Fast Fault Recovery in Switched Networks for Carrying IP Telephony Traffic

Master’s Thesis in Computer Network Engineering

ALI AKBAR EISAZADEH & NORA ESPAHBODI

School of Information Science, Computer and Electrical Engineering
Halmstad University
Fast Fault Recovery in Switched Networks for Carrying IP Telephony Traffic

Master’s Thesis in Computer Network Engineering

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

February 2010
Preface

First of all we would like to express our special gratitude to the Halmstad University for providing us a platform to complete this thesis.

Also we are greatly thankful for the support and helpful comments which we received from our supervisors, Ms. Olga Torstensson, our best lecturer during our studies in Halmstad University and Professor Tony Larsson for all his great advice.

We are very thankful to our Halmstad University friends and classmates who contributed, in whatever form, towards the realization of this thesis.

Ali Akbar Eisazadeh & Nora Espahbodi
February 2010
Abstract

One of the most parts of VOIP management is fault management and, in having a good fault management, finding good mechanisms to detect faults in the network have to be considered.

The main focus of this project is to implement different types of fast fault recovery protocols in networks, especially networks that carry IP telephony. Having a complete understanding of some common link failure detection and fault recovery protocols, such as spanning tree protocol (STP), rapid spanning tree protocol (RSTP) and per-VLAN spanning tree protocol (PVSTP), and also having a complete understanding of three other common techniques for fault detection and fault recovery, such as hot standby routing protocol (HSRP), virtual router redundancy protocol (VRRP) and gateway load balancing protocol (GLBP) will be regarded in the project. We are going to test some fault recovery protocols which can be used in IP telephony networks and choose the best. We intend to focus on this issue in LAN environment in theoretical descriptions and practical implementations.

The final outcome of the thesis is implementation in the Halmstad University’s lab environment to obtain the final result. For doing our thesis, we are going to use some technical tools as hardware tools (Cisco L3 and L2 switches, Routers, IP Phones) and tools which are used for network performance monitoring, like as CommVeiw.

Keyword:
STP (spanning tree protocol), RSTP (rapid spanning tree protocol), PVSTP (per-VLAN Spanning tree protocol), PVRSTP (per-VLAN rapid spanning tree protocol), MSTP (multiple spanning tree protocol), HSRP (hot standby routing protocol), VRRP (virtual route redundancy protocol), GLBP (gateway load balance protocol), VOIP (voice over IP).
Table of Contents

Preface........................................................................................................................ III
Abstract....................................................................................................................... IV
Table of Content....................................................................................................... V
Table and Figures ...................................................................................................... VII

CHAPTER 1 : Introduction ......................................................................................... 1
  1.1 Introduction....................................................................................................... 1
  1.2 Motivation........................................................................................................ 1
  1.3 Goal.................................................................................................................. 1
  1.4 Methodology .................................................................................................. 2
  1.5 Background ................................................................................................... 2

CHAPTER 2 : IP Telephony ...................................................................................... 3
  2.1 IP Telephony Overview .................................................................................. 3
  2.2 VOIP Components ....................................................................................... 3
  2.3 IP Telephony Benefits .................................................................................. 3
  2.4 VOIP Function .............................................................................................. 4
     2.4.1 Signaling................................................................................................. 4
     2.4.2 Data Services ....................................................................................... 4
     2.4.3 Bearer Control.................................................................................... 4
     2.4.4 Codec's Operation ............................................................................ 4
  2.5 VOIP Signaling Protocols............................................................................. 4
     2.5.1 MGCP ................................................................................................. 4
     2.5.2 H.323 ............................................................................................... 5
     2.5.3 SIP ................................................................................................. 5
     2.5.4 SCCP ............................................................................................... 5
  2.6 IP Telephony Problems and Challenges ...................................................... 5
  2.7 Cisco Unified IP Telephone ........................................................................... 6
     2.7.1 Low-End Cisco Unified IP Telephone ................................................... 6
     2.7.2 Mid-Range Cisco Unified IP Telephone .............................................. 6
     2.7.3 High-End Cisco Unified IP Telephone ................................................ 6

CHAPTER 3 : Loop Prevention .................................................................................. 8
  3.1 Problem of Having Redundant Path in the Network ..................................... 8
  3.2 Spanning Tree Protocol ................................................................................ 8
     3.2.1 Bridge Protocol Data Unit (BPU).......................................................... 9
     3.2.2 The STP Root Bridge ......................................................................... 9
     3.2.3 Spanning Tree Operation ................................................................. 10
Tables and Figures

Table 3.1: Recommendation Cost Link.................................................................9
Table 5.1: Hardware used to Build the Network..................................................24
Table 5.2: Applications Running on the Network.................................................25
Table 5.3: Configuration of IP Telephones and Hosts............................................27
Table 5.4: Result of Link Failure.........................................................................28
Table 5.5: Result of Implementation PVSTP without the use of Port Fast.............29
Table 5.6: Result of Implementation PVSTP with the use of Port Fast...................30
Table 5.7: Result of Implementation PVRSTP without the use of Port Fast............30
Table 5.8: Result of Implementation PVRSTP with the use of Port Fast..................30
Table 5.9: Summary of Implementations Results..................................................32
Figure 3.1: Loop..............................................................................................8
Figure 3.2: The Operation of STP.................................................................11
Figure 3.3: The Operation of RSTP..............................................................14
Figure 4.1: Gateway Redundancy in the Network.............................................18
Figure 5.1: Topology....................................................................................24
Figure 5.2: CommView software..............................................................26
Figure 5.3: Main Path of Communication...................................................28
CHAPTER 1

INTRODUCTION

1.1 Introduction

Using IP telephony is more popular in most organizations. There are, at least two reasons for expanding the use of IP telephony in the whole world. The first reason is, as we know, that IP telephony transfers voice traffic over the Internet protocol (IP). Then, a company can use the current infrastructure efficiently for providing both internet telephony and internet access to save money. The second reason is having easy implementation.

However one of important challenge in IP telephony is providing a VOIP network with high quality speech without any packet loss and delay. For achieving these types of network, we should use some mechanism to detect faults and recover quickly before it affects our networks.

In this thesis, different fault recovery protocols are discussed, but mainly two techniques, STP, RSTP, are comparatively studied and implemented. Also, three different high availability mechanisms are described, but mainly just one technique, HSRP, is studied and implemented in lab environments.

Finally STP and RSTP will be implemented and discussed and finally packet loss, ratio factor(R-Factor) and MOS (mean opinion score) will be measured with CommView software to establish which of them provides the best quality of speech and end-to-end connection from source to destination, and vice versa.

1.2 Motivation

In a switched network with carrying IP telephony traffic for achieving end-to-end voice, data, and video communications services and better speech quality, we need to implement a mechanism which will be able to detect faults and then recover as soon as possible. Otherwise, the performance of network will decrease because of increasing packet loss, jitter and delay.

So the model we proposed will definitely improve end-to-end voice, data, and video communications services, and it will increase the performance of network by detecting and recovering the point of fault and consequently decrease packet loss, jitter and delay.

The most important task in this research is to provide the best route from source to destination and the efficient flow of data in the IP telephony network. Also, the task is to implement the high redundant technique which offers and selects better paths for carrying data and voice in a switched network, especially for sending IP telephony traffic.

1.3 Goal

The main goal for the project is to find the number of fault detections and fault recovery protocols or techniques in a switched network and to implement high redundancy protocols to achieve the minimum packet loss, delay and to improve the quality of voice in IP telephony network and compare different types of fault recovery protocol and redundancy.

The main goals are:

• To build a high redundant switched network.
• To detect the best route from the source to destination for IP telephony traffic, then to achieve efficient flow in the network for both voice and data.
• To test and compare different types of STP and RSTP and describe three redundancy mechanisms such as HSRP, VRRP and GLBP.
• To reduce packet loss and increase the quality of voice in a switched network.

1.4 Methodology

The methodology of this project consists of both theoretical comparison and practical implementation. After extracting the useful information from available references, and implementing the proposed topology in the lab environment, the comparison is made.

Implementation is done with available equipment with different scenarios; the details of which is given in the chapter five and configurations are enclosed in the appendix.

1.5 Background

Before the innovation of IP telephony, most of the companies used internet, but they could not transmit data and voice together because they could not be converged together. With innovation of IP telephony, most of companies tried to use IP telephony because, firstly, it can transmit voice and data simultaneously; secondly, the companies had the infrastructure of implementing of IP telephony, such as internet. This issue can result to save money by companies. However the use of IP telephony has became more popular, the major concern with IP telephony is security, having the best quality speech as well as end-to-end data, voice communication services. For achieving the second one, improving a fault management system is required to monitor and analyse the network and detect the fault in the network, and then to recover the fault immediately. If a link from source to destination became down there are some protocols to detect the failure and select the best other route for carrying traffic. Two common types of protocols are STP, RSTP. Also, if a device such as a switch or a router crashes, there will be some techniques to detect it and prepare a redundant path through the other devices to prevent packet loss, delay and latency in the network. We will discuss about HSRP, VRRP and GLBP which are redundancy protocols.
CHAPTER 2

IP TELEPHONY

2.1 IP Telephony Overview

IP telephony or Internet protocol telephony is an applicable word for the technologies that use the IP packets to exchange voice, data, and other kinds of information which have been carried through the dedicated circuit of the public switched telephone network (PSTN) before the innovation of IP telephony. The transportation of telephone calls over the internet framework is known as “voice-over-IP” or “VOIP”. [1]

By using IP telephony, not only can we achieve significant and tremendous money savings, but also we can provide secure, reliable, scalable communications, which bring the advantages of LAN and WAN.

2.2 VOIP Components

The Internet telephony systems are composed of these elements:

- **End devices**: this can be either traditional telephones or special appliances.
- **Gateways**: when the traditional telephone is used to call, gateways translate traffic to format for sending over the internet without the problem of the type of traffic.
- **Gatekeepers**: functions such as centralized call management, call admission control, management of bandwidth, source and destination address translation, authentication, and user location are the task of gatekeepers.
- **Multipoint conference unit (MCU)**: conference management is one of the tasks of MCU. When traffic is transmitted between systems which are not in the same network speed and they do not use the same protocols of communication, the MCU resolves the problems and can prepare transport between these systems.
- **Call agent**: this has responsibility for the registration and management of resources at the media gateway (MG)
- **Application servers**: these are used for extending the functionality of IP telephony solutions.

2.3 IP Telephony Benefits

The most major benefits of using IP telephony are money-saving and easy implementation. Other benefits of IP telephony is shown below:

- To use a single infrastructure for providing access to both the Internet and Internet telephony
- Using data and voice simultaneously in communications can result in better use of bandwidth
- The IP telephony users can use IP telephony base on software. Software may be easily extended and integrated with other services and applications which can result in lower required time and money for users which ensure user satisfaction.
2.4 VOIP Function
There are some features in PSTN networks to establish a voice connection. Features to accomplish a VOIP connection is shown below:

- Signalling
- Database services
- Call connect and disconnect (bearer control)
- CODEC operations

2.4.1 Signalling
Signalling in VOIP network is achieved by the exchange of IP datagram messages between components.

2.4.2 Database services
Database services is necessary to determine an endpoint place as well as to translate the addressing which used by two endpoints. For example, a phone number is used to identify endpoint in PSTN, while VOIP uses the IP address and port numbers to identify an endpoint. A call control database is composed of both mapping and translations.

2.4.3 Call Connects and Disconnects (bearer control)
To establish a call, two endpoints are needed to open communication sessions between each other. In the PSTN, this task is performed by switches, which can be private or public. Connection in VOIP is a multimedia flow such as audio, video or both, which is transported in real time. This channel is a representation of bearer channel and it shows the voice or video being carried.

2.4.4 Codec Operation
Since traditional voice communication is analog, whereas data networking is digital, it is necessary to convert analog traffic to digital flow. This process is done by a coder-decoder. Most conversations are based on pulse codec modulation (PCM) or variations.

In addition, codecs can compress a data stream that can result in the better use of bandwidth. In addition, codecs ensure to avoid call echo which is widespread and this issue annoys users. Some common VOIP codecs are: G.711, G.722, G.723, and G.729 which use different bandwidths. For example, G.711 uses 64 Kbps bandwidth, whereas G.729 has excellent bandwidth utilization.

2.5 VOIP Signalling Protocols
Some of the VOIP signalling protocols are described as follows:

- MGCP (media gateway control protocol)
- H.323
- SIP (session initiation protocol)
- SCCP (skinny client control protocol)

2.5.1 MGCP (Media Gateway Control Protocol)
MGCP is necessary to convert the audio signals which used by traditional telephone circuits to data packets. In the MGCP, the main focus of gateway is the function of the audio
signal translation, whereas the task of call agent can be represented with call signalling and call processing.

2.5.2 H.323

H.323 was designed to provide transformation of audio and video-data of real time applications in networks such as IP networks. Since H.323 can be represented by several different protocols, it is provided to support IP-telephony and its requirements. Most VOIP applications use H.323. This protocol supports call setup, teardown of connection, forwarding of packets. [1]

2.5.3 SIP (Session Initiation Protocol)

SIP is an application layer protocol which provides an identification of the calling numbers (caller) and called numbers (recipient), authentication of the caller and recipient, and the act of call forwarding is the task of SIP. To identify the caller and recipient, SIP uses SIP addresses which seem to be same as e-mail addresses. SIP messages can be sent over either TCP or user datagram protocol (UDP). [2]

2.5.4 SCCP (Skinny Client Control Protocol)

One of expectations of the VOIP solution is the simple use of an end station in the LAN. In addition end stations should be rather cheap and familiar in the user view. SCCP provides a more easily usable architecture than H.323. An H.323 proxy can be provided to alternate with the SCCP.

The main benefit of SCCP is that it is used to support quick changes in the protocol. SCCP is the simplest protocol which is used in VOIP networks. IP Phones which are using SCCP can work with H.323 together. It can be said that SCCP is the protocol for the IP telephony network that is more preferable.

2.6 IP Telephony Problems & Challenges

The general difference between traffic that is carried through PSTN and IP-network is that PSTN is dependent to static switching and geographic location for services to be available, whereas Internet-base topology includes dynamic routing which is not dependent on geographic location. [1]

Some of IP-telephony’s problems and challenges are claimed to be as follows:

- An analog telephone adaptor, IP telephone or a computer is needed for VOIP. All of this equipment requires power and will not continue its task if there is the condition of a shutdown in power. By using UPS backup we can solve this problem.

- Internet vulnerabilities such as denial of service attacks, snooping and spoofing can threaten the VOIP security.

- Latency (delay) is one of the problems in this type of connection also, if security measures are applied to make encryption, the latency factor will grow and it will result in loss of quality of voice.

- Hackers have created problems with the internet and this issue will be present for voice over internet as well.
- Some VOIP protocols do not work with older firewalls and NAT (network address translation).
- When there is a congestion of users in the network and the number of users increase it will affect the use of bandwidth, and also create problems in QoS (quality of service) and reliability for real time applications and can result in loss of words in a conversation.

2.7 Cisco Unified IP Phone

The Cisco Unified IP Phones are classified as low-end, mid-range and high-end IP phones. The applicable Cisco Unified IP Phones for a Cisco Unified CME environment are described as follows: [3]

- Low-end Cisco unified IP phones
- Mid-range Cisco unified IP phones
- High-end Cisco unified IP phones

2.7.1 Low-end Cisco Unified IP Phones

The low-end Cisco unified IP phones include:

- Cisco unified IP phone 7902G
- Cisco unified IP phone 7905G
- Cisco unified IP phone 7910G
- Cisco unified IP phone 7910G+SW
- Cisco unified IP phone 7911G
- Cisco unified IP phone 7912G

2.7.2 Mid-range Cisco Unified IP Phones

When there is a high-traffic situation with extensive call features, such as speakers, headset, Mid-range Cisco unified IP phones are suitable. The mid-range Cisco unified IP phones include:

- Cisco unified IP phone 7940G
- Cisco unified IP phone 7941G
- Cisco unified IP phone 7960G
- Cisco unified IP phone 7961G

We used two Mid-range Cisco unified IP phones (7960G) in our thesis.

2.7.3 High-end Cisco Unified IP Phones

High-end Cisco unified IP phones include the following:

- Cisco unified IP phone 7970G
- Cisco unified IP phone 7971G
The Cisco unified IP phone 7970G has features such as high-resolution, colour touch-screen display, more function keys, and more security features than the mid-range Cisco unified IP phones. [3]
CHAPTER 3

LOOP PREVENTION

3.1 Problem of Having Redundant Path in the Network

In most networks, having a redundant path from source to destination is more important. In this situation, if one path fails, data or voice can send from another path and depends on which redundancy mechanism is used, packet loss, jitter and delay will be different, but by using multi-path between source and destination, loop will happen. This means, as you see in figure 3.1, when PC1 sends packet to PC2, the same packet will be sent through two different switches to the destination, while PC2 can not accept the same packet with the same Mac address.

Therefore, PC2 will broadcast the packet to PC1, and this action will be repeated and a loop will be created. To solve this problem and to have a loop free network, one of those links should be blocked or shut down. One of the best mechanisms to solve this problem is to use STP on the network.

![Figure 3.1: Loop](image)

3.2 Spanning Tree Protocol

Spanning-tree protocol is a protocol which is used to prevent loops in the networks and it provides path redundancy. [4]

As we mentioned earlier, implementing redundancy in a network can create a loop and to solve it, STP is one of the mechanisms which uses spanning tree algorithm (STA) on each of the switches to activate or block redundant links. After implanting STP on the network, STA selects a point, which is called the “references point” to find redundant paths and it can find the best path between source and destination. The references point decides which path should be blocked and which path should be used for forwarding packets. [5]

To understand the operation of STP, we should first know about the bridge protocol data unit (BPDU), the root bridge of STP and the port roles in STP.
3.2.1 Bridge Protocol Data Unit (BPDU)

An STP needs to exchange information between the switches within an LAN. BPDU is used for that purpose and it is a message which is exchanged across bridges to detect loop in a network. If it finds the loop on the network, then it will remove it by turning off the interfaces and it will place the redundant switch ports in a backup, or blocked state. [6]

The information of BPDU contains:

**Root ID:** the lowest bridge ID in the network will be chosen as root ID.

**Cost of path:** this is the cost of link between two switches.

There is a cost link recommendation according to table 3.1: [7]

**Bridge ID (BID):** this is an ID of the switch which is transmitting packet.

**Port ID:** this is an ID of the switch port which is transmitting packet.

**STP Timer Values:** STP uses three timers, which will be explained later.

<table>
<thead>
<tr>
<th>Data Rate</th>
<th>Recommendation cost link values</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Mbps</td>
<td>250</td>
</tr>
<tr>
<td>10 Mbps</td>
<td>100</td>
</tr>
<tr>
<td>16 Mbps</td>
<td>62</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>19</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>4</td>
</tr>
<tr>
<td>10 Gbps</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 3.1: Recommendation cost link

3.2.2 The STP Root Bridge

The first task of STP after implementation on a network is to select a bridge as a reference point which all switches use to establish the forwarded paths. It is called a “root bridge” and a root bridge is a switch with the lowest bridge ID. A bridge ID consists of two parts: first, 2 bytes priority, second, 6 bytes Mac address. If the priority of all switches is the same, then the switch with lowest Mac address will be chosen as root bridge. Each network can only have one root bridge. [5]

The process of electing root bridge on the network is based on evaluating the root ID field in the BPDUs that it receives and it consists of:

- When a switch (sender) boots, it uses the item of the root ID field of outbound BPDUs and puts it in its own BID, then sends BPDUs to other switches. [8]
- The receiver switch compares the sender's bridge ID with its own bridge ID
-If the sender's bridge ID is lower than the receiver's bridge ID, the receiver switched does not forward the BPDU. [8]
-If the sender's bridge ID is higher than the Receiver's bridge ID, the receiver switch populates the root ID field of outbound BPDUs with its own BID and the BPDU is forwarded. It means the first sender is not a root bridge. [8]

After a while, all bridges, except the bridge with the lowest bridge ID, stops sending BPDUs. Therefore, it is chosen as a root bridge. [8]

3.2.3 Spanning Tree protocol Operation

To understand how STP works, first we should establish that. We have four types of port:

Root port

This is the port with the best path to the root bridge. It locates in the non-root bridge and forwards all of the traffic to the root bridge.

Designated port

This can exist on a root bridge and a non-root bridge. In a root bridge, all ports are designated ports because all ports have to receive and forward frames, but on a non-root bridge only one port can play the role of designated port which is capable of sending and receiving frames to/from the root bridge. The election of designated ports is based on the lowest cost of ports.

Non-designated port

This can exist on Non-root Bridge. It is a port which is not shut down, but it can not forward the frame.

Disabled port:

This is a port which is shut down.

Each port on the switch which is running STP has one of five states:

**Disabled:** in this state the port is shut down by the administrator and it can not forward packets.

**Forwarding:** in this state, the port can forward packets and it can send and receive BPDUs.

**Blocking:** in this state, the port can not forward packets. It can only receive BPDUs, because the port was selected as a non-designated port for some reason, such as having a higher cost than other designated ports. This state will last 20 seconds by a default which is called “max age”.

**Listening:** in this state, the port can receive BPDUs from others switches. It builds the loop-free tree and can participate in forwarding frames. This state will last 15 seconds by a default which is called “forward delay”.

**Learning:** in this state, the port can receive and forward BPDUs to/from other switches. It prepares to participate in forwarding frames. This state will last 15 seconds by default, which is called “forward delay”.

The rules of STP operation are: [9]

- The first important part of STP operation is to select a root bridge which is mentioned earlier, the switch with the lowest bridge ID will be chosen as a root bridge. In a root bridge, all ports are designated ports and can forward frames.

- Secondly, at least one port (root port) in a non-root bridge must find the best path to the root bridge. It achieves this by the comparison between all of BPDUs' information. The root port must be able to forward frames towards the root bridge. The election of root port is based on the lowest path cost, lowest sender BID and lowest sender port ID.

- Thirdly, when a port is selected as a root port, other ports will stay in blocking mode and can not forward any frames to prevent loops.

To illustrate the operation of STP, see figure 3.2, which shows a network with four switches. Switch 3560A is a root bridge, and the other three switches such as 3560B, 2960A and 2960B.

![Figure 3.2: The operation of STP](image)
When the link between 2960A and 3560A fails, both switch 2960A and switch 2960B will wait until the maximum age time, by default 20 seconds, to understand the path to the root bridge has become failed. Switch 2960B, after expiring the maximum age, will recognize that there is a path to the root bridge from port 0/1 to port 0/2.

It elects port 0/2 to be its new root port and directs it to switch 2960A through port 0/1. Switch 2960B does not advertise any information to all of other switches to announce them that the link towards to the root bridge has failed. Instead, it provides, by listening and learning, states on the networks which last 30 seconds by default. [10]

When the link between 2960A and 3560A is recovered, the process of electing new root port is described as follows:

- Switch 2960A will receive BPDU from switch 3560A and it chooses the new root port via port 0/1.
- Switch 2960A retires port 0/3 and will use it as a designated port.
- Switch 2960B will receive BPDU from switch 2960A. It retires port 0/2 and makes port 0/1 as a new root port.
- Other switches can understand the new root port, during the learning state and listening state.

In consequence, this procedure will last 30 seconds by default. [10]

3.2.4 Advantages and Disadvantages of STP

STP has some advantages as well as disadvantages. The advantages of STP are:
- STP is easy to implement and it does not have more complex implementation
- The CPU load over switches is low

The disadvantages of STP are:
- STP has very slow convergence time. By default, it needs 20 seconds for forwarding state, 15 seconds for listening state and 15 seconds for learning state.

- There are no load balancing mechanisms for forwarding frames, and then all switches forward frames to a single point, which is called the “reference point”.

Some other loop prevention protocols have invented to overcome the disadvantages of STP such as:
- RSTP (rapid spanning tree protocol)
- PVSTP (per-VLAN spanning tree protocol)
- PVRSTP (per-VLAN rapid spanning tree protocol)
- MSTP (multiple spanning tree protocol)

We are going to describe them.

3.3 Rapid Spanning Tree Protocol (RSTP)

When a network topology changes because of link failure, STP convergence time takes between 30 to 50 seconds, according to the type of failure. It means STP has a low
convergence time and it is not appropriate to use for carrying IP telephony traffic. To solve this problem, RSTP is used, which can provide much better and quicker convergence time. [5]

### 3.3.1 Rapid Spanning Tree Protocol Port State

RSTP has 4 types of port states: [5]

**Forwarding:** in this state, the port can forward packets. This is similar to the STP forwarding port state.

**Discarding:** in this state, the port prevents the forwarding of packets. There is not this type of port state in STP. Instead of discarding port state, STP uses blocking and listening port states which increases convergence time in the networks.

**Learning:** in this state, the port accepts data from all of network and it is prepared to forward data. It is similar to the STP learning port state.

**Disabled:** in this state, the port is shut down by the administrator and it can not forward packets.

### 3.3.2 Rapid Spanning Tree Protocol Port Role

RSTP has five types of port role: [5]

**-Root port:** like STP root port; this is the port with the best pass to the root bridge.

**-Designated port:** the operation is similar to the operation of the STP designated port. All of designated ports on a root bridge and a non-root bridge can receive and forward frames.

**-Alternative port:** this is a switch port which is located on a non-root bridge, and it offers an alternative path from the designated port on the non-root bridge to the root bridge. In fact, it provides a redundant path to the root bridge. When the current designated port is failed, the alternative port is used to forward packet from the designated port on a non-root bridge to the root bridge. By default, the alternative port has discarding state and it goes to forwarding state, if the link fails. STP does not have these types of port.

**-Backup port:** this is a switch port which is located on the non-root bridge as a backup for the designated port and it offers a backup path to a segment. The port ID of the backup port is higher than the port ID of the designated port. STP does not have these types of port.

**Disabled port:** this is a port which is shut down.

### 3.3.3 Rapid Spanning Tree Protocol Operation

STP uses different timers to change the states of port for finding a new path from source to destination, such as the forward delay timer and the max age timer. It causes the network convergence time to become high. Since, RSTP can provide a mechanism to transition the port to the forwarding state without requiring any timers. RSTP uses BPDUs exchanges to
overcome the slow convergence on a port. Also, the BPDUs containments in RSTP are different from STP.

BPDU format in RSTP consists of eight fields:

**Topology change**: this shows the changing topology  
**Proposal**: this proposes the better path to the root bridge  
**Port role**: this has information about the role of ports  
**Learning**: this shows the port is accepting information from the network and it is preparing to go to forwarding state.  
**Forwarding**: this shows the port is forwarding information to all networks.  
**Agreement**: this shows the switch is agree to elect new root port.  
**Topology change acknowledgement**: this shows the switch understands that the topology has changed.

To illustrate the operation of RSTP, see figure 3.3. It shows a network with four switches. Switch 3560A as a root bridge and three other switches, such as 3560B, 2960A and 2960B.

![Figure 3.3: The operation of RSTP](image)

When the link between 2960A and 3560A is failed, four steps are taken to choose the new root port, likes:

- Switch 2960A starts to advertise to switch 2960B. Then, switch 2960B will recognize BPDUs received from 2960A.
- Switch 2960B immediately activates its secondary path through port 0/2 and chooses port 0/2 as a new root port with forwarding state as well as chooses port 0/1 as a designated port to advertise new root path to the switch 2960A.
- Switch 2960A accepts new information and makes port 0/3 its new root port.
- Finally, switch 2960B performs a handshake, called “sync operation”, with switch 2960A to transition port 0/1 into a forwarding state. The sync operation does not need any timers and it just needs a BPDU exchange; it causes sync operation to take place very quickly: in less than one second. [10]

When the link between 2960A and 3560A is recovered, four steps are taken to choose the new root port, likes: [10]

- Switch 3560A (root bridge) will detect a link on port 0/3 and it sends a BPDU to switch 2960A with a proposal flag set to transition this port to a forwarding state.

- Switch 2960A will receive BPDU from switch 3560A which asserts that this is the shortest path to the root. Then it sends a signal to all non-edge designated ports (sync) to put all of the port in blocking mode.

- The Port 0/1 on switch 2960A sends a BPDU back to announce to the root bridge that it agrees with the new topology. The root can understand it with the agreement flag on BPDU and, at this time, port 0/1 on switch 2960A can take the forwarding state without any delays.

- Now, to break the loop between 2960A and 2960B, switch 2960A uses the sync process to make port 0/3 into forwarding state which sends a BPDU to 2960B to inform it that the port 0/2 does not have the role of root port anymore and port 0/1 is a new root port. Then, it sends a signal to all non-edge designated ports (sync) to put all of the port in blocking mode.

As we mentioned earlier, not all of those processes need timers and it is just performed by BPDU exchange. When a link fail happens on the network, it enables RSTP to have very fast convergence time.

### 3.4 Comparison between STP, RSTP

The most significant differences between STP and RSTP are:

- Convergence time in STP is between 30 and 50 seconds, while, in RSTP, it is less than one second.
- In STP implementation, when a link is failed, the switches will recognize that with its own learning and listening state while, in RSTP, each change will be sent by BPDU exchanges.
- STP does not have any alternative or backup port states, while RSTP uses them as a backup for the root port and designated port.
- When two switches have connected directly, to transition a designated port to forwarding state, STP uses a timer, while RSTP uses a handshaking mechanism.
- The containments of BPDU between STP and RSTP are very different.
3.5 Per-VLAN Spanning Tree Protocol (PVSTP)

In STP only a single instance of spanning tree covers all VLANs. The reason for this specification can be reduction of complexity in handling VLANs.

There are some advantages and disadvantages for single instance of spanning tree, such as:

- With using a single spanning-tree, we prepare a switch that is simpler in design and which does not put high load on the CPU.

- On the other hand, using a single spanning tree avoids load balancing and sometimes can result in an imperfect connectivity in a specific VLAN.

Per-VLAN spanning tree protocol (PVSTP) uses a separate spanning tree instance for each VLAN in the network. It permits a trunk for a VLAN to be in the state of forwarding, whereas this trunk plays the role of blocking for other VLANs. Consequently load balancing at layer 2 is provided by using PVSTP in the network and, convergence time may be smaller than the large STP topology. [11]

By using PVSTP, a root bridge and spanning tree protocol topology can be considered for each VLAN, and BPDUs are traded in each VLAN. In addition, switches can use all of the links to forward traffic without having to create a bridge loop. PVSTP gives a network an opportunity to have priority value for each VLAN and, thereby, we can distinguish between each instance in the network.

3.6 Multiple Spanning Tree Protocol (MSTP)

With regard to PVSTP, each VLAN is assigned to each instance; the total number of spanning tree instances can be too much and may lead to an increase in the CPU loading. In addition the handling of all instances is difficult. Since each instance has its own BPDU conversation, the act of election for a root bridge and the right path selection, the problems go further in PVSTP. [5]

By using multiple spanning tree protocol (MSTP), the numbers of instances are decreased to the number of links which are in existence. For example, you can suppose that there is 500 VLANs. In this case, and by using PVSTP, It was supposed to be 500 instances whereas by using MSTP VLANs 1 through 250 using one path and VLANs 251 through 500 using the other path. Therefore each switch has responsibility of two instances information rather than too much number of instances. In MSTP each instance is called “MSTP instance”. In the case of failure, MSTP convergence time is more rapid than PVSTP. [5]

In other words, MSTP allows grouping VLANs in specific instance which each instance has its topology that is not dependent to other instance topologies. We can present some advantages of MSTP:

- Multiple active forwarding paths for traffic are provided by MSTP.
- Enabling of load balancing
- In the case of fault, MSTP makes better fault tolerance over common spanning tree.
3.7 Per-VLAN Rapid Spanning Tree Protocol (PVRSTP)

As we mentioned earlier, one of the big problems in STP is that it has very slow convergence time and, although in PVSTP we will have one instance per VLAN, the convergence time is still slow. To overcome this problem, a combination of RSTP characteristics with PVSTP characteristics is used, and which is called “PVRSTP”.

With using PVRSTP, a tree for each VLAN will be created and it has two advantages:

- PVRSTP can forward the traffic of some VLANs on one trunk, and the rest of VLANs on other VLANs, without creating loop.
- PVRSTP can improve the convergence time, when one link goes down.
CHAPTER 4

GATEWAY REDUNDANCY

4.1 Network Design

Since providing high-availability, scalability and flexibility in today’s network design is an important subject, network designers try to design the best network having regard to the above concerns.

The network is designed with regard to functionality of the network, achieving optimal performance as well as reduction of costs.

As can be seen in figure 4.1, network designers design networks with regard to three main hierarchical layers which are the core layer (backbone layer), the distribution layer and the access layer (local access layer). Typically, the core layer and distribution layer consist of multilayer switches. Multilayer switches can provide routing as well as packet switching. [5]

It can be said that the best layer for implementing QOS (quality of service) policies and access-lists are typically on distribution switches. Hosts can connect to access layer switches, and access layer switches connect to distribution multilayer switches. Distribution layer is more critical than access layer and more attention should be paid to implementing ways to keep this layer safe as much as possible and to implement solutions to condition of failures. [5]

![Figure 4.1: Redundant Network](image)

4.2 Gateway Redundancy in the Network

Typically, end devices are configured with a single default gateway IP address which each change in the network does not change the default gateway IP address. If the router, whose IP address is configured as the default gateway, fails, the local device is unable to send packets out of the local network and will be disconnected from the network. If there is redundant router which can act as a default gateway, it is necessary to implement a method to
present the redundant router IP address as a new gateway address in the event of failure in the network.

One of those methods that can be configured for providing layer 3 redundancies for hosts of network is hot standby routing protocol (HSRP). With HSRP, rapid link failover, as well as a recovery mechanism, can be provided. Virtual router redundancy protocol (VRRP) and gateway load balancing protocol (GLBP) have been developed gradually from HSRP which can make available additional layer 3 redundancy features in the network. HSRP and GLBP are Cisco-proprietary protocols, whereas VRRP is a vendor-neutral, layer 3 redundancy protocol. [5]

4.3 Identifying the Router Redundancy Process

In router redundancy mechanism, a set of routers work with each other to show to all hosts that they work as an individual virtual router. Two or more routers can play same role as a single, “virtual” router by contributing to having an IP address and a Mac (Layer2) address.

The virtual router's IP address is taken as the workstation's default gateway address. When frames are sent from the end station to the default gateway, the end station uses ARP to specify the Mac address associated with the IP address of the default gateway. ARP sends back the Mac address of the virtual router. In a single virtual router, routers use a protocol to determine explicitly which physical router has responsibility for processing the frames which are sent to the Mac or IP address. Also, this redundancy protocol has a mechanism to determine which router should play the active role in forwarding traffic, and when the role is changed to standby position.

4.4 Hot Standby Routing Protocol (HSRP)

HSRP defines a group in which each router has a specific role in the mentioned group. Gateway redundancy is provided by sharing IP and Mac addresses between two routers within the same HSRP group.

An HSRP group is composed of:
- Active router
- Standby router
- Virtual router
- Other routers

4.4.1 Hot Standby Routing Protocol (HSRP) Operations

The virtual router has an IP and Mac address. It is noted that the virtual router does not process physical frames, but exists in software only. The active router processes all packets and frames which are sent to the virtual router’s address. Generally, it can be said that the active router plays the primary role in the HSRP group by the time that it is operable. When the active router becomes inoperable, the HSRP standby router will check the operational status of the HSRP group and take the role of active router. Both active and standby routers propagate Hello message to inform other routers in the group of their status. Routers use destination multicast address 224.0.0.2, with UDP port 1985. [5]

In the event of failure in the active router, the standby router has the responsibility to act as an active router. In this situation, other routers participate in the HSRP group; they compete to be the standby router. [5]
Because the new active router undertakes the duty of both IP and Mac address of the virtual router, the end stations experience no disruption in network and they continue to transmit packets.

4.4.2 Hot Standby Routing Protocol States

The state of a router in an HSRP group can be as follows:

- Initial
- Learn
- Listen
- Speak
- Standby
- Active

Initial state is the first state. It means that HSRP is not running. Learn State indicates that the router is not in the active or standby state and has not enough information to compete to be the standby or active router. Listen state presents that the router is not in the active or standby state. Since the router knows the virtual IP address, in this state the router is listening to the hello message. In the speak state the router sends periodic hello messages, and participates in the election of the active or standby router. In standby state, the router is selected to be next active router, and in an active state, the router forwards packets that are sent to the virtual group. [5]

4.4.3 Hot Standby Routing Protocol Features

Some of the features which are used in HSRP are explained as follows:

**Pre-emption:** pre-emption determines that the router with the higher priority is capable of being an active router after the occurrence of a failure in the network. [12]

**Interface Tracking:** This feature is used in HSRP to track an interface if it is been out of work and inoperable. In the situation in which an interface is down, the priority will be decreased. Consequently, the router with the higher priority undertakes the role as an active router. [12]

**Authentication:** To hide the HSRP priority value, and other HSRP information about HSRP peers in the view of other routers, this feature is used.

4.5 Virtual Router Redundancy protocol (VRRP)

VRRP acts rather like HSRP. Virtual router redundancy protocol allows a group of routers to form a single virtual router. An HSRP group consists of one active router, at least one standby router and, perhaps many listening routers. A VRRP group has one primary router, which called the “master router”, and one or more backup routers. Like HSRP operation, workstations are configured with the virtual router address as their default gateway.

4.5.1 Virtual Router Redundancy Protocol Operation

Somehow, VRRP acts as an HSRP. In VRRP, one router can act as a master for a specific virtual router with a specific default gateway. The mentioned router is backup router
for other virtual router with associated hosts. With VRRP, advertisements (equivalent the HSRP hello message) are sent only by master router. Advertisements are sent on multicast 224.0.0.18, protocol number 112, at the interval time of 1 second.

### 4.5.2 Difference between HSRP and VRRP

Some differences between the two mentioned gateway redundancy protocols are explained as follows:

- VRRP is an IEEE standard (RFC 2338) for router redundancy, whereas HSRP is a Cisco-proprietary protocol.
- The virtual router which indicates a group of routers is known as a “VRRP group” or “virtual router group”.
- The active router in HSRP is referred to as the “master virtual router” in VRRP.
- The master virtual router may have the same IP address as the virtual router group. Multiple routers can act as VRRP backup routers.
- VRRP is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, as well as multiprotocol label switching (MPLS), virtual private networks (VPNs), and VLANs is supported by VRRP.

VRRP provides redundancy for the real IP address of a router or for a virtual IP address shared among the VRRP group members. In the condition where there exists a real IP address, the router with that address will become the master, whereas if a virtual IP address is used, the master will be the router with the highest priority. [5]

### 4.5.3 Virtual Router Redundancy Protocol Timers

In the event of failure, VRRP uses three timers:

**Advertisement interval:** this is the time between advertisements and it is defined in seconds. The default is 1 second.

**Master down interval:** the master down interval is the number of seconds for the backup to proclaim the master has been down and it can get the master role. The default is:

\[
3 \times \text{advertisement interval} + \text{skew time}
\]

**Skew time:** the skew time, \((256 - \text{priority}) / 256\) ms, is used to ensure that the backup router with the highest priority undertakes the role of the new master. [5]

### 4.6 Gateway Load Balancing Protocol (GLBP)

Since only the active router for HSRP, and master router for VRRP groups, transmits traffic for the virtual Mac, resources which are associated with the standby router are not fully utilized. GLBP was designed in 2005. [13]

GLBP is a Cisco proprietary and was designed to allow automatic selection, simultaneous use of multiple gateways as well as rapid fail recovery between those gateways. With GLBP, resources can be completely utilized without any configuration for multiple groups by the network administrator. In addition, by using this protocol, the need for
managing multiple default gateway configurations is removed while there should still be the perfect management for multiple default gateways in HSRP and VRRP. [13]

4.6.1 Gateway Load Balancing Protocol Functions
A summary of GLBP functions is described as follows:

**Active virtual gateway (AVG):** Members of a GLBP group decide to elect one router to be the AVG for that group. In the event that AVG becomes out of work, the other group members will be provided to make backup for the AVG. A virtual Mac address is assigned to each member of the group by AVG.

**Active virtual forwarder (AVF):** In GLBP each gateway has responsibility to forward packets which are sent to the virtual Mac address. AVF is a common name for the mentioned virtual Mac address.

**Communication:** Communication between GLBP members is achieved with hello messages which are sent every 3 seconds to the multicast address 224.0.0.102, user datagram protocol (UDP) port 3222. [13]

4.6.2 Gateway Load Balancing Protocol Features
GLBP has the following features:

**Load sharing:** traffic that is transmitted from LAN clients can be contributed to by multiple routers.

**Multiple virtual routers:** each physical interface of a router can be assigned up to 1024 virtual routers, and can be appointed up to four virtual forwarders per group.

**Pre-emption:** an AVG which has the higher priority backup virtual gateway can be pre-empted.

**Efficient resource utilization:** Since any router in a group can play the role of backup router this issue will eliminate the need for a dedicated and pre devoted backup router. In GLBP, all available routers contribute to handling network traffic. [13]
CHAPTER 5

IMPLEMENTATION

5.1 Overview of Implementation

Default gateway redundancy by using an HSRP mechanism and prevention loop mechanism by using PVSTP and PVRSTP, are set up and configured in a lab environment. A Campus network was constructed using two Cisco Catalyst 3560 multilayer switches in distribution layer, and a Cisco 2801 router is used as core layer and as a CME (call manager express) for supporting voice over IP, and two Cisco Catalyst 2960 layer two switches as access layer. Then, two IP telephones and two computers are connected to access layer switches.

To test the operation of three different STPs after implementing them manually, we created failures on different points of the networks during VOIP (voice over IP) call sessions between two IP telephones located in two different access layers of the network.

To understand which of those mechanisms has the faster convergence time, we used an application which is called “CommView” to measure packet loss during a link failure. Then, we compared all of the results and found which of those mechanisms was good for carrying IP telephony traffic.

5.2 Topology and Equipments

The topology which we used in the lab environment is shown in figure 5.1. All of the IP telephony and PCs can connect to the access layer switches. Two distribution layer switches (3560A and 3560B) configured to use HSRP. It is not very important to configure two access layer switches (2960A and 2960B) with HSRP. This is because, if an access layer switch crashed, 24 calls will only fail. While, if one distribution layer switch crashed, 1152 (24 multiple 48) calls will fail.

A call manager is used to make a call and connection between source and destination, nothing else. When a call is set up between source and destination, if the link between call manager and distribution layer switch fails, the current call will still keep its own connection without any interruption. However, if a new user requests new connection, that will be impossible. Implementing a backup call manager can solve this problem.
Two types of equipments used in Lab environments:

Hardware equipments which are shown in table 5.1

<table>
<thead>
<tr>
<th>Device</th>
<th>Device Type/Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 2801</td>
<td>Router (call manager) as core layer</td>
<td>1</td>
</tr>
<tr>
<td>Cisco Catalyst 3560</td>
<td>Layer 3 switches as distribution layer</td>
<td>2</td>
</tr>
<tr>
<td>Cisco Catalyst 2960</td>
<td>Layer 2 switches as access layer</td>
<td>2</td>
</tr>
<tr>
<td>IP Telephony 7960</td>
<td>Making call</td>
<td>2</td>
</tr>
<tr>
<td>Laptop and PC</td>
<td>Acting as hosts</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 5.1: Hardware used to build the network
- Software equipments which are shown in table 5.2

<table>
<thead>
<tr>
<th>Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IP Communicator</td>
<td>Voice communication software replacing hardware phone</td>
</tr>
<tr>
<td>LAN Analyzer (CommVeiw)</td>
<td>measurement tool</td>
</tr>
</tbody>
</table>

Table 5.2: Applications running on the network

CommView is good software for monitoring and analyzing LAN and it can capture all of the packets and traffic in the network to display some important information, such as packet loss, jitter and so on, as you can see in figure 5.2.

Some of the capabilities of CommView are: [14]

- Display all of information about IP connectivity, such as IP address and ports.
- Capture all of the traffic in the network.
- Make different chart of bandwidth utilization, and Jitter, mean opinion score (MOS) and ratio factor (R_Factor) which will be explained later.

It also consists of a VOIP analyzer to measure the quality of voice and to perform it; an explanation some of items is necessary.

- **Mean Opinion Score (MOS):** it is a number between 1 and 5 which shows the quality of voice. Five is the best and one is the worst. Also, two means poor and three is fair and four is good. The acceptable range for VOIP is from 3.5 to 4.2. [15]

- **Ratio Factor (R_Factor):** this is a number between 0 and 100, and the acceptable range for VOIP is from 80 to 100. The range between 0-50 is not recommended, between 50-60, almost all users are dissatisfied, between 60-70 many users are dissatisfied and between 70-80 some users are satisfied. [15]

- **Packet loss:** this is the number of packets which are lost during a node failure. More packet loss means less quality of voice.
5.3 Common Configuration for All Scenarios

There are four scenarios for implementation:

- Implementation of PVSTP with, or without, the use of port fast
- Implementation of PVRSTP with, or without, the use of port fast

Before explanation, configuration and testing of each scenario, it is necessary to explain the common configuration of all scenarios. To provide VOIP services to IP telephones sets, or for voice client software, Cisco IP communicator is installed on two hosts and the router 2801 is used as a Cisco call manager express (CME). CME is used to set up a voice call, and it provides dial numbers and names for IP telephony and IP communicator clients. When a call is set up from IP telephony to another or from one host with IP communicator software to another, traffic will not flow through CME and voice will be transmitted even if CME is removed from the network. Therefore, CME will not affect the results, which it will measure with CommView software. It means CME is just used for setting a call connection and nothing else.

Two multilayer switches (3560A and 3560B) are used to connect to CME. Two VLANs are defined on the two multilayer switches and DHCP is run on Switches to provide IP address for hosts and IP telephones. HSRP also is implemented on both layer 3 switches. Then, one of the switches is active and other is on standby. If the active switch crashes, the
other (standby) can get the responsibility of activating the switch without creating any delay
on the network.

Two hosts and two IP telephones are connected to two layer 2 switches (2960A and 2960B).
As we mentioned before, they will get IP from DHCP (table 5.3), not manually.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>VOICE</th>
<th>DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>RANGE OF IP addresses</td>
<td>From 192.168.10.1 To 192.168.10.10</td>
<td>From 192.168.20.1 To 192.168.20.10</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default gateway</td>
<td>192.168.10.2</td>
<td>192.168.20.2</td>
</tr>
</tbody>
</table>

Table 5.3: Configuration of IP Telephones and hosts

Having per-packet loading balance on real time communication such as VOIP is not
acceptable. This is because of reordering delayed-packet is not possible in VOIP.

To have load balancing between all of distribution and access layer switches, the default Cisco express forwarding (CEF) load balancing is enabled, therefore, traffic is caused to go from the source to the destination, through the special path based on some parameters such as lower cost link, fewer Mac addresses, manually setting the main path by changing priority or defining root as primary and secondary.

For all scenarios, when a call is set up between source (7960 IP telephone0) and
destination (7960 IP telephone1), the main path is the link between 2960A-3560A (fa0/2),
CME and 3560A-2960B (fa0/4), as you can see in figure 5.3.

In each scenario, first we ran the CommView application to capture the traffic and measure the packet loss and jitter when we had link failure.

Secondly, we made a call between source and destination with using different voice and music as well as using the different periods of time and then we manually disconnected the different links between all switches and made a result table, such as table 5.4.

We had different packet loss and jitter, according to which protocol we used and which link we failed. Lastly, when we compare all the results, we will understand which protocol has the fast convergence time and is suitable to use in our topology.
Table 5.4: Result of link failure

<table>
<thead>
<tr>
<th>protocol name</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Situations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>failed 3560 A F0/3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>failed 3560 B F0/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>failed 3560 B F0/4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>failed 3560 A F0/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>failed 3560 A F0/4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5.3: Main path of communication

Table 5.4: Result of link failure
5.4 Implementation of PVSTP with or without the use of Port Fast

The first implementation is related to configuring PVSTP on all switches without using port fast. As you see in table 5.5, during a call, failing links except the main path links will not affect the call and results. If we fail the main path link, we will have packet loss. The numbers of packet loss depends on the traffic which flows through the source and destination. More traffic means more packet loss. According to the MOS and R-factor, we can understand that using PVRST for carrying IP telephony is not recommended because the acceptable MOS range for it is between 3.5 and 4.2, and also the acceptable R_Factor range for it is between 80 and 100.

<table>
<thead>
<tr>
<th>PVSTP</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R_Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>01:00.6</td>
<td>649,490</td>
<td>0.62</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
</tr>
<tr>
<td>Situations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>failed</td>
<td>3560 A FA0/3</td>
<td>192.168.10.9</td>
<td>00:45.3</td>
<td>485,138</td>
<td>0.63</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
</tr>
<tr>
<td></td>
<td>3560 B FA0/2</td>
<td>192.168.10.7</td>
<td>00:45.8</td>
<td>490,702</td>
<td>1.32</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
</tr>
<tr>
<td>failed</td>
<td>3560 B FA0/4</td>
<td>192.168.10.9</td>
<td>00:49.1</td>
<td>525,584</td>
<td>1.28</td>
<td>32.2%</td>
<td>1.3</td>
<td>20.7</td>
</tr>
<tr>
<td></td>
<td>3560 A FA0/2</td>
<td>192.168.10.9</td>
<td>01:33.5</td>
<td>679,022</td>
<td>1.28</td>
<td>32.2%</td>
<td>1.3</td>
<td>20.7</td>
</tr>
<tr>
<td>failed</td>
<td>3560 A FA0/4</td>
<td>192.168.10.9</td>
<td>02:10.1</td>
<td>1,036,256</td>
<td>0.71</td>
<td>57.7%</td>
<td>1.1</td>
<td>12.2</td>
</tr>
</tbody>
</table>

Table 5.5: Result of implementation PVSTP without the use of Port Fast

The second implementation is related to configuring PVSTP on all switches with using port fast. As we mention earlier, STP has five port states. When a link is failed, each port must wait to complete all of the states, such as the learning and listening states. With using port fast, the port can go quickly to forwarding without going to the listening and learning states. The result (Table 5.6) shows that using port fast will give better results and less packet loss than without using it, but this type of implementation is also not acceptable for carrying IP telephony traffic. Therefore, implementation of PVSTP is not recommended in any situation.
Table 5.6: Result of implementation PVSTP with the use of Port Fast

<table>
<thead>
<tr>
<th>Normal Situations</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>01:03.9</td>
<td>684,586</td>
<td>1.62</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>failed 3560 A FA0/3</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>00:52.1</td>
<td>557,898</td>
<td>0.85</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>failed 3560 B FA0/2</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>00:53.1</td>
<td>568,812</td>
<td>0.73</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>failed 3560 B FA0/4</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>01:05.2</td>
<td>698,068</td>
<td>0.9</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>failed 3560 A FA0/2</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>01:28.9</td>
<td>629,374</td>
<td>0.62</td>
<td>1.5</td>
<td>22.8%</td>
<td>1.2</td>
<td>19.9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>failed 3560 A FA0/4</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>02:11.7</td>
<td>1,087,762</td>
<td>0.73</td>
<td>33.9%</td>
<td>1.2</td>
<td>76.3</td>
<td></td>
</tr>
</tbody>
</table>

5.5 Implementation of PVRSTP with or without the use of Port Fast

The third implementation is related to configuring PVRSTP on all switches without using port fast. As can be seen in table 5.7, as with the implementation of PVST, there is not any packet loss when a non-main path link is failed. However, when a main path link is failed, we will have approximately 4.1% packet loss. This means that implementation of PVRSTP without using port fast will result in better performance than the implementation of PVSTP with/without port fast. However, according to the R_Factor, some users are still dissatisfied (the range of R_Factor is between 70 and 80).

Table 5.7: Result of implementation PVRSTP without the use of Port Fast

<table>
<thead>
<tr>
<th>PVRSTP</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Situations</td>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>01:04.7</td>
<td>692,718</td>
<td>1.36</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>failed 3560 A FA0/3</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>01:03.2</td>
<td>676,668</td>
<td>1.39</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>failed 3560 B FA0/2</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>00:54.6</td>
<td>584,862</td>
<td>1.39</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>failed 3560 B FA0/4</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>00:53.9</td>
<td>576,944</td>
<td>0.7</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>failed 3560 A FA0/4</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>01:29.9</td>
<td>631,248</td>
<td>0.86</td>
<td>1.42</td>
<td>3.2%</td>
<td>3.7</td>
<td>76.3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>failed 3560 A FA0/2</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>02:15.9</td>
<td>1,123,344</td>
<td>1.42</td>
<td>4.1%</td>
<td>3.6</td>
<td>76.3</td>
<td></td>
</tr>
</tbody>
</table>
The fourth implementation is related to configuring PVRSTP on all switches with using port fast. As can be seen in table 5.8, we have the minimum packet loss if a link fails and also the range of MOS and R_Factor shows all of the users are satisfied and the quality of voice is good.

<table>
<thead>
<tr>
<th>PVRSTP</th>
<th>Src IP</th>
<th>Dest IP</th>
<th>Duration</th>
<th>Total Traffic (bytes)</th>
<th>Max Jitter (ms)</th>
<th>Lost Packets</th>
<th>MOS Score</th>
<th>R-Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Situations</td>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>01:03.9</td>
<td>684,586</td>
<td>1.62</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
</tr>
<tr>
<td>failed FA0/3</td>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>00:46.5</td>
<td>498,620</td>
<td>0.79</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
</tr>
<tr>
<td>failed FA0/2</td>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>00:46.8</td>
<td>501,188</td>
<td>1.68</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
</tr>
<tr>
<td>failed FA0/4</td>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>00:48.6</td>
<td>520,234</td>
<td>0.46</td>
<td>0</td>
<td>4.4</td>
<td>93.2</td>
</tr>
<tr>
<td>failed FA0/4</td>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>01:28.4</td>
<td>624,666</td>
<td>1.34</td>
<td>2.0%</td>
<td>4.2</td>
<td>88.9</td>
</tr>
<tr>
<td>failed FA0/2</td>
<td>192.168.10.9</td>
<td>192.168.10.7</td>
<td>02:12.2</td>
<td>1,101,326</td>
<td>1.06</td>
<td>2.4%</td>
<td>4.1</td>
<td>86.8</td>
</tr>
</tbody>
</table>

Table 5.8: Result of implementation PVRSTP with the use of Port Fast
5.6 Results of Implementations

Table 5.9 shows the summary of our implementation results. We have measured packet loss, MOS and R_Factor two times with different total traffic on the network. The total traffic at the first time was about 630,000 bytes and at the second time was about 1,100,000 bytes. We can say:

-Using PVRSTP with port fast (configuration is available on appendix) for carrying IP telephony traffic will cause the minimum packet loss during the link failure, and MOS is more than 4; this means that it is acceptable. In this situation, R_Factor is more than 80, and it means all of users are satisfied.

-Using PVRSTP without port fast for carrying IP telephony traffic can be used. The range of MOS is more than 3.5 and R_Factor is between 70 and 80. This means that some users are still dissatisfied.

-Using PVSTP with or without port fast for carrying IP telephony, the traffic is terrible. This protocol must not be used on the VIOP network to overcome the link failure. The packet loss is high and the range of MOS is below 3.5, which is not acceptable and also the range of R_Factor is between 0 and 50, which means that it is not recommended to be used.

<table>
<thead>
<tr>
<th>Results</th>
<th>PVSTP</th>
<th>PVRSTP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>without port fast</td>
<td>with port fast</td>
</tr>
<tr>
<td>Packet loss (percentage)</td>
<td>32.2</td>
<td>22.8</td>
</tr>
<tr>
<td>MOS</td>
<td>1.3</td>
<td>1.5</td>
</tr>
<tr>
<td>R_Factor</td>
<td>20.7</td>
<td>27.1</td>
</tr>
<tr>
<td></td>
<td>12.2</td>
<td>19.9</td>
</tr>
</tbody>
</table>

Table 5.9: Summary of Implementations Results
Conclusion

This thesis describes some advantages and challenges of using IP telephones on the network. The implementation of redundant path on VOIP network is necessary to achieve fast fault recovery. In addition, redundant paths will make some loops on the network. There are some protocols which are used to prevent loop and create redundant paths on the networks. Some protocols explained briefly and two protocols, PVSTP and PVRSTP, were implemented in the lab environment. The important result of implementation is that PVSTP has slow convergence time during a link failure, and it causes more packet loss, which is not recommended for carrying IP telephony traffic, even it is implemented with port fast.

On the other hand, implementation of PVRSTP has quick convergence time during a link failure and it causes less packet loss. It also has the acceptable range of MOS and R_Factor, which ensures all users are satisfied, for carrying IP telephony, especially with using port fast on all switches.

This thesis also describes how call manager express is just used to set up a call between source and destination and it does not affect results which we got during the different implementations in the lab. Also, this thesis includes some investigation into the use of other protocols to achieve redundancy on the network, such as HSRP, VRRP and GLBP. This thesis gives an overview of how to make a better switched network for carrying IP telephony traffic.
References

Retrieved November 22, 2009 from World Wide Web:

[2] VOIP Signalling Protocols - Setting Up and Tearing Down the Call
Retrieved November 22, 2009 from World Wide Web:
 http://voip-facts.net/h323.php


[5] Cisco Networking Academy Materials version 5.1 for Multilayer switching course
Retrieved December 2, 2009 from World Wide Web:

[6] What is Bridge Protocol Data Unit (BPDU)?
Retrieved December 2, 2009 from World Wide Web:
 http://www.webopedia.com/TERM/b/bpdu.html

Retrieved November 25, 2009 from World Wide Web:


[9] Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches
Retrieved December 4, 2009 from World Wide Web:

[10] Wald Wojdak, Rapid Spanning Tree Protocol: A new solution from an old technology,
Reprinted from CompactPCI Systems, March 2003


ISBN: 0-596-10151-1


[14] CommView, Network Monitor and Analyzer
Retrieved December 17, 2009 from World Wide Web:
http://www.tamos.com/products/commview/

Retrieved December 17, 2009 from World Wide Web:
http://www.voiptroubleshooter.com/basics/mosr.html
Appendix

CME#sh run
Building configuration...

Current configuration : 1954 bytes
!
! Last configuration change at 20:14:51 UTC Mon Dec 14 2009
!
Version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CME
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef
!
!
!
!
!
!
!
!
!
!
!
voice-card 0
!
!
!
!
!
!
!
interface FastEthernet0/0
  no ip address
  shutdown
duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
duplex auto
  speed auto
!
interface FastEthernet0/1.10
  encapsulation dot1Q 10
  ip address 192.168.10.1 255.255.255.0
  no snmp trap link-status
!
interface FastEthernet0/1.20
  encapsulation dot1Q 20
  ip address 192.168.20.1 255.255.255.0
  no snmp trap link-status
!
interface Serial0/1/0
  no ip address
  shutdown
clock rate 125000
!
interface Serial0/1/1
  no ip address
  shutdown
clock rate 125000
!
interface Serial0/2/0
  no ip address
  shutdown
clock rate 125000
!
interface Serial0/2/1
  no ip address
  shutdown
clock rate 125000
router eigrp 1
network 192.168.0.0 0.0.255.255
no auto-summary
!
!
ip http server
no ip http secure-server
!
!
!
!
!
!

ip http server
no ip http secure-server
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
! ephone-dn 4
  number 1994
!
ephone-dn 5
  number 1995
  name Ali
!
ephone 1
  mac-address 001E.4AA9.78D4
  button 1:1
!
ephone 2
  mac-address 001E.4AA9.73C7
  button 1:2
!
ephone 3
  mac-address 001B.24B4.B7D1
  button 1:3 2:4
!
ephone 4
  mac-address 001E.EC99.3720
  button 1:5
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
  login
!
scheduler allocate 20000 1000
end

3560A(config)#do sh run
Building configuration...
Current configuration : 2204 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3560A
!
no aaa new-model
system mtu routing 1500
!
ip subnet-zero
ip routing
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
!
ip dhcp pool VOICE
    network 192.168.10.0 255.255.255.0
    option 150 ip 192.168.10.1
    default-router 192.168.10.2
!
ip dhcp pool DATA
    network 192.168.20.0 255.255.255.0
    default-router 192.168.20.2
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree extend system-id
spanning-tree vlan 1,10,20 priority 24576
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
    switchport trunk encapsulation dot1q
    switchport mode trunk
!
interface FastEthernet0/2
    switchport trunk encapsulation dot1q
switchport mode trunk
! interface FastEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
! interface FastEthernet0/4
switchport trunk encapsulation dot1q
switchport mode trunk
! interface FastEthernet0/5
! interface FastEthernet0/6
! interface FastEthernet0/7
! interface FastEthernet0/8
! interface FastEthernet0/9
! interface FastEthernet0/10
! interface FastEthernet0/11
! interface FastEthernet0/12
! interface FastEthernet0/13
! interface FastEthernet0/14
! interface FastEthernet0/15
! interface FastEthernet0/16
! interface FastEthernet0/17
! interface FastEthernet0/18
! interface FastEthernet0/19
! interface FastEthernet0/20
! interface FastEthernet0/21
! interface FastEthernet0/22
! interface FastEthernet0/23
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
ip address 192.168.10.5 255.255.255.0
standby 1 ip 192.168.10.2
standby 1 timers msec 50 msec 152
standby 1 priority 150
standby 1 preempt
standby 1 track FastEthernet0/2 60
!
router eigrp 1
network 192.168.0.0 0.0.255.255
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.10.1 254
ip http server
!
!
control-plane
!
!
line con 0
eexec-timeout 0 0
logging synchronous
line vty 0 4
login
line vty 5 15
login
!
end

3560B#sh run
Building configuration...

Current configuration : 1657 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3560B
!
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
ip routing
!
!
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree extend system-id
spanning-tree vlan 1,10,20 priority 28672
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8  
!
interface FastEthernet0/9  
!
interface FastEthernet0/10  
!
interface FastEthernet0/11  
!
interface FastEthernet0/12  
!
interface FastEthernet0/13  
!
interface FastEthernet0/14  
!
interface FastEthernet0/15  
!
interface FastEthernet0/16  
!
interface FastEthernet0/17  
!
interface FastEthernet0/18  
!
interface FastEthernet0/19  
!
interface FastEthernet0/20  
!
interface FastEthernet0/21  
!
interface FastEthernet0/22  
!
interface FastEthernet0/23  
!
interface FastEthernet0/24  
!
interface GigabitEthernet0/1  
!
interface GigabitEthernet0/2  
!
interface Vlan1  
  no ip address  
  shutdown  
!
interface Vlan10  
  ip address 192.168.10.4 255.255.255.0  
  standby 1 ip 192.168.10.2  
  standby 1 timers msec 50 msec 152  
  standby 1 preempt
router eigrp 1
   network 192.168.0.0 0.0.255.255
no auto-summary
!
ip classless
ip http server
!
!
control-plane
!
!
line con 0
line vty 5 15
!
end

2960A#sh run
Building configuration...

Current configuration : 2284 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2960A
!
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
!
interface FastEthernet0/4
switchport mode trunk
!
interface FastEthernet0/5
switchport mode trunk
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/6
switchport mode trunk
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/7
switchport mode trunk
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/8
switchport mode trunk
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/9
switchport mode trunk
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/10
switchport mode trunk
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/11
switchport access vlan 20
switchport mode access
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/12
switchport access vlan 20
switchport mode access
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/13
switchport access vlan 20
switchport mode access
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/14
switchport access vlan 20
switchport mode access
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/15
switchport access vlan 20
switchport mode access
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
no ip route-cache
! ip http server
!
control-plane
!
line con 0
line vty 5 15
!
monitor session 1 source interface Fa0/7
monitor session 1 destination interface Fa0/11
end
2960B#sh run
Building configuration...

Current configuration : 2217 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2960B
!
!
no aaa new-modl
system mtu routing 1500
ip subnet-zero
!
!
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
switchport mode trunk
!
interface FastEthernet0/5
switchport mode trunk
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/6
switchport mode trunk
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/7
switchport mode trunk
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/8
switchport mode trunk
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/9
switchport mode trunk
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/11
switchport access vlan 20
switchport mode access
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/12
switchport access vlan 20
switchport mode access
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/13
switchport access vlan 20
switchport mode access
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/14
switchport access vlan 20
switchport mode access
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/15
switchport access vlan 20
switchport mode access
switchport voice vlan 10
spanning-tree portfast
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
no ip route-cache
!
ip http server
!
control-plane
line con 0
line vty 5 15
end