



## High Availability Campus Network Design - Routed Access Layer using EIGRP or OSPF System Assurance Guide

### Cisco Validated Design

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit [www.cisco.com/go/validateddesigns](http://www.cisco.com/go/validateddesigns).

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

*High Availability Campus Network Design - Routed Access Layer using EIGRP or OSPF System Assurance Guide*  
© 2007 Cisco Systems, Inc. All rights reserved.



## Preface

---

## Document Purpose

This document presents recommendations and results for the System Assurance validation of the High Availability Campus Network Design - Routed Access Layer using EIGRP or OSPF.

## Definitions

This section defines words, acronyms, and actions that may not be readily understood.

**Table 1**      **Acronyms and Definitions**

|       |                                            |
|-------|--------------------------------------------|
| CSSC  | Cisco Secure Service Client                |
| CTI   | Common Test Interface                      |
| CUCM  | Cisco Unified Communication Manager        |
| CUWN  | Cisco Unified Wireless Network             |
| CVD   | Cisco Validated Design                     |
| DR    | Designated Router                          |
| DHCP  | Dynamic Host Configuration Protocol        |
| DNS   | Domain Name Service                        |
| EIGRP | Enhanced Interior Gateway Routing Protocol |
| FTP   | File Transfer Protocol                     |
| HA    | High Availability                          |
| HTTP  | Hyper Text Transfer Protocol               |
| IAM   | Information Access Manager                 |
| IGP   | Interior Gateway Protocol                  |
| IGMP  | Internet Group Management Protocol         |
| LWAPP | Light Weight Access Point Protocol         |
| MSDP  | Multicast Source Discovery Protocol        |
| NTP   | Network Time Protocol                      |

**Table 1**      **Acronyms and Definitions**

|           |                                                |
|-----------|------------------------------------------------|
| OSPF      | Open Shortest Path First Routing Protocol      |
| PIM       | Protocol Independent Multicast                 |
| PIM-Bidir | Protocol Independent Multicast - Bidirectional |
| PSQM      | Perceptual Speech Quality Measurement          |
| POP3      | Post Office Protocol 3                         |
| QoS       | Quality of Service                             |
| RP        | Rendezvous Point                               |
| SCCP      | Skinny Call Control Protocol                   |
| SPT       | Shortest Path Tree                             |
| SIP       | Session Initiation Protocol                    |
| TFTP      | Trivial File Transfer Protocol                 |
| VLAN      | Virtual Local Area Network                     |
| WLAN      | Wireless Local Area Network                    |
| WLC       | WLAN Controller                                |
| WiSM      | Wireless Service Module for Catalyst 6500      |



# CONTENTS

## **Executive Summary 1-1**

## **Cisco Validated Design Program 2-1**

### 2.1 Cisco Validated Design 2-1

### 2.2 CVD System Assurance 2-1

## **High Availability Campus Routed Access with EIGRP or OSPF 3-1**

### 3.1 Solution Overview 3-1

#### 3.1.1 Redundant Links 3-3

#### 3.1.2 Route Convergence 3-5

#### 3.1.3 Link Failure Detection Tuning 3-6

#### 3.1.4 Features List 3-8

### 3.2 HA Campus Routed Access Test Coverage Matrix - Features 3-39

### 3.3 HA Campus Routed Access Test Coverage Matrix - Platforms 3-41

### 3.4 CVD System Assurance Test Strategy 3-41

#### 3.4.1 Baseline Configuration 3-41

#### 3.4.2 Extended Baseline Configuration 3-41

#### 3.4.3 Testbed Setup 3-42

#### 3.4.4 Test Setup - Hardware and Software Device Information 3-43

#### 3.4.5 Test Types 3-44

#### 3.4.6 Sustaining Coverage 3-45

### 3.5 CVD System Assurance - Feature Implementation Recommendations 3-46

#### 3.5.1 Routing 3-46

#### 3.5.2 Link Failure Detection 3-47

#### 3.5.3 Multicast 3-48

#### 3.5.4 Wireless 3-48

#### 3.5.5 Voice over IP 3-49

## **Test Cases Description and Test Results 4-1**

### 4.1 Convergence Tests with Extended Baseline Configuration 4-1

#### 4.1.1 Link and Node Failure Analysis 4-4

### 4.2 Impact of Redundant Link Failures on Video Quality 4-5

#### 4.2.1 Analysis of Various Link Failures 4-7

### 4.3 Impact of Redundant Link Failures on Voice Quality during Convergence 4-8

#### 4.3.1 PSQM - Perceptual Speech Quality Measure 4-9

|                                                            |      |
|------------------------------------------------------------|------|
| 4.3.2 Jitter                                               | 4-10 |
| 4.3.3 Delay                                                | 4-11 |
| 4.3.4 RTP Packet Loss / Convergence Time                   | 4-12 |
| 4.4 Impact of Congestion on Voice Traffic with QoS Enabled | 4-13 |
| 4.5 Routing - IPv4 – EIGRP and OSPF                        | 4-16 |
| 4.6 Negative tests - EIGRP and OSPF                        | 4-19 |
| 4.7 Multicast Tests - EIGRP and OSPF                       | 4-21 |
| 4.8 VoIP Tests - EIGRP and OSPF                            | 4-24 |
| 4.8.1 Wireless Tests - EIGRP and OSPF                      | 4-29 |

## **Related Documents and Links** A-1

## **Defects** B-1

|                 |     |
|-----------------|-----|
| B.1 CSCek78468  | B-1 |
| B.2 CSCek75460  | B-1 |
| B.3 CSCsk10711  | B-1 |
| B.4 CSCsh94221  | B-2 |
| B.5 CSCsk01448  | B-2 |
| B.6 CSCsj48453  | B-2 |
| B.7 CSCsj45951  | B-2 |
| B.8 CSCsm08419  | B-3 |
| B.9 CSCsm33116  | B-3 |
| B.10 CSCsm35240 | B-3 |

## **Technical Notes** C-1

|                       |     |
|-----------------------|-----|
| C.1 Technical Note 1: | C-1 |
|-----------------------|-----|



## FIGURES

|             |                                                                                   |      |
|-------------|-----------------------------------------------------------------------------------|------|
| Figure 3-1  | High Availability Campus Routed Access Design - Layer 3 Access                    | 3-1  |
| Figure 3-2  | Comparison of Layer 2 and Layer 3 Convergence                                     | 3-2  |
| Figure 3-3  | Equal-cost Path Traffic Recovery                                                  | 3-3  |
| Figure 3-4  | Equal-cost Uplinks from Layer3 Access to Distribution Switches                    | 3-4  |
| Figure 3-5  | Traffic Convergence due to Distribution-to-Access Link Failure                    | 3-5  |
| Figure 3-6  | Summarization towards the Core bounds EIGRP queries for Distribution block routes | 3-10 |
| Figure 3-7  | Campus OSPF Area Design                                                           | 3-12 |
| Figure 3-8  | Convergence Results                                                               | 3-14 |
| Figure 3-9  | Default OSPF Area Configuration and Associated Route Table Impact                 | 3-15 |
| Figure 3-10 | OSPF Stub Area Configuration and Associated Route Table Impact                    | 3-15 |
| Figure 3-11 | OSPF Totally Stub Area Configuration and Associated Route Table Impact            | 3-16 |
| Figure 3-12 | Default Route and Distribution ABRs                                               | 3-17 |
| Figure 3-13 | OSPF Route Summarization Limits Propagation of LSAs                               | 3-18 |
| Figure 3-14 | Basic Multicast Service                                                           | 3-27 |
| Figure 3-15 | Shared Distribution Tree                                                          | 3-28 |
| Figure 3-16 | Unidirectional Shared Tree and Source Tree                                        | 3-30 |
| Figure 3-17 | Bidirectional Shared Tree                                                         | 3-31 |
| Figure 3-18 | Anycast RP                                                                        | 3-33 |
| Figure 3-19 | Intra-controller roaming                                                          | 3-35 |
| Figure 3-20 | L2 - Inter-controller roaming                                                     | 3-36 |
| Figure 3-21 | High Availability Campus Routed Access design - Manual testbed                    | 3-42 |
| Figure 4-1  | Traffic Flow Upstream Black Hole and Downstream Reroute                           | 4-5  |
| Figure 4-2  | Traffic Flow Upstream Black Hole and Downstream Reroute                           | 4-9  |
| Figure 4-3  | Summary (Variance)                                                                | 4-10 |
| Figure 4-4  | Jitter Statistics                                                                 | 4-11 |
| Figure 4-5  | Delay Statistics                                                                  | 4-11 |
| Figure 4-6  | RTP packet loss in 5 seconds                                                      | 4-12 |
| Figure 4-7  | Results for EIGRP                                                                 | 4-14 |
| Figure 4-8  | Results for OSPF                                                                  | 4-15 |

*This page is intentionally left blank*





## T A B L E S

|                  |                                                                          |             |
|------------------|--------------------------------------------------------------------------|-------------|
| <i>Table 1</i>   | <a href="#">Acronyms and Definitions</a>                                 | <b>1-3</b>  |
| <i>Table 1-1</i> | <a href="#">CVD System Assurance Guide Publication Status</a>            | <b>1-1</b>  |
| <i>Table 3-1</i> | <a href="#">Port Debounce Timer Delay Time</a>                           | <b>3-7</b>  |
| <i>Table 3-4</i> | <a href="#">HA Campus Routed Access Test Coverage Matrix - Platforms</a> | <b>3-41</b> |
| <i>Table 3-5</i> | <a href="#">Hardware and Software Device Information</a>                 | <b>3-43</b> |
| <i>Table C-1</i> | <a href="#">Wireless Controller Upgrade Path</a>                         | <b>C-1</b>  |

*This page is intentionally left blank*



# CHAPTER 1

## Executive Summary

---

This document validates the High Availability Campus Routed Access Design using EIGRP or OSPF as IGP in the Core, Distribution and Access layers and provides implementation guidance to achieve faster convergence.

Deterministic convergence times of less than 200 msec were measured for any redundant links or nodes failure in an equal-cost path in this design with EIGRP and OSPF routing protocols and this was the success criteria.

The aim of this solution testing is to accelerate customer deployments of this Campus routed Access design by validating in an environment where multiple integrated services like multicast, voice and wireless interoperate.

Extensive manual and automated testing was conducted in a large scale, comprehensive customer representative network. The design was validated with a wide range of system test types, including system integration, fault and error handling, redundancy, and reliability to ensure successful customer deployments. An important part of the testing was end-to-end verification of multiple integrated services like voice, and video using components of the Cisco Unified Communications solution. Critical service parameters such as packet loss, end-to-end delay and jitter for voice and video were verified under load conditions.

As an integral part of the CVD SYSTEM ASSURANCE program, an automated sustaining validation model was created for an on-going validation of this design for any upcoming IOS software releases on the targeted platforms. This model significantly extends the life of the design, increases customer confidence and reduces deployment time.

**Table 1-1**      **CVD System Assurance Guide Publication Status**

| Design Guide                                                                             | CVD System Assurance |
|------------------------------------------------------------------------------------------|----------------------|
| <i>High Availability Campus Network Design - Routed Access Layer Using EIGRP or OSPF</i> | Passed               |

The following guide was the source for this validation effort:

[\*High Availability Campus Network Design-Routed Access Layer using EIGRP or OSPF\*](#)

Supervisor redundancy at the Access layer along with Cisco Nonstop Forwarding (NSF) with Stateful Switchover (SSO) provides increased network service availability and protection against unplanned downtime due to hardware (Supervisor failure) or software problems.

This document also provides IGP timer recommendations to achieve Nonstop Forwarding of Layer3 traffic in the Catalyst 6500 system running redundant Supervisor modules in SSO mode.



## CHAPTER 2

# Cisco Validated Design Program

---

The Cisco® Validated Design Program (CVD) consists of systems and solutions that are designed, tested, and documented to facilitate faster, more reliable and more predictable customer deployments. These designs incorporate a wide range of technologies and products into a broad portfolio of solutions that meet the needs of our customers.

## 2.1 Cisco Validated Design

Cisco Validated Designs are systems or solutions that have been validated through architectural review and validation testing in a Cisco lab. These designs provide guidance for the deployment of new technology or in applying enhancements to existing infrastructure.

## 2.2 CVD System Assurance

The CVD System Assurance programs provide intense ongoing validation of combinations of Cisco Validated Designs and best practices designed to represent target and typical customer deployments. The System Assurance programs are focus on major network architectures (e.g. Places in the Network - Datacenter, Branch/WAN, Campus) or technologies (e.g. Unified Communications). One of the key deliverables from these programs is the CVD Assurance Guide (this document) which provides system or solution baseline recommendations for general customer use in the context of the target architecture/technology and associated designs. Baseline recommendations defines key functional and architectural aspects of a design that have been thoroughly tested end-to-end or within a given product family. This includes common customer design and configuration examples and should serve as a foundational starting point for new deployments or technological upgrades

The System Assurance programs are supported with forward looking designs and associated assurance test roadmaps to promote new technology and products or design adoption for major network deployments or enhancements. Each phase of the assurance program enhances and expands the scope of the associates test environment. This assures that new technologies, products and designs (which may have been validated in isolation) continue to operate in a complex network incorporating a wide range of network services and technologies that would typically exist in a customer network. The scope of each phase of the assurance programs is defined based on key customer and deployment requirements, CVD and technology roadmaps.

The general attributes / objectives of the Assurance Program test phases are :-

- "Generally aimed at a particular network architecture or technology and leverage the guidance from multiple design guides, deployment best practices and key customer deployments or requirements
- "The recommendations been reviewed and updated for general deployment
- "Evidence that solution requirements have been successfully tested in a scaled customer representative environment
- Confirm that there are no observable operationally impacting defects within the scope of the recommendations.
- Software release recommendations and associated platform and network role
- A record of the tests undertaken which provides documents the associated test activity and observed results (supplemented by Traffic profiles, memory and CPU profiling as necessary)
- Key configuration guidance and examples

For more information on Cisco CVD program, refer to:

[http://cisco.com/en/US/partner/netsol/ns741/networking\\_solutions\\_program\\_home.html](http://cisco.com/en/US/partner/netsol/ns741/networking_solutions_program_home.html)



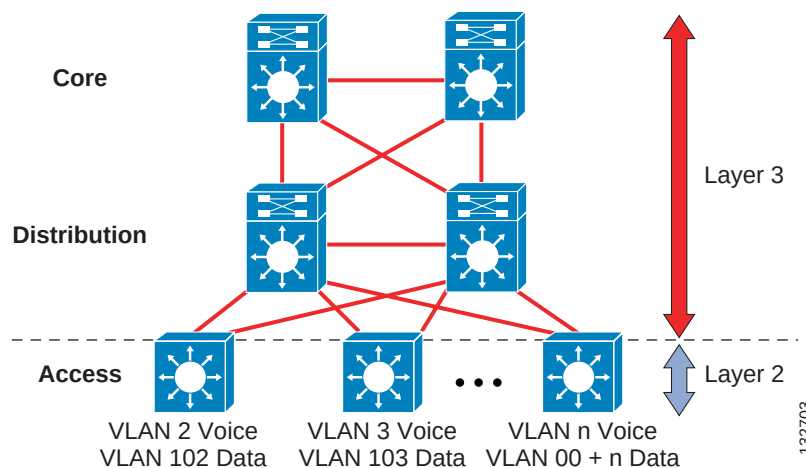
# CHAPTER 3

## High Availability Campus Routed Access with EIGRP or OSPF

### 3.1 Solution Overview

The hierarchical design segregates the functions of the network into separate building blocks to provide for availability, flexibility, scalability, and fault isolation. The Distribution block provides for policy enforcement and Access control, route Aggregation, and the demarcation between the Layer 2 subnet (VLAN) and the rest of the Layer 3 routed network. The Core layers of the network provide high capacity transport between the attached Distribution building blocks and the Access layer provides connectivity to end devices such as PCs, PoE, Unified Communication components like IP phone, voicemail, e-mail, and instant messaging etc.

**Figure 3-1** High Availability Campus Routed Access Design - Layer 3 Access



For campus designs requiring a simplified configuration, common end-to-end troubleshooting tools and fastest convergence, a distribution block design using Layer 3 switching in the access layer (routed access) in combination with Layer 3 switching at the distribution layer provides the fastest restoration of voice and data traffic flows.

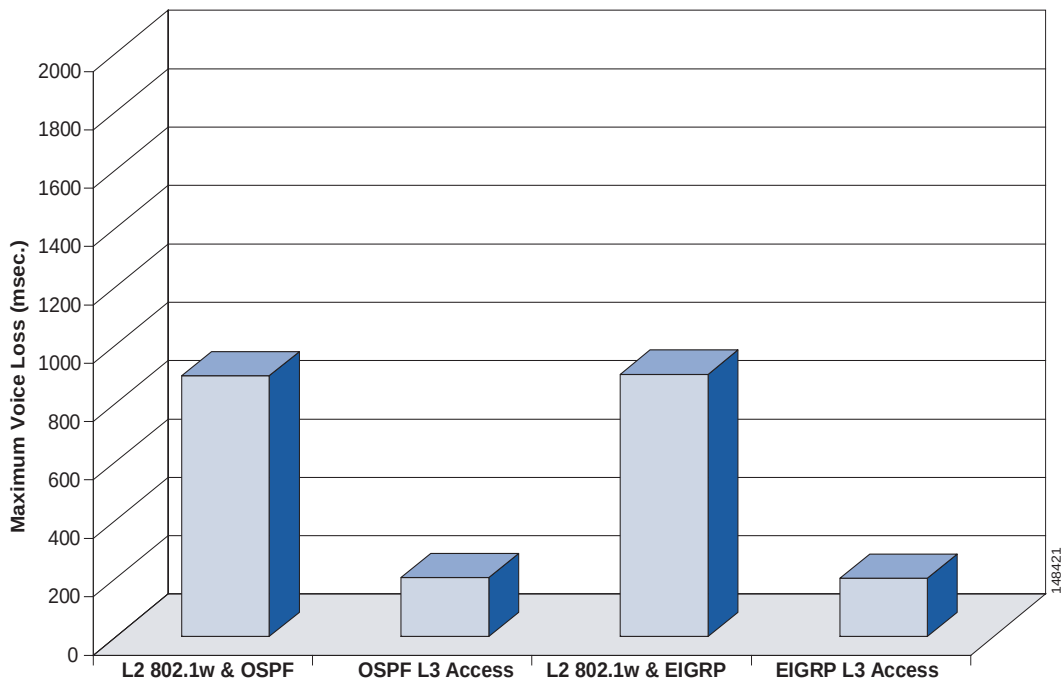
Many of the potential advantages of using a Layer 3 access design include the following:

- Improved convergence
- Simplified multicast configuration
- Dynamic traffic load balancing

- Single control plane
- Single set of troubleshooting tools (eg. ping and traceroute)
- HSRP / VRRP not required

Of these, perhaps the most significant is the improvement in network convergence times possible when using a routed access design configured with EIGRP or OSPF as the routing protocol. Comparing the convergence times for an optimal Layer 2 access design against that of the Layer 3 access design, four fold improvement in convergence times can be obtained, from 800-900msec for Layer 2 design to less than 200 msec for the Layer 3 access.

**Figure 3-2 Comparison of Layer 2 and Layer 3 Convergence**



Although the sub-second recovery times for the Layer 2 Access designs are well within the bounds of tolerance for most enterprise networks, the ability to reduce convergence times to a sub-200 msec range is a significant advantage of the Layer 3 routed Access design. This reduction in convergence times to sub 200 msec reduces the impact on voice and video to minimal disruption and supports critical data environments.

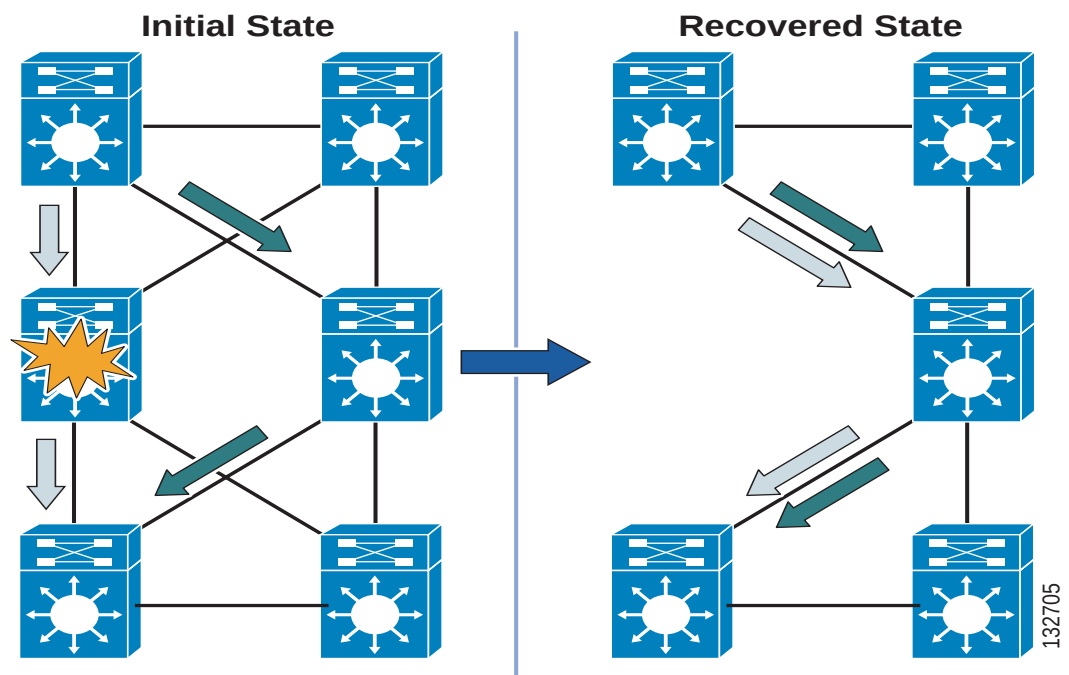
For those networks using a routed Access (Layer 3 Access switching) within their Distribution blocks, Cisco recommends that a full-featured routing protocol such as EIGRP or OSPF be implemented as the Campus Interior Gateway Protocol (IGP). Using EIGRP or OSPF end-to-end within the Campus provides faster convergence, better fault tolerance, improved manageability, and better scalability than a design using static routing or RIP, or a design that leverages a combination of routing protocols (for example, RIP redistributed into OSPF).



### 3.1.1 Redundant Links

The most reliable and fastest converging campus design uses a tiered design of redundant switches with redundant equal-cost links. A hierarchical campus using redundant links and equal-cost path routing provides for restoration of all voice and data traffic flows in less than 200 msec in the event of either a link or node failure without having to wait for a routing protocol convergence to occur for all failure conditions except one (see section 3.1.3 Route Convergence, on page 11 for an explanation of this particular case). Figure 3-3 shows an example of equal-cost path traffic recovery.

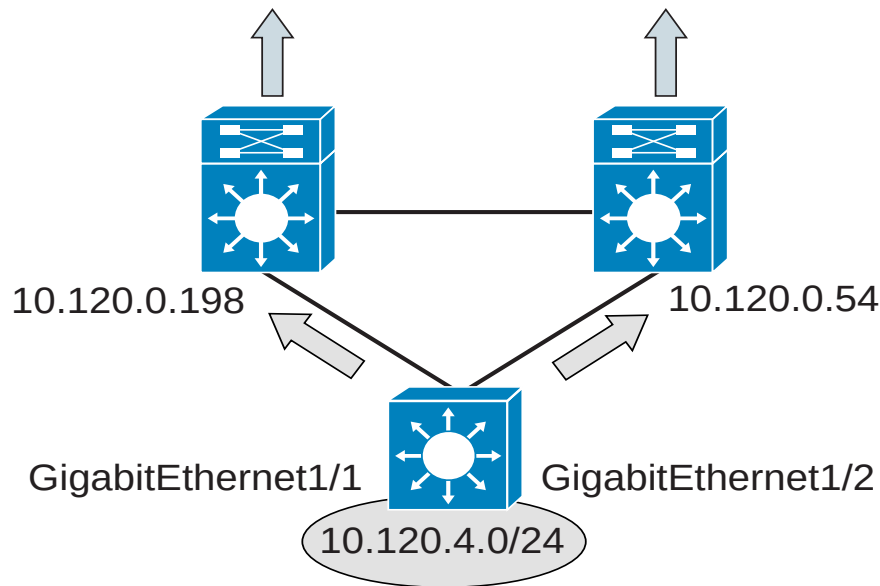
**Figure 3-3** Equal-cost Path Traffic Recovery



In the equal-cost path configuration, each switch has two routes and two associated hardware Cisco Express Forwarding (CEF) forwarding adjacency entries. Before a failure, traffic is forwarded using both of these forwarding entries. When an adjacent link or neighbor failure occurs, the switch hardware and software immediately remove the forwarding entry associated with the lost neighbor. After the removal of the route and forwarding entries associated with the lost path, the switch still has a remaining valid route and associated CEF forwarding entry. Because the switch still has an active and valid route, it does not need to trigger or wait for a routing protocol convergence, and is immediately able to continue forwarding all traffic using the remaining CEF entry. The time taken to reroute all traffic flows in the network depends only on the time taken to detect the physical link failure and to then update the software and associated hardware forwarding entries.

Cisco recommends that Layer 3 routed campus designs use the equal-cost path design principle for the recovery of upstream traffic flows from the access layer. Each access switch needs to be configured with two equal-cost uplinks, as shown in Figure 3-4. This configuration both load shares all traffic between the two uplinks as well as provides for optimal convergence in the event of an uplink or distribution node failure.

In the following example, the Layer 3 access switch has two equal-cost paths to the default route 0.0.0.0

**Figure 3-4 Equal-cost Uplinks from Layer3 Access to Distribution Switches**

132706

```
Layer3-Access#sh ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - OSPF, EX - OSPF external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 10.120.0.198 to network 0.0.0.0
```

```
10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
C      10.120.104.0/24 is directly connected, Vlan104
C      10.120.0.52/30 is directly connected, GigabitEthernet1/2
C      10.120.4.0/24 is directly connected, Vlan4
C      10.120.0.196/30 is directly connected, GigabitEthernet1/1
D*EX 0.0.0.0/0 [170/5888] via 10.120.0.198, 00:46:00, GigabitEthernet1/1
        [170/5888] via 10.120.0.54, 00:46:00, GigabitEthernet1/2
```

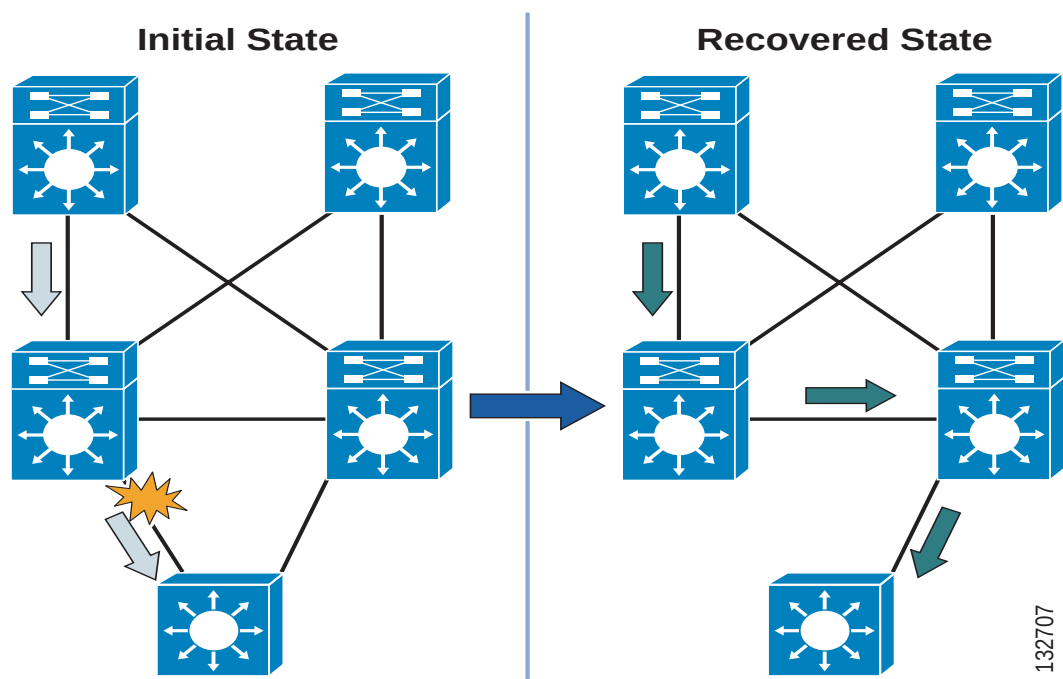
## 3.1.2 Route Convergence

The use of equal-cost path links within the core of the network and from the access switch to the distribution switch allows the network to recover from any single component failure without a routing convergence, except one. As in the case with the Layer 3 design, every switch in the network has redundant paths upstream and downstream except each individual distribution switch, which has a single downstream link to the access switch. In the event of the loss of the fiber connection between a distribution switch and the access switch, the network must depend on the control plane protocol to restore traffic flows.

For downstream traffic, one cannot avoid the downstream traffic re-route (convergence) at the Distribution routers during Access to Distribution link failure.

For the upstream traffic from Access to Distribution, Access switch has two equal cost routes to the two Distribution routers. Upon Access to Distribution router link failure, the Access switch will update the next-hop entries in hardware, thus reducing black holing of the traffic.

**Figure 3-5** Traffic Convergence due to Distribution-to-Access Link Failure



To ensure the optimal recovery time for voice and data traffic flows in the campus, it is necessary to optimize the routing design to ensure a minimal and deterministic convergence time for this failure case.

The length of time it takes for EIGRP, OSPF, or any routing protocol to restore traffic flows within the campus is bounded by the following three main factors:

- The time required to detect the loss of a valid forwarding path.
- The time required to determine a new best path (which is partially determined by the number of routers involved in determining the new path, or the number of routers that must be informed of the new path before the network can be considered converged).

- The time required to update software and associated CEF hardware forwarding tables with the new routing information.

In the cases where the switch has redundant equal-cost paths, all three of these events are performed locally within the switch and controlled by the internal interaction of software and hardware. In the case where there is no second equal-cost path, EIGRP must determine a new route, and this process plays a large role in network convergence times.

In the case of EIGRP, the time is variable and primarily dependent on how many EIGRP queries the switch needs to generate and how long it takes for the response to each of those queries to return to calculate a feasible successor (path). The time required for each of these queries to be completed depends on how far they have to propagate in the network before a definite response can be returned. To minimize the time required to restore traffic flows, in the case where a full EIGRP routing convergence is required, it is necessary for the design to provide bounds on the number and range of the queries generated.

### 3.1.3 Link Failure Detection Tuning

*The recommended best practice for campus design uses point-to-point fiber connections for all links between switches.* In addition to providing better electromagnetic and error protection, fewer distance limitations and higher capacity fiber links between switches provide for improved fault detection versus and copper link. In a point-to-point fiber campus design using GigE and 10GigE fiber, remote node and link loss detection is normally accomplished using the remote fault detection mechanism implemented as a part of the 802.3z and 802.3ae link negotiation protocols. In the event of physical link failure, local or remote transceiver failure, or remote node failure, the remote fault detection mechanism triggers a link down condition that then triggers software and hardware routing and forwarding table recovery. The rapid convergence in the Layer 3 campus design is largely because of the efficiency and speed of this fault detection mechanism.

See IEEE standards 802.3ae and 802.3z for details on the remote fault operation for 10GigE and GigE respectively.

#### 3.1.3.1 Carrier-delay Timer

Configure carrier-delay timer on the interface to a value of zero (0) to ensure no additional delay in the notification that a link is down. The default behavior for Catalyst switches is to use a default value of 0 msec on all Ethernet interfaces for the carrier-delay time to ensure fast link detection. It is still recommended as a best practice to hard code the carrier-delay value on critical interfaces with a value of 0 msec to ensure the desired behavior.

```
interface GigabitEthernet1/1
description Uplink to Distribution 1
ip address 10.120.0.205 255.255.255.252
logging event link-status
load-interval 30
carrier-delay msec 0
```

Confirmation of the status of carrier-delay can be seen by looking at the status of the interface.

```
GigabitEthernet1/1 is up, line protocol is up (connected)
. . .
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Carrier delay is 0 msec
Full-duplex, 1000Mb/s, media type is SX
input flow-control is off, output flow-control is off
. . .
```

**Note**

On Catalyst 6500, "LINEPROTO-UPDOWN" message appears when the interface state changes before the expiration of the carrier-delay timer configured via the "carrier delay" command on the interface. This is an expected behavior on Catalyst 6500 and is documented in CSCsh94221. For details, refer to [Appendix B](#).

### 3.1.3.2 Link Debounce Timer

It is important to review the status of the link debounce along with carrier delay configuration. By default, GigE and 10GigE interfaces operate with a 10 msec debounce timer that provides for optimal link failure detection. The default debounce timer for 10 / 100 fiber and all copper link media is longer than that for GigE fiber, and is one reason for the recommendation of a high-speed fiber deployment for switch-to-switch links in a routed campus design. It is good practice to review the status of this configuration on all switch-to-switch links to ensure the desired operation via the command "show interfaces TenGigabitEthernet4/1 debounce."

```
DistributionSwitch1#show interfaces tenGigabitEthernet 4/2 debounce
```

```
Port    Debounce time  Value(ms)
Te4/2    disable
```

The default and recommended configuration for debounce timer is "disabled", which results in the minimum time between link failure and notification of the upper layer protocols. [Table 3-1](#) below lists the time delay that occurs before notification of a link change.

**Table 3-1 Port Debounce Timer Delay Time**

| Port Type                                                                     | Debounce Timer Disabled | Debounce Timer Enabled |
|-------------------------------------------------------------------------------|-------------------------|------------------------|
| Ports operation at 10 Mbps or 100 Mbps                                        | 300 milliseconds        | 3100 milliseconds      |
| Ports operation at 1000 Mbps or 10 Gbps over copper media                     | 300 milliseconds        | 300 milliseconds       |
| Ports operation at 1000 Mbps or 10 Gbps over fiber media except WS-X6502-10GE | 10 milliseconds         | 100 milliseconds       |
| WS-X6502-10GE 10-Gigabit ports                                                | 1000 milliseconds       | 3100 milliseconds      |

**Note**

On Catalyst 6500 with Supervisor 32 module, the default debounce interval for 8x1 GigabitEthernet or 2 x TenGigabitEthernet interfaces is 300msec instead of 10msec. Debounce interval of TenGigabitEthernet interfaces on WS-X6708-10GE line card is 300msec instead of 10msec.

This is documented in CSCsm08419. For details, refer to [Defects, page B-1](#)

For more information on the configuration and timer settings of the link debounce timer, see the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/intrface.htm#wp1044898>

## 3.1.4 Features List

The validation coverage is outlined as follows:

- High Availability Campus Network design - Routed Access using EIGRP - EIGRP Stub, EIGRP timers tuning, EIGRP summarization, EIGRP route filters
- High Availability Campus Network design - Routed Access using OSPF - OSPF Area Design, OSPF Stubby and Totally Stubby Distribution Area, Distribution ABR Route Summarization, SPF and LSA Throttle Tuning, Interface Timer Tuning
- Multicast - PIM Sparse-mode, Static RP/Auto-RP, PIM bidir, MSDP, PIM Stub
- Wireless - Intra-controller and L2 Inter-controller Roaming, Voice over Wireless, dot1x authentication, WiSM
- Voice - SCCP, SIP, Delay/Jitter, PSQM
- Interoperability among multiple Cisco platforms, interfaces, and IOS releases
- Validation of successful deployment of actual applications (Cisco IP Telephony streams) in the network.
- End-to-end system validation of all the solutions together in a single integrated customer representative network

### 3.1.4.1 Implementing Routed Access using EIGRP

For those enterprise networks that are seeking to reduce dependence on spanning tree and a common control plane, are familiar with standard IP troubleshooting tools and techniques, and desire optimal convergence, a routed access design (Layer 3 switching in the access) using EIGRP as the campus routing protocol is an excellent option. To achieve the optimal convergence for the routed access design, it is necessary to follow basic hierarchical design best practices and to use advanced EIGRP functionality, including stub routing, route summarization, and route filtering for EIGRP as defined in this document.

This section includes the following:

- EIGRP Stub
- Distribution Summarization
- Route Filters
- Hello and Hold Timer Tuning

#### 3.1.4.1.1 EIGRP Stub

Configuring the access switch as a "stub" router enforces hierarchical traffic patterns in the network. In the campus design, the access switch is intended to forward traffic only to and from the locally connected subnets. The size of the switch and the capacity of its uplinks are specified to meet the needs of locally connected devices. The access switch is never intended to be a transit or intermediary device for any data flows that are not to or from locally connected devices. The network is designed to support redundant capacity within each of these aggregation layers of the network, but not to support the re-route of traffic through an access layer. Configuring each of the access switches as EIGRP stub routers ensures that the large aggregated volumes of traffic within the core are never forwarded through the lower bandwidth links in the access layer, and also ensures that no traffic is ever mistakenly routed through the access layer, bypassing any distribution layer policy or security controls.

```
router eigrp 100
  passive-interface default
  no passive-interface GigabitEthernet1/1
  no passive-interface GigabitEthernet1/2
  network 10.0.0.0
  no auto-summary
  eigrp router-id 10.120.4.1
  eigrp stub connected
```

The EIGRP stub feature when configured on all layer three access switches and routers prevents the distribution router from generating downstream queries.

By configuring the EIGRP process to run in the "stub connected" state, the access switch advertises all connected subnets matching the network range. It also advertises to its neighbor routers that it is a stub or non-transit router, and thus should never be sent queries to learn of a path to any subnet other than the advertised connected routes. With this design, the impact on the distribution switch is to limit the number of queries generated in case of a link failure which provides optimal performance and smaller query boundaries.

#### 3.1.4.1.2 Distribution Summarization

Configuring EIGRP stub on all of the Access switches reduces the number of queries generated by a Distribution switch in the event of a downlink failure, but it does not guarantee that the remaining queries are responded to quickly. In the event of a downlink failure, the Distribution switch generates three queries; one sent to each of the Core switches, and one sent to the peer Distribution switch. The queries generated request information about the specific subnets lost when the Access switch link failed. The peer Distribution switch has a successor (valid route) to the subnets in question via its downlink to the Access switch, and is able to return a response with the cost of reaching the destination via this path. The time to complete this event depends on the CPU load of the two Distribution switches and the time required to transmit the query and the response over the connecting link.

The update of the CEF hardware FIB and adjacency entries is performed by the system software engine, and the entries in the tables are processed in a linear fashion. The greater the number of entries that need to be modified, the longer it takes for all entries to be modified. It is necessary to assume that the last entry updated impacts some traffic flows, and convergence time is calculated based on the time it takes for the last entry to be updated. When the number of routes in the Access switches is increased, the time taken to ensure all traffic flows have been restored also increases.

This fast response from the peer Distribution switch does not ensure a fast convergence time, however. EIGRP recovery is bounded by the longest query response time. The EIGRP process has to wait for replies from all queries to ensure that it calculates the optimal loop free path. Responses to the two queries sent towards the Core must be received before EIGRP can complete the route recalculation. To ensure that the Core switches generate an immediate response to the query, it is necessary to summarize the block of Distribution routes into a single summary route advertised towards the Core.

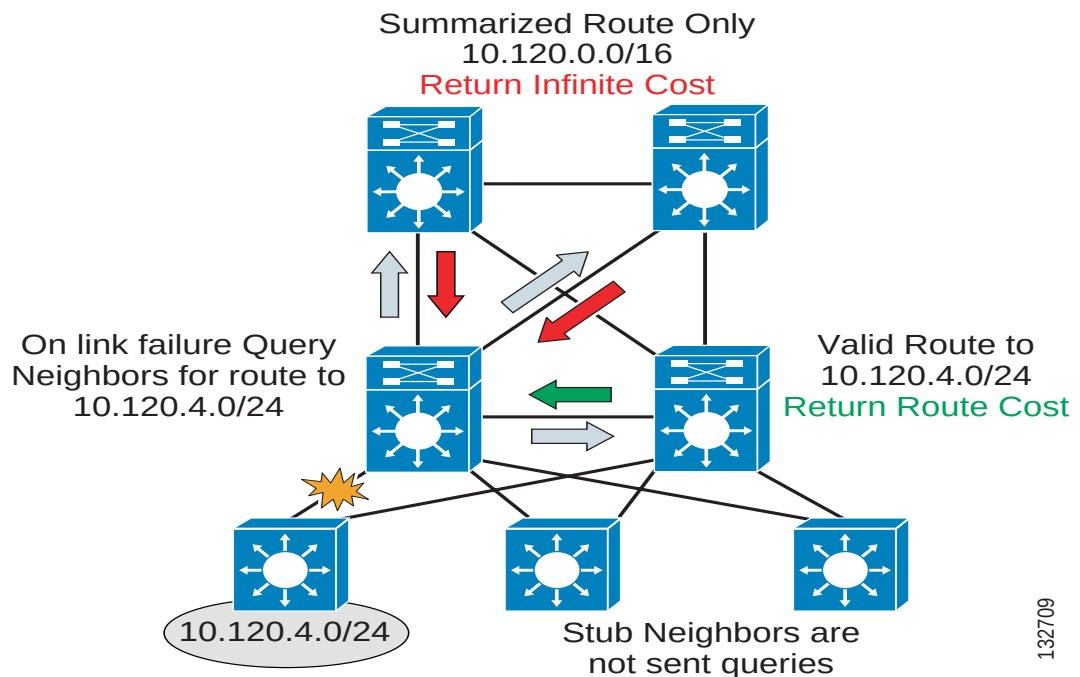
The summary-address statement is configured via the “ip summary-address eigrp 100 10.120.0.0 255.255.0.0 5” command on the uplinks from each Distribution switch to both Core nodes. In the presence of any more specific route, say 10.120.1.0/24 address space, this command causes EIGRP to generate a summarized route for the 10.120.0.0/16 network, and to advertise only that route upstream to the Core switches.

```
interface TenGigabitEthernet4/1
description Distribution 10 GigE uplink to Core 1
ip address 10.122.0.26 255.255.255.254
ip pim sparse-mode
ip hello-interval eigrp 100 1
ip hold-time eigrp 100 3
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 eigrp
ip summary-address eigrp 100 10.120.0.0 255.255.0.0 5
mls qos trust dscp
```

With the upstream route summarization in place, whenever the Distribution switch generates a query for a component subnet of the summarized route, the Core switches reply that they do not have a valid path (cost = infinity) to the subnet query. The Core switches are able to respond within less than 100 msec if they do not have to query other routers before replying back to the subnet in question.

Summarization of directly connected routes is done on the Distribution switches. Therefore, a Layer 3 link between the two Distribution routers is required to exchange specific routes between them. This Layer 3 link prevents the Distribution switches from black holing traffic if either Distribution switches lose the connection to the Access switch.

**Figure 3-6** Summarization towards the Core bounds EIGRP queries for Distribution block routes



132709



Using a combination of stub routing and summarization of the Distribution block routes up-stream to the Core both limits the number of queries generated and bounds those that are generated to a single hop in all directions. Keeping the query period bounded to less than 100 msec keeps network convergence similarly bounded under 200 msec for Access uplink failures. Access downlink failures are the worst case scenario because there are equal-cost paths for other Distribution or Core failures that provide immediate convergence.

### 3.1.4.1.3 Route Filters

As a complement to the use of EIGRP stub, Cisco recommends applying a distribute-list to all the Distribution downlinks to filter the routes received by the Access switches. The combination of “stub routing” and route filtering ensures that the routing protocol behavior and routing table contents of the Access switches are consistent with their role, which is to forward traffic to and from the locally connected subnets only. Cisco recommends that a default or “quad zero” route (0.0.0.0 mask 0.0.0.0) be the only route advertised to the Access switches.

```
router eigrp 100
  network 10.120.0.0.0.255.255
  network 10.122.0.0.0.0.255
  ...
  distribute-list Default out GigabitEthernet3/3
  ...
  eigrp router-id 10.120.200.1

!
ip Access-list standard Default
  permit 0.0.0.0
```

### 3.1.4.1.4 Hello and Hold Timer Tuning

Cisco recommends in the Layer 3 campus design that the EIGRP hello and hold timers be reduced to one and three seconds, respectively. The loss of hellos and the expiration of the hold timer provide a backup to the L1/L2 remote fault detection mechanisms. Reducing the EIGRP hello and hold timers from defaults of five and fifteen seconds provides for a faster routing convergence in the rare event that L1/L2 remote fault detection fails to operate, and hold timer expiration is required to trigger a network convergence because of a neighbor failure.

```
interface TenGigabitEthernet4/3
  description 10 GigE to Distribution 1
  ip address 10.122.0.26 255.255.255.254
  ...
  ip hello-interval eigrp 100 1
  ip hold-time eigrp 100 3
  ...
interface TenGigabitEthernet2/1
  description 10 GigE to Core 1
  ip address 10.122.0.27 255.255.255.254
  ...
  ip hello-interval eigrp 100 1
  ip hold-time eigrp 100 3
  ...
```

Ensure Timers are  
consistent on both  
ends of the link

132710

### 3.1.4.2 Implementing Routed Access using OSPF

For those enterprise customers that are seeking to reduce dependence on spanning tree and desire optimal convergence, a routed Access design (Layer 3 switching in the Access), implementing OSPF as the routing protocol is another viable option.

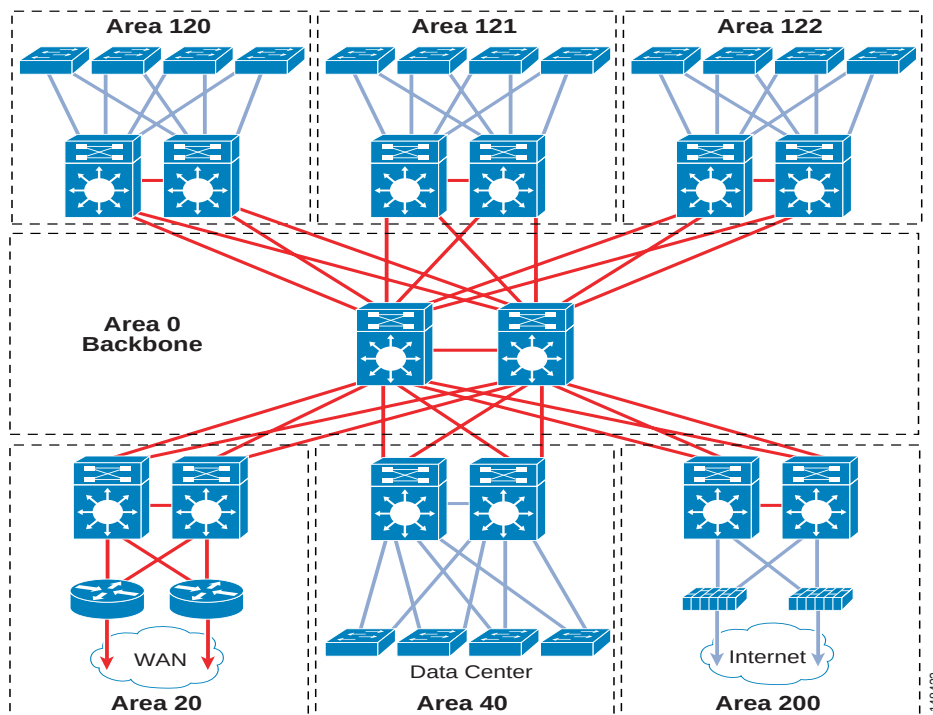
This section includes the following:

- OSPF Area Design
- OSPF Stubby and Totally Stubby Distribution Area
- Distribution ABR Route Summarization
- SPF and LSA Throttle Tuning
- Interface Timer Tuning

#### 3.1.4.2.1 OSPF Area Design

Although ensuring the maximum availability for a routed OSPF Campus design requires consideration of many factors, the primary factor is how to implement a scalable area design. The convergence, stability, and manageability of a routed Campus and the network as a whole depend on a solid routing design. OSPF implements a two-tier hierarchical routing model that uses a Core as a backbone tier known as “area zero.” Attached to that backbone via area boarder routers (ABRs) are a number of secondary tier areas. The hierarchical design of OSPF areas is well-suited to the hierarchical Campus design. The Campus Core provides the backbone function supported by OSPF area 0, and the Distribution building blocks with redundant Distribution switches can be configured in different areas with the Distribution switches acting as the ABRs.

**Figure 3-7 Campus OSPF Area Design**



In many OSPF area designs, the question of optimal size of the area (number of nodes and links) is often a primary consideration in specifying the OSPF area boundaries, but does not play as key a role in the Campus as it can in a general design. Mapping the area boundaries to the hierarchical physical design enforcing hierarchical traffic patterns, minimizing convergence times, and maximizing stability of the network are more significant factors in designing the OSPF Campus than is optimizing the number of nodes in the area or the number of areas in the network.

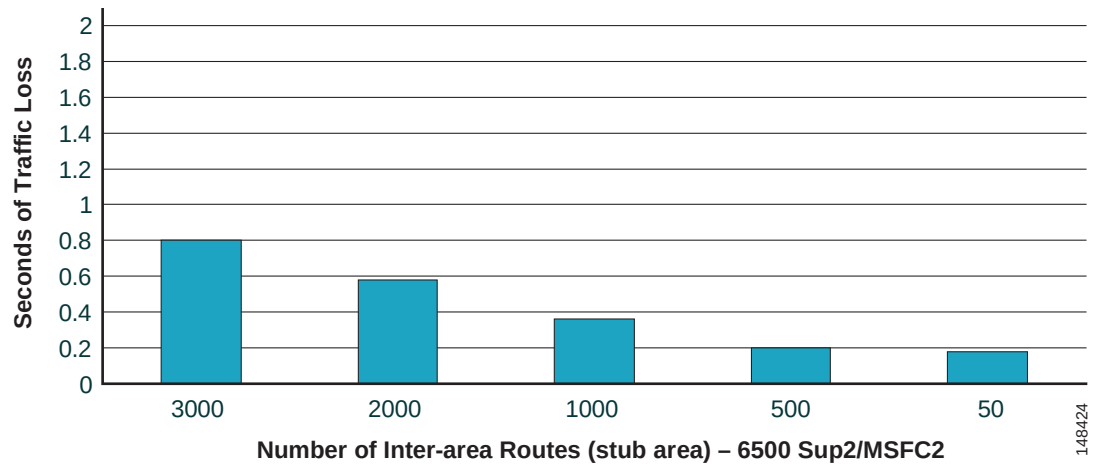
Mapping a unique OSPF area to each Distribution block directly maps the basic building block of the OSPF routing design (the area) onto the basic building block of the Campus network (the Distribution block). The function of the Distribution switch as a point of control for traffic to and from all Access segments is directly supported by the functions of the ABR to control routing information into and out of the area. The boundary for route convergence events provided by the ABR supports the desire to have the Distribution block provide for fault containment, and also serves to aid in controlling the time required for routing convergence by restricting the scope of that routing convergence. Additionally, leveraging the properties of an OSPF stub area makes it relatively simple to enforce the rule that traffic not destined to an address within the Distribution block is never forwarded into or through the area. As mentioned above in Implementing Layer 3 Access using EIGRP, the capacity of the Access switches and their uplinks are specified to meet the needs of locally-connected devices only. Configuring each Distribution block as a unique area ensures that the large aggregated volumes of traffic within the Core are never forwarded through the lower bandwidth links in the Access layer, and also ensures that no traffic is ever mistakenly routed through the Access layer, bypassing any Distribution layer policy or security controls.

#### 3.1.4.2.2 OSPF Stubby and Totally Stub Distribution Area

Within each Distribution stub area, convergence of traffic is best optimized through a combination of an equal-cost path design and the use of stub OSPF area. Although there are many types of stub areas, Cisco recommends that “totally stubby” area configurations be used for Campus Distribution blocks to minimize the size of routing and forwarding tables in the Access switches.

As discussed above, the convergence for traffic flows upstream from the Access switches depends on equal-cost path recovery. As discussed above in the section on hierarchical design, one of the key mechanisms for ensuring very fast network recovery is leveraging the fast convergence behavior of equal cost path routing. When equal cost paths exist, the failure of one path requires only local hardware and software routing and forwarding updates to restore all traffic flows. However, the time to complete these routing and forwarding table updates is not constant, but varies depending on the specific hardware platform and more importantly on the number of routes or forwarding entries in the system.

The update of the CEF hardware FIB and adjacency entries is performed by the system software engine, and the entries in the tables are processed in a linear fashion. The greater the number of entries that need to be modified, the longer it takes for all entries to be modified. It is necessary to assume that the last entry updated impacts some traffic flows, and convergence time is calculated based on the time it takes for the last entry to be updated. When the number of routes in the Access switches is increased, the time taken to ensure all traffic flows have been restored also increases.

**Figure 3-8 Convergence Results**

The time taken for convergence with 3000 inter-area routes in addition to the intra-area routes is still sub-seconds. However, to meet the design goal of sub-200 msec recovery, it is necessary to reduce the number of total routes in the Distribution block Access switches. Controlling the summarization of routes in the network aids in the reduction of the number of inter-area and external routes. The use of a stub area configuration for the Distribution block area prevents the propagation of external routes into the Distribution block. However, Cisco recommends configuring the Distribution block areas as totally stub areas, which stops the propagation of all inter-area routes into the Access switches. In totally stub area configurations, each of the Distribution switch ABRs creates a default route that provides the forwarding path for the majority of traffic in the Distribution block. As shown in [Figure 3-9](#), the use of the no-summary command creates a totally stub area that contains only a single default inter-area route, and reduces the total number of routes in the hardware forwarding tables significantly.

The stub parameter in the area configuration command blocks “external” LSAs from entering the area through the ABR. The no-summary command used with the stub parameter blocks inter-area “summary” LSAs from entering the area. The ABRs also inject a default route (0.0.0.0) into the stub area to provide access to the routes not propagated into the area.

**Figure 3-9 Default OSPF Area Configuration and Associated Route Table Impact**

```

router ospf 100
router-id 10.120.250.6
ispf
log-adjacency-changes
auto-cost reference-bandwidth 10000
timers throttle spf 10 100 5000
timers throttle lsa all 10 100 5000
timers lsa arrival 80
network 10.120.0.0 0.0.255.255 area 120

```

```

Access-Switch#sh ip route summary
IP routing table name is Default-IP-Routing-Table(0)
Route Source      Networks      Subnets      Overhead      Memory (bytes)
connected         1             6             776           1120
static            0             0             0             0
ospf 100          2             3626          459648        580480
  Intra-area: 70 Inter-area: 3055 External-1: 1 External-2: 502
  NSSA External-1: 0 NSSA External-2: 0
internal          7             8260
Total             10            3632          460424        589860

```

148/25

**Figure 3-10 OSPF Stub Area Configuration and Associated Route Table Impact**

```

router ospf 100
router-id 10.120.250.6
ispf
log-adjacency-changes
auto-cost reference-bandwidth 10000
area 120 stub
timers throttle spf 10 100 5000
timers throttle lsa all 10 100 5000
timers lsa arrival 80
network 10.120.0.0 0.0.255.255 area 120

```

```

Access-Switch#sh ip route summary
IP routing table name is Default-IP-Routing-Table(0)
Route Source      Networks      Subnets      Overhead      Memory (bytes)
connected         1             6             792           1120
static            0             0             0             0
ospf 100          1             3196          404480        511520
  Intra-area: 140 Inter-area: 3057 External-1: 0 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal          6             7080
Total             8             3202          405272        519720

```

148/25

**Figure 3-11 OSPF Totally Stub Area Configuration and Associated Route Table Impact**

```

router ospf 100
  router-id 10.120.250.6
  ispf
  log-adjacency-changes
  auto-cost reference-bandwidth 10000
  area 120 stub no-summary
  timers throttle spf 10 100 5000
  timers throttle lsa all 10 100 5000
  timers lsa arrival 80
  network 10.120.0.0 0.0.255.255 area 120

```

```

Access-Totally-Stubby#sh ip route sum
IP routing table name is Default-IP-Routing-Table(0)
Route Source      Networks      Subnets      Overhead      Memory (bytes)
connected         1             6             792           1120
static            0             0             0             0
ospf 100          1             140           13568         22560
  Intra-area: 140 Inter-area: 1 External-1: 0 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal          3
Total             5             146          14360         27220

```

The use of a stub, or better yet a totally stubby area, can have a positive impact on convergence times by reducing route table size. However, configuring stub and in particular totally stubby areas requires some attention. Stub areas create an artificial default route sourced from each of the Distribution ABRs, which is propagated as a type-3 network summary route into the stub area. This concept is shown in [Figure 3-11](#) as the single inter-area route in the “show ip route sum” output. This default route is created to represent the “rest” of the network to the stub area routers. It is used to build a forwarding path back to the Distribution ABRs for all traffic external to the OSPF domain in the case of a stub configuration, and both the external and inter-area routes in the case of a totally stub area. (See [Figure 3-12](#)).

**Figure 3-12 Default Route and Distribution ABRs**

```

Access-Switch#sh ip ospf data summary

OSPF Router with ID (10.120.250.6) (Process ID 100)

Summary Net Link States (Area 120)

Routing Bit Set on this LSA
LS age: 1122
Options: (No TOS-capability, DC, Upward)
LS Type: Summary Links(Network)
Link State ID: 0.0.0.0 (summary Network Number)
Advertising Router: 10.122.102.1
LS Seq Number: 8000051A
Checksum: 0x6FC4
Length: 28
Network Mask: /0
      TOS: 0  Metric: 1

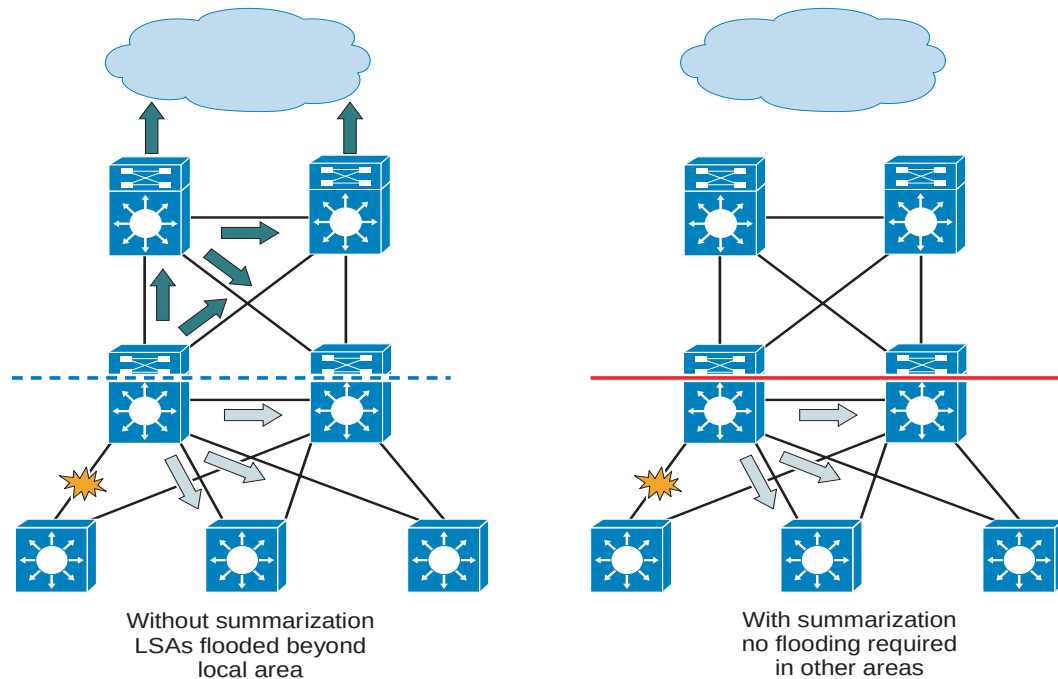
Routing Bit Set on this LSA
LS age: 1120
Options: (No TOS-capability, DC, Upward)
LS Type: Summary Links(Network)
Link State ID: 0.0.0.0 (summary Network Number)
Advertising Router: 10.122.102.2
LS Seq Number: 80000001
Checksum: 0xAAA6
Length: 28
Network Mask: /0
      TOS: 0  Metric: 1

```

In the normal case where all Distribution switch interfaces configured in area 0 are directly connected to the Core switches, this design works very effectively. Traffic from all the Access switches follows the default route and is forwarded to the Distribution switches, which either forward back to the correct Access switch or forward to the Core switches. However, in the case where a loopback or any other interface not providing connectivity to the backbone (area 0) is incorrectly configured to reside in area “0”, the Distribution switch may incorrectly advertise a default route to the Access switches, potentially creating a routing black hole.

### 3.1.4.2.3 Distribution ABR Route Summarization

Controlling the extent of topology changes and the number of routes advertised throughout the network are key to good routing design. (Figure 3-8) Reducing the number of active routes that must be maintained in the forwarding tables can also help fine tune the time taken for the network to converge. Additionally, implementing a well-structured summarization scheme reduces the scope of network topology updates in the event of link or node failures. The hierarchical Campus design provides an excellent opportunity to minimize the scope of topology changes while simultaneously reducing the route count in the network. The network is designed for traffic to flow within each layer, for local traffic to remain within each Distribution area, and for all other traffic to flow to the Core and then to the correct destination area. This design philosophy provides an ideal environment to implement route controls such as stub area design and to complement it with route summarization.

**Figure 3-13 OSPF Route Summarization Limits Propagation of LSAs**

Summarization of Distribution area routes is accomplished using the `area range` command. The range command defines which subnets within the specified Distribution area are summarized into a single outbound summary network advertisement. Cisco recommends that the cost of the advertised summary network route be specified with a static or hard coded cost, as shown in the following configuration example.

```
router ospf 100
router-id 10.122.102.2
ispf
log-adjacency-changes
auto-cost reference-bandwidth 10000
area 120 stub no-summary
area 120 range 10.120.0.0 255.255.0.0 cost 10
timers throttle spf 10 100 5000
timers throttle lsa all 10 100 5000
timers lsa arrival 80
network 10.120.0.0 0.0.255.255 area 120
network 10.122.0.0 0.0.255.255 area 0
```

Using summarized routes is consistent with the design principles of the Campus network with its tiered traffic flows. In the structured hierarchical Campus design, there is no need to propagate any specific routing information from a Distribution area into the rest of the network. All traffic within the Distribution area is routed via Distribution switches, and all traffic to and from the Access subnets is also routed through the Distribution nodes. The need to advertise specific subnet routes from an OSPF area



into the backbone of the network is usually a result of the need to engineer traffic flows to ensure an optimal path and/or manage traffic volumes. In the hierarchical Campus, highly granular traffic load balancing is achieved via hardware CEF forwarding on the Core and Distribution switches. This allows traffic flows to be load balanced on a per session basis. Additionally, the recommended structured design provides direct connectivity between both ABRs and all destination subnets, ensuring that no sub-optimal traffic paths are used. The hierarchical Campus design also uses redundant high capacity GigE and 10 GigE links to ensure sufficient capacity on all traffic paths. The need to engineer traffic flows is significantly reduced in the hierarchical Campus design, and the advantages in terms of route reduction and controls on LSA flooding outweigh most any advantages gained through a more granular routing design.

#### 3.1.4.2.4 SPF and LSA Throttle Tuning

The design of the Layer 3 Access Campus is very similar to a branch WAN. The Access switch provides same routing functionality as the Branch router, and the Distribution switch provides the same routing functions as the WAN Aggregation router.

Default timers for OSPF convergence are conservative and have been chosen to give priority to network stability especially Wide Area Networks and reduction of routing update overhead. The basic topology of the routed campus is similar to but not exactly the same as the WAN environment.

Keep in mind the following differences between the two environments when optimizing the campus routing design:

- Fewer bandwidth limitations in the Campus allow for more aggressive tuning of control plane traffic(for example, hello packet intervals)
- Direct fiber interconnects simplify neighbor failure detection as well as provide a more stable environment than a typical WAN
- Lower cost redundancy in the campus allow for use of the optimal redundant design
- Hardware L3 switching ensures dedicated CPU resources for control plane processing

The optimal OSPF design for routed Access must include improving the convergence time for the OSPF routing protocol itself. The time required to restore traffic flows depends on the following three factors:

- Time to detect the failure
- Time to determine the new optimal path
- Time to update the software and hardware forwarding tables

Of these three times, the first and third can be controlled through a combination of physical design and routing design. The second factor is also partially achieved by optimal area and routing design. However, optimization of the design by itself is not always sufficient to meet convergence requirements. Cisco recommends tuning the OSPF timers and process. OSPF uses a link-state routing algorithm that uses LSAs to propagate information about the links and nodes in the network, and the Djiskstra SPF algorithm to calculate the network topology. Updates to the switches routing table involve a process of flooding and receiving updated LSAs, followed by an update of the network topology by the SPF algorithm. The time taken to complete this process depends on the following:

- Number of LSAs
- Number of nodes that need to receive the LSAs
- Time required to transmit the LSAs
- Time required run the SPF calculation

### 3.1.4.2.5 SPF Throttle Tuning

Tune the initial timer to 1 second to allow for all LSAs flooded as a result of a network failure to be received by the switch before running the initial SPF calculation. This allows the hold timer to be set at a large enough value, usually 5 seconds, to prevent any catastrophic system overload. To improve OSPF convergence and provide stable sub-second convergence, implement the newer SPF throttle capabilities.

With the introduction of the new SPF throttle mechanism, the interaction of the throttle timers has been improved to implement an exponential back-off mechanism in the event of multiple triggers for sequential SPF runs. The throttle timer is now configured with three values:

```
spf-start (default 5000ms), spf-hold (default 10000ms), spf-max-wait (default 10000ms).
```

```
router ospf 100
router-id 10.120.250.101
log-adjacency-changes
auto-cost reference-bandwidth 10000
area 120 stub no-summary
timers throttle spf <spf-start> <spf-hold> <spf-max-wait>
network 10.120.0.0 0.0.255.255 area 120
```

280509

The three parameters interoperate to determine how long it takes for an SPF calculation to be run after notification of a topology change event (arrival of an LSA). On the arrival of the first topology notification, the `spf-start` or initial hold timer controls how long to wait before starting the SPF calculation. If no subsequent topology change notification arrives (new LSA) during the hold interval, the SPF is free to run again as soon as the next topology change event is received. However, if a second topology change event is received during the hold interval, the SPF calculation is delayed until the hold interval expires. Additionally, in the second case, the hold interval is temporarily doubled. In the event of more topology changes occurring during this new hold interval, the hold interval continues to grow until the maximum period configured is reached. After the expiration of any hold interval, the timer is reset and any future topology changes trigger an SPF again based on the initial timer.

With the introduction of the new SPF throttle timers, it is now possible to safely reduce the initial SPF timer to a sub-second value and improve the convergence time of the network.

The recommended values are as follows:

```
spf-start:      10 msec
spf-hold:       100 to 500 msec
spf-max-wait:   5 seconds

router ospf 100
router-id 10.120.250.101
log-adjacency-changes
auto-cost reference-bandwidth 10000
area 120 stub no-summary
timers throttle spf 10 100 5000
network 10.120.0.0 0.0.255.255 area 120
```

280610

When designing a routed Access Campus to achieve sub-second convergence, the most important of the three timers to modify is the spf-start, or initial wait timer. By reducing this timer from the previously recommended 1 second value to the new throttle feature value of 10 msec, the convergence time can be significantly reduced. It is still not recommended to set this timer to 0. Providing a slight wait interval provides a window in which multiple LSA events caused by multiple interface changes can be processed together. Cisco recommends that the wait interval be at least 10 msec (equivalent to the interface debounce timer on GigE and 10GigE fiber links). Configuring a short but non-zero initial wait timer should allow most local interface changes occurring simultaneously because of a major fiber cut or line card failure to be processed concurrently.

When considering tuning the hold timer, it is advisable to consider the stability of the Campus infrastructure. Increasing the value of the hold timer reduces the number of iterations of the SPF algorithm in the event of a flapping link.

In a stable Campus environment with a well-summarized area design, there are mitigating factors on the probability of a flapping condition such that lowering the hold timer should not normally present a problem. However, this should be balanced against the understanding that in the hierarchical Campus design, reducing the hold timer normally has little impact on the ability of the network to restore traffic flows.

For more information on the configuration of SPF throttle timers, see the following URL:

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products\\_feature\\_guide09186a0080134ad8.html](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134ad8.html)

### 3.1.4.2.6 LSA Throttle Tuning

The use of SPF throttle timer tuning can aid in improving the convergence of the Campus network to within the sub-second threshold, but is not sufficient to ensure optimal convergence times. Two factors impact the ability of OSPF to converge: the time waiting for an SPF calculation, and the time waiting for an LSA to be received indicating a network topology change.

The same design and physical factors that allow for SPF tuning in the Campus environment also make it amenable to tuning of the LSA timers. The use of routed point-to-point interfaces in the Campus removes the need to consider the loss of multiple logical links in the event of a single interface failure. The use of direct fiber connections between devices also reduces the probability for link loss and ensures a higher degree of accurate link status detection. Interface-specific features such as debounce timers and

IP event dampening also lessens the probability of false or flapping interface conditions. The combination of these factors serves to mitigate the factors with which the LSA timers were initially designed to address.

Tuning LSA throttle timers uses an approach similar to that described above for SPF. Three configuration values are used: an initial delay timer, a hold timer, and a maximum hold timer. Using a similar approach to that discussed above results in the use of the same timer values for the LSA configuration as for the SPF configuration.

The recommended values are as follows:

```
lsa-start:      10 msec
lsa-hold:       100 to 500 msec
lsa-max-wait:   5 seconds

router ospf 100
router-id 10.120.250.101
log-adjacency-changes
auto-cost reference-bandwidth 10000
area 120 stub no-summary
timers throttle spf 10 100 5000
timers throttle lsa all 10 100 5000
network 10.120.0.0 0.0.255.255 area 120
```

In tuning the throttle timer controlling the generation of LSAs, it is necessary to make a similar configuration to the throttle timer controlling the receipt of LSAs. The “lsa arrival” timer controls the rate at which a switch accepts a second LSA with the same LSA ID. If Distribution switch A is configured to generate LSAs with a hold time of 100 msec, it is necessary for the adjacent switches, such as Distribution switch B for example, to be configured to accept LSAs at a rate at least equal to that with which they are generated. The best practice is to tune the arrival rate to some value less than the generated rate to accommodate for any buffering or internal process timer scheduling delays. Using a hold time of 100 msec, an LSA arrival value of 80 msec is considered sufficient.

```
router ospf 100
router-id 10.120.250.1
log-adjacency-changes
auto-cost reference-bandwidth 10000
area 120 stub no-summary
timers throttle spf 10 100 5000
timers throttle lsa all 10 100 5000
timers lsa arrival 80
network 10.120.0.0 0.0.255.255 area 120
```

280511

For more information on configuration of LSA throttle timers, see the following URL:

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products\\_feature\\_guide09186a0080161064.html](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a0080161064.html)

### 3.1.4.2.7 Interface Timer Tuning

#### 3.1.4.2.8 Hello and Dead Timer Tuning

The best practice for the Campus design uses point-to-point GigE and 10GigE fiber connections for all links between switches. Remote node and link loss detection is normally accomplished using the remote fault detection mechanism implemented as a part of the 802.3z and 802.3ae link protocols. It is still recommended in the Layer 3 Campus design that the OSPF hello and dead timers be reduced to 250 msec and 1 second. The loss of hellos and the expiration of the dead timer is not the primary fault detection mechanism in the Campus, but does provide a backup to the L1/2 remote fault detection mechanisms. In the rare case where a routed interface remains up after link loss, OSPF hello and dead timers are needed to detect neighbor loss to initiate convergence around a failed link or neighbor.

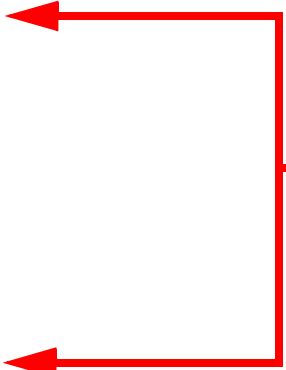
In the configuration example shown below, the hello interval is not explicitly configured but is calculated by taking the minimal dead interval of 1 second, as specified by the `minimal` keyword, and then dividing it by the hello-multiplier value configured.

##### Hello Interval Configuration

```
interface GigabitEthernet3/11
  description Link to Access Switch
  dampening
  ip address 10.120.0.204 255.255.255.254
  ip pim sparse-mode
  ip ospf dead-interval minimal hello-multiplier 4
  ip ospf priority 255
  logging event link-status
  load-interval 30
  carrier-delay msec 0
  mls qos trust dcsp

interface GigabitEthernet1/1
  description Uplink to Distribution 1
  dampening
  ip address 10.120.0.205 255.255.255.254
  ip pim sparse-mode
  ip ospf dead-interval minimal hello-multiplier 4
  ip ospf priority 0
  logging event link-status
  load-interval 30
  carrier-delay msec 0
  mls qos trust dcsp
```

Ensure timers  
are consistent  
on both sides  
of the link



In the above example, 1 second divided by 4 intervals gives an interval value of 250 msec. The selection for the number of hellos sent in the 1 second interval should be at least 3 to allow for enough resiliency in case of potential packet loss (a very low probability in a fiber-based Campus network but still possible).

For more information on configuring sub-second hello timers, see the following URL:

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products\\_feature\\_guide09186a00801039b1.html](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a00801039b1.html)

#### 3.1.4.2.9 Designated Router

Although the Campus is configured with point-to-point GigE links, OSPF still negotiates the designated and backup designated router on each of the switch-to-switch links. In the Campus environment, the selection of which switch is selected as DR has no impact on the stability or speed of convergence of the

network. However, it is still recommended that the Distribution switch be configured to act as DR on each of the Access-Distribution uplinks. In the event of an Access-Distribution uplink fiber failure, the Distribution switch acting as the DR can directly propagate updated network LSAs to all connected Access and Distribution switch peers in the area.

#### Designated Router Configuration

```
interface GigabitEthernet3/11
  description Link to Access Switch
  dampening
  ip address 10.120.0.204 255.255.255.254
  ip pim sparse-mode
  ip ospf dead-interval minimal hello-multiplier 4
  ip ospf priority 255
  logging event link-status
  load-interval 30
  carrier-delay msec 0
  mls qos trust dcsp

interface GigabitEthernet1/1
  description Uplink to Distribution 1
  dampening
  ip address 10.120.0.205 255.255.255.254
  ip pim sparse-mode
  ip ospf dead-interval minimal hello-multiplier 4
  ip ospf priority 0
  logging event link-status
  load-interval 30
  carrier-delay msec 0
  mls qos trust dcsp
```

Configure  
Distribution switch to  
act as DR on  
access-distribution  
links

#### 3.1.4.2.10 Implementing Supervisor Redundancy Using NSF/SSO

The basic principle of network high availability is to provide seamless connectivity to business applications any time and anywhere, both in terms of bandwidth and consistent response time. In the hierarchical design, supervisor redundancy is designed to address downtime, both planned (maintenance and testing) and unplanned (system crash). In a hierarchical network, redundant supervisor configurations provide not only full component redundancy for the highest mean time between failure designs, but also the least possible traffic loss during exception conditions. In addition, they provide a consistent topology during failure, thus maintaining capacity and bandwidth at each layer in the campus network.

The hierarchical design shown in [Figure 3-7](#) has built-in physical redundancy at the Core and Distribution layers, both in terms of node and link level, providing quick traffic recovery. However, during failure, route convergence and reduced link bandwidth impact the application response time, so redundant nodes and redundant links may not be sufficient. NSF/SSO uses underlying hardware capability to achieve protocol-level redundancy.

In traditional designs, most host end devices such as PCs are connected to a single closet switch, which is the single point of failure. Therefore, the critical application of Supervisor redundancy is at the Access layer. For the Routed Access design, where the Access layer operates at Layer2 and Layer3, NSF provides additional protection when used in conjunction with SSO.

Section [3.1.4.2.8 Hello and Dead Timer Tuning](#), [page 3-23](#) discusses the benefits of tuning OSPF Hello and Dead timers. Specifying a smaller dead interval (*seconds*) provides faster detection of a neighbor being down thus improving convergence time. This technique quickly removes an OSPF router from the network during failure. In comparison, NSF is a technique that avoids routing convergence.

This section simply highlights the role of OSPF fast hellos and NSF and does not explore the application of NSF/SSO at the Core, Distribution or the Access layer.

For details on NSF/SSO and configuration, refer to the following URL:

<http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/nsfsso.html>

#### 3.1.4.2.11 Stateful Switchover (SSO) Operation

SSO establishes one of the supervisor engines as active while the other supervisor engine is designated as standby, and then SSO synchronizes information between them. A switchover from the active to the redundant supervisor engine occurs when the active supervisor engine fails, or is removed from the switch, or is manually shut down for maintenance. This type of switchover ensures that Layer 2 traffic is not interrupted.

In networking devices running SSO, both supervisor engines must be running the same configuration so that the redundant supervisor engine is always ready to assume control following a fault on the active supervisor engine. SSO switchover also preserves FIB and adjacency entries and can forward Layer 3 traffic after a switchover. Configuration information and data structures are synchronized from the active to the redundant supervisor engine at startup and whenever changes to the active supervisor engine configuration occur. Following initial synchronization between the two supervisor engines, SSO maintains state information between them, including forwarding information.

During switchover, system control and routing protocol execution is transferred from the active supervisor engine to the redundant supervisor engine. The switch control plane requires between 0 and 3 seconds to switchover from the active to the redundant supervisor engine.

#### 3.1.4.2.12 Nonstop Forwarding (NSF) Operation

Cisco NSF always runs with SSO and provides redundancy for Layer 3 traffic. NSF works with SSO to minimize the amount of time that a network is unavailable following a switchover. The main purpose of NSF is to continue forwarding IP packets following a supervisor engine switchover.

Cisco NSF is supported by the BGP, OSPF, and IS-IS protocols for routing and is supported by Cisco Express Forwarding (CEF) for forwarding. These routing protocols have been enhanced with NSF-capability and awareness, which means that routers running these protocols can detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from peer devices. The OSPF protocol can be configured to use state information that has been synchronized between the active and the redundant supervisor engine to recover route information following a switchover instead of information received from peer devices.

A networking device is NSF-aware if it is running NSF-compatible software. A device is NSF-capable if it has been configured to support NSF.

Each protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. After the routing protocols have converged, CEF updates the FIB table and removes stale route entries. CEF then updates the line cards with the new FIB information.

### 3.1.4.2.13 Cisco NonStop Forwarding and IGP Timers

Cisco NSF with SSO is a Cisco innovation for systems with dual route processors. Cisco NSF with SSO allows a router that has experienced a hardware or software failure of an active route processor to maintain data link layer connections and to continue forwarding packets during the switchover through the hot standby route processor. This forwarding can continue despite the loss of routing protocol peering arrangements with other routers. Routing information is recovered dynamically in the background, while packet forwarding proceeds uninterrupted.



#### Note

OSPF and EIGRP NSF require that all neighbor networking devices be NSF-aware. If an NSF-capable router discovers that it has non-NSF-aware neighbors on a particular network segment, it will disable NSF capabilities for that segment. Other network segments composed entirely of NSF-capable or NSF-aware routers will continue to provide NSF capabilities.

For a list of NSF benefits and restrictions, refer to Configuring NSF with SSO Supervisor Engine Redundancy guide at the following URL:

<http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/nsfss.html>

- OSPF – Configuration:
  - interface GigabitEthernet1/1
    - ip ospf hello-interval 2
    - ip ospf dead-interval 8
  - router ospf 100
  - ...
  - nsf
  - timers throttle spf 10 100 5000
  - timers throttle lsa all 10 100 5000
- EIGRP Configuration:
  - interface GigabitEthernet1/1
    - ...
    - ip hello-interval eigrp 100 2
    - ip hold-interval eigrp 100 8
  - router eigrp 100
  - ...
  - nsf

NSF is designed on the premise of “convergence avoidance.” This fits well with the principle of making the fault domain local. The above OSPF and EIGRP timer settings avoid adjacency resets when NSF is enabled.



**Note**

Ensure that the timers are consistent on both ends of the link.

For a list of NSF benefits and restrictions, refer to Configuring NSF with SSO Supervisor Engine Redundancy guide at the following URL:

<http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/nsfssso.html>

### 3.1.4.3 IP Multicast

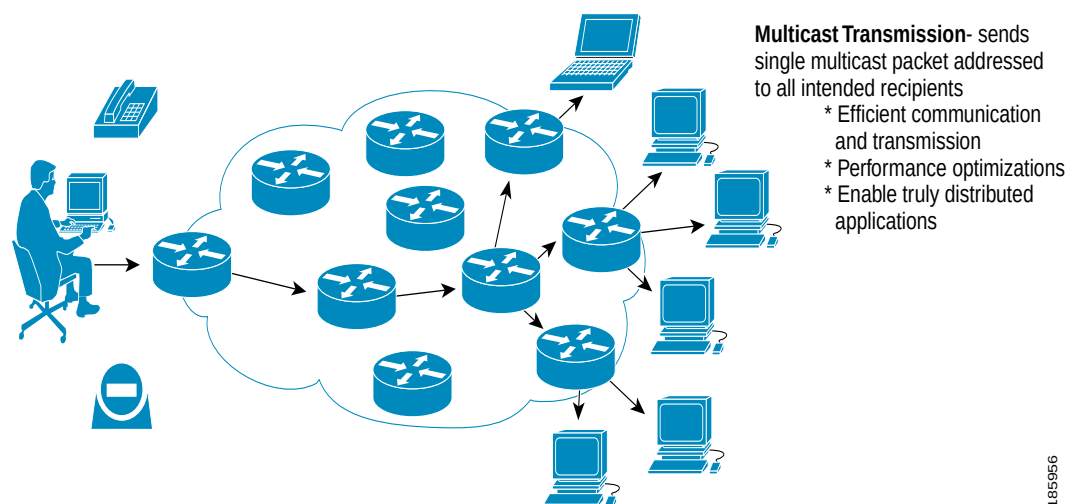
IP multicast allows for a streamlined approach to data delivery whenever multiple hosts need to receive the same data at the same time. For example:

- When configured for IP multicast services, Music-on-Hold (MoH) can stream the same audio file to multiple IP phones without the overhead of duplicating that stream one time for each phone on hold.
- IP/TV allows for the streaming of audio, video, and slides to thousands of receivers simultaneously across the network. High-rate IP/TV streams that would normally congest a low-speed WAN link can be filtered to remain on the local Campus network.

#### 3.1.4.3.1 Multicast Forwarding

IP multicast delivers source traffic to multiple receivers using the least amount of network resources as possible without placing additional burden on the source or the receivers. Multicast packets are replicated in the network by Cisco routers and switches enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols.

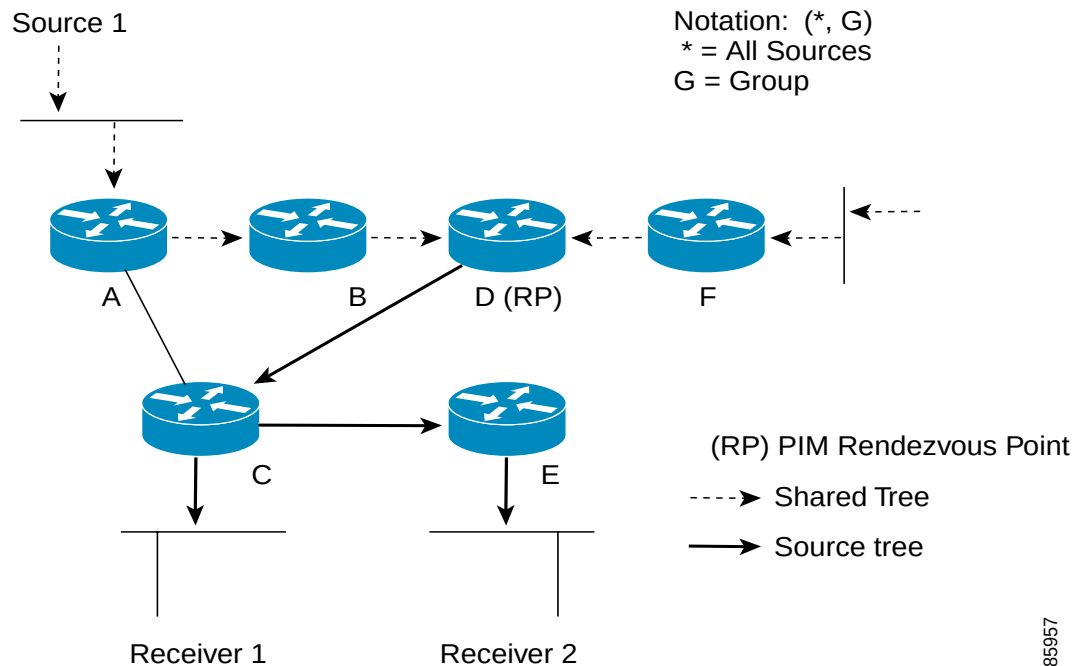
**Figure 3-14 Basic Multicast Service**



Multicast capable routers create "distribution trees" that control the path that IP Multicast traffic takes through the network in order to deliver traffic to all receivers. PIM uses any unicast routing protocol to build data distribution trees for multicast traffic.

The two basic types of multicast distribution trees are source trees and shared trees.

- Source trees-The simplest form of a multicast distribution tree is a source tree with its root at the source and branches forming a tree through the network to the receivers. Because this tree uses the shortest path through the network, it is also referred to as a shortest path tree (SPT).
- Shared trees-Unlike source trees that have their root at the source, shared trees use a single common root placed at some chosen point in the network. This shared root is called a Rendezvous Point (RP).

**Figure 3-15 Shared Distribution Tree**

In the example above, the RP has been informed of Sources 1 and 2 being active and has subsequently joined the SPT to these sources.

PIM uses the concept of a designated router (DR). The DR is responsible for sending Internet Group Management Protocol (IGMP) Host-Query messages, PIM Register messages on behalf of sender hosts, and Join messages on behalf of member hosts.

### 3.1.4.3.2 Features of IP Multicast

The primary difference between multicast and unicast applications lies in the relationships between sender and receiver. There are three general categories of multicast applications:

- One to many, as when a single host sends to two or more receivers.
- Many-to-one refers to any number of receivers sending data back to a (source) sender via unicast or multicast. This implementation of multicast deals with response implosion typically involving two-way request/response applications where either end may generate the request.
- Many-to-many, also called N-way multicast, consists of any number of hosts sending to the same multicast group address, as well as receiving from it.

One-to-many are the most common multicast applications. The demand for many-to-many N-way is increasing with the introduction of useful collaboration and videoconferencing tools. Included in this category are audio-visual distribution, Webcasting, caching, employee and customer training,

announcements, sales and marketing, information technology services and human resource information. Multicast makes possible efficient transfer of large data files, purchasing information, stock catalogs and financial management information. It also helps monitor real-time information retrieval as, for example, stock price fluctuations, sensor data, security systems and manufacturing.

### 3.1.4.3.3 PIM Sparse Mode

The PIM Sparse Mode is a widely deployed IP Multicast protocol and is highly scalable in Campus networks. *This mode is suitable for one-to-many (one source and many receivers) applications for Enterprise and Financial customers.*

PIM Sparse Mode can be used for any combination of sources and receivers, whether densely or sparsely populated, including topologies where senders and receivers are separated by WAN links, and/or when the stream of multicast traffic is intermittent.

- *Independent of unicast routing protocols* - PIM can be deployed in conjunction with any unicast routing protocol.
- *Explicit-join* - PIM-SM assumes that no hosts want the multicast traffic unless they specifically ask for it via IGMP. It creates a shared distribution tree centered on a defined "rendezvous point" (RP) from which source traffic is relayed to the receivers. Senders first send the data to the RP, and the receiver's last-hop router sends a join message toward the RP (explicit join).
- *Scalable* - PIM-SM scales well to a network of any size including those with WAN links. PIM-SM domains can be efficiently and easily connected together using MBGP and MSDP to provide native multicast service over the Internet.
- *Flexible* - A receiver's last-hop router can switch from a PIM-SM shared tree to a source-tree or shortest-path distribution tree whenever conditions warrant it, thus combining the best features of explicit-join, shared-tree and source-tree protocols.

In a PIM-SM environment, RPs (Rendezvous Point) act as matchmakers, matching sources to receivers. With PIM-SM, the tree is rooted at the RP not the source. When a match is established, the receiver joins the multicast distribution tree. Packets are replicated and sent down the multicast distribution tree toward the receivers.

Sparse mode's ability to replicate information at each branching transit path eliminates the need to flood router interfaces with unnecessary traffic or to clog the network with multiple copies of the same data. *As a result, PIM Sparse Mode is highly scalable across an enterprise network and is the multicast routing protocol of choice in the enterprise.*

For more details, refer to [Cisco AVVID Network Infrastructure IP Multicast Design](#)

[http://www.cisco.com/application/pdf/en/us/guest/tech/tk363/c1501/ccmigration\\_09186a008015e7cc.pdf](http://www.cisco.com/application/pdf/en/us/guest/tech/tk363/c1501/ccmigration_09186a008015e7cc.pdf)

### 3.1.4.3.4 PIM bidir

PIM bidir was simultaneously configured in addition to PIM-SM. Separate multicast streams for Bidir and PIM-SM were running at the same time and a few multicast receivers were configured to receive both, Bidir and PIM-SM streams.

In many-to-many deployments (many sources and many receivers) PIM bidir is recommended.

Bidir-PIM is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast.

In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address need not be a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. Using this technique is the preferred configuration for establishing a redundant RP configuration for bidir-PIM.

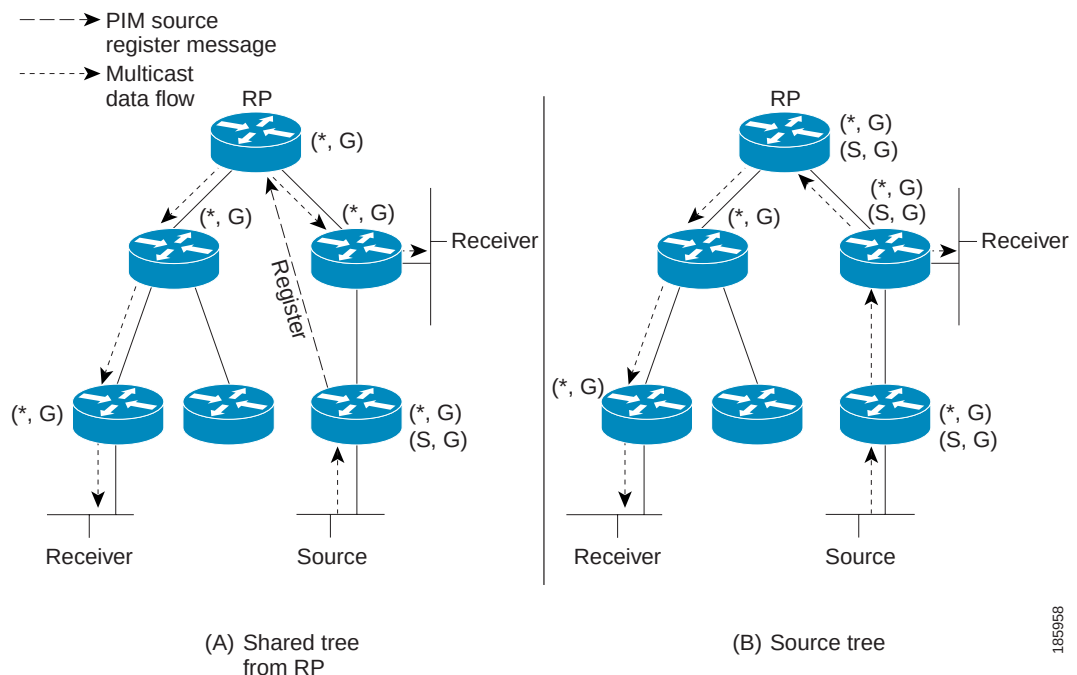
Membership to a bidirectional group is signaled via explicit join messages. Traffic from sources is unconditionally sent up the shared tree toward the RP and passed down the tree toward the receivers on each branch of the tree.

Bidir-PIM is designed to be used for many-to-many applications within individual PIM domains. Multicast groups in bidirectional mode can scale to an arbitrary number of sources without incurring overhead due to the number of sources.

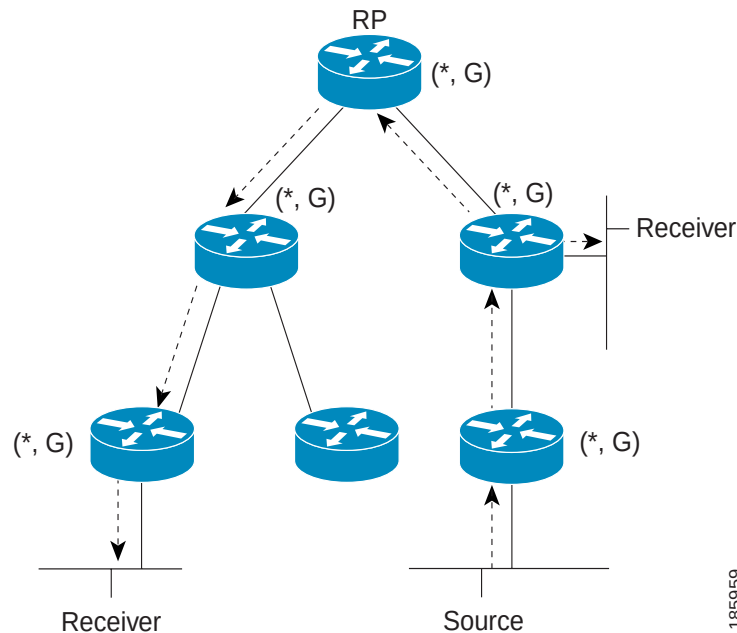
Bidir-PIM is derived from the mechanisms of PIM sparse mode (PIM-SM) and shares many shortest path tree (SPT) operations. Bidir-PIM also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but no registering process for sources as in PIM-SM. These modifications are necessary and sufficient to allow forwarding of traffic in all routers solely based on the (\*, G) multicast routing entries. This feature eliminates any source-specific state and allows scaling capability to an arbitrary number of sources.

Figure 3-16 and Figure 3-17 show the difference in state created per router for a unidirectional shared tree and source tree versus a bidirectional shared tree.

**Figure 3-16 Unidirectional Shared Tree and Source Tree**



185958

**Figure 3-17 Bidirectional Shared Tree**

Main advantages with this mode are better support with intermittent sources and no need for an actual RP (works with Phantom RP). There is no need for MSDP for source information.

**Note**

PIM bidir is currently not supported on Catalyst 4500 series.

For more details on PIM bidir refer to [Bidirectional PIM Deployment Guide](#).

<http://www.cisco.com/warp/public/732/Tech/Multicast/docs/bidirdeployment.pdf>

### 3.1.4.3.5 PIM Stub

Multicast control plane traffic is always seen by every router on a LAN environment. The Stub IP Multicast is used to reduce and minimize the unnecessary multicast traffic that is seen on LAN in the access layer and save the bandwidth on the media to forward multicast traffic to the upstream distribution/core layer.

In the Catalyst 3750 and 3560 Series Switches, the PIM Stub Multicast feature supports multicast routing between the distribution layer and access layer. This feature is currently available on Catalyst 3500/3700 platforms and restricts PIM control packets. This in turn helps reduce CPU utilization.

It supports two types of PIM interfaces: uplink PIM interfaces and PIM passive interfaces. In particular, a routed interface configured with the PIM Passive mode does not pass/forward PIM control plane traffic; it only passes/forwards IGMP traffic.

Complete these steps to configure PIM Stub Routing:

**Step 1** Issue this command to enable multicast routing globally on the switch or switch stack:

```
mix_stack(config)#ip multicast-routing distributed
```

**Step 2** Issue this command to enable PIM Stub Routing on the VLAN interface:

```
mix_stack(config)#interface vlan100
mix_stack(config-if) ip pim passive
```

### 3.1.4.3.6 IGMP Snooping

IP multicast uses the host signaling protocol IGMP to indicate that there are multicast receivers interested in multicast group traffic.

Internet Group Management Protocol (IGMP) snooping is a multicast constraining mechanism that runs on a Layer 2 LAN switch. IGMP snooping requires the LAN switch to examine some Layer 3 information (IGMP join/leave messages) in the IGMP packets sent between the hosts and the router. When the switch hears the "IGMP host report" message from a host for a multicast group, it adds the port number of the host to the associated multicast table entry. When the switch hears the "IGMP leave group" message from a host, the switch removes the host entry from the table.

**Note**

---

IGMP snooping is enabled by default and no explicit configuration is required.

---

*IGMP v2 is widely deployed for PIM sparse as well as PIM bidir and therefore was implemented in our setup.*

### 3.1.4.3.7 RP Deployment

Anycast RP is the preferred deployment model as opposed to a single static RP deployment. It provides for fast failover of IP multicast (within milliseconds or in some cases seconds of IP Unicast routing) and allows for load-balancing.

There are several methods for deploying RPs.

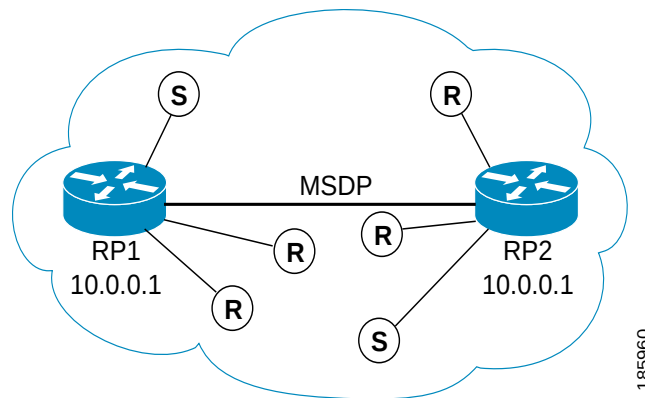
- RPs can be deployed using a single, static RP. This method does not provide redundancy or load-balancing and is not recommended.
- Auto-RP is used to distribute group-to-RP mapping information and can be used alone or with Anycast RP. Auto-RP alone provides failover, but does not provide the fastest failover nor does it provide load-balancing.
- Anycast RP is used to define redundant and load-balanced RPs and can be used with static RP definitions or with Auto-RP. *Anycast RP is the optimal choice as it provides the fast failover and load-balancing of the RPs.*

In the PIM-SM model, multicast sources must be registered with their local RP. The router closest to a source performs the actual registration. Anycast RP provides load sharing and redundancy across RPs in PIM-SM networks. It allows two or more RPs to share the load for source registration and to act as hot backup routers for each other (multicast only).

### 3.1.4.3.8 Anycast RP / MSDP

A very useful application of MSDP is Anycast RP. This is a technique for configuring a multicast Sparse Mode network to provide for fault tolerance and load sharing within a single multicast domain.

Two or more RPs are configured with the same IP address on loopback interfaces, say 10.0.0.1 for example:

**Figure 3-18 Anycast RP**

The loopback address should be configured as a 32 bit address. All the downstream routers are configured so that they know that their local RP's address is 10.0.0.1. IP routing automatically selects the topologically closest RP for each source and receiver. Since some sources might end up using one RP, and some receivers a different RP there needs to be some way for the RPs to exchange information about active sources. This is done with MSDP. All the RPs are configured to be MSDP peers of each other. Each RP will know about the active sources in the other RP's area. If any of the RPs was to fail, IP routing will converge and one of the RPs would become the active RP in both areas.

**Note**

For Anycast RP configuration, create loopback1 interface for duplicate IP address on the RP routers and configure loopback0 interface with unique IP address used as router IDs, MSDP peer addresses etc.

### 3.1.4.3.9 MSDP

Multicast Source Discovery Protocol (MSDP) allows RPs to share information about active sources and is the key protocol that makes Anycast RP possible.

Sample configuration:

```
ip msdp peer 192.168.1.3 connect-source loopback 0
ip msdp cache-sa-state
ip msdp originator-id loopback0
```

### 3.1.4.3.10 Adjusting Timers for IP Multicast

Two timers can be adjusted to facilitate faster failover of multicast streams. The timers control the:

- PIM Query Interval
- Send-RP Announce Interval

#### PIM Query Interval

The `ip pim query-interval` command configures the frequency of PIM Router-Query messages. Router Query messages are used to elect a PIM DR. The default value is 30 seconds. *For faster failover of multicast streams, Cisco recommends 1 second interval in Campus networks.*

To verify the interval for each interface, issue the `show ip pim interface` command, as shown below.

```
svrL-dist#show ip pim interface
```

```

Address Interface Version/Mode Nbr    Query DR
Count Intvl
10.5.10.1 Vlan10 v2/Sparse0110.5.10.1
10.0.0.37 GigabitEthernet0/1 v2/Sparse1110.0.0.38
10.0.0.41 GigabitEthernet0/2 v2/Sparse1110.0.0.42

```

#### Send-RP Announce Interval

The **ip pim send-rp-announce** command has an interval option. Adjusting the interval allows for faster RP failover when using Auto-RP. The default interval is 60 seconds and the holdtime is 3 times the interval. So the default failover time is 3 minutes. The lower the interval, the faster the failover time.

Decreasing the interval will increase Auto-RP traffic but not enough to cause any kind of a performance impact. *For faster failover time, Cisco recommends values of 3 to 5 seconds in Campus networks*

#### 3.1.4.3.11 Multicast - Sources, Receivers, Streams

Multicast sources for PIM sparse mode, PIM bidir and IPTV were connected to access switches in the Services Block.

Multicast receivers were connected to wiring closet switches.

Real IPTV streams (PIM-SM) and simulated multicast streams (PIM-SM and PIM-bidir) from traffic generators were part of the traffic profile during this validation.

### 3.1.4.4 Wireless

With WiSM and 4404 series as Cisco wireless controller, wireless deployment was verified in the HA Campus Routed Access environment with wireless AP's connected to Access switches. Clients authenticate using Dot1x with a Radius server as the authentication server. The Authenticator on the clients was Cisco Secure Service Client (CSSC).

The Cisco Unified Wireless Network (CUWN) architecture centralizes WLAN configuration and control into a device called a WLAN Controller (WLC). This allows the WLAN to operate as an intelligent information network and support advanced services, unlike the traditional 802.11 WLAN infrastructure that is built from autonomous, discrete entities. The CUWN simplifies operational management by collapsing large numbers of managed end-points-autonomous access points-into a single managed system comprised of the WLAN controller(s) and its corresponding, joined access points.

In the CUWN architecture, APs are "lightweight," meaning that they cannot act independently of a WLC. APs are "zero-touch" deployed and no individual configuration of APs is required. The APs learn the IP address of one or more WLC via a controller discovery algorithm and then establish a trust relationship with a controller via a "join" process. Once the trust relationship is established, the WLC will push firmware to the AP if necessary and a configuration. APs interact with the WLAN controller via the Lightweight Access Point Protocol (LWAPP).

#### 3.1.4.4.1 Client Roaming

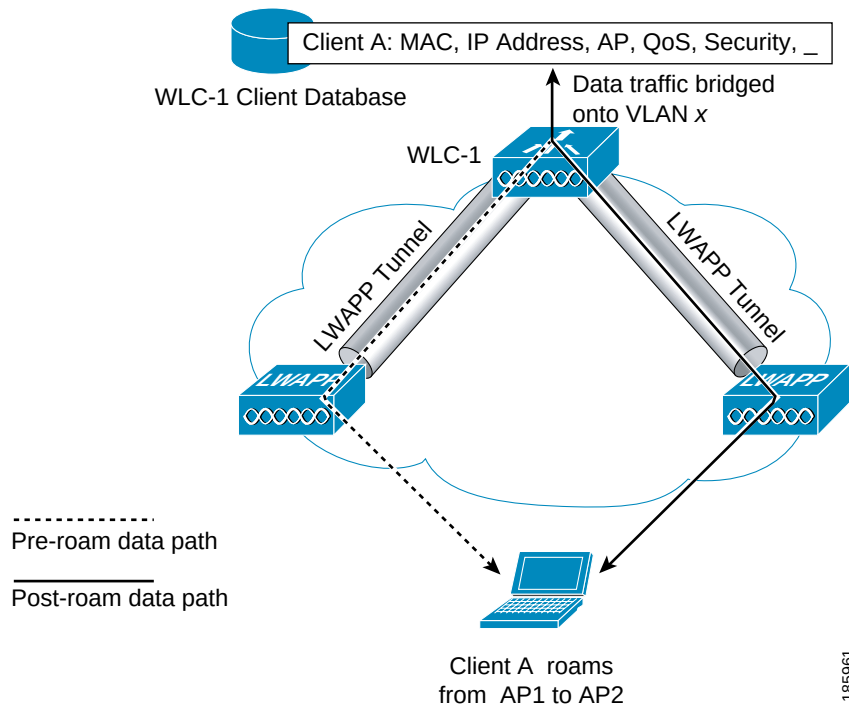
When a wireless client associates and authenticates to an AP, the AP's joined WLC places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, security context and associations, and QoS context, WLAN and associated AP. The WLC uses this information to forward frames and manage traffic to and from the wireless client.



### 3.1.4.4.2 Intra-controller Roaming

The wireless client roams from one AP to another when both APs are associated with the same WLC. This is illustrated in [Figure 3-19](#).

**Figure 3-19** Intra-controller roaming

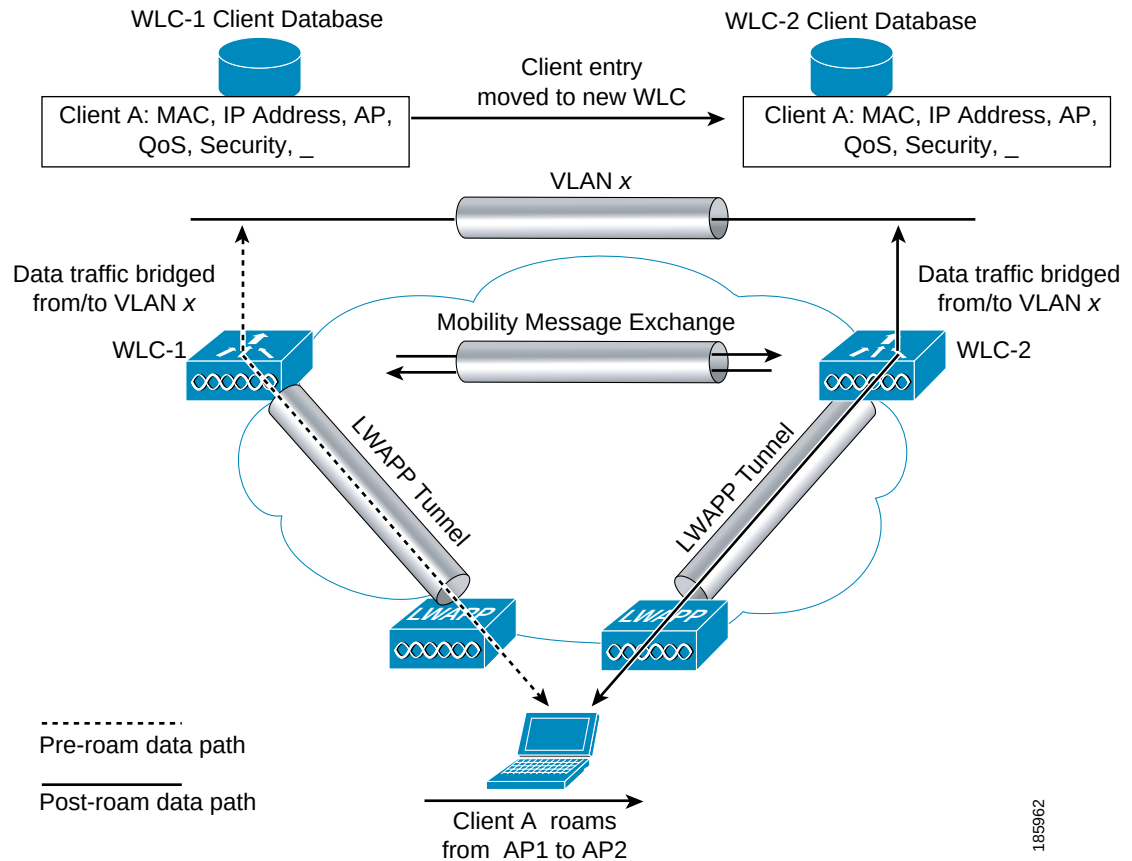


When the wireless client moves its association from one AP to another, the WLC simply updates the client database with the new associated AP.

### 3.1.4.4.3 Layer-2 Inter-Controller Roaming

The wireless client roams from an AP joined to one WLC and an AP joined to a different WLC.

**Figure 3-20** L2 - Inter-controller roaming



185962

As shown in Figure 3-20, Layer 2 roam occurs when the controllers bridge the WLAN traffic on and off the same VLAN and the same IP subnet. When the client re-associates to an AP connected to a new WLC, the new WLC exchanges mobility messages with the original WLC and the client database entry is moved to the new WLC. New security context and associations are established if necessary and the client database entry is updated for the new AP. All of this is transparent to the end-user. Also, the client retains the IP address during this process.

### 3.1.4.4.4 WiSM

The Cisco WiSM is a member of the Cisco wireless LAN controller family. It works in conjunction with Cisco Aironet lightweight access points, the Cisco WCS, and the Cisco wireless location appliance to deliver a secure and unified wireless solution that supports wireless data, voice, and video applications.

The Cisco WiSM consists of two Cisco 4404 controllers on a single module. The first controller is considered the WiSM-A card, while the second controller is considered WiSM-B card. Interfaces and IP addressing have to be considered on both cards independently. WiSM-A manages 150 access points, while WiSM-B manages a separate lot of 150 access points. These controllers can be grouped together in a mobility group, forming a cluster.

Wireless features were implemented in accordance with [Enterprise Mobility 3.0 Design Guide](#).

**Note**

Multicast over wireless was validated only using a Cisco 4404 wireless controller.

**Note**

Due to problems described in CSCsj48453, Multicast over wireless using WiSM module for catalyst 6500 could not be verified. Due to this DDTS, Catalyst 6500 does not forward multicast traffic to WiSM module when catalyst 6500 is configured in L3 mode. During validation this DDTS was being worked on by Cisco developers and could not be tested. However, at the time of writing this document, this DDTS is resolved.

### 3.1.4.5 Voice over IP

The Cisco Unified Communications System delivers fully integrated communications by enabling data, voice, and video to be transmitted over a single network infrastructure using standards-based Internet Protocol (IP).

The foundation architecture for Cisco IP Telephony includes of the following major components:

#### 3.1.4.5.1 Cisco IP Network Infrastructure

The Routed Access network design provides support for multiple clients such as hardware Cisco IP phones and video phones. Interface to PSTN network and traditional POTS phones are not in the scope of this design.

Campus LAN infrastructure design is extremely important for proper IP telephony operation on a converged network. Proper LAN infrastructure design requires following basic configuration and design best practices for deploying a highly available network.

Fast convergence of the network adds availability to the VoIP services.

- **Campus Access Layer**

The access layer of the Campus LAN includes part of the network from the desktop port(s) to the wiring closet switch.

Proper access layer design starts with assigning a single IP subnet per VLAN. Due to Routed Access network design, a VLAN cannot span multiple wiring closet switches; that is, a VLAN should have presence in one and only one access layer switch. More importantly, confining a VLAN to a single access layer switch also serves to limit the size of the broadcast domain. There is the potential for large numbers of devices within a single VLAN or broadcast domain to generate large amounts of broadcast traffic periodically, which can be problematic. A good rule of thumb is to limit the number of devices per VLAN to about 512, which is equivalent to two Class C subnets (that is, a 23-bit subnet masked Class C address). Typical access layer switches include the stackable Cisco Catalyst 3500 and 3700 series and the larger, higher-density Catalyst 4000 and 6000 switches.

- **Network Services**

The deployment of an IP Communications system requires the coordinated design of a well structured, highly available, and resilient network infrastructure as well as an integrated set of network services including Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), and Network Time Protocol (NTP).

### 3.1.4.5.2 Call Processing Agent

Cisco Unified Communications Manager (CUCM) is the core call processing software for the Cisco IP Telephony solution. It builds call processing capabilities on top of the Cisco IP network infrastructure. CUCM software extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, voice gateways, and multimedia applications.

Typically, Cisco Unified Communications Manager cluster servers, including media resource servers, reside in a data center or services block or server farm environment.

- **Single-site Model**

In this testing, single-site call processing model was used.

The single-site model for IP telephony consists of a call processing agent located at a single site, or campus, with no telephony services provided over an IP WAN.

The single-site model has the following design characteristics:

- Single CUCM or CUCM cluster.
- Maximum of 30,000 Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP) IP phones or SCCP video endpoints per cluster.
- High-bandwidth audio (for example, G.711, G.722, or Cisco Wideband Audio) between devices within the site.
- High-bandwidth video (for example, 384 kbps or greater) between devices within the site. The Cisco Unified Video Advantage Wideband Codec, operating at 7 Mbps, is also supported.

### 3.1.4.5.3 Communication Endpoints

A communication endpoint is a user instrument such as a desk phone or even a software phone application that runs on a PC. In the IP environment, each phone has an Ethernet connection. IP phones have all the functions you expect from a telephone, as well as more advanced features such as the ability to access World Wide Web sites.

In this design, Cisco IP phones and Video telephones could be used for endpoints.

Under this infrastructure, SCCP phones were connected to access layer of the campus network, with IP addresses routable to CUCM. These phones get registered with CUCM which then devices a route plan to find and connect to the numbers dialed.

To implement voice that is representative of an enterprise customer network, following design guides were used together to reflect the complexity in the field. These guides were the design basis for the CVD voice test suite. SCCP and SIP voice protocols were tested with Cisco Unified Call Manager.

- *Cisco Unified Communications SRND*

[http://www/en/US/products/sw/voicesw/ps556/products\\_implementation\\_design\\_guide\\_book09186a0080783d84.html](http://www/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a0080783d84.html)

- *Guide to Cisco Systems' VoIP Infrastructure Solution for SIP*

[http://www/en/US/tech/tk652/tk701/technologies\\_configuration\\_guide\\_book09186a00800eaa0e.html](http://www/en/US/tech/tk652/tk701/technologies_configuration_guide_book09186a00800eaa0e.html)

- *Cisco IOS SIP Configuration Guide*

[http://www/en/US/products/sw/iosswrel/ps5207/products\\_configuration\\_guide\\_book09186a00807517b8.html](http://www/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_book09186a00807517b8.html)

## 3.2 HA Campus Routed Access Test Coverage Matrix - Features

**Table 3-2 HA Campus Routed Access Test Coverage Matrix EIGRP as IGP- Features**

| EIGRP as IGP                              | CVD | CVD SYSTEM ASSURANCE |
|-------------------------------------------|-----|----------------------|
| EIGRP Stub                                | ✓   | ✓                    |
| Route Summarization                       | ✓   | ✓                    |
| Route Filters                             | ✓   | ✓                    |
| Hello and Hold timers tuning              | ✓   | ✓                    |
| EIGRP Authentication                      | ✓   | ✓                    |
| MLS CEF loadsharing                       | ✓   | ✓                    |
| Interface carrier-delay                   | ✓   | ✓                    |
| PIM Sparse-mode                           | ✓   | ✓                    |
| PIM bidir-mode                            |     | ✓                    |
| IGMP Snooping                             |     | ✓                    |
| Auto RP                                   |     | ✓                    |
| Accept-register filter                    |     | ✓                    |
| Multicast limits                          |     | ✓                    |
| MSDP / Anycast RP                         |     | ✓                    |
| MSDP SA-filters                           |     | ✓                    |
| Voice SCCP                                |     | ✓                    |
| Voice SIP                                 |     | ✓                    |
| Wireless Dot1x                            |     | ✓                    |
| Intra-controller Roaming                  |     | ✓                    |
| L2 Inter-controller Roaming               |     | ✓                    |
| Voice over Wireless                       |     | ✓                    |
| Convergence time for voice traffic        | ✓   | ✓                    |
| Convergence time for unicast data traffic | ✓   | ✓                    |
| Convergence time for multicast traffic    |     | ✓                    |
| Impact on voice traffic during congestion |     | ✓                    |

**Table 3-3 HA Campus Routed Access Test Coverage Matrix OSPF as IGP- Features**

| OSPF as IGP                                | CVD | CVD SYSTEM ASSURANCE |
|--------------------------------------------|-----|----------------------|
| OSPF Totally Stub                          | ✓   | ✓                    |
| Route Summarization                        | ✓   | ✓                    |
| SPF and LSA Throttle tuning                | ✓   | ✓                    |
| Hello and Dead timers tuning               | ✓   | ✓                    |
| OSPF Authentication                        | ✓   | ✓                    |
| MLS CEF loadsharing                        | ✓   | ✓                    |
| Interface carrier-delay                    | ✓   | ✓                    |
| PIM Sparse-mode                            | ✓   | ✓                    |
| PIM bidir-mode                             |     | ✓                    |
| IGMP Snooping                              |     | ✓                    |
| Auto RP                                    |     | ✓                    |
| Accept-register filter                     |     | ✓                    |
| Multicast limits                           |     | ✓                    |
| MSDP / Anycast RP                          |     | ✓                    |
| MSDP SA-filters                            |     | ✓                    |
| Voice SCCP                                 |     | ✓                    |
| Voice SIP                                  |     | ✓                    |
| Wireless Dot1x                             |     | ✓                    |
| Intra-controller Roaming                   |     | ✓                    |
| L2 Inter-controller Roaming                |     | ✓                    |
| Voice over Wireless                        |     | ✓                    |
| Convergence time for voice traffic         | ✓   | ✓                    |
| Convergence time for unicast data traffic  | ✓   | ✓                    |
| Convergence time for multicast traffic     |     | ✓                    |
| Impact on voice quality during convergence |     | ✓                    |
| Impact on video quality during convergence |     | ✓                    |
| Impact on voice traffic during congestion  |     | ✓                    |

## 3.3 HA Campus Routed Access Test Coverage Matrix - Platforms

**Table 3-4** HA Campus Routed Access Test Coverage Matrix - Platforms

| Platform | Role         | CVD | CVD SYSTEM ASSURANCE |
|----------|--------------|-----|----------------------|
| Cat6500  | Core         | ✓   | ✓                    |
| Cat6500  | Distribution | ✓   | ✓                    |
| Cat4500  | Distribution |     | ✓                    |
| Cat6500  | Access       | ✓   | ✓                    |
| Cat4500  | Access       |     | ✓                    |
| Cat3750  | Access       | ✓   | ✓                    |
| Cat3560  | Access       |     | ✓                    |
| Cat3750E | Access       |     | ✓                    |
| Cat3560E | Access       |     | ✓                    |

## 3.4 CVD System Assurance Test Strategy

Two sets of network device configurations were used to validate the HA Campus Routed Access design.

### 3.4.1 Baseline Configuration

The first set is the "Baseline configuration," as described in the [High Availability Campus Network Design-Routed Access Layer using EIGRP or OSPF](#) Design Guide recommendations.

Only convergence tests were executed with this set of baseline configuration.

### 3.4.2 Extended Baseline Configuration

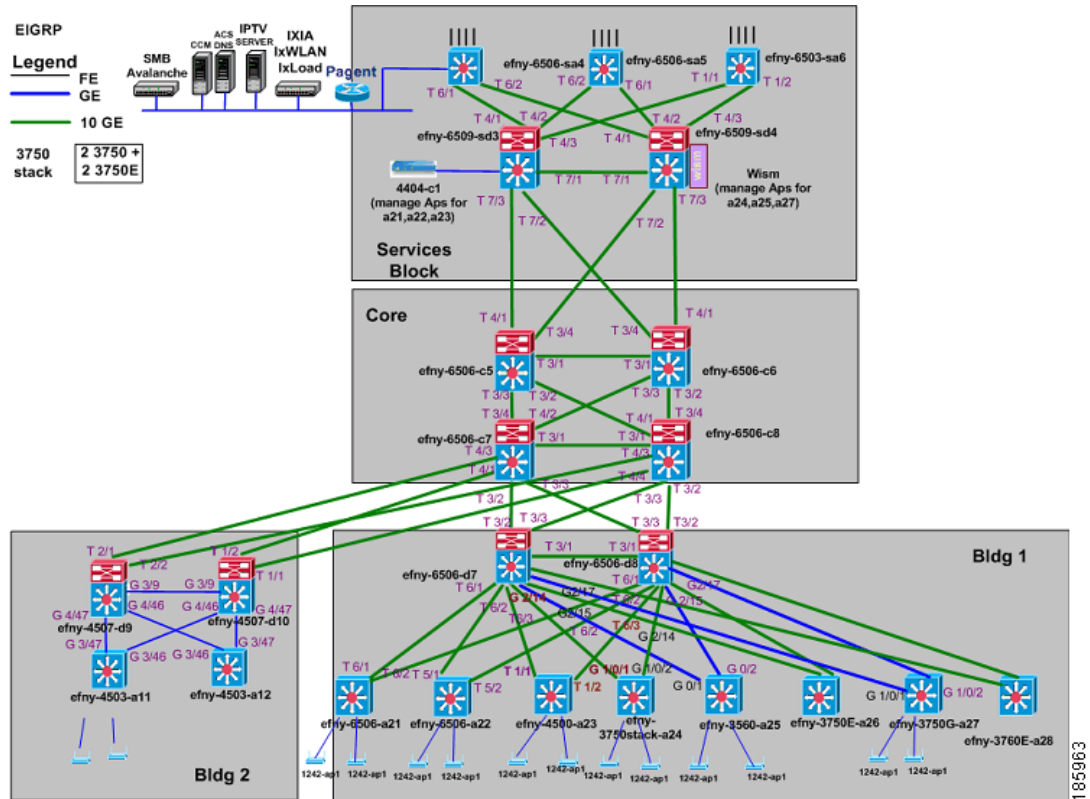
The second set is the "Extended Baseline configuration," which is the Baseline configuration with additional technologies such as Wireless and Multicast.

All tests, including convergence tests were executed using the Extended Baseline configuration.

### 3.4.3 Testbed Setup

The validation network consists of a three-layered Campus topology with access, distribution and core devices. The setup has three distribution blocks, user access and server access switches along with a set of core routers. The Cisco Unified Call Manager is connected to a server side distribution router for provisioning voice in the network. The wireless controller is also connected to the distribution router in services block. Wireless access points are connected to access switches.

**Figure 3-21** High Availability Campus Routed Access design - Manual testbed



In addition, real world services such as the Cisco Call Manager, IP Phones, IPTV, Multicast, voice and Video were validated end-to-end.



### 3.4.3.1 Baseline Traffic

The following constitutes "Baseline traffic" that ran for every test that was executed:

- 3000 EIGRP routes (in Core)
- 5000 mroutes (in RP routers)
- 100 Stateful sessions per Access switch (TELNET + FTP + HTTP + DNS + POP3)
- 100 Mbps QoS traffic per Access switch (includes Voice, Multicast Video, Call Control, bulk data, critical data and best effort traffic) based on the [Enterprise QoS Solution Reference Network Design Guide](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a008049b062.pdf).

[http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration\\_09186a008049b062.pdf](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a008049b062.pdf)

## 3.4.4 Test Setup - Hardware and Software Device Information

**Table 3-5 Hardware and Software Device Information**

| Hardware Platform                     | Role         | DRAM                     | Software Version | Line Cards/Interfaces                                                                                                     |
|---------------------------------------|--------------|--------------------------|------------------|---------------------------------------------------------------------------------------------------------------------------|
| Catalyst 6500 Sup720-3BXL             | Core         | RP – 1GB<br>SP – 1GB     | 12.2(18)SXF8     | WS-X6704-10GE - DFC-3BXL<br>WS-X6748-GE-TX - DFC-3BXL                                                                     |
| Catalyst 6500 Sup720-3BXL             | Distribution | RP – 1GB<br>SP – 1GB     | 12.2(18)SXF8     | WS-X6704-10GE - DFC-3BXL<br>WS-X6708-10GE - DFC-3BXL<br>WS-X6724-SFP - DFC-3BXL<br>WS-X6748-SFP - DFC-3BXL<br>WS-SVC-WISM |
| Catalyst 6500 Sup720-3BXL             | Access       | RP – 1GB<br>SP – 1GB     | 12.2(18)SXF8     | WS-X6748-GE-TX - DFC-3BXL<br>WS-X6704-10GE - DFC-3BXL                                                                     |
| Catalyst 6500 Sup32-3B                | Access       | RP – 512MB<br>SP – 512MB | 12.2(18)SXF8     | WS-X6548V-GE-TX                                                                                                           |
| Catalyst 4500 Sup V-10GE              | Access       | 512 MB                   | 12.2(31)SGA      | WS-X4548-GB-RJ45                                                                                                          |
| Catalyst 3750 / 3750E and mixed stack | Access       | 256 MB                   | 12.2(37)SE       | WS-C3750-24P<br>WS-C3750E-24P                                                                                             |
| Catalyst 3750G                        | Access       | 128 MB                   | 12.2(37)SE       | WS-C3750G-24PS                                                                                                            |

**Table 3-5 Hardware and Software Device Information**

|                       |                       |        |            |                                  |
|-----------------------|-----------------------|--------|------------|----------------------------------|
| Catalyst 3560 / 3560E | Access                | 256 MB | 12.2(37)SE | WS-C3560G-24PS<br>WS-C3560E-24PD |
| AIR-(L)AP1242         | Access-point          |        | 4.0.206.0  |                                  |
| AIR-WLC4404-K9        | Wireless controller   |        | 4.0.206.0  |                                  |
| CCM                   | Cisco Call Manager    |        | 5.1        |                                  |
| ACS                   | Access control server |        | 4.1        |                                  |

## 3.4.5 Test Types

Validation tests are divided into the following categories:

- System Integration
- Negative/Redundancy
- Reliability

System integration and negative/redundancy tests were executed in manual as well as automated regression testing. Reliability tests were executed manually only.

### 3.4.5.1 System Integration Test

System Integration has two major components, feature combination and feature interaction.

Feature combination focuses on testing a feature when various combinations of other features are enabled.

Feature interaction tests were conducted to verify dependencies between features.

The following test suites were executed using extended baseline configuration:

- Routing - EIGRP and OSPF
- Multicast
- Voice
- Wireless

The System Integration Tests combines all the features required for multiple features inter-operability. End-to-end service validation was performed for IP, Multicast, voice and video traffic. The services validated include Multicast using IPTV viewer, IP Telephony using Cisco IP Phones and data connectivity and Wireless using IXWLAN.

Health checks were performed before and after tests. These checks included memory and CPU utilization, tracebacks, memory alignment errors, deviations in number of routes and mroutes, interface errors, line card status and syslog messages.

All test cases under the System Integration Test were automated and test cases were executed in parallel.

### 3.4.5.2 Redundancy Test

Negative testing concerns error handling and robustness. Erroneous inputs were applied at the system level to verify behavior against error handling specifications. Unspecified inputs or conditions and faults were injected to evaluate system level robustness.

All the negative test cases were grouped together for better test management. During iterations of the negative tests, traffic was fully loaded and CPU and memory usage of the devices in the testbed were monitored.

The negative tests were categorized under the following failure scenarios:

- **Redundancy / High Availability:** Redundant router/link failover. (Reload the primary router and shut/no shut the links) for measuring convergence times with voice, Multicast and Unicast traffic streams.
- **Hardware:** Interface shut/no shut and monitor CPU spikes and memory utilization.
- **Control-plane:** Clear routing tables, flap routes, MSDP SA filters, Accept-Register filters and PIM Neighbor filters.

All test cases under the Redundancy Test were automated and test cases were executed serially.

### 3.4.5.3 Reliability Test

150-hour reliability test was executed for the entire testbed to ensure that the various solutions interoperate without memory or CPU issues or any operationally impacting defects. The total number of routes and mroutes are verified on UUT devices. Devices were monitored for tracebacks, alignment and interface errors, and syslogs for any error messages. End-to-end connectivity was maintained during this test.

During this phase of reliability testing, System Integration Test Suites were executed in parallel.

## 3.4.6 Sustaining Coverage

Except for reliability test cases all other test cases were automated.

Sustaining test coverage included the following components:

- Automated test scripts for each automation test case
- Common library for managing the testbed, collecting and reporting test results
- Automated procedures to capture the manual execution results

All the real applications used in the manual validation phase, including IPTV server/client, Cisco Call Manager server and IP phones, were not automated. Instead, traffic tools were used to generate simulated voice and video traffic on the network.

## 3.5 CVD System Assurance - Feature Implementation Recommendations

These recommendations are based on:

- Cisco recommended Best Practices in various technologies.
- Years of field experience from Cisco engineers who work with complex networks and many of the largest customers.
- Issues encountered and successfully resolved during validation.

### 3.5.1 Routing

**EIGRP Stub:** Configure on all Access routers under `router eigrp`

```
Configuration: router eigrp 100
                eigrp stub connected
```

**Summarization:** Route summarization is done at the distribution routers on interfaces (uplink to core router) connecting the distribution routers to core.

```
Configuration: interface TenGigabitEthernet4/1
                ip summary-address eigrp 100 10.120.0.0 255.255.0.0 5
```



#### Note

Summarization of directly connected routes is done on the distribution switches. Hence a layer3 link between the two distribution routers is required to exchange specific routes between them. This layer 3 link prevents the distribution switches from black holing traffic if either distribution switches lose the connection to the access switch.

**Route filtering:** Traffic flows pass from access through the distribution to the core and should never pass through the access layer unless they are destined to locally attached devices. Apply a distribute-list to all the distribution downlinks to filter the routes received by the access switches.

```
Configuration: router eigrp 100
                distribute-list default out GigabitEthernet3/3
                !
                ip access-list standard default
                permit 0.0.0.0
```

**EIGRP Hello and Hold timer tuning:** Tuning the EIGRP Hello and Hold timers provides for faster routing convergence in the rare event that L1 and L2 remote fault detection fails to operate. Hello and Hold timers are reduced to 1 and 3 seconds respectively.

```
Configuration: interface TenGigabitEthernet4/3
                ...
                ip hello-interval eigrp 100 1
                ip hold-time eigrp 100 3
```



#### Note

Ensure that the timers are consistent on both ends of the link

**OSPF SPF and LSA Throttle tuning:** Tuning the OSPF SPF and LSA throttle timers provides for faster routing convergence. The SPF-start, SPF-hold and SPF-max-wait are reduced to 10ms, 100ms and 5 seconds respectively, the LSA-start, LSA-hold and LSA-max-wait are reduced to Hello and Hold timers are reduced to 10ms, 100ms and 5 seconds respectively.

```
Configuration: router ospf 1
               timers throttle spf 10 100 5000
               timers throttle lsa all 10 100 5000
               timers lsa arrival 80
```

**OSPF – Interface Hello and Dead timer tuning:** Tuning the OSPF Hello and Dead timers provides for faster routing convergence in the rare event that L1 and L2 remote fault detection fails to operate. Hello and Dead timers are reduced to 250ms and 1 second respectively.

```
Configuration: interface TenGigabitEthernet4/3
               ...
               ip ospf dead-interval minimal hello-multiplier 4
```

**Note**


---

Ensure that the timers are consistent on both ends of the link

---

**Designated Router:** Configure the Distribution switch to act as DR on each of the Access-Distribution uplinks.

**Configuration – Access switches:**

```
interface GigabitEthernet1/1
description Link to Distribution 1
ip ospf priority 255
```

**Configuration – Distribution switches**

```
interface GigabitEthernet3/11
description Link to Access Switch
ip ospf priority 0
```

**CEF load balancing:** To achieve best CEF load balancing, alternate L3 and L4 hashing on access, distribution and core routers.

Configuration: On access and core - mls ip cef load-sharing simple

On distribution - mls ip cef load-sharing full

## 3.5.2 Link Failure Detection

**Carrier-delay timer:** The default behavior for Catalyst switches is to use a default value of 0 msec on all Ethernet interfaces for the carrier-delay time to ensure fast link detection. It is still recommended as a best practice to hard code the carrier-delay value on critical interfaces with a value of 0 msec to ensure the desired behavior.

```
Configuration: interface GigabitEthernet1/1
               carrier-delay msec 0
```

**Note**

On Catalyst 6500, "LINEPROTO-UPDOWN" message appears when the interface state changes before the expiration of the carrier-delay timer configured via the "carrier delay" command on the interface. This is an expected behavior on Catalyst 6500 and is documented in CSCsh94221. For details, refer to [Appendix B](#).

**Link Debounce timer:** By default, GigE and 10GigE interfaces operate with a 10 msec debounce timer that provides for optimal link failure detection. The default debounce timer for 10 / 100 fiber and all copper link media is longer than that for GigE fiber, and is one reason for the recommendation of a high-speed fiber deployment for switch-to-switch links in a routed campus design. It is good practice to review the status of this configuration on all switch-to-switch links to ensure the desired operation via the command "show interfaces TenGigabitEthernet4/1 debounce"

## 3.5.3 Multicast

**PIM Sparse mode:** Configure PIM Sparse mode on all the interfaces.

Configuration: `ip pim sparse-mode`

**RP:** Configure routers in the core as Anycast RP.

**PIM query interval:** Configure PIM query-interval to 1 sec on interfaces to facilitate faster failover of Multicast streams.

Configuration: `ip pim query-interval 1`

**Send-RP announce interval:** For faster Anycast Auto-RP failover, configure send-rp announce interval to 5 sec.

Configuration: `ip pim send-rp-announce <interface> <RP announcement scope> interval 5`

**Limit Multicast states:** Configure mroute-limit and igmp-limit on all PIM routers.

Configuration: `ip multicast route-limit 11000`

`ip igmp limit 20`

## 3.5.4 Wireless

**Wireless controller:** Connect wireless controller to distribution routers in Services Block.

**Multicast over wireless:** Do not use WiSM module for multicast over wireless. Instead, use Cisco 4404 wireless controller.

**Note**

Due to DDTS CSCsj48453, Catalyst 6500 does not forward multicast traffic to WISM module when catalyst 6500 is configured in L3 mode. During validation this DDTS was being worked on by Cisco developers and could not be tested. However, at the time of writing this document, this DDTS is resolved. This caveat is documented in section [3.1.4.4.4 WISM, page 3-36](#) as well as [Appendix B](#) of this document.

## 3.5.5 Voice over IP

High Availability Campus Routed Access design provides a highly available, fault-tolerant infrastructure which is essential for easier migration to IP telephony, integration with applications such as video streaming and video conferencing in enterprise networks, and expansion of your IP telephony deployment across the WAN or to multiple CUCM clusters.

*This page is intentionally left blank*





## CHAPTER 4

# Test Cases Description and Test Results

---

## 4.1 Convergence Tests with Extended Baseline Configuration

The Routed Access design provides the fastest convergence for voice and data traffic. The expected convergence time for voice traffic with this design (codec G711a) is within 200 msec.

The purpose of this test is to measure convergence times for voice, unicast and multicast traffic during various redundant links and node failures. Expected convergence times are in the sub-second range. In this test suite, convergence is measured from the data source to the receiver (end-to-end network convergence). During convergence, packet loss is determined for each individual flow. For example, a packet rate of 1000 pps corresponds to 1 millisecond (ms) convergence time for each packet dropped.

### Traffic flow

Voice and Unicast – Bidirectional (5 upstream and 5 downstream) traffic flows are provisioned between each Access switch and the switch in the Service block.

Multicast flows are unidirectional and each Access switch receives 8 multicast groups from the source in services block. These multicast groups run in PIM sparse-mode.

### Traffic rate

Voice: Codec type: G711A (50 pps per flow - 1 packet every 20 (msec))

Packet size = 218 bytes

Call Duration - 90 secs for each flow

20 flows (10 upstream and 10 downstream) for each Access switch

Multicast: Eight multicast groups per each Access switch

Packet size = 180 bytes

15pps per flow

Unicast: Packet size = 128 bytes

Upstream flow = 82pps per flow

Downstream flow = 23 pps per flow

## 4.1 Convergence Tests with Extended Baseline Configuration

Redundant links and nodes were failed to simulate network failures.

Each superscript number below corresponds to section [4.1.1 Link and Node Failure Analysis, page 4-4](#).

**Table 4-1 Results of Various Redundant Link Failures**

| Failure Type | Description              |             | Traffic Type | EIGRP               |                   |                   |          | OSPF                |                   |                   |          |
|--------------|--------------------------|-------------|--------------|---------------------|-------------------|-------------------|----------|---------------------|-------------------|-------------------|----------|
|              |                          |             |              | Downstream Recovery |                   | Upstream Recovery |          | Downstream Recovery |                   | Upstream Recovery |          |
|              |                          |             |              | High msec           | Low msec          | High msec         | Low msec | High msec           | Low msec          | High msec         | Low msec |
| Link Failure | Services Block-to-Core   |             | Voice        | 60                  | 20                | 160               | 120      | 140                 | 100               | 100               | 80       |
|              | Core-to-Core             |             | Voice        | 100                 | 60                | 120               | 80       | 120                 | 80                | 60                | 40       |
|              | Core-to-Distribution     |             | Voice        | 160                 | 140               | 100               | 80       | 120                 | 80                | 60                | 40       |
|              | Access -to- Distribution | Access 6506 | Voice        | 160                 | 140               | 20                | 0        | 100                 | 80                | 40                | 20       |
|              |                          | Access 4500 | Voice        | 840 <sup>1</sup>    | 820 <sup>1</sup>  | 20                | 0        | 120                 | 120               | 20                | 0        |
|              |                          | Access 3750 | Voice        | 180                 | 100               | 20                | 0        | 100                 | 100               | 20                | 0        |
|              |                          | Access 3560 | Voice        | 160                 | 80                | 20                | 0        | 80                  | 60                | 20                | 0        |
|              | Services Block-to-Core   |             | UCast        | 43                  | 43                | 158               | 146      | 59                  | 51                | 79                | 67       |
|              | Core-to-Core             |             | UCast        | 43                  | 36                | 97                | 85       | 59                  | 42                | 79                | 60       |
|              | Core-to-Distribution     |             | UCast        | 60                  | 43                | 85                | 73       | 76                  | 59                | 109               | 103      |
|              | Access -to- Distribution | Access 6506 | UCast        | 130                 | 130               | 24                | 12       | 102                 | 68                | 36                | 18       |
|              |                          | Access 4500 | UCast        | 869 <sup>1</sup>    | 869 <sup>1</sup>  | 12                | 0        | 136                 | 136               | 18                | 6        |
|              |                          | Access 3750 | UCast        | 86                  | 86                | 12                | 0        | 179                 | 85                | 24                | 6        |
|              |                          | Access 3560 | UCast        | 173                 | 173               | 12                | 0        | 162                 | 162               | 12                | 6        |
|              | Services Block-to-Core   |             | MCast        | 600 <sup>5</sup>    | 533 <sup>5</sup>  | NA                | NA       | 600                 | 533               | NA                | NA       |
|              | Core-to-Core             |             | MCast        | 600 <sup>5</sup>    | 600 <sup>5</sup>  | NA                | NA       | 533                 | 533               | NA                | NA       |
|              | Core-to-Distribution     |             | MCast        | 600 <sup>5</sup>    | 600 <sup>5</sup>  | NA                | NA       | 600                 | 600               | NA                | NA       |
|              | Access -to- Distribution | Access 6506 | MCast        | 600 <sup>5</sup>    | 533 <sup>5</sup>  | NA                | NA       | 666                 | 533               | NA                | NA       |
|              |                          | Access 4500 | MCast        | 600 <sup>5</sup>    | 600 <sup>5</sup>  | NA                | NA       | 600                 | 600               | NA                | NA       |
|              |                          | Access 3750 | MCast        | 1000 <sup>2</sup>   | 1000 <sup>2</sup> | NA                | NA       | 866 <sup>2</sup>    | 866 <sup>2</sup>  | NA                | NA       |
|              |                          | Access 3560 | MCast        | 1000 <sup>2</sup>   | 1000 <sup>2</sup> | NA                | NA       | 1333 <sup>2</sup>   | 1266 <sup>2</sup> | NA                | NA       |

Table 4-2 Results of Various Redundant Node Failures

| Failure Type | Description    |             | Traffic Type | EIGRP               |                   |                   |                | OSPF                |                |                   |                |
|--------------|----------------|-------------|--------------|---------------------|-------------------|-------------------|----------------|---------------------|----------------|-------------------|----------------|
|              |                |             |              | Downstream Recovery |                   | Upstream Recovery |                | Downstream Recovery |                | Upstream Recovery |                |
|              |                |             |              | High msec           | Low msec          | High msec         | Low msec       | High msec           | Low msec       | High msec         | Low msec       |
| Node Reload  | Services Block |             | Voice        | 120                 | 80                | 140               | 80             | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0 <sup>4</sup> |
|              | Core           |             | Voice        | 140                 | 100               | 100               | 60             | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0 <sup>4</sup> |
|              | Distribution   | Access 6506 | Voice        | 160                 | 140               | 240 <sup>3</sup>  | 0 <sup>4</sup> | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0              |
|              |                | Access 4500 | Voice        | 160                 | 120               | 220 <sup>1</sup>  | 0 <sup>4</sup> | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0              |
|              |                | Access 3750 | Voice        | 160                 | 120               | 40                | 0 <sup>4</sup> | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0              |
|              |                | Access 3560 | Voice        | 160                 | 100               | 40                | 0 <sup>4</sup> | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0              |
|              | Services Block |             | UCast        | 42                  | 34                | 164               | 91             | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0 <sup>4</sup> |
|              | Core           |             | UCast        | 128                 | 59                | 109               | 79             | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0 <sup>4</sup> |
|              | Distribution   | Access 6506 | UCast        | 188                 | 85                | 256 <sup>3</sup>  | 0 <sup>4</sup> | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0              |
|              |                | Access 4500 | UCast        | 188                 | 85                | 524 <sup>3</sup>  | 0 <sup>4</sup> | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0              |
|              |                | Access 3750 | UCast        | 179                 | 85                | 42                | 0 <sup>4</sup> | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0              |
|              |                | Access 3560 | UCast        | 179                 | 85                | 54                | 0 <sup>4</sup> | 0 <sup>4</sup>      | 0 <sup>4</sup> | 0 <sup>4</sup>    | 0              |
|              | Services Block |             | MCast        | 631 <sup>5</sup>    | 631 <sup>5</sup>  | NA                | NA             | 13                  | 13             | NA                | NA             |
|              | Core           |             | MCast        | 565 <sup>5</sup>    | 565 <sup>5</sup>  | NA                | NA             | 39                  | 39             | NA                | NA             |
|              | Distribution   | Access 6506 | MCast        | 736 <sup>5</sup>    | 578 <sup>5</sup>  | NA                | NA             | 52                  | 26             | NA                | NA             |
|              |                | Access 4500 | MCast        | 1065 <sup>1</sup>   | 1065 <sup>1</sup> | NA                | NA             | 52                  | 39             | NA                | NA             |
|              |                | Access 3750 | MCast        | 631 <sup>5</sup>    | 631 <sup>5</sup>  | NA                | NA             | 52                  | 52             | NA                | NA             |
|              |                | Access 3560 | MCast        | 592 <sup>5</sup>    | 592 <sup>5</sup>  | NA                | NA             | 39                  | 39             | NA                | NA             |

## 4.1.1 Link and Node Failure Analysis

### 1. Convergence times greater than 200msec

Catalyst 4500 series switches with 10GigE fiber interfaces may take longer than 200msec to converge during failure. The problem is due to the delay in bringing down the link. This is being tracked in DDTS CSCsm35240.

### 2. Multicast convergence times greater than 800msec

Catalysts 3500 and 3700 series switches may take longer than 800msec to converge multicast traffic during failure. This issue is due to the delay in triggering RPF and is being tracked in CSCsm33116.

### 3. Debounce timer on 10GigE fiber interfaces

Supervisor engine 32 modules with 1GigE and 10GigE fiber interfaces have a default debounce timer of 300msec. Also, the default debounce timer for 10GigE interfaces on WS-X6708-10GE, 8 port 10GigE modules is 300msec. The aforementioned times lead to higher convergence times during failovers. CSCsm08419 addresses this issue.

### 4. Zero packet loss during Core and Distribution router failures

Zero packet loss is observed when the graceful shutdown feature is implemented in OSPF. This feature is enabled by default.

When a Cisco router running OSPF is shutdown via the reload command, it sends out an OSPF max-metric LSA to all routers multicast address. Upon receiving this max-metric LSA, OSPF neighbor routers remove this peer without waiting for the dead timer to expire thereby avoiding black holing transit traffic. This speeds up routing convergence and improves network stability.

The graceful shutdown feature for EIGRP is available in 12.2(18)SXF11. Since the 12.2(18)SXF8 IOS software version was validated in the context of the Routed Access design, packet loss is seen with Core and Distribution router failures running EIGRP.



#### Note

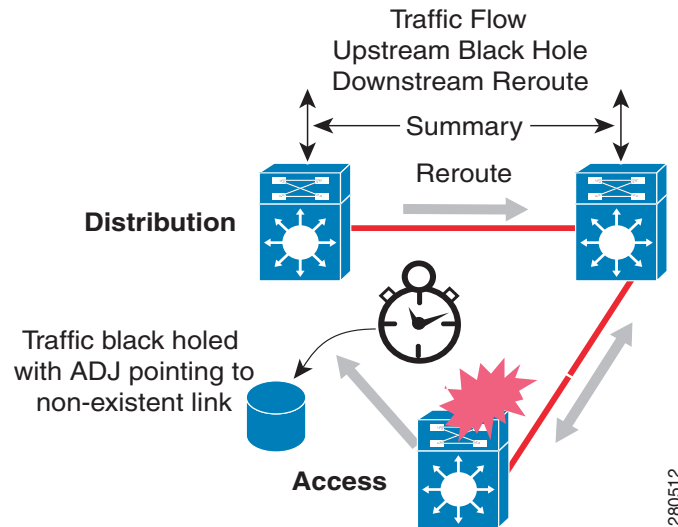
This feature is different from NSF because the router actively discourages its neighbors from sending traffic to itself.

### 5. Multicast convergence times

Multicast convergence times are expected to be < 800msec (not within 200msec as expected for voice traffic). This is due to 500msec default RPF backoff delay plus the PIM related processing time.

#### Variable convergence numbers

The network availability in Core and Distribution blocks is primarily controlled by fully meshed redundant nodes. However, the wiring closet or the Access switch uplink redundancy design uses the ports on the supervisor or the line card for connection to Distribution layer devices.

**Figure 4-1 Traffic Flow Upstream Black Hole and Downstream Reroute**

In this design, downstream traffic re-route (convergence) cannot be avoided at the Distribution routers during an Access to Distribution link failure. Without summarization at the Distribution layer, downstream convergence can be further affected by route convergence beyond the Distribution layer resulting in a longer convergence time.

For the upstream traffic, the Access switch has two equal cost routes to the two Distribution routers. When an Access to Distribution router link failure occurs, the Access switch updates the next-hop entries in hardware, thereby reducing black holing of the traffic. This operation takes place in the hardware and therefore is much faster than re-routing traffic at the Distribution router.

## 4.2 Impact of Redundant Link Failures on Video Quality

The following series of tests were performed with OSPF as the IGP to evaluate the impact of redundant link failures on video quality in the Campus Routed Access environment.

Test tools were used to emulate video source, video client and to simulate video traffic with the objective of measuring and evaluating video quality during convergence.

The test tool interface connected to the Access switch located in the Services block was the source of video traffic. The test tool interface connected to the Access switch in Bldg 1 block served as the client.

### Server traffic

Protocol: IPTV/Video  
 Mode: Video Server  
 Channel type: VOD – Listen Port: 554  
 Range type: IP only - IPv4  
 Server - # of hosts: 1  
 Type of Service: TOS/DSCP disabled

## Client traffic

Protocol: IPTV/Video  
Mode: Video client  
Client emulation: Real player  
Client - # of hosts: 100  
Range type: IP only - IPv4  
IGMP version: IGMPv3  
Transport protocol: RTP / UDP  
Type of Service: TOS/DCSP disabled

## Stream setting

Payload: Real payload  
Stream type: MPEG2 transport stream  
Stream count: 1  
Bit Rate: 1.915412 Mbps  
Channel Type: VoD  
Duration: 120 secs  
Transport: RTP/UDP

## TCP/IP parameters

Transmit Buffer size: 4096 bytes  
Receive Buffer size: 4096 bytes  
FIN timeouts: 60 sec  
Keepalive time: 75 sec  
Keepalive probes: 9  
Keepalive interval: 7200 sec  
SYN retries: 5  
SYN/ACK retries: 5  
Retransmit retries: 15  
Impairment: Disabled.

## Quality Metrics

Update interval: 2000 ms  
Jitter Buffer Emulator (JBE) Mode: Fixed  
Nominal Delay: 20 ms  
Min and Max Delay: 20/80 ms

I, P and B frames were enabled for collection of frame statistics

**Table 4-3 Results of Various Link Failures**

| Scenarios                                                  | MDI-DF | MOS_V | MDI-MLR | RTP Packet Loss | MPEG2 Packet Loss | Video Service Quality |
|------------------------------------------------------------|--------|-------|---------|-----------------|-------------------|-----------------------|
| Steady state                                               | 5.511  | 4.297 | 0       | 0               | 0                 | 100                   |
| SA4 – Access to Distribution_link failure (Server)         | 5.513  | 4.297 | 0       | 1-3             | 7-21              | 100                   |
| A21 - Distribution to Access link failure (Client)         | 5.524  | 4.276 | 0       | 12-24           | 84-168            | 100                   |
| D3-D4 - Distribution to Access (SA4 - Server) link failure | 5.513  | 4.297 | 0       | 1-3             | 7-21              | 100                   |
| D7-D8 - Distribution to Access (A21 - Client) link failure | 5.513  | 4.297 | 0       | 6-11            | 42-77             | 100                   |
| C7-C8 - Core to Distribution (Client end) Link failure     | 5.513  | 4.297 | 0       | 1-3             | 7-21              | 100                   |
| D3-D4 - Distribution to Core (server end) link failure     | 5.513  | 4.297 | 0       | 1-3             | 7-21              | 100                   |
| Core-to-Core Link failure                                  | 5.521  | 4.297 | 0       | 2-6             | 14-42             | 100                   |

## 4.2.1 Analysis of Various Link Failures

In summary, MDI-DF, MDI-MLR and MOS\_V values are on par with the values noticed with network in steady state.

MOS\_V (Mean Opinion Score \_Video) value of 4.297 was observed when the network was in steady state and was consistent for all the various link failures.

MDI\_DF (Media Delivery Index – Delay Factor) values in msec observed did not vary

MDI\_ML (Media Delivery Index – Media Loss) values indicate no loss

During each of the link failures, RTP packets lost were consistent ranging from 1 to 3 while the MPEG2 packets lost were 7 to 21 ( 1 RTP packet = 7 MPEG2 packets)

During the execution of the above tests, Video content and quality was visually observed. The human eye was unable to perceive any problems when the network was in a steady state and as it converged due to all the above mentioned link failures.

### 4.2.1.1 Metric Definitions

MDI – (Media Delivery Index )defines a measurement that can be used as a diagnostic tool as a quality indicator for monitoring a network intended to transport streaming media such as MPEG video.

MLR – (Media Loss Rate) is the number of lost or out-of-order media packets counted over a selected time interval. For a given MDI, if the Delay Factor (DF) is high and/or the DF Max-Min captured over a significant measurement period is high, then Jitter has been detected. Due to transient network failures, packets may be lost within the network which is indicated by the MLR component.

Video statistics provide two main measures of the quality of a video stream:

- **Video Service Quality** - A factor in the range from 0 to 120, provides an assessment of the capability of the RTP channel to support video transmission. The Video Service Quality factor starts with a base value that varies according to the codec and stream bit rate. The Video Service Quality base value establishes a theoretical maximum score for a stream under perfect network conditions. The amount of degradation imposed by the network (jitter and packet loss) is assessed and applied to adjust the Video Service Quality factor.
- **MOS\_V** - (Mean Opinion Score) for Video, a score in the range from 0 to 5, provides a codec-dependent objective quality score which is based on the Video Service Quality factor

## 4.3 Impact of Redundant Link Failures on Voice Quality during Convergence

The following series of tests were performed with OSPF as the IGP to evaluate the impact of link failures on voice quality in the Campus Routed Access environment.

All IP phones were connected to Access switches. Test tools connected to two Access switches were used to emulate 50 originating and 50 terminating end points with the objective of evaluating voice quality during link failures.

Each Access switch was dual attached via layer 3 links to two Distribution routers for high availability. Due to the per-flow load balancing algorithm, voice calls were distributed across these two paths based on the source-destination IP addresses. Because of this, only a select number of voice calls were impacted during link failure between Access and Distribution routers.

50 channels were programmed to initiate SIP phone calls and another 50 channels were configured as receivers. A real wave file was used as streaming media. The G711 codec was used. All 50 phone calls were initiated simultaneously and the call length was configured for three minutes. After all phone calls were successfully established and stable, one of the redundant links connecting Access to Distribution was shutdown to simulate network failures.

The test tool does not have the capability of displaying all channel results individually at the same time. The PSQM window shows one channel PSQM distribution during the test. An average of all the channels involved is displayed in the Summery Variance window.

The test tool also does not have the capability to display all channel RTP packet loss over time results individually. Five channels out of the total 100 channels are selected to display the RTP packet loss versus time during convergence. An average of all the channels involved is displayed in the Summery Variance window.

In each sample period, Jitter, RTP Jitter and the Delay number for all channels were collected. Their distribution, Jitter/Delay value are plotted against their total number of occurrences. This gives a global view of the distribution of variance.



## 4.3.1 PSQM - Perceptual Speech Quality Measure

The PSQM value is a measure of signal quality degradation and ranges from 0 (no degradation) to 6.5 (highest degradation).

Figure 4-2 shows the PSQM statistics for a single SIP phone. Channel 21 is used as an example. The X axis shows the PSQM value and Y axis shows the number of samples. During the 3 minute test interval, channel 21 was sampled eight times. PSQM value of 0.1 was observed during convergence. Before and after the network converged, PSQM value was a perfect zero.

**Figure 4-2 Traffic Flow Upstream Black Hole and Downstream Reroute**

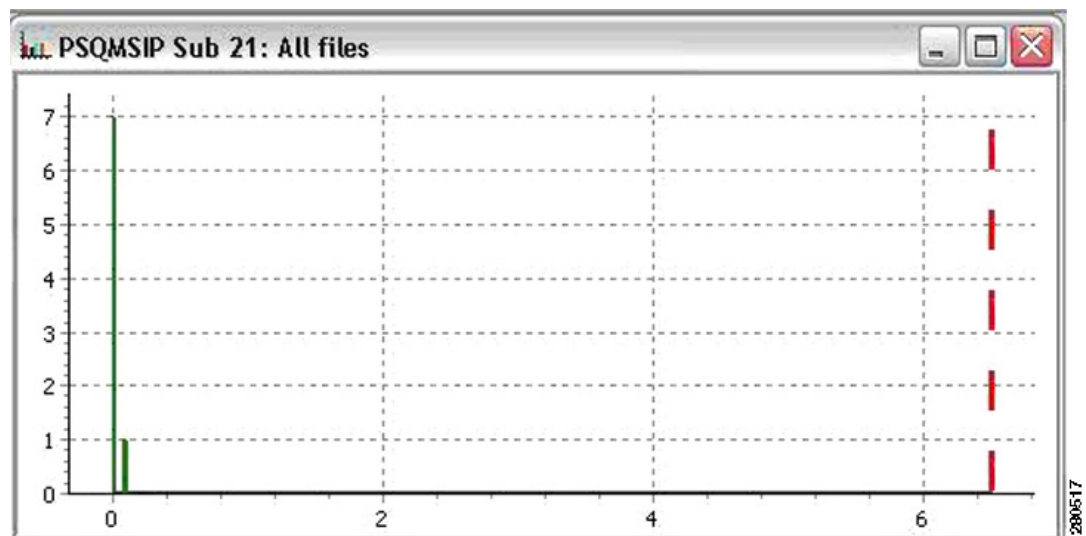
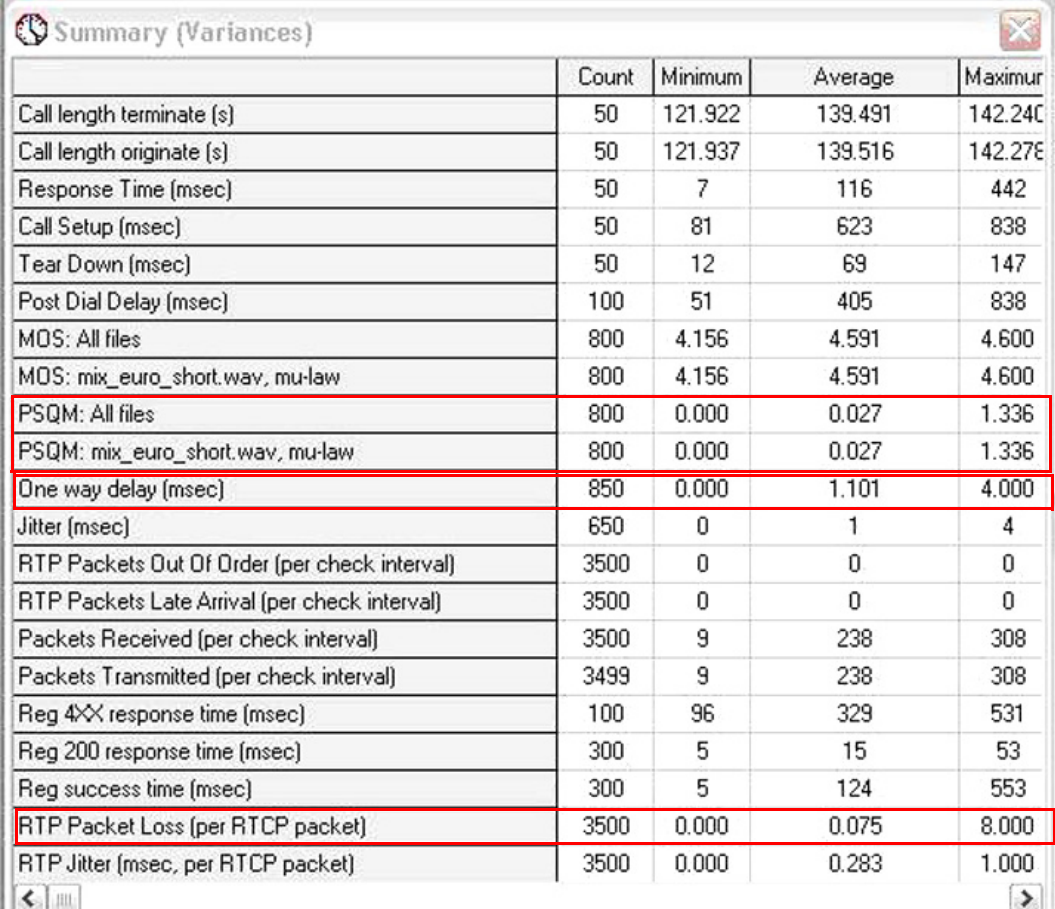


Figure 4-3 tallies the PSQM result for all 100 channels. Out of 800 samples taken during the 3 minutes, 700 plus scores a perfect 0. Even the worst sample result is less than 1.5, which is still good quality.

PSQM values for all 100 channels are shown in Figure 4-3. Out of 800 PSQM samples during 3 minutes of testing, the maximum (worse number, gathered during convergence) is 1.336, while the average of all samples is 0.027.

Figure 4-3 shows RTP packets lost during convergence and the recorded PSQM value of **1.336** which is well within the range of good speech clarity and voice quality.

Figure 4-3 Summary (Variance)



|                                               | Count | Minimum | Average | Maximum |
|-----------------------------------------------|-------|---------|---------|---------|
| Call length terminate (s)                     | 50    | 121.922 | 139.491 | 142.240 |
| Call length originate (s)                     | 50    | 121.937 | 139.516 | 142.276 |
| Response Time (msec)                          | 50    | 7       | 116     | 442     |
| Call Setup (msec)                             | 50    | 81      | 623     | 838     |
| Tear Down (msec)                              | 50    | 12      | 69      | 147     |
| Post Dial Delay (msec)                        | 100   | 51      | 405     | 838     |
| MOS: All files                                | 800   | 4.156   | 4.591   | 4.600   |
| MOS: mix_euro_short.wav, mu-law               | 800   | 4.156   | 4.591   | 4.600   |
| PSQM: All files                               | 800   | 0.000   | 0.027   | 1.336   |
| PSQM: mix_euro_short.wav, mu-law              | 800   | 0.000   | 0.027   | 1.336   |
| One way delay (msec)                          | 850   | 0.000   | 1.101   | 4.000   |
| Jitter (msec)                                 | 650   | 0       | 1       | 4       |
| RTP Packets Out Of Order (per check interval) | 3500  | 0       | 0       | 0       |
| RTP Packets Late Arrival (per check interval) | 3500  | 0       | 0       | 0       |
| Packets Received (per check interval)         | 3500  | 9       | 238     | 308     |
| Packets Transmitted (per check interval)      | 3499  | 9       | 238     | 308     |
| Reg 4XX response time (msec)                  | 100   | 96      | 329     | 531     |
| Reg 200 response time (msec)                  | 300   | 5       | 15      | 53      |
| Reg success time (msec)                       | 300   | 5       | 124     | 553     |
| RTP Packet Loss (per RTCP packet)             | 3500  | 0.000   | 0.075   | 8.000   |
| RTP Jitter (msec, per RTCP packet)            | 3500  | 0.000   | 0.283   | 1.000   |

## 4.3.2 Jitter

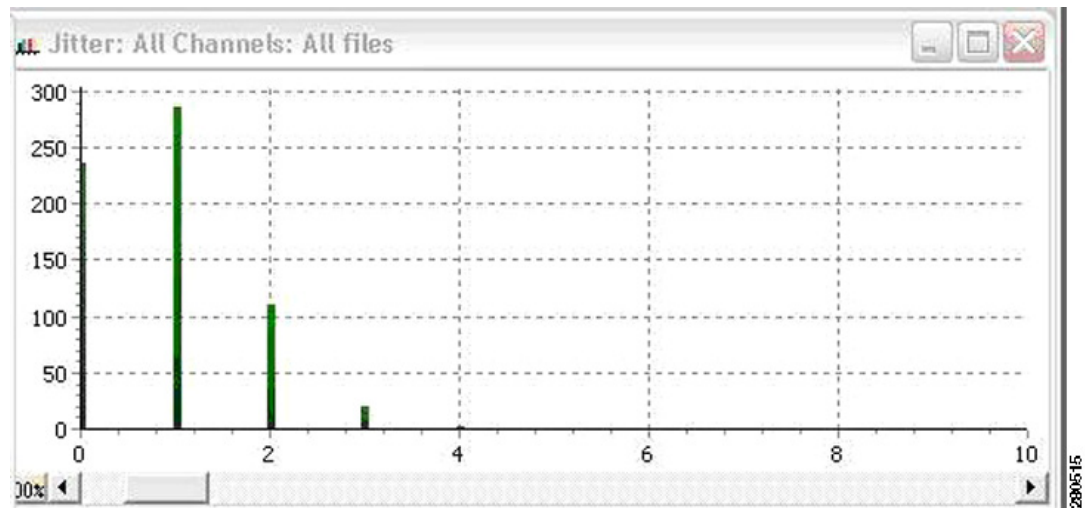
Figure 4-4 shows the Jitter statistics for all the SIP streams. X axis is the Jitter value in msec. and Y axis shows the number of samples.

During the 3 minutes test time, 50 voice traffic streams were sampled 650 times. Jitter is contained within 4ms. While 240 samples show no jitter at all, 280 samples show a 1ms jitter, 110 samples show 2ms jitter, less than 20 samples show 3 ms and less than 10 show 4ms jitter.



### Note

The test tool's resolution for **Jitter** is **1ms**.

**Figure 4-4 Jitter Statistics**

## 4.3.3 Delay

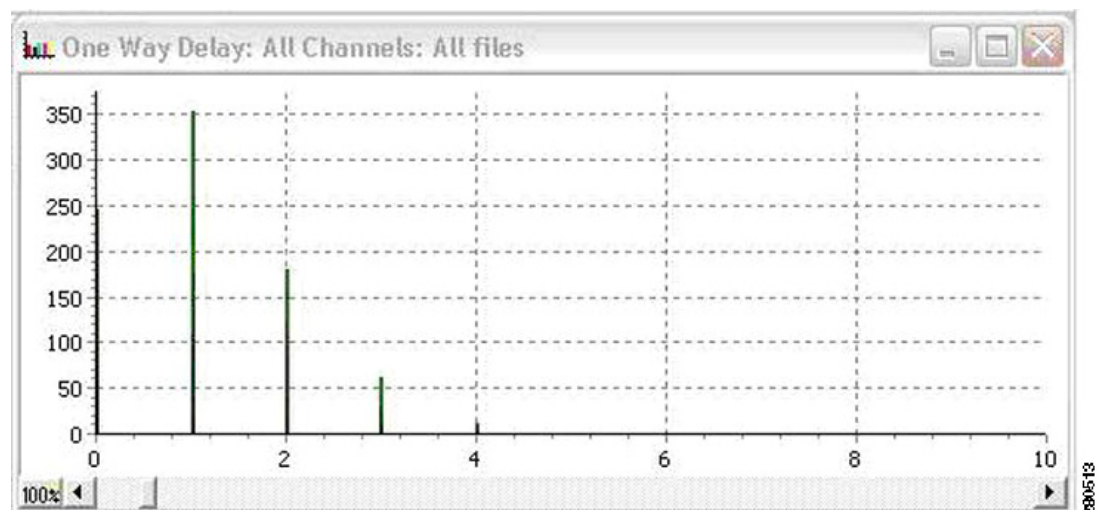
Figure 4-5 shows the Delay statistics for all SIP streams. X axis is the Delay value in msec. and Y axis is the number of samples taken.

During the 3 minutes test time, 50 voice traffic streams were sampled 850 times. Delay is contained within 4ms. While 250 samples show no delay at all, 350 samples show a 1ms delay, 180 samples show 2ms delay, less than 60 samples show 3ms and less than 10 show 4ms delay.



### Note

The test tool's resolution for **Delay** is **1ms**.

**Figure 4-5 Delay Statistics**

## 4.3.4 RTP Packet Loss / Convergence Time

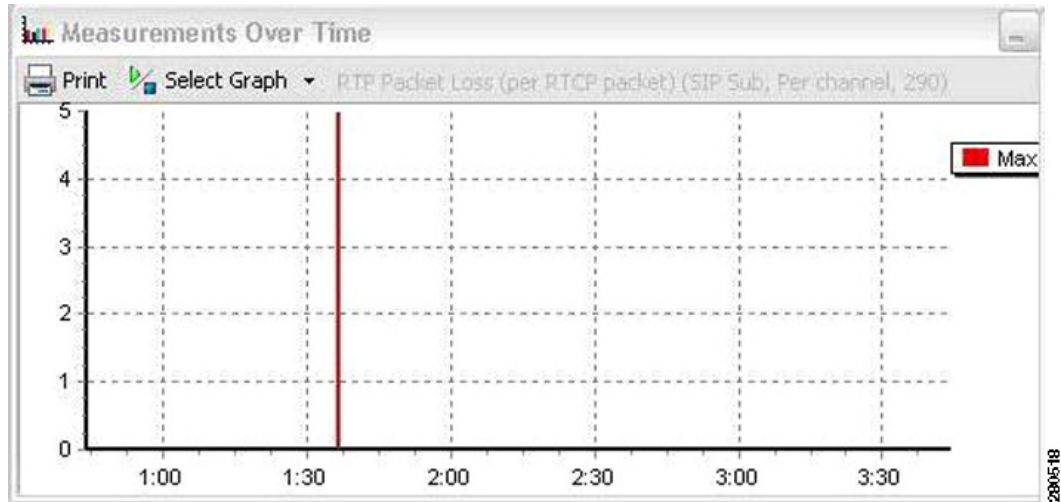
Maximum RTP packet loss for any channel is 8 as shown in [Figure 4-3](#), which translates to  $20\text{ms} * 8 = 160\text{ms}$ .

This is in line with the network convergence time for Routed Access design guide and proves the quality of voice is acceptable during failure.

### 4.3.4.1 RTP Packet Loss

Since the test tool collect RTP packet loss in 5 seconds intervals, the Packet Loss Versus Time plot only shows 1 occurrence of RTP packet loss for the 5 seconds time period when the convergence occurs. This graph proves that the voice traffic was only disrupted once during the link down, and no further network instability occurred later

**Figure 4-6 RTP packet loss in 5 seconds**



## 4.4 Impact of Congestion on Voice Traffic with QoS Enabled

The purpose of these tests is to validate the impact of congestion on voice traffic with QoS enabled. The goal was to confirm if voice traffic is dropped in the event of link congestion. Evaluation was done with EIGRP and OSPF routing protocols.

Test setup:

- Manual call setup and RTP signaling verification with and without congestion using Cisco IP phone 7970 series
- End-to-end traffic from A21 Access switch to SA4 in Services block.
- Use test tool to verify the following with and without congestion:
  1. Delay
  2. Jitter
  3. RTP packet loss
  4. PSQM

The link between Access and Distribution router was congested with test traffic to ensure voice traffic was given priority. Voice traffic was started and the results were recorded.

QoS was enabled and wherever applicable. Interfaces were configured to trust DCSP (mls qos trust dscp). In order to verify that voice packets are properly marked, the QoS policy was applied on the egress interface which was congested.

In summary, voice packets were given precedence over the default traffic and no voice packet drops were encountered.

## 4.4 Impact of Congestion on Voice Traffic with QoS Enabled

Figure 4-7 Results for EIGRP

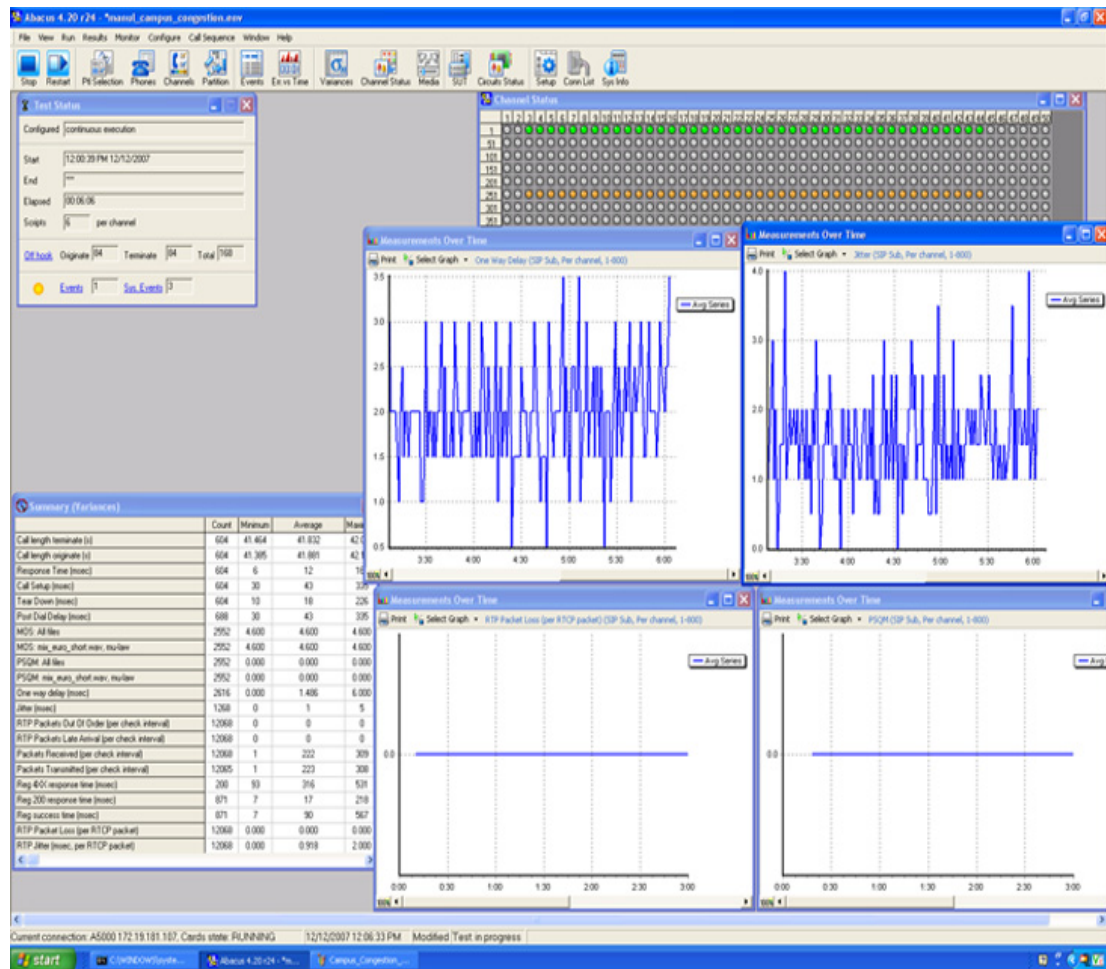
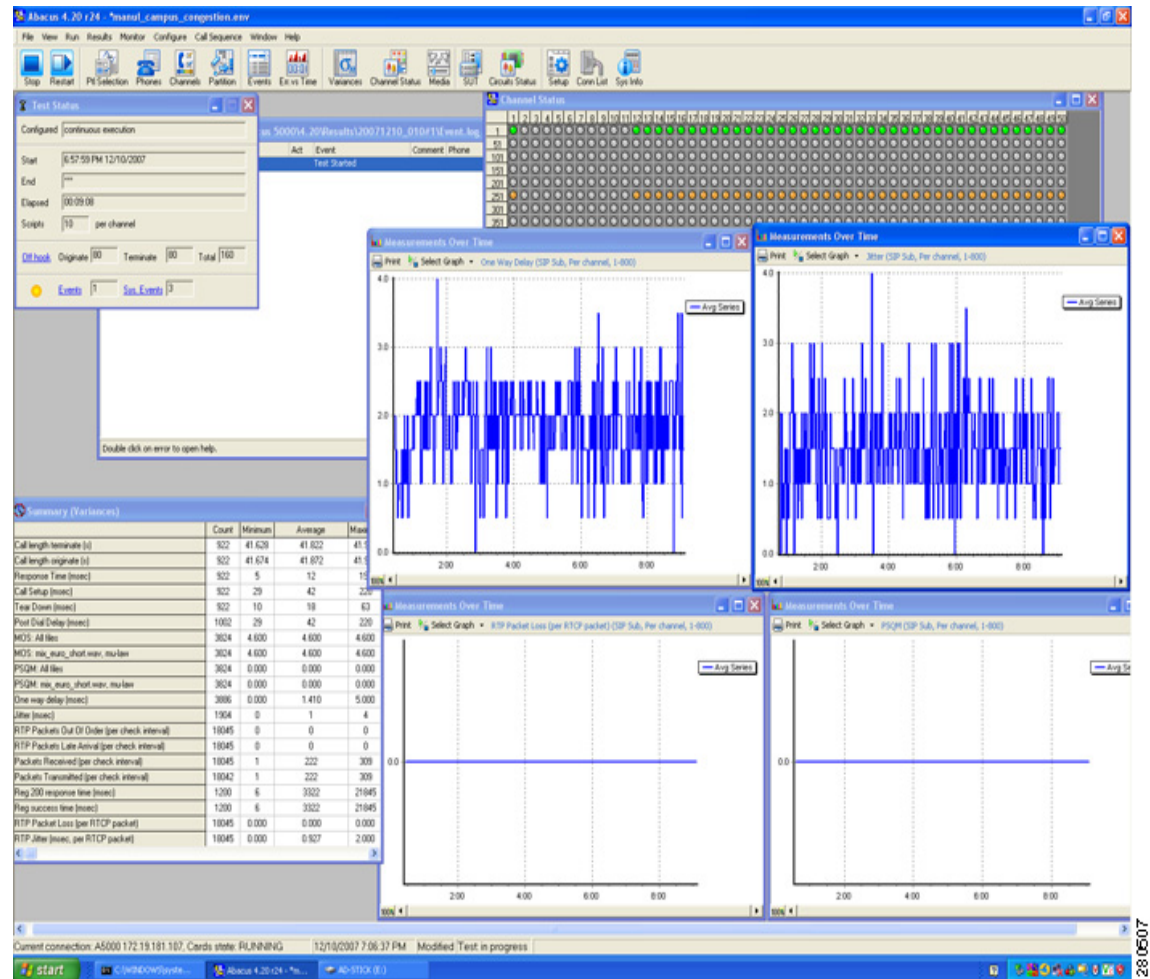


Figure 4-8 Results for OSPF





## 4.5 Routing - IPv4 – EIGRP and OSPF

**Table 4-4**      *Routing - IPv4 – EIGRP and OSPF*

| Test                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Manual Test Case | Defects | Automation Test Case | Defects    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------|----------------------|------------|
| <b>System Integration Test Suite:</b> This test suite is run in Campus Routed Access test network environment and all test cases within this test suite will run in parallel. Device configurations used for this test case will have feature combination and feature interaction with configurations from other test suites like Voice and Multicast test suites. This test suite will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic, and voice traffic. |                  |         |                      |            |
| <b>EIGRP Neighbors Authentication</b><br>This test case will setup and verify the EIGRP neighbor relationship is established between each router across the whole Campus, using EIGRP MD5 authentication method. Specifically, in Routed Access Campus Design, configure the routers in Access layer as layer 3 devices using EIGRP protocol. Verify that each Access router has established the EIGRP neighbor relationship with routers in Distribution layer.                                                                    | Passed           | —       | Passed               | —          |
| <b>EIGRP Stub</b><br>This test case will set up and verify EIGRP stub routing on the Access routers. In Routed Access Campus design, configuring the EIGRP stub feature on the layer 3 Access routers prevents the Distribution routers from sending downstream queries, which helps the convergence time.                                                                                                                                                                                                                          | Passed           | —       | Failed               | CSCek78468 |
| <b>EIGRP Timers Tuning</b><br>This test case will set up and verify the EIGRP hello, and dead timers are reduced to 1 and 3 seconds, in routed Access design, reducing the EIGRP hello and hold timer from defaults of 5 and 15 second provides for a faster routing convergence in the rare event that L1/2 remote fault detection fails to operate.                                                                                                                                                                               | Passed           | —       | Passed               | —          |
| <b>EIGRP Summarization</b><br>This test case will set up and verify the EIGRP route summarization on the interfaces of Distribution routers to the Core routers. Specifically in Routed Access Campus Design, configure the route summarization on Distribution routers helps to reduce the convergence time by bounding those queries to a single hop in all direction.                                                                                                                                                            | Passed           | —       | Passed               | —          |



|                                                                                                                                                                                                                                                                                                                                                                                                                                                             |        |   |        |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|
| <b>EIGRP Route Filters</b><br>This test case will set up and verify the EIGRP route filtering is applied on the Distribution routers to ensure that the Access router is only using the default routes (gateway) to the remote network as well as reduced routing table.                                                                                                                                                                                    | Passed |   | Passed | — |
| <b>OSPF Neighbors Authentication</b><br>This test case will setup and verify the OSPF neighbor relationship is established between each router across the whole campus, using OSPF MD5 authentication method. Specifically, in Routed Access Campus Design, configure the routers in access layer as layer 3 devices using OSPF protocol. Verify that each access router has established the OSPF neighbor relationship with routers in distribution layer. | Passed | — | Passed | — |
| <b>OSPF Totally Stub</b><br>This test case will set up and verify OSPF Totally Stub routing on the access routers. In Routed Access Campus design, configuring the OSPF Totally stub feature on the layer 3 access routers, to decrease the number of routes down to routing table and have default routes to distribution routers as well, which helps the convergence time.                                                                               | Passed | — | Passed | — |
| <b>OSPF Summarization</b><br>This test case will set up and verify the OSPF route summarization on the interfaces of distribution routers which is ABR to the core routers. Specifically in Routed Access Campus Design, configure the route summarization on distribution routers helps to reduce the convergence time.                                                                                                                                    | Passed | — | Passed | — |

|                                                                                                                                                                                                                                                                                                                    |        |   |        |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|
| <b>OSPF SPF and LSA Timers Tuning</b><br>This test case will set up and verify the by tuning OSPF SPF-start, SPF-hold and SPF-max-wait into 10ms, 100ms and 5 seconds respectively, the LSA-start, LSA-hold and LSA-max-wait into 10ms, 100ms and 5 seconds respectively, can reduce the network convergence time. | Passed | — | Passed | — |
| <b>OSPF Hello and HoldTimers Tuning</b><br>This test case will set up and verify that by tuning the OSPF Hello and Hold timers into to 10ms, 100ms and 5 seconds respectively, can provides for a faster routing convergence.                                                                                      | Passed | — | Passed | — |

## 4.6 Negative tests - EIGRP and OSPF

**Table 4-5**      *Negative tests - EIGRP and OSPF*

| Test                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Manual Test Case | Defects    | Automation Test Case | Defects |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|------------|----------------------|---------|
| <b>Negative Test Suite:</b><br>A negative test case will introduce certain conditions or failures to the network that will make other positive test cases fail in a system test environment; therefore, negative test cases are grouped together in a separate test suite for better test management.                                                                                                                                                                                                                                                                                                                                                                                                                      |                  |            |                      |         |
| <b>Interface Shut/Noshut</b><br>The purpose of this test is to verify the effects of the interface of the core router/switch when it goes down and comes back up and what level of disruption of network connectivity does occur on the device and the network. The expected result is that after the interface is brought back up, the routing table will resume. In addition to that, the system experiencing an interface that goes down and up scenario should still have normal CPU utilization and there should not be any memory leak, traceback, or CPU hog etc.<br>It is required that the core layer of the network provides the necessary scalability, load sharing, fast convergence, and high speed capacity. | Passed           | —          | Passed               | —       |
| <b>Clear IP Routes</b><br>The purpose of this test is to verify that router functionality is not interrupted and the ip routing table resumes after the routing table is reset by the clear ip route command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Failed           | CSCsk10711 | Passed               | —       |
| <b>EIGRP Flapping</b><br>The purpose of this test is to verify that when there are small portions of EIGRP routes that are unstable and flapping, the core switch should be able to handle this behavior without negative impact on the network. The system should be up and continue to handle routing and the redirection of traffic properly. CPU utilization should remain in the normal range and there should be no memory leak, tracebacks, or CPU hogs.                                                                                                                                                                                                                                                            | Passed           | —          | Passed               | —       |
| <b>PIM Neighbor Filters</b><br>The purpose of this test is to verify PIM Neighbor Filters operation. The "pim neighbor-filter" command is to limit and prevent the other neighbors to form PIM neighbors. This can help to achieve stub Multicast routing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Passed           | —          | Passed               | —       |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |        |   |        |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|
| <b>MSDP SA filters</b><br><p>The purpose of this test is to verify MSDP SA filters. With a default configuration, MSDP exchanges SA messages without filtering them for specific source or group addresses.</p> <p>To improve the scalability of MSDP in the native IP Multicast Internet, and to avoid global visibility of domain local (S,G) information, MSDP SA filters are used to reduce unnecessary creation, forwarding, and caching of some of these well-known domain local sources.</p>                                 | Passed |   | Passed | — |
| <b>Accept Register filters</b><br><p>Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.</p> <p>Accept register filter feature can be used on the RP to limit the sources that register for a particular Multicast group. This also only gives limited security since the source traffic may flow down the *,G or S,G tree of an active flow without registering at the RP.</p> | Passed | — | Passed | — |

## 4.7 Multicast Tests - EIGRP and OSPF

**Table 4-5, Part 1** Multicast tests - EIGRP and OSPF

| Test                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Manual Test Case | Defects | Automation Test Case | Defects |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------|----------------------|---------|
| <b>System Integration Test Suite: Multicast Tests</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                  |         |                      |         |
| <p>The purpose of this test is to provision and test Multicast in Routed Access setup. This test suite was run in Campus Routed Access test network environment setup and all testcases will be run in parallel with other test cases within this test suite. Device configurations used for this test case will have feature combination and feature interaction with configurations from other test suites, Routing, Wireless test suites. Test cases will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, Multicast traffic and voice traffic.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                  |         |                      |         |
| <b>PIM Sparse-Mode</b><br><br>PIM Sparse-mode is able to support full spectrum of Multicast applications either one-to-many or many-to-many. For running Multicast traffic with PIM Sparse mode, static RPs are defined on core routers. Separate RPs are defined for the publish groups (Source in Services Block) and the subscribe groups (Feedback traffic sourced in user distribution). The Shortest Path Tree (SPT) threshold value was set to infinity to ensure that Multicast traffic used only the shared tree.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Passed           | —       | Passed               | —       |
| <b>PIM bidir-mode</b><br><br>The purpose of this testcase is to provision PIM bidir in Routed Access test environment and verify that it inter-operation with PIM Sparse-mode. PIM bidir helps deploy emerging communication and financial applications that rely on many-to-many model.<br><br>This test will verify basic functionality of bidirectional PIM groups, mode flags, and the designated forwarder (DF) mode. Supervisor's Engine 720 (Sup720) supports hardware forwarding of IPv4 bidirectional PIM groups. To support IPv4 bidirectional PIM groups, the Sup720 implements a new mode called designated forwarder (DF) mode. The DF is the router elected to forward packets to and from a segment for an IPv4 bidirectional PIM group. In DF mode, the supervisor engine accepts packets from the RPF and from the DF interfaces. When the supervisor engine is forwarding IPv4 bidirectional PIM groups, the RPF interface is always included in the outgoing interface list of (*, G) entry, and the DF interfaces are included depending on IGMP/PIM joins. If the route to the RP becomes unavailable, the group is changed to dense mode. Should the RPF link to the RP become unavailable, the IPv4 bidirectional PIM flow is removed from the hardware forwarding information base (FIB). | Passed           | —       | Passed               | —       |

## 4.7 Multicast Tests - EIGRP and OSPF

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |        |   |        |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|
| <b>IGMP Snooping</b><br>The purpose of this test is to verify the functionality of the IGMP snooping feature. This test configures a switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or IGMP snooping. IGMP snooping constrains IPv4 Multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 Multicast traffic only to those ports that want to receive it.                                                                                                                                                                                                                                                                            | Passed | — | Passed | — |
| <b>Multicast Limiters</b><br>The purpose of this test is to enable multicast limiter features in the test environment without any negative impact to multicast traffic and its states. These limiters were not stress tested.<br>Multicast route limit, the PIM register rate limit, the MSDP SA limit, and the IGMP limit were enabled in the test environment and deployed with Multicast traffic and states. These will help safe guard network against anomalies in Multicast states. There are many commands that can limit the amount of state that can be created by Multicast traffic. This test uses the Multicast route-limit, pim register-rate-limit, msdp sa-limit, and igmp limits commands. | Passed | — | Passed | — |
| <b>Auto RP</b><br>The purpose of this test is to verify the functionality of the auto-RP and auto-RP listener features when static RP's also defined. Auto RP is defined for different set of Multicast groups than static RP groups.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Passed | — | Passed | — |
| <b>MSDP/ Anycast RP</b><br>The purpose of this test is to verify the basic functionality of MSDP and MSDP/Anycast. For running Multicast traffic, static rendezvous points (RPs) are defined. Redundant RPs are configured with MSDP to facilitate Anycast-RP. Separate RPs are defined for the publish groups and the feedback groups building floors.                                                                                                                                                                                                                                                                                                                                                    | Passed | — | Passed | — |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |        |   |        |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|
| <p><b>PIM Stub</b></p> <p>The PIM stub feature supports Multicast routing between distribution layer and access layer. The PIM stub router contains two types of PIM interfaces:</p> <p>Uplink PIM interfaces and PIM passive interfaces. The uplink PIM interfaces have full PIM functionality and are used to connect to distribution routers.</p> <p>The PIM passive interfaces are connected to layer 2 access domains (for example, VLANs). The PIM stub feature provides the following restricted Multicast routing support:</p> <p>(1) The PIM stub router does not route the transit traffic between distribution routers. This behavior is enforced by Unicast (EIGRP) stub routing. The proper Unicast stub routing configuration is required to assist this PIM stub router behavior. The PIM stub feature does not prevent router administrator configuring RIP, static routes or PIM RP to bypass this restriction.</p> <p>(2) Only direct-connected Multicast (IGMP) receivers and sources are allowed in the layer 2 access domains. The PIM protocol is not supported in access domains. The PIM passive interface do not send or process any received Multicast control packets include PIM, DVMRP messages. Those Multicast control packets come in from PIM passive interfaces are ignored and dropped.</p> <p>The non-RPF traffic from PIM passive interface is dropped.</p> <p>(3) The redundant PIM stub router topology is not supported. The redundant topology here means that more than one PIM router forward Multicast traffic to a single access domain. Because of blocking PIM messages, the PIM assert and DR election mechanisms are not supported on PIM passive interface.</p> <p>Only the non-redundant access router topology is supported by PIM stub feature. The PIM passive interface assumes that it is the only interface and DR (Designated Router) on that access domain.</p> | Passed | — | Passed | — |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|

## 4.8 VoIP Tests - EIGRP and OSPF

**Table 4-6** VoIP Tests - EIGRP and OSPF

| Test                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Manual Test Case | Defects | Automation Test Case | Defects |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------|----------------------|---------|
| <b>System Integration Test Suite: VoIP</b><br>This testcase is run in Campus Routed Access test network environment setup and will run in serial with "SCCP to SCCP", "SCCP to SIP", "Quality of Voice", "SRTP", and "Video Telephony" test cases within this test suite. Device configurations used for this testcase will have feature combination and feature interaction with configurations from other test suites, routing, and Multicast test suites. This test case will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and Multicast traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                  |         |                      |         |
| <b>SIP to SIP</b><br>The purpose of this test is to provision SIP-to-SIP calls and verify calls will be successful. In this test, ABACUS VoIP traffic/quality generation/verification test tool will be used to emulate 1,000 SIP client end-points (IP Phones) and to generate 500 VoIP call signaling and RTP (Real-Time Transport Protocol) traffic streams over the campus for 10 times. Total CSR (Call Success Rate) should be greater than 99.9%. In order to achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in campus should be working and functioning properly.<br>The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. SIP has the following features:<br>- Lightweight, in that SIP has only six methods, reducing complexity.<br>- Transport-independent, (SIP can be used with UDP, TCP, ATM, etc.).<br>- Text-based, allowing for humans to read SIP messages.<br>SIP clients use TCP or UDP typically using port 5060 to connect to SIP servers and other SIP endpoints. SIP is primarily used in setting up and tearing down voice or video calls. However, it can be used in any application where session initiation is a requirement. These include Event Subscription and Notification, Terminal mobility. | Passed           | —       | Passed               | —       |



|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |        |   |        |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|
| <p><b>SCCP to SCCP</b></p> <p>The purpose of this test is to provision SCCP-to-SCCP calls and verify calls be will be successful. In this test, ABACUS VoIP traffic/quality generation/verification test tool will be used to emulate 1,000 SCCP client end-points (IP Phones) and to generate 500 VoIP call signaling and RTP (Real-Time Transport Protocol) traffic streams over the campus for 10 times. Total CSR (Call Success Rate) should be greater than 99.9%. In order to achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in campus should be working and functioning properly.</p> <p><b>SCCP (Skinny Client Control Protocol)</b> is a proprietary terminal control protocol owned and defined by Cisco Systems, Inc. as a messaging set between a skinny client and the Cisco CallManager. Examples of skinny clients include the Cisco 7900 series of IP phone and the 802.11b wireless Cisco 7920. Skinny is a lightweight protocol that allows for efficient communication with Cisco Call Manager. Call Manager acts as a signaling proxy for call events initiated over other common protocols such as H.323, SIP, ISDN and/or MGCP.</p> <p>A skinny client uses TCP/IP to and from one or more Call Managers in a cluster. RTP/UDP/IP is used to and from a similar skinny client or H.323 terminal for the bearer traffic (real-time audio stream). SCCP is a stimulus-based protocol and is designed as a communications protocol for hardware endpoints and other embedded systems, with significant CPU and memory constraints.</p> | Passed | — | Passed | — |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |        |   |        |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|
| <p><b>SIP to SCCP and SCCP to SIP</b></p> <p>The purpose of this test is to verify SCCP-to-SIP and SIP-to-SCCP calls. In this test, ABACUS VoIP traffic/quality generation/verification test tool will be used to emulate 200 SCCP and 200 SIP client end-points and to generate 100 SIP-to-SCCP and 100 SCCP-to-SIP VoIP call signaling and RTP (Real-Time Transport Protocol) traffic streams over the campus for 10 times. Total CSR (Call Success Rate) should be greater than 99.9%. In order to achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in campus should be working and functioning properly.</p> <p>The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. SIP has the following features:</p> <ul style="list-style-type: none"> <li>- Lightweight, in that SIP has only six methods, reducing complexity.</li> <li>- Transport-independent, (SIP can be used with UDP, TCP, ATM, etc.).</li> <li>- Text-based, allowing for humans to read SIP messages.</li> </ul> <p>SIP clients use TCP or UDP typically using port 5060 to connect to SIP servers and other SIP endpoints. SIP is primarily used in setting up and tearing down voice or video calls. However, it can be used in any application where session initiation is a requirement. These include Event Subscription and Notification, Terminal mobility, and so on. SCCP (Skinny Client Control Protocol) is a proprietary terminal control protocol owned and defined by Cisco Systems, Inc. as a messaging set between a skinny client and the Cisco CallManager. Examples of skinny clients include the Cisco 7900 series of IP phone and the 802.11b wireless Cisco 7920. Skinny is a lightweight protocol that allows for efficient communication with Cisco Call Manager. Call Manager acts as a signaling proxy for call events initiated over other common protocols such as H.323, SIP, ISDN and/or MGCP.</p> <p>A skinny client uses TCP/IP to and from one or more Call Managers in a cluster. RTP/UDP/IP is used to and from a similar skinny client or H.323 terminal for the bearer traffic (real-time audio stream). SCCP is a stimulus-based protocol and is designed as a communications protocol for hardware endpoints and other embedded systems, with significant CPU and memory constraints.</p> | Passed | — | Passed | — |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |        |   |        |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|
| <p><b>Media Transport Delay</b></p> <p>The purpose of this test is to measure delay. In this test, ABACUS VoIP traffic/quality generation/verification test tool will be used to emulate 200 SIP client end-points and to generate 100 VoIP call signaling and RTP (Real-Time Transport Protocol) traffic streams over the campus for 10 times. Average one-way delay should be less than 100 ms. In order to achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in campus should be working and functioning properly.</p> <p>This testcase will run with traffic streams flowing in the background that includes stateful traffic, stateless traffic, and Multicast traffic.</p> <p>One-Way Delay (OWD)</p> <p>One-way delay measures time interval between the time a voice pattern leaves the transmitting device and the time reaches the receiving device. The accuracy of this measurement is <math>\pm 2</math> ms, and the resolution is 1. In Simplex mode, the number of measurements for one-way delay on a channel should equal the number of PSQM values.</p> | Passed | — | Passed | — |
| <p><b>Jitter</b></p> <p>The purpose of this test is to measure RTP jitter which is measured during the interval between the sending of two RTCP packets.</p> <p>In this test, ABACUS VoIP traffic/quality generation/verification test tool will be used to emulate 200 SIP client end-points and to generate 100 VoIP call signaling and RTP (Real-Time Transport Protocol) traffic streams over the campus for 10 times. Average RTP jitter should be less than 50 ms. In order to achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in campus should be working and functioning properly.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Passed |   | Passed | — |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |        |   |        |   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|
| <p><b>Quality of Voice</b></p> <p>The purpose of this test is to measure Quality of Voice using PSQM model.</p> <p>PSQM uses a psychoacoustic model that aims to mimic the perception of sound in real life. Although it was originally developed to test Codecs, it was widely used for testing VoIP systems. The algorithm tested Codec by comparing the signal after it has been through the coder and decoder process with the original signal. A network can be similarly tested by replacing the coder-decoder elements with an SUT.</p> <p>PSQM provides an output in the range 0 to 6.5, where 0 indicates a good channel, and 6.5 indicates a very poor channel. PSQM Value:</p> <p>In this test, ABACUS VoIP traffic/quality generation/verification test tool will be used to emulate 200 SIP client end-points and to generate 100 VoIP call signaling and RTP (Real-Time Transport Protocol) traffic streams over the campus for 10 times.</p> | Passed | — | Passed | — |
| <p><b>Video Telephony</b></p> <p>The purpose of this test is to provision H.264 and verify call success. H.264/AVC/MPEG-4 Part 10 contains a number of new features that allow it to compress video much more effectively than older standards and to provide more flexibility for application to a wide variety of network environments. H.264 is supported with Cisco 7900 Video IP Phones.</p> <p>In this test, ABACUS VoIP traffic/quality generation/verification test tool will be used to emulate 200 SIP client end-points and to generate 100 VoIP call signaling and H.264 RTP (Real-Time Transport Protocol) traffic streams over the campus 10 times. Total CSR (Call Success Rate) should be greater than 99.9%. In order to achieve the goal, all technology aspects of layer2, IP routing, QoS, Security in campus should be working and functioning properly.</p>                                                                           | Passed | — | Passed | — |

## 4.8.1 Wireless Tests - EIGRP and OSPF

**Table 4-7**      **Wireless Tests - EIGRP and OSPF**

| Test                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Manual Test Case | Defects | Automation Test Case | Defects |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------|----------------------|---------|
| <b>System Integration Test Suite: Wireless</b><br>This test suite is targeted to deploy and verify a campus wireless solution with a Routed Access Campus Topology using the WiSM, 4404 Wireless controller and Light Weight Access Points. This Test Suite is to verify that all traffic (data, voice, video, Multicast) can successfully coexist between the wireless clients and a wireless campus network.                                                                                                                      |                  |         |                      |         |
| <b>Wireless Controller System</b><br>This test case will configure the WiSM controller and verify that it functions as expected. The Cisco WiSM is a Cisco Wireless LAN 4404 Controller Module in a Catalyst 6k. It works in conjunction with the Cisco Lightweight Access Points (LWAPP) protocol to support wireless data, voice, and video applications. This test case will verify that the WiSM can manage the LWAPP Access Points. This test will also run on the Cisco 4404 wireless controllers in the manual testbed only. | Passed           | —       | Passed               | —       |
| <b>Dot1x Authentication</b><br>This test case will verify that a wireless PC Client employee account can associate successfully with a WLAN using Dot1x Authentication and can transmit/receive wireless data traffic across campus network.<br>The Cisco Secure Services Client will be used as the dot1x supplicant.                                                                                                                                                                                                              | Passed           | —       | Passed               | —       |
| <b>Voice over Wireless</b><br>This test case will verify VoIP on wireless network. The Cisco Unified Wireless IP Phone 7920 is an easy to use IEEE 802.11b wireless IP phone that provides comprehensive voice communications in conjunction with Cisco Unified CallManager and the Cisco wireless infrastructure. This test case will verify that a Cisco Unified Wireless IP Phone 7920 transparently delivers voice traffic across campus network over the 4404/WISM Controllers.                                                | Passed           | —       | Passed               | —       |
| <b>Intra-controller Roaming</b><br>Intra-controller roaming enables a client to change its connection between access points in the same subnet (Intra-controller roaming) to support time-sensitive applications such as VoIP, video streaming, and client/server-based applications. This test case will verify the ability of a wireless client Intra-controller roaming between the APs.                                                                                                                                         | Passed           | —       | Passed               | —       |

## 4.8.1 Wireless Tests - EIGRP and OSPF

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |        |   |        |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---|--------|---|
| <b>L2 Inter-controller Roaming</b><br>L2 inter-controller roaming enables a client to change its connection between access points between subnets to support time-sensitive applications such as voice/video streaming and client/server-based applications. L2 inter-controller roaming includes two features -access-point-assisted channel scanning and fast IEEE 802.1X rekeying. This test case will verify the ability of a wireless client L2 inter-controller roaming between the APs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Passed |   | Passed | — |
| <b>Wireless control system verification</b><br>Cisco Wireless Control System (WCS) is the industry-leading platform for wireless LAN planning, configuration, and management. It works in conjunction with Cisco Aironet Lightweight Access Points, Cisco wireless LAN controllers and the Cisco Wireless Location Appliance. With Cisco WCS, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and wireless LAN systems management. Robust graphical interfaces make wireless LAN deployment and operations simple and cost-effective. Cisco WCS includes tools for wireless LAN planning and design, RF management, location tracking, Intrusion Prevention System (IPS), and wireless LAN systems configuration, monitoring, and management.<br>This test case will verify that WCS can manage the wireless networks across the campus network | Passed | — | Passed | — |
| <b>Multicast over wireless</b><br>This test case will verify that IP/TV Multicast traffic can be successfully delivered to Wireless PC clients.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Passed | — | NA     | — |

*This page is intentionally left blank*







# APPENDIX A

## Related Documents and Links

---

- [High Availability Campus Network Design-Routed Access Layer using EIGRP or OSPF](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a00805fcbf.pdf)  
[http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration\\_09186a00805fcbf.pdf](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a00805fcbf.pdf)
- [Cisco AVVID Network Infrastructure IP Multicast Design](http://www.cisco.com/application/pdf/en/us/guest/tech/tk363/c1501/ccmigration_09186a008015e7cc.pdf)  
[http://www.cisco.com/application/pdf/en/us/guest/tech/tk363/c1501/ccmigration\\_09186a008015e7cc.pdf](http://www.cisco.com/application/pdf/en/us/guest/tech/tk363/c1501/ccmigration_09186a008015e7cc.pdf)
- [Bidirectional PIM Deployment Guide](http://www.cisco.com/warp/public/732/Tech/Multicast/docs/bidirdeployment.pdf)  
<http://www.cisco.com/warp/public/732/Tech/Multicast/docs/bidirdeployment.pdf>
- Wireless features - [Enterprise Mobility 3.0 Design Guide](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration_09186a00808118de.pdf)  
[http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration\\_09186a00808118de.pdf](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration_09186a00808118de.pdf)
- [VOIP Infrastructure Solution Guide](http://www/en/US/tech/tk652/tk701/technologies_configuration_guide_book09186a00800eaa0e.html)  
[http://www/en/US/tech/tk652/tk701/technologies\\_configuration\\_guide\\_book09186a00800eaa0e.html](http://www/en/US/tech/tk652/tk701/technologies_configuration_guide_book09186a00800eaa0e.html)
- [Cisco Unified Communications SRND](http://www/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a0080783d84.html)  
[http://www/en/US/products/sw/voicesw/ps556/products\\_implementation\\_design\\_guide\\_book09186a0080783d84.html](http://www/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a0080783d84.html)
- [Cisco IOS SIP Configuration Guide](http://www/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_book09186a00807517b8.html)  
[http://www/en/US/products/sw/iosswrel/ps5207/products\\_configuration\\_guide\\_book09186a00807517b8.html](http://www/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_book09186a00807517b8.html)
- [Cisco Nonstop Forwarding and Stateful Switchover Deployment Guide](http://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd801dc5e2.html)  
[http://www.cisco.com/en/US/technologies/tk869/tk769/technologies\\_white\\_paper0900aecd801dc5e2.html](http://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd801dc5e2.html)
- [NSF benefits and restrictions](http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/nsfsso.html)  
<http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/nsfsso.html>

*This page is intentionally left blank*



# APPENDIX B

## Defects

---

Ten software defects were identified during test execution.

### B.1 CSCek78468

When `eigrp stub connected` is configured under router EIGRP process, this configuration changes to `eigrp stub connected summary` after reload.

Severity: Moderate

Workaround: Manually configure “eigrp stub connected” after reload.

Status: Resolved

The fix has been integrated in 12.2(31)SGA04

### B.2 CSCek75460

Loopback interface appears under show IP protocol even after it is deleted.

Severity: Minor

Workaround: Removing and configuring EIGRP protocol clears this problem.

Status: Resolved

The fix has been integrated in the following releases:

12.0(32.03)S06 12.2(32.08.11)XIB62.16 12.4(16.09)T

### B.3 CSCsk10711

Installation of static routes into the routing table takes about 5 to 6 seconds after executing `clear ip route *`. This delay was noticed during negative testing.

Severity: Moderate

Workaround: None.

Status: Closed. This issue will be resolved via routing infrastructure changes in future IOS releases.

## B.4 CSCsh94221

The “LINEPROTO-UPDOWN” message appears when the interface state changes before the expiration of the carrier-delay timer configured via the `carrier delay` command on the interface On Catalyst 6500.

Severity: Moderate

Workaround: None.

Status: Closed since this is an expected behavior on Catalyst 6500.

## B.5 CSCsk01448

Tracebacks in the syslogs due to CPU hog by PIM process during router reload.

Severity: Moderate

Workaround: None.

Status: Unreproducible

This DDTS was closed since the problem could not be recreated.

## B.6 CSCsj48453

Catalyst 6500 does not forward multicast traffic to WISM module when catalyst 6500 is configured in L3 mode.

Severity: Catastrophic

Workaround: None.

Status: Resolved

The fix has been integrated into flowing releases:

12.2(18.13.03)SXF 12.2(32.08.11)SX152 12.2(33.01.11)SXH

## B.7 CSCsj45951

Digital Optical Monitoring polling may cause Link flaps on some Xenpak transceivers. Link flaps may intermittently occur on TenGigabitEthernet interfaces with certain 10GBase-SR Xenpaks.

Severity: Severe

Workaround: None

Status: Resolved

The fix has been integrated in 12.2(18)SXF11

## B.8 CSCsm08419

On Catalyst 6500 with Supervisor 32 module, the default debounce interval for 8x1 GigabitEthernet or 2 x TenGigabitEthernet interfaces is 300msec instead of 10msec. Debounce interval of TenGigabitEthernet interfaces on WS-X6708-10GE line card is 300msec instead of 10msec.

Severity: Severe

Workaround: None

Status: Resolved

The fix integrated in 12.2(18)SXF13

## B.9 CSCsm33116

Catalysts 3500 and 3700 series switches may take longer than 800msec to converge multicast traffic during failure. This is due to the delay in triggering RPF.

Severity: Moderate

Workaround: None

Status: Assigned

## B.10 CSCsm35240

Catalyst 4500 series switches with 10GigE fiber interfaces may take longer than 200msec to converge during failure. The problem is due to the delay in bringing down the link.

Severity: Moderate

Workaround: None

Status: Assigned

*This page is intentionally left blank*



# APPENDIX C

## Technical Notes

---

### C.1 Technical Note 1:

**Wireless controller software should be upgraded in sequence.**

It is a good practice to back up the configuration file before upgrading or downgrading the software to avoid losing all or part of the configuration stored in NVRAM. While upgrading the software on wireless controller, follow the upgrade path outlined below.

**Table C-1**      **Wireless Controller Upgrade Path**

| Desired Upgrade       | Upgrade Path                                                                                                                          |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| 3.2 or earlier to 4.1 | Use the following steps to upgrade to 4.1:<br><b>Step 1</b> Upgrade to software release 4.0.<br><b>Step 2</b> Upgrade to release 4.1. |
| 4.0 to 4.1            | No restriction. Upgrade directly to 4.1                                                                                               |



**Note**

In some cases, when upgrading to software release 4.1 directly from release 3.2 or earlier, upgrade may not be successful or some features may not function as expected.