 AM
⊟ 1.3	Create virtual machine	12 %	6/27/2015 9:10:12 AM	
⊟ 1.3.1	Create virtual machine in cl...	12 %	6/27/2015 9:10:12 AM	
⊟ 1.3.1.1	Create virtual machine	12 %	6/27/2015 9:10:13 AM	
1.3.1.1.1	Create virtual machine	Completed	6/27/2015 9:10:14 AM	6/27/2015 9:10:17 AM
1.3.1.1.2	Deploy file (using Fast File...	0 %	6/27/2015 9:10:17 AM	

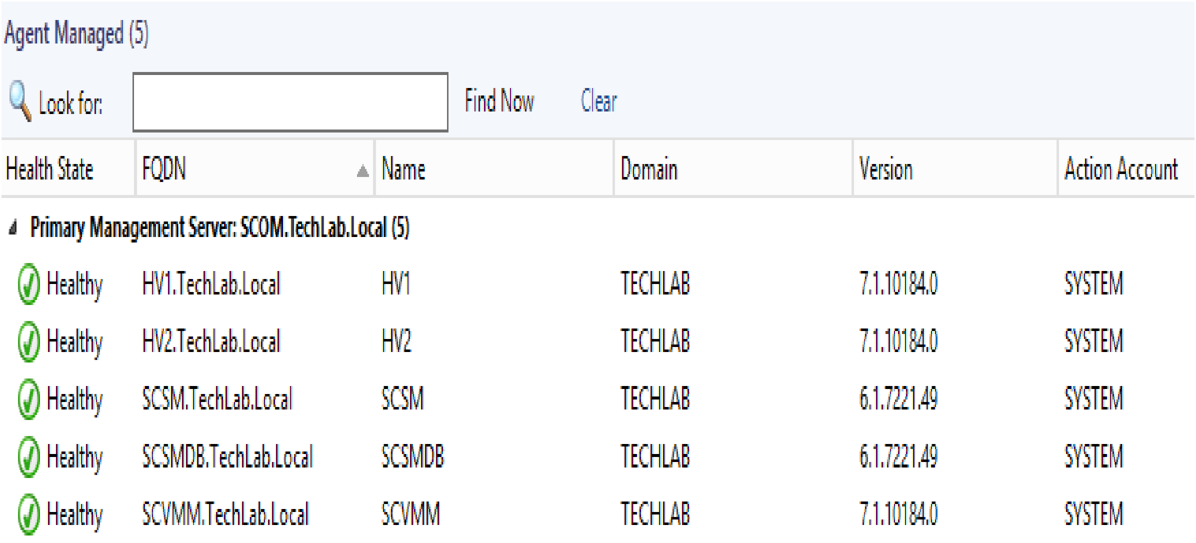
□ Show this window when new objects are created

✓ Figure 6.26

6.3 System Center Operations Manager:

As said before we use System Center Operations Manager to monitor our IT environment. So I can use to check if there are some errors with devices in our IT environment, and according to these errors, we start to fix our environment to keep it consistent and reliable and clean of errors.

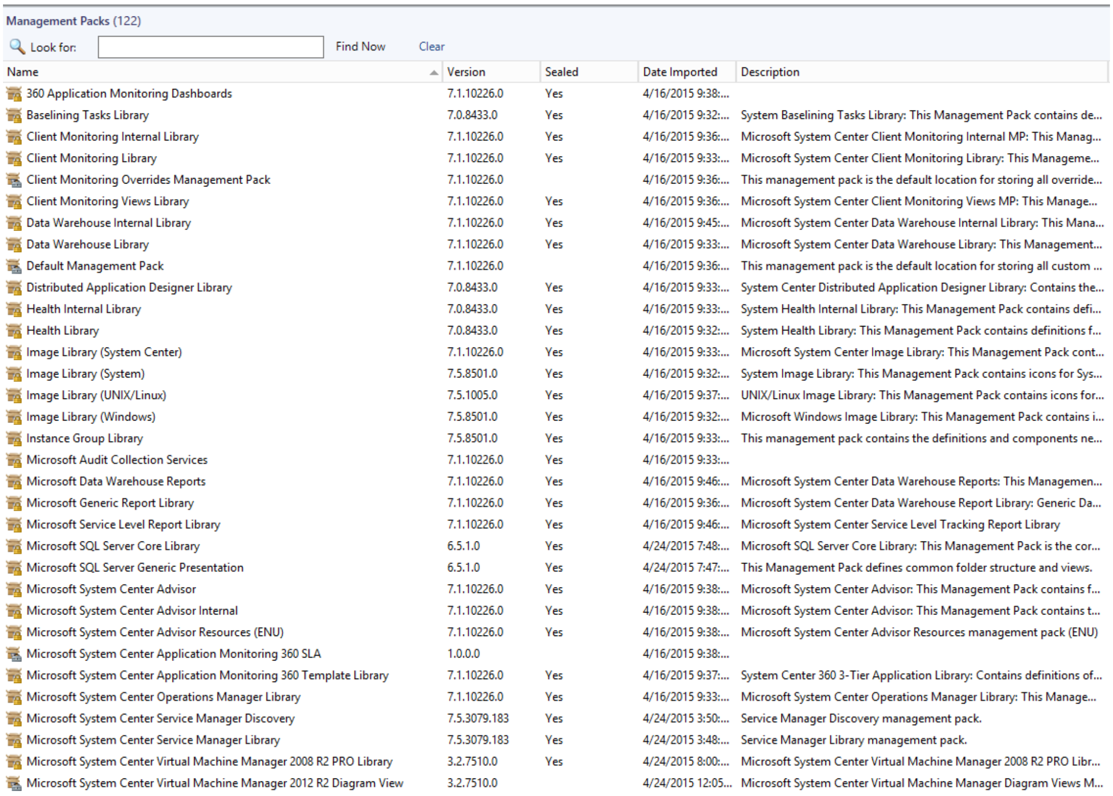
Here are some servers that are monitored by system center operations manager and they are in healthy state:



Health State	FQDN	Name	Domain	Version	Action Account
Primary Management Server: SCOM.TechLab.Local (5)					
Healthy	HV1.TechLab.Local	HV1	TECHLAB	7.1.10184.0	SYSTEM
Healthy	HV2.TechLab.Local	HV2	TECHLAB	7.1.10184.0	SYSTEM
Healthy	SCSM.TechLab.Local	SCSM	TECHLAB	6.1.7221.49	SYSTEM
Healthy	SCSMDB.TechLab.Local	SCSMDB	TECHLAB	6.1.7221.49	SYSTEM
Healthy	SCVMM.TechLab.Local	SCVMM	TECHLAB	7.1.10184.0	SYSTEM

✓ Figure 6.27

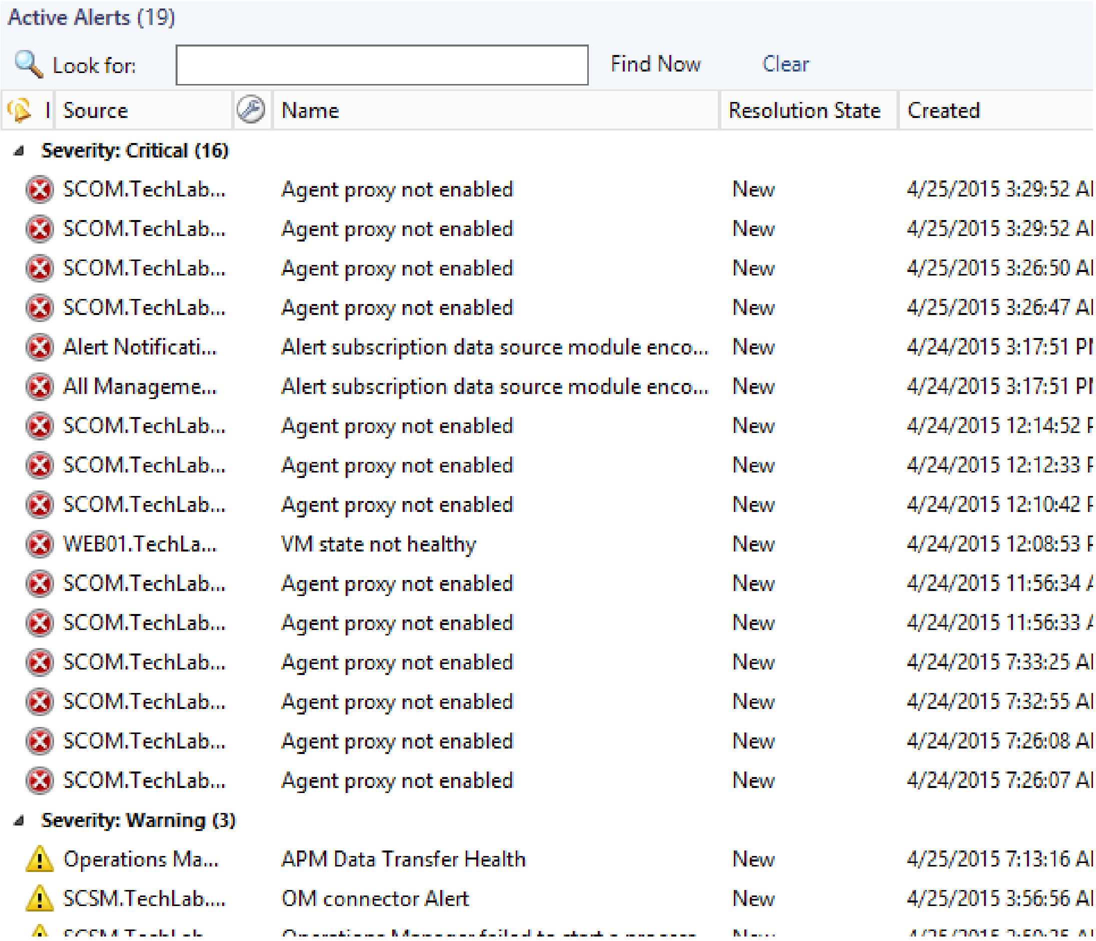
Therefore, we use something called "Management Packs" that determine in which case to trigger alerts. Here are some of the Management Packs we use in our project:



Name	Version	Sealed	Date Imported	Description
360 Application Monitoring Dashboards	7.1.10226.0	Yes	4/16/2015 9:38:...	
Baselining Tasks Library	7.0.8433.0	Yes	4/16/2015 9:32:...	System Baselining Tasks Library: This Management Pack contains de...
Client Monitoring Internal Library	7.1.10226.0	Yes	4/16/2015 9:36:...	Microsoft System Center Client Monitoring Internal MP: This Manag...
Client Monitoring Library	7.1.10226.0	Yes	4/16/2015 9:33:...	Microsoft System Center Client Monitoring Library: This Manageme...
Client Monitoring Overrides Management Pack	7.1.10226.0		4/16/2015 9:36:...	This management pack is the default location for storing all override...
Client Monitoring Views Library	7.1.10226.0	Yes	4/16/2015 9:36:...	Microsoft System Center Client Monitoring Views MP: This Manage...
Data Warehouse Internal Library	7.1.10226.0	Yes	4/16/2015 9:45:...	Microsoft System Center Data Warehouse Internal Library: This Mana...
Data Warehouse Library	7.1.10226.0	Yes	4/16/2015 9:33:...	Microsoft System Center Data Warehouse Library: This Management...
Default Management Pack	7.1.10226.0		4/16/2015 9:36:...	This management pack is the default location for storing all custom ...
Distributed Application Designer Library	7.0.8433.0	Yes	4/16/2015 9:33:...	System Center Distributed Application Designer Library: Contains the...
Health Internal Library	7.0.8433.0	Yes	4/16/2015 9:33:...	System Health Internal Library: This Management Pack contains defi...
Health Library	7.0.8433.0	Yes	4/16/2015 9:32:...	System Health Library: This Management Pack contains definitions f...
Image Library (System Center)	7.1.10226.0	Yes	4/16/2015 9:33:...	Microsoft System Center Image Library: This Management Pack cont...
Image Library (System)	7.5.8501.0	Yes	4/16/2015 9:32:...	System Image Library: This Management Pack contains icons for Sys...
Image Library (UNIX/Linux)	7.5.1005.0	Yes	4/16/2015 9:37:...	UNIX/Linux Image Library: This Management Pack contains icons for...
Image Library (Windows)	7.5.8501.0	Yes	4/16/2015 9:32:...	Microsoft Windows Image Library: This Management Pack contains i...
Instance Group Library	7.5.8501.0	Yes	4/16/2015 9:33:...	This management pack contains the definitions and components ne...
Microsoft Audit Collection Services	7.1.10226.0	Yes	4/16/2015 9:33:...	
Microsoft Data Warehouse Reports	7.1.10226.0	Yes	4/16/2015 9:46:...	Microsoft System Center Data Warehouse Reports: This Managemen...
Microsoft Generic Report Library	7.1.10226.0	Yes	4/16/2015 9:36:...	Microsoft System Center Data Warehouse Report Library: Generic Da...
Microsoft Service Level Report Library	7.1.10226.0	Yes	4/16/2015 9:46:...	Microsoft System Center Service Level Tracking Report Library
Microsoft SQL Server Core Library	6.5.1.0	Yes	4/24/2015 7:48:...	Microsoft SQL Server Core Library: This Management Pack is the cor...
Microsoft SQL Server Generic Presentation	6.5.1.0	Yes	4/24/2015 7:47:...	This Management Pack defines common folder structure and views.
Microsoft System Center Advisor	7.1.10226.0	Yes	4/16/2015 9:38:...	Microsoft System Center Advisor: This Management Pack contains f...
Microsoft System Center Advisor Internal	7.1.10226.0	Yes	4/16/2015 9:38:...	Microsoft System Center Advisor: This Management Pack contains t...
Microsoft System Center Advisor Resources (ENU)	7.1.10226.0	Yes	4/16/2015 9:38:...	Microsoft System Center Advisor Resources management pack (ENU)
Microsoft System Center Application Monitoring 360 SLA	1.0.0.0		4/16/2015 9:38:...	
Microsoft System Center Application Monitoring 360 Template Library	7.1.10226.0	Yes	4/16/2015 9:37:...	System Center 360 3-Tier Application Library: Contains definitions of...
Microsoft System Center Operations Manager Library	7.1.10226.0	Yes	4/16/2015 9:33:...	Microsoft System Center Operations Manager Library: This Manage...
Microsoft System Center Service Manager Discovery	7.5.3079.183	Yes	4/24/2015 3:50:...	Service Manager Discovery management pack.
Microsoft System Center Service Manager Library	7.5.3079.183	Yes	4/24/2015 3:48:...	Service Manager Library management pack.
Microsoft System Center Virtual Machine Manager 2008 R2 PRO Library	3.2.7510.0	Yes	4/24/2015 8:00:...	Microsoft System Center Virtual Machine Manager 2008 R2 PRO Libr...
Microsoft System Center Virtual Machine Manager 2012 R2 Diagram View	3.2.7510.0		4/24/2015 12:05...	Microsoft System Center Virtual Machine Manager Diagram Views M...

✓ Figure 6.28

Moreover, here are some alerts that have been triggered based on what we determined in the management packs:



Active Alerts (19)

🔍 Look for: Find Now Clear

I	Source	Name	Resolution State	Created
Severity: Critical (16)				
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/25/2015 3:29:52 AI
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/25/2015 3:29:52 AI
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/25/2015 3:26:50 AI
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/25/2015 3:26:47 AI
☒	Alert Notificati...	Alert subscription data source module enco...	New	4/24/2015 3:17:51 PI
☒	All Manageme...	Alert subscription data source module enco...	New	4/24/2015 3:17:51 PI
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/24/2015 12:14:52 F
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/24/2015 12:12:33 F
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/24/2015 12:10:42 F
☒	WEB01.TechLa...	VM state not healthy	New	4/24/2015 12:08:53 F
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/24/2015 11:56:34 /
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/24/2015 11:56:33 /
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/24/2015 7:33:25 AI
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/24/2015 7:32:55 AI
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/24/2015 7:26:08 AI
☒	SCOM.TechLab...	Agent proxy not enabled	New	4/24/2015 7:26:07 AI
Severity: Warning (3)				
⚠	Operations Ma...	APM Data Transfer Health	New	4/25/2015 7:13:16 AI
⚠	SCSM.TechLab....	OM connector Alert	New	4/25/2015 3:56:56 AI
⚠	SCSM.TechLab...	Operations Manager failed to start a process	New	4/25/2015 3:50:35 AI

✓ Figure 6.29

6.4 System Center Orchestrator:

We have used System Center Orchestrator in order to automate our tasks that takes a lot of human interaction and sometimes result in some errors. In brief, it makes our environment more flexible and eliminate redundancy.

6.5 Integrating the Applications together:

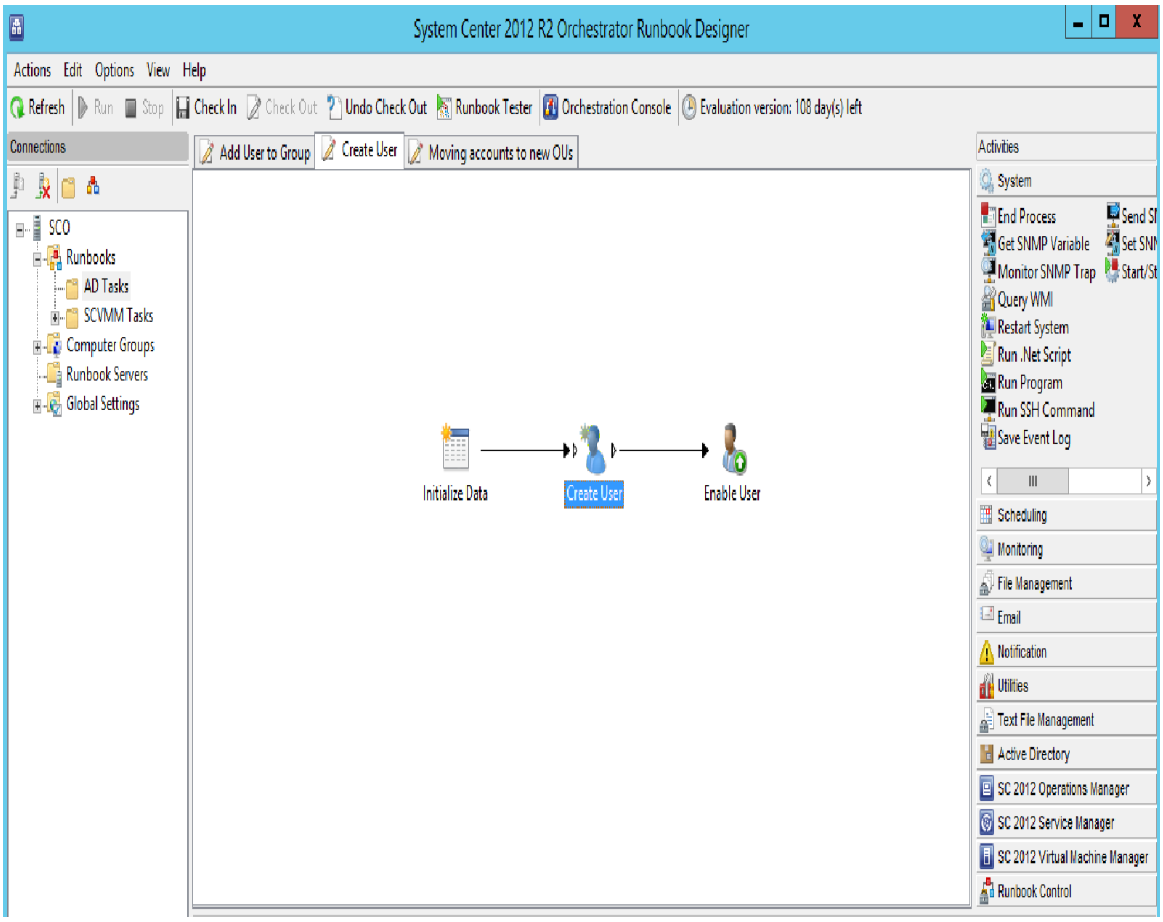
In order to get the best out of our IT environment we have integrated some of the applications together.

For instance, we have integrated:

- ✓ System Center Virtual Machine Manager with System Center Operations Manager.
- ✓ System Center Orchestrator with Active Directory
- ✓ System Center Orchestrator with System Center Operations Manager
- ✓ System Center Orchestrator with System Center Virtual Machine Manager

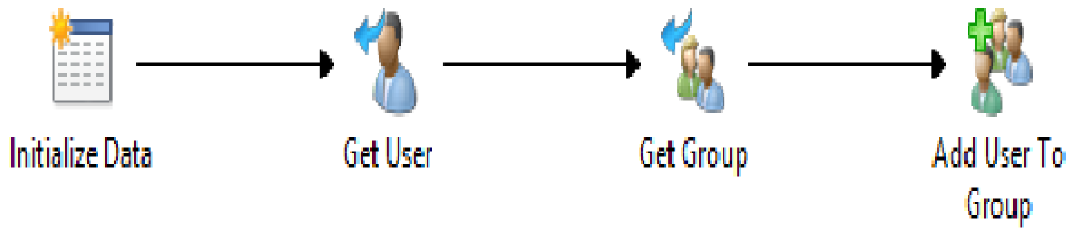
Here are some activities we have automated after integrating System Center Orchestrator with Active Directory:

1. Auto Created Users using the following runbook:



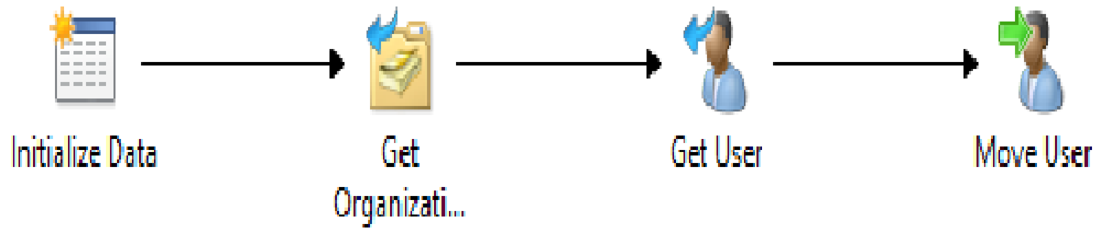
- Figure 6.30

2. Adding a user to a group automatically



- Figure 6.31

3. Adding users to Organizational units automatically



- Figure 6.32

Conclusion

In this documentation we have illustrated a very simple overview of "How it is going on" in our Project.

Starting with Network Infrastructure where we:

- Used the Cables, Routers, and Switches to build our environment
- Used Routing and Switching Protocols to ensure that the data packets we send reach to the specified user whether it is on the same network or not
- Used other techniques to ensure the stability of our environment such as (VPN, NAT, Frame Relay…etc.)
- Used Cisco VoIP to increase the collaboration in our environment
- Used Cisco security to keep our environment safe from malicious attacks.
- Built our System Infrastructure Platforms (Windows Server, SQL Server)
- Used Exchange Server to increase collaboration locally and externally
- Used System Center Products to build our Private Cloud
- Integrated System Center Products to ensure that our environment is Flexible, Scalable, Automated, and Agile.