



PureConnect®

2018 R5

Generated:

12-November-2018

Content last updated:

6-April-2018

See [Change Log](#) for summary of changes.



PureConnect Quality of Service

Technical Reference

Abstract

This document presents information regarding tested configurations that are proven to provide Quality of Service (QoS) with the PureConnect line of products. When QoS is applied correctly, it can resolve problems with audio and delays in Voice-over-Internet-Protocol (VoIP) communications.

For the latest version of this document, see the PureConnect Documentation Library at: <http://help.genesys.com/cic>.

For copyright and trademark information, see https://help.genesys.com/cic/desktop/copyright_and_trademark_information.htm.

Table of Contents

Table of Contents	2
Introduction	3
PureConnect Quality of Service driver	4
Supported products for the PureConnect QoS driver	4
PureConnect QoS driver installations	5
PureConnect QoS driver installation properties	5
Install Interactive QoS driver with CIC User Applications	5
Other options for PureConnect QoS	7
Driver_status.exe QoS utility	7
Use SAPI TTS without the PureConnect QoS driver	8
RTP port usage	9
Marking	10
Virtual Local Area Networks (VLANs) and QoS	13
Basic LAN QoS (Cisco) and VLANs in a single switch network	13
Advanced Security Design in VLANs with a single switch network	15
VLAN trunking	18
Larger networks with multiple switches	19
The required method for Layer 3 switches	20
Alternative method for older switches (not recommended)	21
Ingress DSCP mapping (Cisco)	21
AutoQoS (Cisco)	22
WAN QoS (Cisco)	23
Class Based Weighted Fair Queuing / Low Latency Queue CBWFQ/LLQ	23
Call Admission Control (CAC)	27
Basic LAN QoS (Dell)	28
Multiple VLAN with trunks	28
CIC switchover and QoS	30
Telephones	31
Polycom	31
Soft phones	31
Fax	32
Interaction Gateway	33
Opening client ports	35
Interaction Media Server	36
References and further reading	37
Appendix A: OpenSSL Copyright	38
Change log	40
Copyright and Trademark Information	41

Introduction

The purpose of this document is to provide tested configurations proven to provide Quality of Service with the PureConnect line of products. When you apply QoS correctly, it can resolve problems with "choppy" audio, voice quality, and delays that make interaction difficult. This document assumes that the reader is familiar with Basic QoS principles and network characteristics such as bandwidth, delay, jitter, and packet loss.

Genesys provides the examples on the following pages as a courtesy so don't take them as exact representations of any customer environment. It's possible that the configurations presented aren't the best solution for larger, more complex networks. The intent of this document is to demonstrate some best practices and to provide a resource for network engineers before implementation.

PureConnect Quality of Service driver

Supported products for the PureConnect QoS driver

The PureConnect product suite installs and uses its own QoS driver for its servers and client applications. This driver operates independently of the Microsoft QoS Packet Scheduler, which was the recommended QoS driver in CIC version 3.0. The PureConnect QoS driver is available in 64-bit and 32-bit versions and installs based on the supporting operating system.

The following product installation packages install the PureConnect QoS driver:

Product	.ISO image directory	Installation file	Supported operating system
Interaction Media Server	\Off-ServerComponents	MediaServer_20nn_Rn.msi	64-bit
Interaction Recorder Extreme Query	\Off-ServerComponents	IRExtremeQueryServer_20nn_Rn.msi	64-bit
Interaction Recorder Remote Content Service	\Off-ServerComponents	IRRemoteContentService_20nn_Rn.msi	64-bit
IC Session Manager (Off-host)	\Off-ServerComponents	SessionManager_20nn_Rn.msi	64-bit
IC Status Aggregator	\Off-ServerComponents	StatusAggregator_20nn_Rn.msi	64-bit
Loquendo Automatic Speech Recognition	\Off-ServerComponents	LoquendoASR_20nn_Rn.msi	64-bit
Nuance Recognizer	\Off-ServerComponents	ASRServerNuanceRecognizer_20nn_Rn.msi	64-bit
CIC User Applications (32-bit)	\ServerComponents	ICUserApps_32bit_20nn_Rn.msi with at least one of the following applications selected: <ul style="list-style-type: none">• SIP Soft Phone• Interaction Screen Recorder Capture Client	32-bit
CIC User Applications (64-bit)	\ServerComponents	ICUserApps_64bit_20nn_Rn.msi with at least one of the following applications selected: <ul style="list-style-type: none">• SIP Soft Phone• Interaction Screen Recorder Capture Client	64-bit

Note: It's possible for future releases of PureConnect products to include the QoS driver in their installations.

PureConnect QoS driver installations

By default, the products that use the PureConnect QoS driver install that driver silently. The installation programs also install the required driver certificate to the Trusted Publishers list. The only exceptions are the CIC user application installation packages.

Following are situations where you do not want to install the PureConnect QoS driver:

- You use another form of QoS in your network environment.
- You want to use the PureConnect QoS driver, but do not want to add the certificate to the Trusted Publishers list.

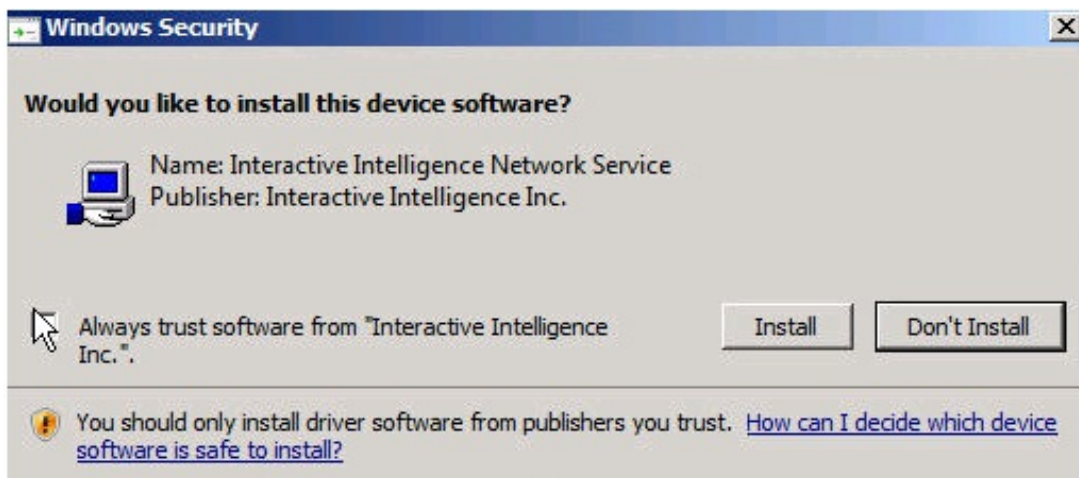
For these situations, do not install the .msi file through Windows Explorer or a command line interface without parameters. PureConnect installation packages support the following alternative methods, which allow you to determine how to install the PureConnect QoS driver:

- Group Policy.
- Startup or logon script.
- Command line interface with parameters.

PureConnect QoS driver installation properties

With properties, you can specify certain aspects of the installation of the PureConnect QoS driver. The following list provides these properties and the associated functionality:

- `DONOTINSTALL_ININQOSDRIVER` - This property, when set to 1, prohibits installation of the QoS driver and the driver certificate.
- `DONOTADDCERTOTRUSTEDPUBLIST` - This property, when set to 1, allows installation of the QoS driver but does not install the driver certificate to the Trusted Publishers list. When you set this property, the installation program prompts you to confirm installation of the PureConnect QoS driver.



When this message box appears, click **Install** to install the PureConnect QoS driver.

Important!

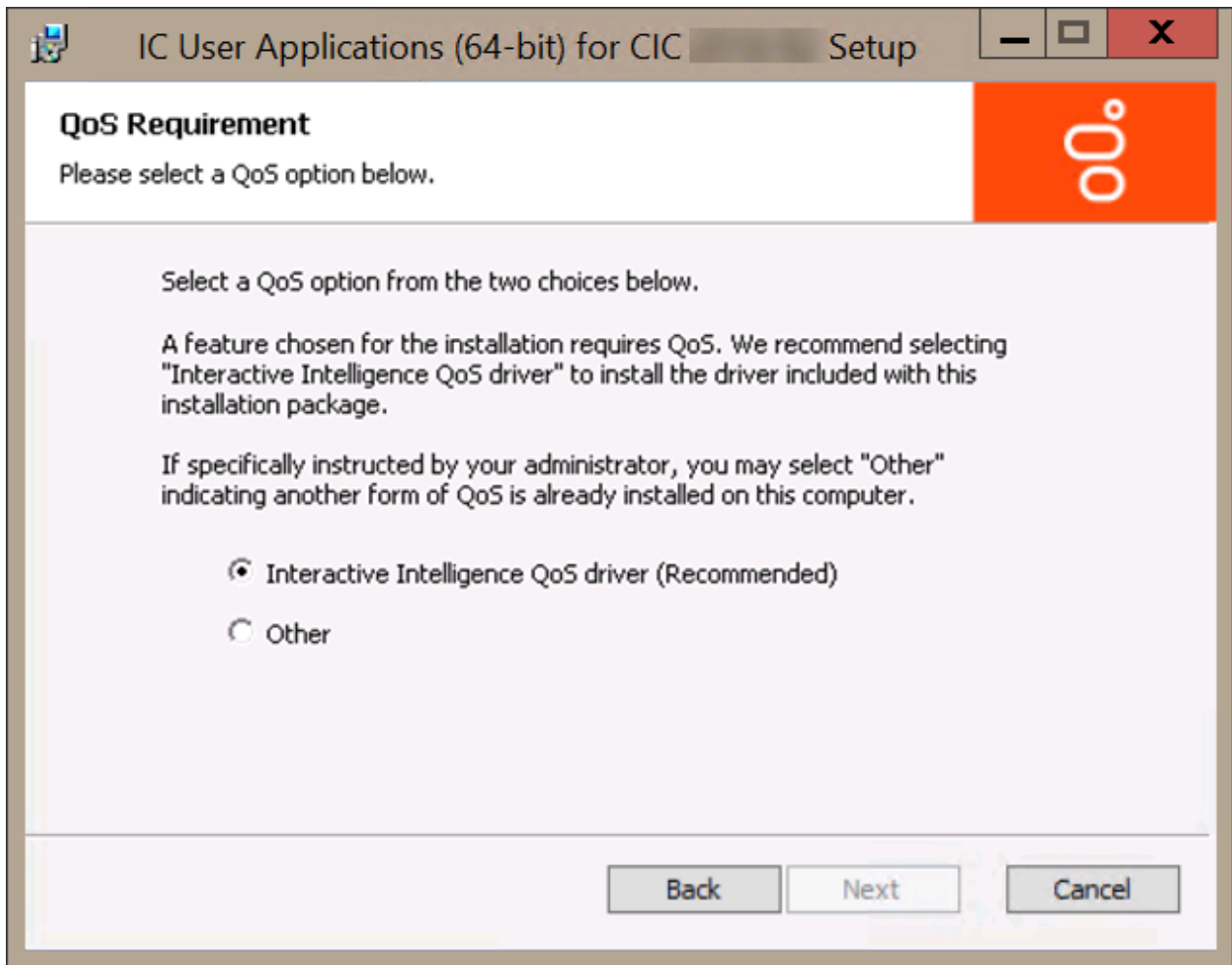
If you do not want to install the driver certificate to the Trusted Publishers list, leave the **Always trust software from "Genesys"** check box cleared.

Install Interactive QoS driver with CIC User Applications

When you install CIC User Applications with SIP Soft Phone or Interaction Screen Recorder Capture Client selected, the workstation on which it installs has the following behaviors, depending on your installation method:

- Group policy, startup or logon script, or command line Modify the properties as stated in the [PureConnect QoS driver installation properties](#) topic to control installation of the QoS driver and the driver certificate.
- Full installation When you run the `ICUserApps_32bit_20nn_Rn.msi` or `ICUserApps_64bit_20nn_Rn.msi` installation program, the following dialog box displays when you select a **Custom** installation.

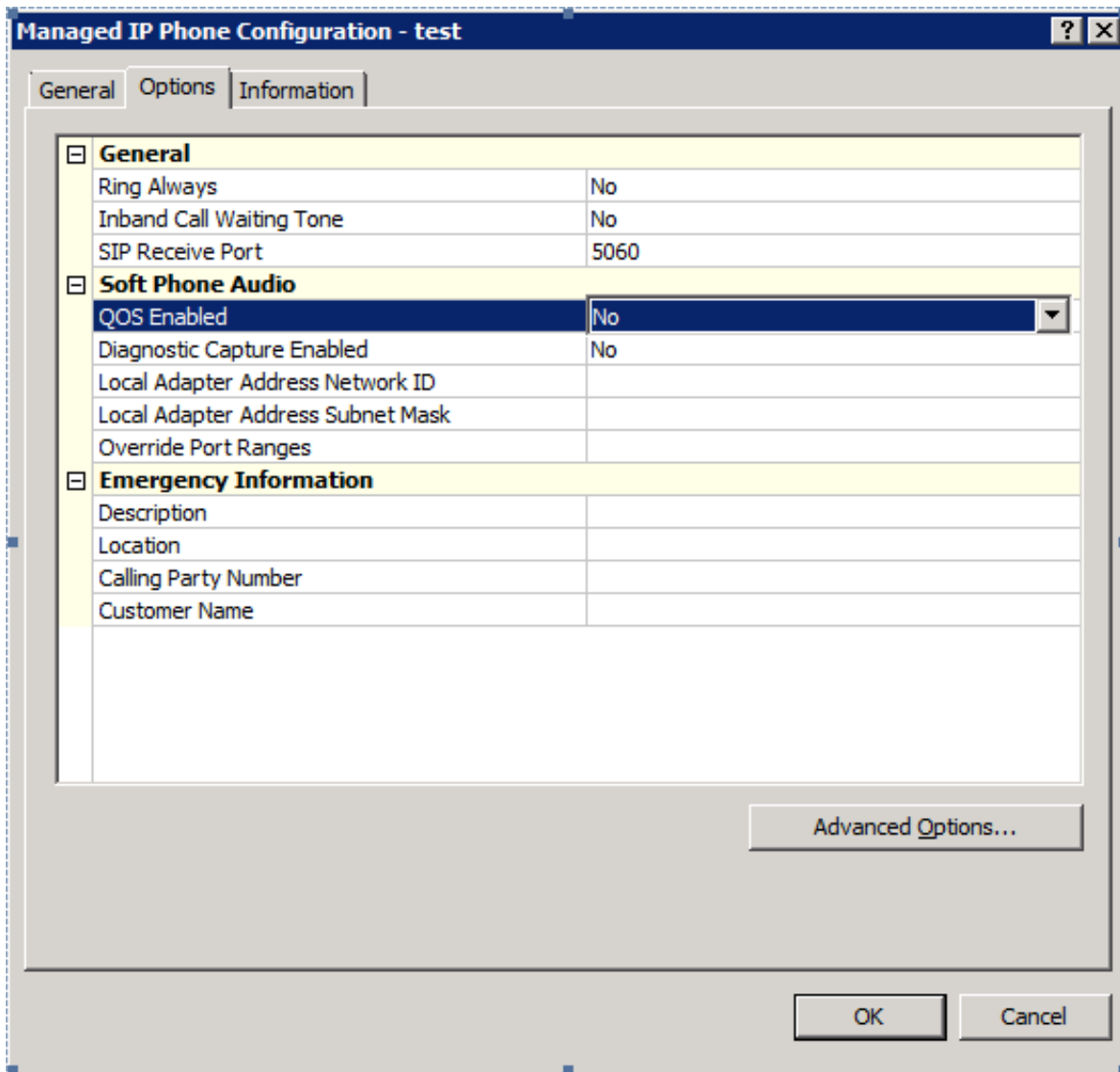
Note: If you do not select the **Custom** installation type, the PureConnect QoS driver and driver certificate install silently.



PureConnect QoS driver (Recommended): If selected, both the driver certificate and the QoS driver install. If the current permissions on the workstation do not allow modification of the Trusted Publishers list, a message indicating such appears.

Other: If selected, the program doesn't add the driver certificate to the Trusted Publishers list and the doesn't install the QoS driver. Use this option only when you have another QoS solution in place on the workstation.

Note: If you install SIP Soft Phone and click the **Other** option because another form of QoS is present on the workstation already, you must set the **QoS Enabled** option in the **Interaction Administrator Managed IP Phone Configuration** to **No**. Otherwise, the user cannot receive calls.



Note: During installation of the PureConnect QoS driver, including upgrades, the network connections of the personal computer interrupt briefly.

Other options for PureConnect QoS

The following list provides more information for working with the PureConnect QoS driver and driver certificate:

- If you uninstall PureConnect products that included the installation of the QoS driver and the driver certificate, the uninstall process removes the driver certificate from the Trusted Publishers list.
- You can manually add or remove the QoS driver certificate using the `certmgr.msc` utility or through a Group Policy.

Driver_status.exe QoS utility

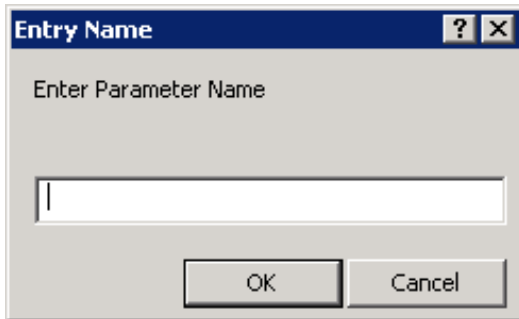
Each installation of the PureConnect QoS driver includes the `driver_status.exe` file. Run this utility, without switches or parameters, to check the status of the QoS driver.

Use SAPI TTS without the PureConnect QoS driver

If you do not install the PureConnect QoS driver, you can still configure CIC to play SAPI TTS through VoIP calls.

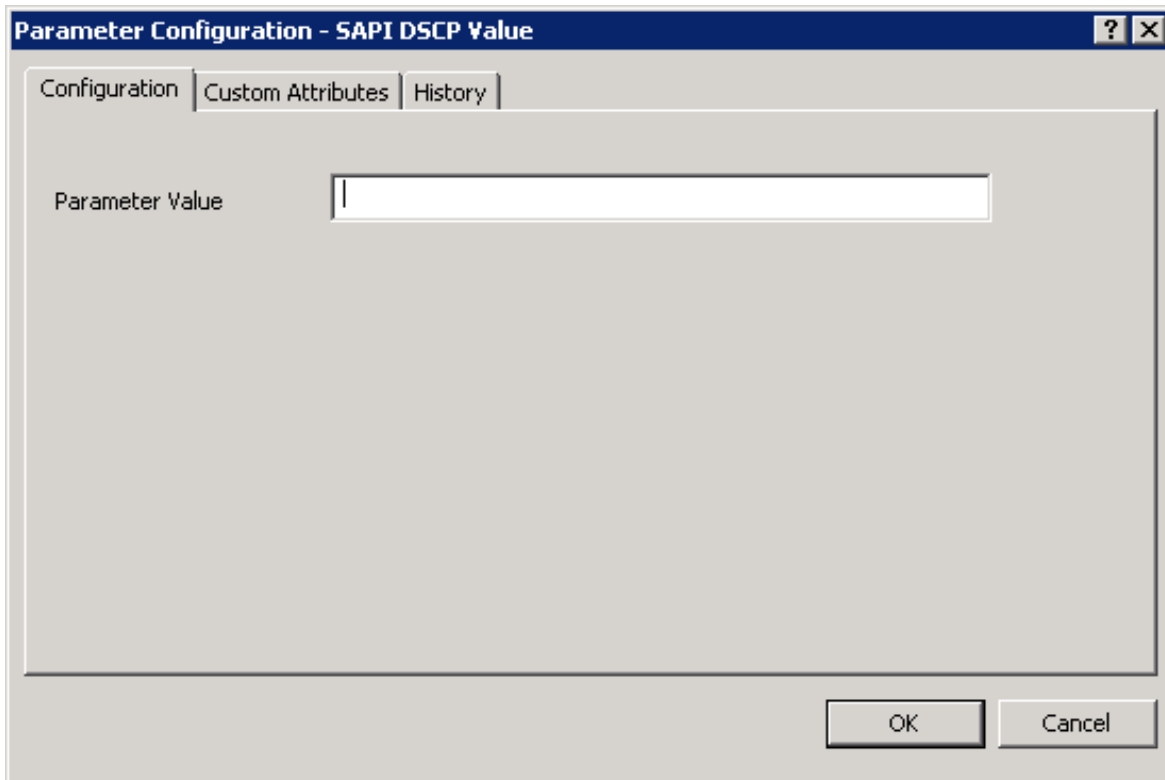
To configure CIC to play SAPI TTS without the QoS driver installed:

1. On the CIC server or from a remote computer connected to the CIC server, start Interaction Administrator.
2. In the expanded list under the name of your CIC server, click the **Server Parameters** object. The right pane of the **Interaction Administrator** window displays all current server parameters and their associated values.
3. In the right pane, right-click and then click **New** from the resulting shortcut menu. The **Entry Name** dialog box appears.



The **Entry Name** dialog box is a small window with a title bar containing a question mark and a close button. The main area contains the text "Enter Parameter Name" above a single-line text input field. At the bottom, there are two buttons: "OK" and "Cancel".

4. In the **Enter Parameter Name** box, type `SAPI DSCP Value` and then click **OK**. The **Parameter Configuration** dialog box appears.



The **Parameter Configuration - SAPI DSCP Value** dialog box has a title bar with a question mark and a close button. It features three tabs: "Configuration" (selected), "Custom Attributes", and "History". The main area contains the text "Parameter Value" followed by a single-line text input field. At the bottom, there are two buttons: "OK" and "Cancel".

5. In the **Parameter Value** box, type `0x0` and then click **OK**. The new server parameter and its value appear at the bottom of the table in the right pane of the **Interaction Administrator** window.
The `0x0` value represents the Differentiated Services Code Point (DSCP) value that inserts in RTP packets of VoIP interactions. You can also set the DSCP value to any value between `0x00` and `0x3f`.

RTP port usage

VoIP devices often use different Realtime Transfer Protocol (RTP) ports. PureConnect products use RTP ports depending on the intrinsic architecture used. Most IP telephones and other VoIP devices use varying RTP port ranges. Consult the documentation for your VoIP devices to determine the available RTP port ranges.

For the full list of supported IP telephone devices, gateways, and other VoIP devices, see <http://testlab.genesys.com>

For common network port ranges used with RTP, see the [*CIC Port Maps and Data Flow Diagrams Technical Reference*](#).

Marking

PureConnect products use Differentiated Services (DiffServ), and Class Selector PHB in some cases, to mark packets on an IP Network. RFC 2474 "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers "describe these standards.

When possible, always mark packets at the source. PureConnect products provide the ability to mark packets as they leave Interaction Media Server, Interaction Gateway, telephones, and other PureConnect products. Configure all switches and routers that handle data and call flows to guarantee that the marked IP packets honor the QoS as they propagate through the network.

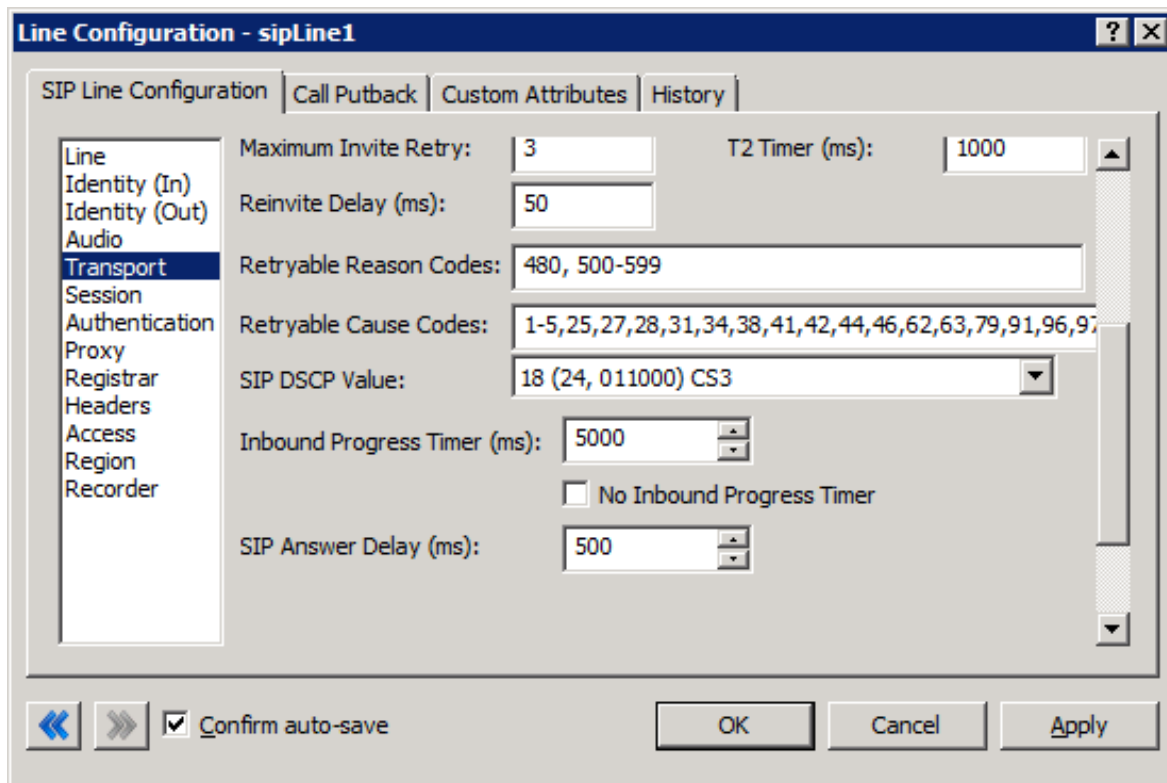
The endpoints QoS mark the RTP Packets, which use UDP, and SIP Packets, which through configuration can use UDP, TCP, or TLS. The QoS markings are in the 6-bit DSCP field of the ToS Byte of the IP header. The recommended (Default) value for RTP (voice) is 101110, which is EF / Expedited Forwarding. The recommended (Default) value for SIP Signaling is 011000, which is CS3 / Class Selector.

Source Endpoint Device Recommended Markings for RTP (voice) Recommended Markings for SIP (signaling) Where are the Configurations

SIP in C/C server	NA	SIP packets marked with 011000 (which is CS3 / Class Selector)	To alter this setting in Interaction Administrator, do the following steps: <ol style="list-style-type: none"> 1. In the left pane, select the Lines object. 2. In the right pane, double-click the Configuration item. 3. In the Line Configuration dialog box, select the SIP Line Configuration tab. 4. In the list box, click the Transport item. 5. Scroll down to the SIP DSCP Value list box and select the value that you want to assign.
IC Notifier	Notifier packets marked with 101110 (EF / Expedited Forwarding)		This DSCP marking value is not currently configurable. If you need different values, contact PureConnect Customer Care.
Interaction Media Server	RTP packets marked with 101110 (which is EF / Expedited Forwarding)	NA	Interaction Media Server RTP is marked with EF. Interaction Media Server does not use SIP signaling. For more Information about marking on Interaction Media Server, see <i>Interaction Media Server Technical Reference</i> .
Interaction Gateway	RTP packets marked with 101110 (which is EF / Expedited Forwarding)	SIP packets marked with 011000 (which is CS3 / Class Selector)	To alter this setting on Interaction Gateway, do the following steps: <ol style="list-style-type: none"> 1. Log on to the Interaction Gateway web interface with administrative credentials. 2. In the upper-right corner of the page, select the Settings icon. 3. On the left side of the page, select the Media tab. 4. In the RTP DSCP Value (hex) list box, select the value that you want to assign to RTP packets. 5. On the left side of the page, select the Spans tab. 6. In the SIP Span section, select the Modify button. 7. In the DSCP Value (hex) list box of the resulting page, select the value that you want to assign to SIP packets. Interaction Gateway exposes these values with the entire TOS Byte. The default value is 2E (46, 101110) EF.
AudioCodes Mediant Gateway	RTP packets marked with 101110 (which is EF / Expedited Forwarding)	SIP packets marked with 011000 (which is CS3 / Class Selector)	The Mediant gateway defaults to DSCP value 101100 and marks packets by default. You can change this setting on the following page under Full Configuration\Network Settings\QoS Settings . Change the Default setting of 44 decimal (101000) for Control Premium QoS to 24 decimal (011000) for SIP signaling to use CS3.
Polycom Phones	RTP packets marked with 101110 (which is EF / Expedited Forwarding)	SIP packets marked with 011000 (which is CS3 / Class Selector)	Legacy Polycom telephones that cannot be provisioned by the CIC server must be configured manually with a <code>sip.cfg</code> file. Provisioned Phone markings can be controlled in Interaction Administrator.

Interaction SIP Station	RTP packets marked with 101110 (which is EF / Expedited Forwarding)	SIP packets marked with 011000 (which is CS3 / Class Selector)	To alter this setting in Interaction Administrator, do the following steps: <ol style="list-style-type: none"> 1. In the left pane, expand the server object. 2. Expand the Stations object. 3. Highlight the Default Station object 4. In the right pane, double-click the Configuration item. 5. In the Default Station Configuration dialog box, select the Global SIP Station tab. 6. In the list box, select the Transport item. 7. In the SIP DSCP Value list box, select the value that you want to assign to SIP packets.
SIP Soft Phone	RTP packets marked with 101110 (which is EF / Expedited Forwarding)	SIP packets marked with 011000 (which is CS3 / Class Selector)	See <i>CIC Managed IP Phones Administrator's Guide</i> .
Any soft phone for CIC	RTP packets marked with 101110 (which is EF / Expedited Forwarding)	SIP packets marked with 011000 (which is CS3 / Class Selector)	See <i>CIC Managed IP Phones Administrator's Guide</i> .

The following image displays an example of setting the SIP QoS in the Line Configuration that is available through Interaction Administrator. Ensure that you are consistent with any changes that you make and consider the SIP lines and stations that you use. You can enter 18 in the SIP Line Configuration SIP DSCP Value field to have it display 011000 (which is CS3) correctly if you wish to use DSCP. No restart of Telephony Services is required. The next call from the server will use the new value.



Genesys highly recommends that you ensure the IP packets are getting marked correctly with the WireShark application, formerly known as Ethereal (<http://www.wireshark.org>). The following example displays the RTP header from a Polycom phone and the proper marking that is applied:

```
▣ Differentiated Services Field: 0xb8 (DSCP 0x2e: Expedited Forwarding; ECN: 0x00)
  1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (0x2e)
  .... ..0. = ECN-Capable Transport (ECT): 0
  .... ...0 = ECN-CE: 0
  Total Length: 200
```

It is not possible to mark the SIP Signaling coming from the CIC server. This can be accomplished at the switch level with a service-policy if necessary. Let's assume that the CIC server is using port fast0/1 in the following example. This example can extend to other application flows that need to be marked. Marking can be CPU intensive for routers and switches. Always ensure that you have properly sized your equipment for Marking.

1. Enable QoS on the Switch

Start in the privileged exec mode:

```
switch(config)#mls qos

switch(config)#policy-map mark-signal
switch(config-pmap)#class voice-signal
switch(config-pmap-c)#set dscp cs3
switch(config-pmap-c)#exit
switch(config-pmap)#exit
```

2. Create access lists to identify the SIP signaling traffic as it leaves the CIC server

Start in the privileged exec mode:

```
switch(config)#access-list 100 permit tcp any any eq 5060
switch(config)#access-list 100 permit tcp any any eq 8060
```

3. Create a Class-Map that uses the Access List

Start in the privileged exec mode:

```
switch (config)#class-map match-all voice-signal
switch(config-cmap)#match access-group 100
switch(config-cmap)#exit
```

4. Apply the Class-Map to a Policy

Start in the privileged exec mode:

```
switch(config)#policy-map mark-signal
switch(config-pmap)#class voice-signal
switch(config-pmap-c)#set dscp cs3
switch(config-pmap-c)#exit
switch(config-pmap)#exit
```

5. Apply the Service-Policy to the CIC server interface

Start in the privileged exec mode:

```
switch(config)#int fast 0/12
switch(config-if)#service-policy input mark-signal
switch(config-if)#exit
```

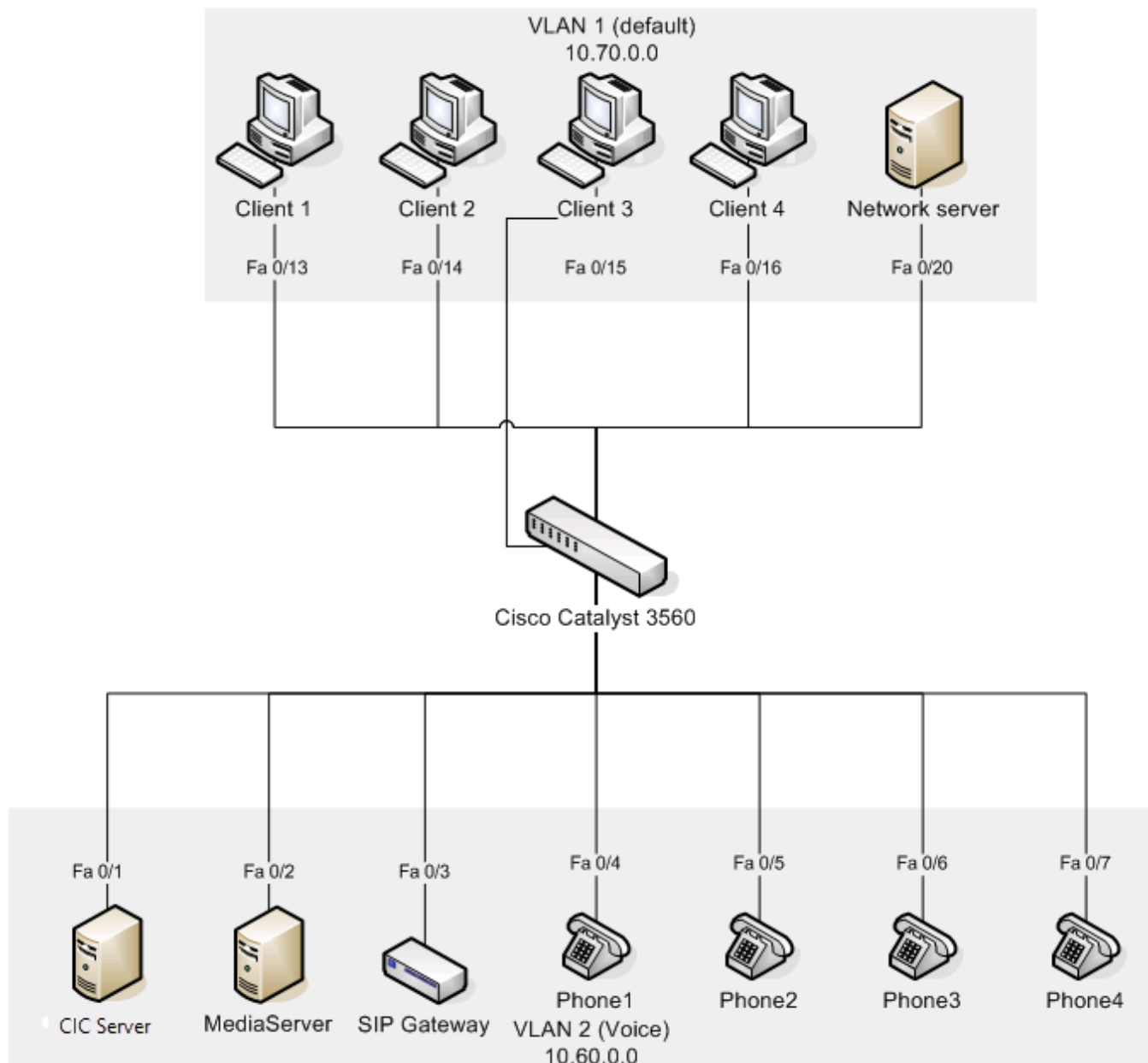
Virtual Local Area Networks (VLANs) and QoS

Basic LAN QoS (Cisco) and VLANs in a single switch network

When deploying IP telephones, Genesys recommends that you place IP telephones in a voice virtual local area network (VLAN). A voice VLAN can protect the telephones from broadcast traffic as well as provide security. You should place all voice endpoints including the Interaction Media Servers and other servers in the CIC network environment in the voice VLAN. CIC clients should remain in a Data VLAN or the Default VLAN. The SIP Soft Phone can also be placed on the Default VLAN. Currently, it requires dual Network Interface Cards (NICs) if splitting the traffic was a requirement. This configuration is only possible on switches that support Layer 3 routing. Layer 3 routing is required to let the different networks communicate with each other. This is all done in the routing table on the switch.

VLAN	Purpose	Recommended Number
Data	The Default for Clients, Data Traffic	100
Voice	IP Phones, CIC server, Interaction Media Server, Interaction SIP Proxy, etc.	200

This example configuration is based on the recommended setup and the following network model using a Cisco Catalyst 3560 switch.



1. Create the VLAN for Voice.

Start in the privileged exec mode:

```
configure terminal
vlan 200
name "Voice"
exit
```

2. Configure the VLAN interfaces with IP addresses.

From the global configuration mode:

```
interface vlan 100
ip address 10.70.0.1 255.255.0.0

interface vlan 200
ip address 10.60.0.1 255.255.0.0
```

3. Assign the switch ports to the respective VLANs using static port assignment.

From the global configuration mode:

```
interface range FastEthernet 0/1-12
switchport access vlan 200
exit
```

4. If using CDP (alternative to step 3)

Some environments may only have one data drop to the user. In this case, it is possible to make use of the **PC** port on the back of most of the Polycom telephone models.

The Polycom telephones support CDP to configure the correct VLANs for voice and data. The client personal computer can be plugged into the **PC** port of the Polycom telephone and still appear on VLAN 100 while the voice traffic from the telephone appears on VLAN 200.

Other endpoints that do not support CDP need to have static VLAN assignments on the switch. In the following example, ports 1-4 are statically assigned, and ports 5-12 are assigned using CDP.

From the global configuration mode:

```
interface range FastEthernet 0/1-4
switchport access vlan 200
mls qos trust dscp

interface range FastEthernet 0/5-12
mls qos trust dscp
switchport voice vlan 200

exit
```

5. Enable Layer 3 routing between the VLANs on the switch.

From the global configuration mode:

```
router rip
version 2
network 10.0.0.0

ip routing

ip route 10.60.0.0 255.255.0.0 Vlan200
ip route 10.70.0.0 255.255.0.0 Vlan100
ip route 0.0.0.0 0.0.0.0 Vlan100 10.0.0.1 //default route
```

6. Enable DHCP relay on the voice VLAN 200.

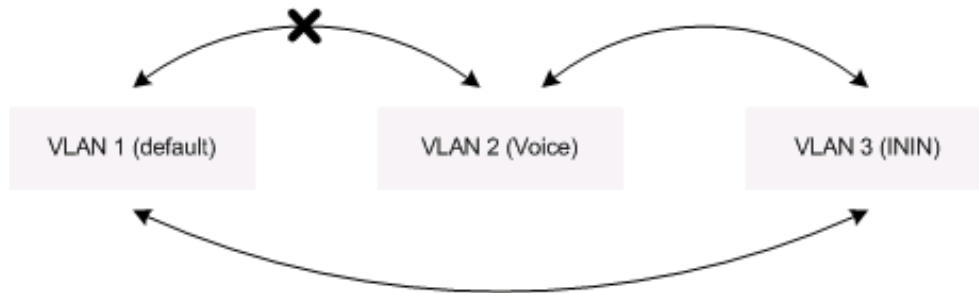
By design, DHCP broadcasts are not forwarded across VLANs. The following configuration enables the relay of DHCP broadcasts from VLAN 100 to VLAN 200. This is assuming the DHCP server resides on the default VLAN 100 and has an IP address of 10.70.0.5

From the global configuration mode:

```
interface vlan 200
ip helper-address 10.70.0.5
exit
```

Advanced Security Design in VLANs with a single switch network

The following diagram displays how you could use VLANs to design a security environment where the voice network cannot contact or be contacted by the data network. Only the "ININ" VLAN is routed to the require networks. This may be needed for extra security-conscious deployments but note that it does increase the level of complexity.

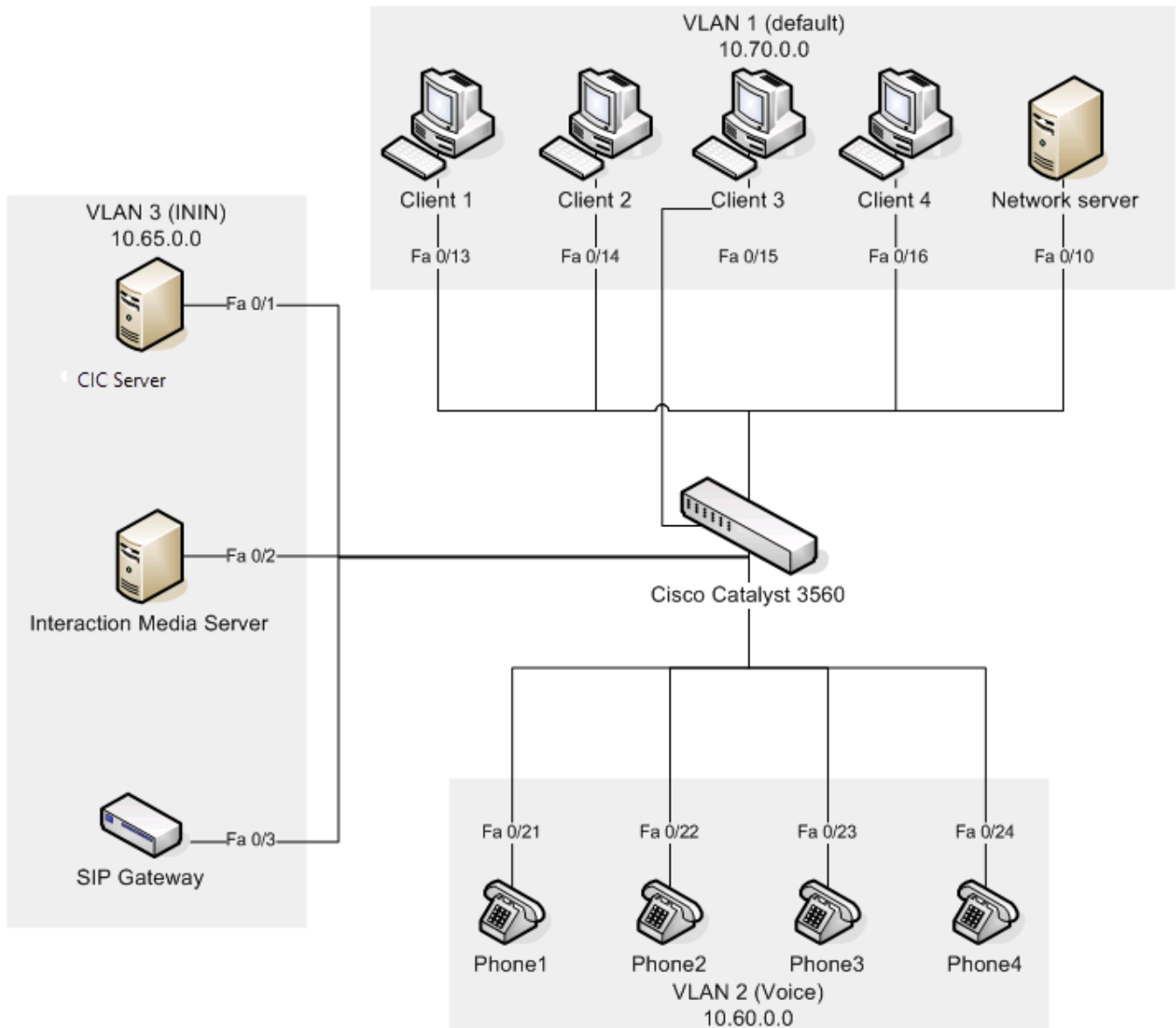


When deploying IP telephones, it is recommended to place telephones in a voice VLAN. A voice VLAN can protect the telephones from broadcast traffic as well as provide security. CIC clients should remain in a data VLAN or the default VLAN. The SIP Softphone can also be placed on the Default VLAN. Currently, it requires dual Network Interface Cards (NICs) if splitting the traffic was a requirement. This configuration is only possible on switches that support Layer 3 routing. The Layer 3 routing is required to let the different networks communicate with each other. This is all done in the routing table on the switch.

VLAN	Purpose	Recommended Number
Data	The Default for Data Traffic	100
Voice	IP Phones only	200
ININ	CIC server, Interaction Media Server, Interaction SIP Proxy, and others	300

The VLANs are configured in such a way that the data VLAN 100 is not able to communicate with the voice VLAN 200. This creates a higher level of security by preventing RTP sniffing. Interaction Media Servers, Interaction Gateways, and the CIC servers that are on VLAN 3 are able to communicate with the default VLAN 100. This is to enable client connections and also to enable Web-based configuration from the client machines. If desired, you can place the Interaction Gateways and the Interaction Media Servers in the voice VLAN 200 for added security. However, in that case, Web-based configuration for the Interaction Gateways and other systems may only be performed from the CIC server.

This example configuration is based on the recommended setup and the following network model using a Cisco Catalyst 3560 switch:



1. Create the VLANs for voice and CIC devices.
Start in the privileged exec mode.

```
configure terminal
vlan 200
name "Voice"

vlan 300
name "ININ"

exit
```

2. Configure the VLAN interfaces with IP addresses.
From the global configuration mode:

```
interface vlan 100
ip address 10.70.0.1 255.255.0.0

interface vlan 200
ip address 10.60.0.1 255.255.0.0

interface vlan 300
ip address 10.50.0.1 255.255.0.0
```


3. Assign the switch ports to the respective VLANs using static port assignment.

From the global configuration mode:

```
interface range FastEthernet 0/1-4
switchport access vlan 300

interface range FastEthernet 0/21-24
switchport access vlan 200

exit
```

4. If using CDP: (alternative to Step 3)

Some environments may only have one data drop to the user. In this case, it is possible to make use of the **PC** port on the back of most of the Polycom telephone models.

The Polycom telephones support CDP to configure the correct VLANs for voice and data. Therefore, in this case, the client personal computer can be plugged into the **PC** port of the Polycom telephone and still appear on VLAN 100 while the voice traffic from the telephone appears on VLAN 200.

Other endpoints that do not support CDP need to have static VLAN assignments on the switch. In the following example, ports 1-4 are statically assigned, and ports 5-12 are assigned using CDP.

From the global configuration mode:

```
interface range FastEthernet 0/1-4
switchport access vlan 300
mls qos trust dscp

interface range FastEthernet 0/21-24mls qos trust dscp
switchport voice vlan 200

exit
```

5. Enable Layer 3 routing between the VLANs on the switch.

From the global configuration mode:

```
ip routing
ip route 10.60.0.0 0.0.255.255 Vlan200
ip route 10.65.0.0 0.0.255.255 Vlan300
ip route 10.70.0.0 0.0.255.255 Vlan100
ip route 0.0.0.0 0.0.0.0 Vlan100
```

6. Enable DHCP relay on the voice VLAN 200.

By design, DHCP broadcasts are not forwarded across VLANs. The following set of commands enables the relay of DHCP broadcasts to VLAN 200 only. This is assuming that the DHCP server resides on the default VLAN 100 and has an IP address of 10.70.0.5.

Important!

IP addresses should be statically assigned on the devices in VLAN 300. Or, if required, the following can also be applied to VLAN 300.

From the global configuration mode:

```
interface vlan 200
ip helper-address 10.70.0.5
exit
```

7. Implement security.

Extended access-lists are used to restrict access to the voice VLAN from the data VLAN. The access-list should be applied to the egress of the VLAN 200 interface (10.60.x.x is the voice VLAN and 10.70.x.x is the data VLAN).

From the global configuration mode:

```
access-list 101 deny ip 10.70.0.0 0.0.255.255 10.60.0.0 0.0.255.255
access-list 101 permit any any

interface vlan 200
ip access-group 101 out
```

VLAN trunking

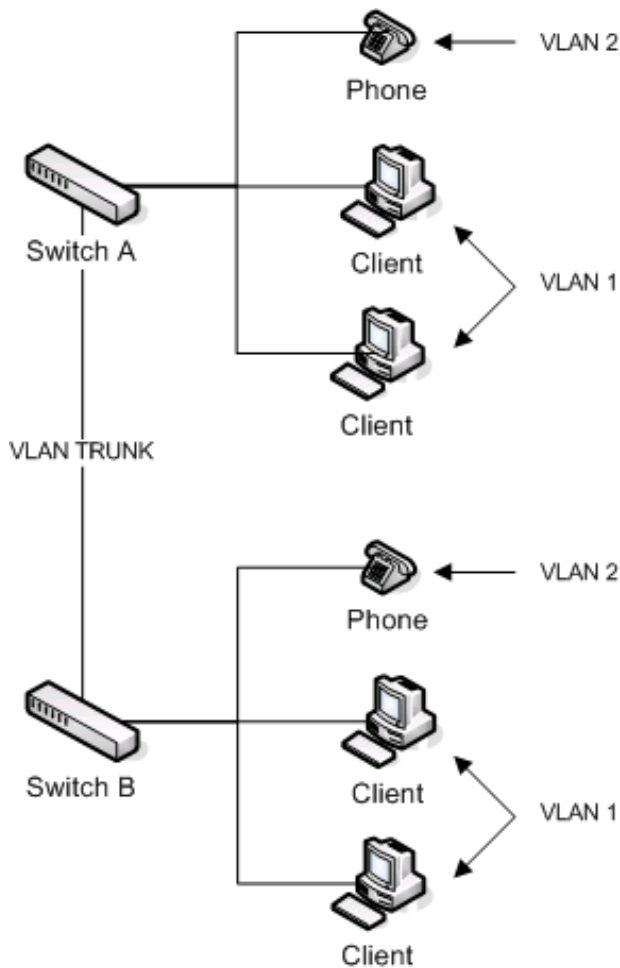
If the need arises to use more than one switch in the network, you can create VLAN trunks between two switches using VLAN Trunk Protocol (VTP). The configuration can be propagated through the network by administering it at a single switch.

Warning!

Some networking professionals have strong opinions on using VTP because of security concerns.

This example configuration is based on the following network model that consists of two Cisco Catalyst switches and two VLANs.

In this case, Switch A is a Cisco Catalyst 3560 switch and is the server in the VTP domain. Switch B is a Catalyst 3500 XL, a client in the VTP domain. For the purposes of this test, the VTP domain is named `qostest` and password authentication is disabled. Enabling password authentication for the VTP domain is strongly encouraged for a production environment. Switch A and B are connected to each other through ports `fa0/12` on each switch. That port is configured as a trunk port on both switches.



1. Set up the VLAN trunks on both of the switches. These commands must be run on both switches.

From the privileged exec mode:

```
configure terminal
interface fa0/12
switchport trunk encapsulation dot1q
switchport mode trunk
```

2. Set up VTP on switch A / Catalyst 3560.

From the privileged exec mode:

```
configure terminal
```

```
vtp mode server
vtp domain qostest
vtp file vtpinfo
```

3. Set up VTP on switch B / Catalyst 3500 XL

From the privileged exec mode:

```
configure terminal

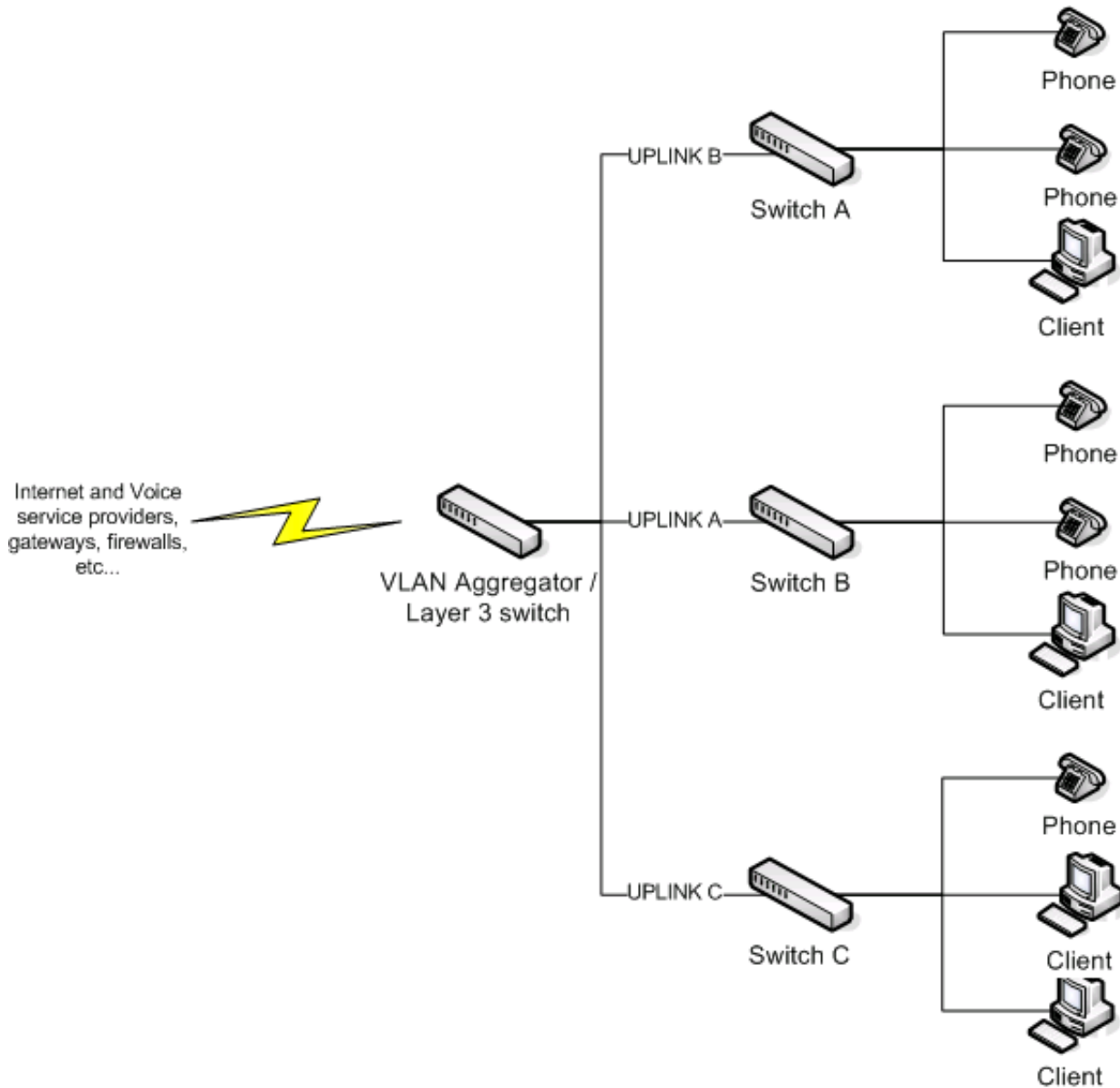
vlan database
vtp client
vtp domain qostest
```

Of course, since both the voice and data VLAN information is set down a single trunk port, network congestion can occur in the trunk links. The next section deals with enabling QoS on the switches.

Larger networks with multiple switches

Using VLANs is useful for separating the voice traffic from the data traffic. This creates some freedom for the voice traffic from network congestion. In a single switch network, since voice traffic does not leave a switch to reach its destination, QoS issues are not experienced. But, in the case of larger LAN configurations, the voice VLAN could span across multiple switches and the bottlenecks could occur at the trunk or uplink ports. Along with the recommended VLAN configuration, the specific uplink interfaces on the switches should have QoS enabled for the voice traffic.

In the scenario pictured in the following diagram, clients from switch A are generating traffic to the clients on switch B. Both switches A and B are up linked to a Layer 3 switch which does the routing. The uplinks between switch A and B are saturated with data traffic which can cause audio problems for calls going from network A to network B.



Note:

Enabling QoS on the physical ports that connect directly to the voice devices and telephones improves the quality of audio as the switch gives priority to the IP packets marked with DSCP when switch queuing is configured.

The required method for Layer 3 switches

This method works and is tested on the Cisco Catalyst 3560. Assume an IP telephone is connected to FastEthernet 0/4. To enable QoS on interface fa0/4 of a switch, you must enter the following commands. Always use DSCP when possible as it can traverse Layer 2. The marking is maintained as the packet moves from Layer 2 to Layer 3.

From the privileged exec mode:

```
configure terminal
mls qos

interface fa0/4
mls qos trust dscp
end
```

Alternative method for older switches (not recommended)

The Cisco Catalyst 3500 XL series and other older switches are Layer 2 switches. They cannot see Layer 3 DSCP markings and, as a result, perform QoS with the old Layer 2 Class of Service (CoS) markings. You can configure these switches to mark all incoming packets from the physical ports where the telephones are connected with a Layer 2 default CoS value. The switch queues the higher priority IP packets with preference over the default untagged data. The following configuration has been tested on a Cisco Catalyst 3500 XL switch with 12 ports. You must make sure that you have a strategy in place to remark Layer 2 CoS to Layer 3 DSCP if you must use a Layer 2 switch.

From the privileged exec mode:

```
configure terminal
interface fa0/4
switchport priority default 5
```

Ingress DSCP mapping (Cisco)

As mentioned previously, Cisco Catalyst switches support trusting using DSCP (DiffServ), IP Precedence, or CoS values on ingress frames. Internally, the switch maps the IP precedence or CoS value to a DSCP value. The following tables illustrate the default mapping tables for CoS-to-DSCP and IP Precedence-to-DSCP, respectively. Based on these mappings, the packets are placed in the appropriate queue.

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

IP Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

The above mappings are configurable. For example, the following command changes the mappings from the default CoS-to-DSCP map to this custom table. This command is automatically run during Cisco's AutoQoS. AutoQoS should not be used. AutoQoS is designed for Cisco products.

From the privileged exec mode:

```
configure terminal
mls qos map cos-dscp 0 8 16 26 32 46 48 56
exit
```

AutoQoS (Cisco)

AutoQoS is a Cisco proprietary method for simplifying QoS configuration. It is not designed for PureConnect products nor any other non-Cisco Voice-over-Internet-Protocol (VoIP) deployment. Depending on how AutoQoS is implemented, it is very likely to result in an incorrect network configuration for a CIC system and is not recommended.

AutoQoS sometimes relies on Network Based Application Recognition (NBAR) to find VoIP traffic, and then apply an appropriate static template. If this is applied prior to deployment of the VoIP system, then the resulting template can be incorrect. Likewise, in cases where the live system is changed post deployment—for example when an IP phone is plugged in to a new switch port—then AutoQoS has no built-in mechanism for compensating. AutoQoS may have already configured the port for a "workstation".

Important!

Currently, the configurations generated by AutoQoS are static. If parameters are modified in these cases, Cisco AutoQoS needs to be disabled and re-enabled to take the [modifications] into consideration for enabling the appropriate QoS parameters.

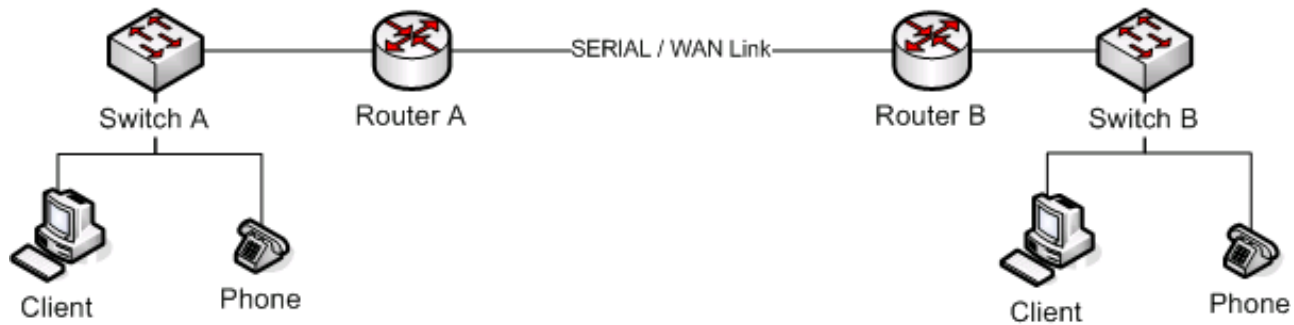
Disable Cisco AutoQoS before changing these configuration parameters and then re-apply it again.

http://www.cisco.com/en/US/technologies/tk543/tk879/technologies_gas0900aecd8020a589_ps6613_Products_Q_and_A_Item.html

WAN QoS (Cisco)

When working with a remote link, bandwidth can be limited and expensive. QoS becomes a requirement in these situations. The following configuration was verified on a Cisco Catalyst 3640 and a Cisco Catalyst 2811 using a serial link configured at 1.5Mbps. In our test, the link was saturated with data traffic and we were unable to have clear telephone conversations. All calls experienced "choppy" audio.

After applying the QoS commands, the excessive data was delay or dropped from the queue on the gateways and the audio became clear. Below is the tested configuration with Cisco IOS version QoS configuration best practices. This example is based on a Cisco Catalyst 2811 and Cisco Catalyst 3640 in the following network scenario:



1. Make class maps to match voice packets and SIP signaling:

Start in privileged exec mode:

```
configure terminal
access-list 101 permit tcp any eq 8060 any
access-list 101 permit tcp any any eq 8060
class-map match-any voice
match ip dscp ef
exit
class-map match-any voip-control
match protocol sip
match access-group 101
exit
```

Note:

Using keywords such as `sip` match only standard IANA port numbers.

2. Make policy-maps and the bandwidth assignments.

Note:

Recommended values are used for bandwidth assignment. Fair-queuing is used for non-voice traffic.

From the global configuration mode:

```
policy-map voip-qos
class voip-control
bandwidth percent 2
class voice
bandwidth percent 70
class class-default
fair-queue
exit
```

3. Associate the policy to the WAN interface. In this example the serial interface is used.

From the global configuration mode:

```
interface serial 1/0
service-policy output voip-qos
```

Many more tweaks are possible and there are many other ways this could be accomplished. This example gives you general guidelines. Shaping and policing may also be required on a WAN connection.

Class Based Weighted Fair Queuing / Low Latency Queue CBWFQ/LLQ

CBWFQ/LLQ is considered the best practice for implementing QoS on WAN networks at the core edge routers. The configuration is based on the assumption that trust boundaries are established on the network infrastructure and traffic is marked at the access layer according to the following template:

Application/Protocol	DSCP Marking	CoS Value
Voice traffic (RTP) PureConnect Notifier	EF	5
Recordings	AF22	1
Bulk transfer traffic (Web/FTP/etc)	AF11 AF12 AF13	1
Transactional applications (Databases etc)	AF21 AF22 AF23	2
Mission critical applications (Core business traffic)	AF31 AF32 AF33	3
Interactive video traffic	AF41 AF42 AF43	4
IP routing (RIP, BGP, OSPF etc)	CS6	6
Streaming video	CS4	4
Voice/Video signaling (SIP, etc)	CS3	3
Network management traffic (SNMP etc)	CS2	2
Scavenger traffic	CS1	1
Unclassified traffic	CS0 (BE)	0

This document concentrates on voice traffic only. As mentioned previously, all PureConnect voice endpoints are capable of marking their packets. Assuming there are no QoS problems on the LAN side, the issue arises on the edge devices where bandwidth is limited when connecting to a service provider or any other edge device of another network.

Reclassification, queuing, and congestion avoidance using CBWFQ/LLQ with a WRED tail drop policy is the best recommended configuration for such a scenario. PureConnect products do not use WRED extensions such as ECN.

The following table outlines the best practices for reclassification, queuing and congestion avoidance:

Application/Protocol	Original DSCP Marking	New DSCP Marking	Drop Policy	Queue used
Voice traffic (RTP) PureConnect Notifier Traffic	EF	EF	Not applied	LLQ
Recordings	AF11	AF22	DSCP-based	CBWFQ
Bulk transfer traffic (Web/FTP/etc)	AF11 AF12 AF13	AF22	DSCP-based	CBWFQ
Transactional applications (Databases etc)	AF21 AF22 AF23	AF32	DSCP-based	CBWFQ
Mission critical applications (Core business traffic)	AF31 AF32 AF33	AF31	DSCP-based	CBWFQ
Interactive video traffic	AF41 AF42 AF43	CS4	DSCP-based	LLQ
IP routing (RIP, BGP, OSPF etc)	CS6	CS6	DSCP-based	CBWFQ
Streaming video	CS4	CS4	DSCP-based	CBWFQ
Voice/Video signaling (SIP, etc)	CS3	CS3	DSCP-based	CBWFQ
Network management traffic (SNMP etc)	CS2	AF21	DSCP-based	CBWFQ
Scavenger traffic	CS1	CS0	DSCP-based	CBWFQ
Unclassified traffic	CS0 (BE)	CS0	DSCP-based	CBWFQ

The following example configuration outlines an implementation on the edge router of the network. The voice traffic is given a LLQ of 25% of the available bandwidth.

1. Make class maps to match network traffic on the edge router.

Start in privileged exec mode:

```
configure terminal
class-map match-any voice
match ip dscp ef
class-map match-any bulk-data
match ip dscp af11
match ip dscp af12
match ip dscp af13
class-map match-any transactional
match ip dscp af21
match ip dscp af22
match ip dscp af23
class-map match-any mission-critical
match ip dscp af31
match ip dscp af32
match ip dscp af33
class-map match-any routing
match ip dscp cs6
class-map match-any voice-signaling
```

```
match ip dscp cs3
match protocol sip
class-map match-any net-management
match ip dscp cs2
exit
```

2. Make policy-maps that will handle the re-classification, queuing, and dropping.

Note:

The class voice-media and voice-signaling together get 25% priority (21+4).

From the global configuration mode:

```
policy-map qos-policy
class voice-
priority percent 21
class bulk-data
bandwidth percent remaining 20
set ip dscp af22
random-detect dscp-based
class transactional
bandwidth percent remaining 15
set ip dscp af32
class mission-critical
bandwidth percent remaining 30
set ip dscp af32
class routing
bandwidth percent remaining 5
set ip dscp cs6
class voice-signaling
priority percent 4
set ip dscp cs3
class net-management
bandwidth percent remaining 5
set ip dscp af21
class class-default
set ip dscp 0
random-detect dscp-based
```

3. Associate the policy to the WAN interface.

In this example, a serial link running at T1 speed is used.

From the global configuration mode:

```
interface serial 1/0
bandwidth 1544
service-policy output qos-policy
```

Call Admission Control (CAC)

CIC has built-in Call Admission Control on the SIP Line. It can be used in situations where you must limit the amount of calls that the system should place. Adding just one more call can degrade the voice quality of all the other active calls when there is not sufficient bandwidth to support it. In the example below, you can see that we have limited the CIC server to have a maximum of 10 calls associated with this SIP line. This setting does not account for bandwidth. The person doing the implementation must plan for the codec type and layer 2 overhead required.

Note:

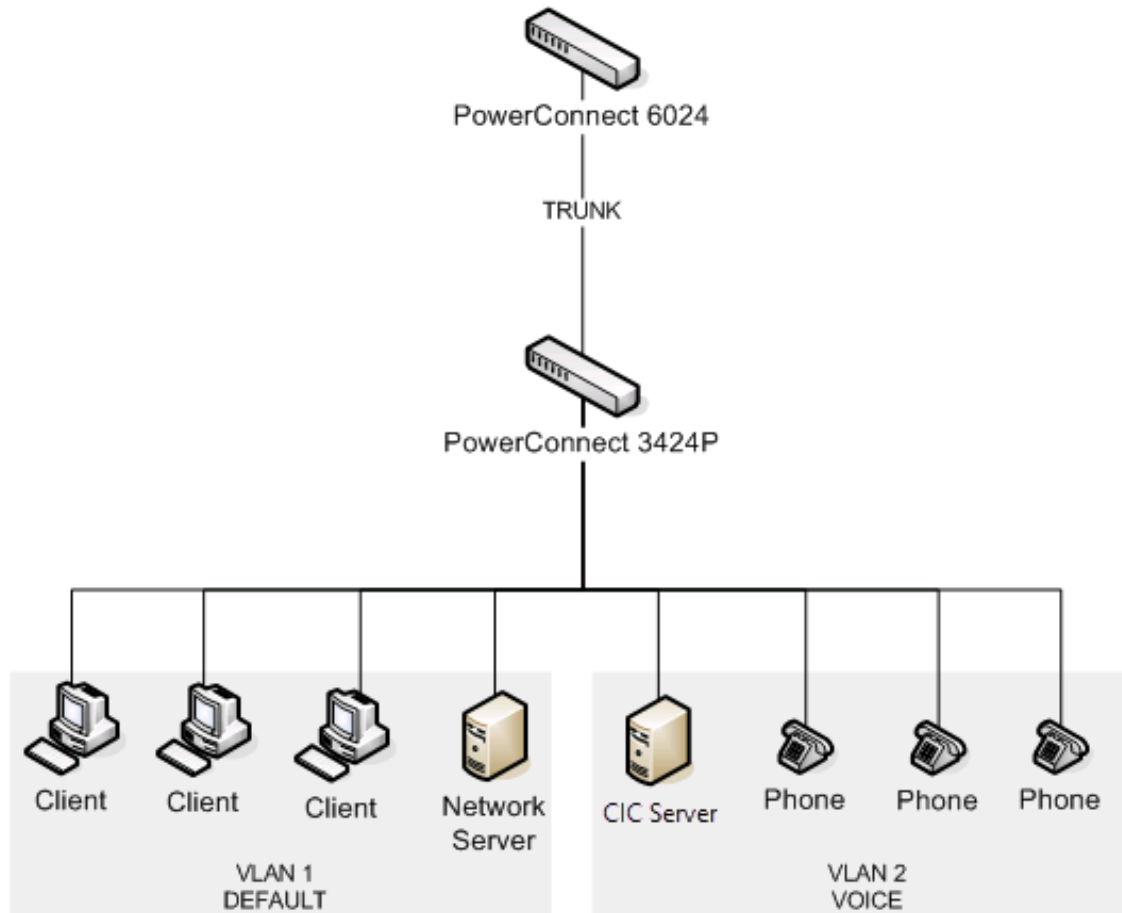
CIC cannot guarantee the bandwidth needed for other activities on the WAN in this configuration.

The screenshot shows the 'Line Configuration - sipLine1' dialog box. The 'SIP Line Configuration' tab is active. The 'Line' section is selected in the left-hand tree view. The 'Active' checkbox is checked. The 'Line Usage' dropdown is set to 'General Purpose'. The 'Domain Name' text box contains 'Clay'. The 'Maximum Number of Calls' section is expanded, showing 'Combined' selected with a value of 10. The 'Enable T.38 Faxing' and 'Enable Fax Detection' checkboxes are also checked. At the bottom, there are navigation arrows, a 'Confirm auto-save' checkbox (checked), and 'OK', 'Cancel', and 'Apply' buttons.

Basic LAN QoS (Dell)

Multiple VLAN with trunks

The following example deals with configuring the two VLAN model using Dell hardware. The Dell PowerConnect 6024 has layer 3 routing capability and is used to route between the VLANs and the Dell PowerConnect 3424P was used for end point connectivity to the clients and the telephones. The 3424P switch was selected because it supports IEEE 802.3AF inline power. The network model used in this following example:



1. Configure VLANs on the 6024 and the 3424P.
On the 6024 – From the privileged exec mode:

```
configure
vlan database
vlan 2
exit
```

On the 3424P – From the privileged exec mode:

```
configure
vlan database
vlan 2
exit
interface range ethernet e1-10
switchport mode access
switchport access vlan 1
exit

interface range ethernet e10-20
switchport mode access
switchport access vlan 2
```

```
exit
```

2. Configure VLAN trunks on both switches.

Run these commands on both devices. The assumption is that port 24 is the uplink/trunk port on both switches.

From the privileged exec mode:

```
configure
interface ethernet g24 //e24 for the 3424P
switchport mode trunk
switch port trunk allow vlan add 1,2
exit
```

3. Configure routing and DHCP forwarding on the 6024.

The assumption is that the DHCP server has an IP address of 10.70.0.5 and exists on VLAN1. On the Dell 6024 switch, VLAN routing is enabled by default and is not necessary to create routes for VLANs that appear directly connected to the switch.

From the privileged exec mode:

```
configure
ip dhcp relay enable
ip dhcp address 10.70.0.5
router rip enable
exit
```

4. Configure QoS on the 3424P.

Unlike the Cisco switches, the QoS trust commands on the Dell switches are applied globally instead of on the individual interfaces.

From the privileged exec mode:

```
configure
qos trust dscp
exit
```

CIC switchover and QoS

CIC enables you to have the switchover feature, which uses one CIC server as a backup should the first CIC server become unresponsive or have a system hardware failure. In this situation, the secondary CIC server can use the PureConnect QoS driver to enable QoS for the ping and the auxiliary connection. To enable this feature, you must set the **Switchover Use Qos For Ping** server parameter to **enabled**. You can also set the following CIC server parameters for more QoS functionality:

- **Switchover Qos DSCP** – When this parameter is enabled, set it to the value in the QoS byte. Differentiated Service Code Point (DSCP) is the six most significant bits of a packet. You can use DSCP to prioritize QoS traffic on switchover.
- **Switchover Ping on Aux Connection** – When this parameter is enabled, set it to **Yes** or **1** to move the TS ping from the main data connection to the auxiliary connection.

Note:

To enable QoS on the ping on the auxiliary connection (not the main connection), you must enable both the **Switchover Ping on Aux Connection** and the **Switchover Use Qos For Ping** parameters. QoS will not be used on ping if only the **Switchover Use Qos For Ping** parameter is enabled.

Telephones

Polycom

Polycom telephones can be provisioned by the CIC server. This feature greatly reduces setup, configuration, and maintenance time. Polycom has chosen (101100) as the default DSCP value for SIP signaling. A future enhancement may allow for this to be modified. They are using the recommended value (101110) EF for RTP. You can modify this in the **Advanced Options** section in the **Managed Phone** configuration.

Legacy Polycom telephones will mark RTP and SIP. The version of the firmware load will determine the default values, but this can be adjusted in the `Sip.cfg` file.

```
<QOS>
<Ethernet>
  <RTP qos.ethernet.rtp.user_priority="5"/>
  <CallControl qos.ethernet.callControl.user_priority="5"/>
  <Other qos.ethernet.other.user_priority="2"/>
</Ethernet>
<IP>
  <RTP qos.ip.rtp.min_delay="1" qos.ip.rtp.max_throughput="1" qos.ip.rtp.max_reliability="0"
qos.ip.rtp.min_cost="0" qos.ip.rtp.precedence="5"/>
  <CallControl qos.ip.callControl.min_delay="1" qos.ip.callControl.max_throughput="0"
qos.ip.callControl.max_reliability="0" qos.ip.callControl.min_cost="0" qos.ip.callControl.precedence="5"/>
</IP>
</QOS>
```

Soft phones

See *CIC Managed IP Phones Administrator's Guide* for details on setting the DSCP for soft phones. The PureConnect QoS driver, by default, marks voice traffic (RTP) with an EF DSCP value. The associated SIP signaling is marked with a CS3 DSCP value. These values are set once the softphone is provisioned through Interaction Administrator.

Fax

The T.30 and T.38 fax protocols are sensitive to network conditions and should always have QoS set. The priority is based on the SIP line setting or station (ToS byte) in Interaction Administrator. Genesys recommends that you change this to EF (See [Marking](#)). Fax stations do not use this setting with TX T.38 packets. When the voice call switches to fax, the time constraints are handled within the fax protocol itself. The fax image is not voice. The fax tones (RTP) are considered to be voice. Telephony Services should not mark the DSF of the packet.

Related standards		
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	http://tools.ietf.org/html/rfc2474
RFC 2475	An Architecture for Differentiated Services	http://tools.ietf.org/html/rfc2475
RFC 2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals	http://tools.ietf.org/html/rfc2833
RFC 3260	New Terminology and Clarifications for Diffserv	http://tools.ietf.org/html/rfc3260
ITU T.38	Procedures for real-time Group 3 facsimile communication over IP networks	http://www.itu.int/rec/T-REC-T.38/e
ITU T.30	Procedures for document facsimile transmission in the general switched telephone network	https://www.itu.int/rec/T-REC-T.30/en

In the case of WAN deployments with business critical applications, it might be necessary to provide higher priority to the T.30 or T.38 traffic. The recommended solution is to classify the fax traffic using the Cisco MQC and assign higher priority as explained in the [WAN QoS](#) section of this document. Using the information below, you can change the default ports for T.30 or T.38 and use an access list or a class map to mark the T.30 or T.38 traffic.

Interaction Gateway

By default, Interaction Gateway sets all voice packets with a DSCP value of (101110) EF. You can also configure the SIP Marking from the default of CS3.

On the **Settings > Media** page of the Interaction Gateway web user interface, select **Set RTP Marking on the Media > Type of Service and Signaling on Spans > Type of Service**. Interaction Gateway exposes these values with the entire TOS Byte, depending on the release level. B8 is the same as EF and 60 is the same as CS3.

Interaction Gateway
EDGE-01X8
Version 4.0 SU2

Status Settings Logout Help

Settings

	Audio	Fax
RTP DSCP Value (hex)	2E (46, 101110) EF	Fax Tone Detection CNG
UDPTL DSCP Value (hex)	2E (46, 101110) EF	Fax Direction Inbound/Outbound
EC Tail Length	Disabled	Fax Max Rate 14400 bps
Disconnect on Idle RTP	No	Fax Redundancy Depth 2
		Fax ECM Yes

Apply Cancel

Call Routes
Channel Groups
Spans
Media
Alerts
Certificates
Access List
Import / Export
Administration



Settings



Call Routes



Channel Groups



Spans



Media



Alerts



Certificates



Access List



Import / Export



Administration

TDM Spans

Span	State	Protocol	Variant	
Tdm1	Ready	ISDN PRI	5ESS	<input type="button" value="Modify"/>
Tdm2	Not Ready	ISDN PRI	5ESS	<input type="button" value="Modify"/>
Tdm3	Ready	ISDN PRI	NI2	<input type="button" value="Modify"/>
Tdm4	Ready	ISDN PRI	NI2	<input type="button" value="Modify"/>

[NFAS Span Groups](#)

SIP Span

Span	State	Protocol	Port	
Sip1 (00-26-FD-A0-05-28)	Ready	UDP	5060	<input type="button" value="Modify"/>
	Ready	TCP	5060	
	Ready	TLS	5061	

[Cause Codes](#)

Opening client ports

CIC client applications also need a way to contact the CIC server from the accounting side of the PIX. You can map the ports that are needed through the firewall. Those ports depend on the applications that are deployed.

CIC application	Port
CIC clients	TCP 3952
Interaction Fax	TCP 3952
Interaction Voicemail	TCP 3952
Interaction Recorder Client	TCP 5597
Interaction Supervisor	TCP 5597
Interaction Designer	TCP 5597
Interaction Attendant	TCP 5597
Interaction Recorder Client	TCP 3952
SIP Soft Phone	TCP 3952

Interaction Media Server

For more information about Interaction Media Server and QoS, see *Interaction Media Server Technical Reference*.

References and further reading

Enterprise QoS Solution Reference Network Design Guide (SRND)

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/Enterprise_QoS_SRND.pdf

Cisco QoS support information

http://www.cisco.com/en/US/tech/tk543/tk759/tsd_technology_support_protocol_home.html

Cisco QoS Exam Certification Guide

Authors: Odom, Cavanaugh

Publisher: Cisco Press

CCNP Switching Study Guide

Authors: Lammle, Quinn

Publisher: Sybex

Dell PowerConnect support and white pages

<http://www.dell.com>

Appendix A: OpenSSL Copyright

NOTICE

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

Copyright © 1998-2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)."
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e., this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Change log

Date	Changes
24-October-2011	Initial release for Interaction Center 4.0
6-March-2012	IC-93044 - QoS functionality for SAPI TTS should be optional
30-November-2012	Remove erroneous content regarding VLAN tagging capability
6-August-2013	<ul style="list-style-type: none">Removed references to obsolete productsUpdated screen shotsUpdated references to external standards and resourcesIC-107632 - Warning should prompt when network driver gets reset during an install
5-September-2014	Updated documentation to reflect changes required in the transition from version 4.0 SU# to CIC 2015 R1, such as updates to product version numbers, system requirements, installation procedures, references to Interactive Intelligence Product Information site URLs, and copyright and trademark information.
13-April-2015	<ul style="list-style-type: none">Update "Copyright and Trademark Information" pageModify formatting to new corporate standards
13-October-2015	<ul style="list-style-type: none">Updated cover page with new corporate brandingUpdated "Copyright and Trademark Information" pageReplace rebranded graphics displaying example interfacesMinor edits
2-January-2017	<ul style="list-style-type: none">Updated "Copyright and trademark information" pageIC-141374 - Modify QoS document to include Notifier QoS traffic with media server - Updated instances of Notifier DSCP marking from AF41 to EFIC-141949 - Tables need port ranges - Removed instances referencing Cisco IP telephones that are no longer supported. Updated RTP port usage topic. Added cross-reference to CIC Port Maps and Data Flow Diagrams Technical Reference.
21-September-2017	Rebranded to Genesys.
6-April-2018	Updated document format.

Copyright and Trademark Information

Interactive Intelligence, Interactive Intelligence Customer Interaction Center, Interaction Administrator, Interaction Attendant, Interaction Client, Interaction Designer, Interaction Tracker, Interaction Recorder, Interaction Mobile Office, Interaction Center Platform, Interaction Monitor, Interaction Optimizer, and the "Spirograph" logo design are registered trademarks of Genesys Telecommunications Laboratories, Inc. *Customer Interaction Center, EIC, Interaction Fax Viewer, Interaction Server, ION, Interaction Voicemail Player, Interactive Update, Interaction Supervisor, Interaction Migrator, and Interaction Screen Recorder* are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©1997-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Interaction Dialer and Interaction Scripter are registered trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2000-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Messaging Interaction Center and MIC are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2001-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Interaction Director is a registered trademark of Genesys Telecommunications Laboratories, Inc. *e-FAQ Knowledge Manager and Interaction Marquee* are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2002-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Interaction Conference is a trademark of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2004-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Interaction SIP Proxy and Interaction EasyScripter are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2005-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Interaction Gateway is a registered trademark of Genesys Telecommunications Laboratories, Inc. *Interaction Media Server* is a trademark of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2006-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Interaction Desktop is a trademark of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2007-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Interaction Process Automation, Deliberately Innovative, Interaction Feedback, and Interaction SIP Station are registered trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2009-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Interaction Analyzer is a registered trademark of Genesys Telecommunications Laboratories, Inc. *Interaction Web Portal and IPA* are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2010-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Spotability is a trademark of Genesys Telecommunications Laboratories, Inc. ©2011-2018. All rights reserved.

Interaction Edge, CaaS Quick Spin, Interactive Intelligence Marketplace, Interaction SIP Bridge, and Interaction Mobilizer are registered trademarks of Genesys Telecommunications Laboratories, Inc. *Interactive Intelligence Communications as a ServiceSM* and *Interactive Intelligence CaaSSM* are trademarks or service marks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2012-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Interaction Speech Recognition and Interaction Quality Manager are registered trademarks of Genesys Telecommunications Laboratories, Inc. *Bay Bridge Decisions and Interaction Script Builder* are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2013-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Interaction Collector is a registered trademark of Genesys Telecommunications Laboratories, Inc. *Interaction Decisions* is a trademark of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2013-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Interactive Intelligence Bridge Server and Interaction Connect are trademarks of Genesys Telecommunications Laboratories, Inc. The foregoing products are ©2014-2018 Genesys Telecommunications Laboratories, Inc. All rights reserved.

The veryPDF product is ©2000-2018 veryPDF, Inc. All rights reserved.

This product includes software licensed under the Common Development and Distribution License (6/24/2009). We hereby agree to indemnify the Initial Developer and every Contributor of the software licensed under the Common Development and Distribution License (6/24/2009) for any liability incurred by the Initial Developer or such Contributor as a result of any such terms we offer. The source code for the included software may be found at <http://wpflocalization.codeplex.com>.

A database is incorporated in this software which is derived from a database licensed from Hexasoft Development Sdn. Bhd. ("HDSB"). All software and technologies used by HDSB are the properties of HDSB or its software suppliers and are protected by Malaysian and international copyright laws. No warranty is provided that the Databases are free of defects, or fit for a particular purpose. HDSB shall not be liable for any damages suffered by the Licensee or any third party resulting from use of the Databases.

Other brand and/or product names referenced in this document are the trademarks or registered trademarks of their respective companies.

DISCLAIMER

GENESYS TELECOMMUNICATIONS LABORATORIES (GENESYS) HAS NO RESPONSIBILITY UNDER WARRANTY, INDEMNIFICATION OR OTHERWISE, FOR MODIFICATION OR CUSTOMIZATION OF ANY GENESYS SOFTWARE BY GENESYS, CUSTOMER OR ANY THIRD PARTY EVEN IF SUCH CUSTOMIZATION AND/OR MODIFICATION IS DONE USING GENESYS TOOLS, TRAINING OR METHODS DOCUMENTED BY GENESYS.

Genesys Telecommunications Laboratories, Inc.
2001 Junipero Serra Boulevard
Daly City, CA 94014
Telephone/Fax (844) 274-5992
www.genesys.com