OVERVIEW

System survivability is is achived in different ways for the VIPedge systems and IPedge systems.

VIPedge

With the VIPedge solution running in the cloud on virtual servers, survivability is built in. Survivability is provided at the data center, server, and WAN level. The data center is designed for survivability with multiple ISP connections, a building with a building design and even on-site power generators. For more details refer to the VIPedge General Description. For the servers that are running the VIPedge application, there are stand by servers ready to take over when a failure is detected.

For survivability of WAN network outages that a customer's site may experience there is the Follow-me feature of VIPedge. This allows customers to receive their VIPedge calls on their cell phone even when they are experiencing a network outage.

IPedge

The Toshiba IPedge system achieves survivability by combining technologies from IPedge Net multi-route programming, IP Mobility and SIP Trunking. By combining these technologies, the Toshiba IP telephones are able to survive by automatically connecting to a secondary IPedge system and still maintain station-to-station calling, inter-node calling, outbound dialing, and access to voicemail resources and Call Manager. Incoming call routing can be achieved by having the service provider manually re-route all the incoming calls to the secondary IPedge system. The secondary must be an EC or EM server.

The IPT will fail-over to the Secondary server by sending a Register message to the Secondary server. If the IPT is on a peer-to-peer call when the failure occurs the fail-over will occur after the call is finished.

When the Primary IPedge server is back on line the IPT will register to the Primary server (fail-back) when IPT has no active call and is not in use by the station user.

Because the IP telephones, SoftIPT, and Call Manager will be re-registering to the secondary backup IPedge system, there must be enough endpoint licenses and hardware resources to support the surviving IP telephones on the secondary IPedge system. The following is the Survivability overview.

Function	Overview
Automatic fail-over	1. **IPT Power-on / IPT reboot** At the beginning, IPT tries the primary server connection for a certain period of time. When IPT cannot connect to the primary server, IPT tries the secondary server connection automatically.[1] 2. **When IPT detects Keep-alive failure** When IPT detects Keep-alive failure, IPT changes the connection into the secondary server.[2]
Automatic fail-back	While an IPT connects to the non-primary server, the IPT continues to check the status of the primary server. The IPT changes the server connection back to the primary server automatically when the primary server connection is enabled and the IPT is not in use and IPT has no active call.

Function	Overview
Speech Path Survivability	The IPT keeps the speech path connection even when the IPT detects Keep-alive failure.[2] The IPT executes fail-over and fail-back without rebooting.
Telephony Service Survivability	The IPedge detects the survivability terminal's fail-over and fail-back status and selects the appropriate destination server without complex system data programming or user setting.

1. If the IPT connects to the secondary (fail-over) server and the user wishes to register to the primary use one of the following:

   Remove then, apply IPT power to cause an IPT reboot.

   Disconnect the LAN cable from the IPT, wait 30 seconds then, connect the cable to cause a keep-alive failure.

   Manually reset the IPT (9-line LCD IPTs only)

2. Keep-alive failure is no keep alive packet from the server for 20 seconds.

License The survivability feature requires an endpoint license for each survivable IPT in the primary server. A survivability license is required for each survivable IPT in the secondary server that IPT will 'fail-over' to. The licenses are:

I-CP-USR-SUR-EP

I-CP-USR-SUR-EC

I-CP-USR-SUR-EM

Important! The secondary IPedge server, the server an IPT will ‘fail-over’ to, cannot be an EP server. Call Manager, SoftIPT, and IPTs can only fail-over to an EC or EM server.

Upgrade From R1.0

CAUTION! Basic Survivability programming (an IPedge R1.0 feature) must be removed before Survivability (R1.1 and later) can be configured.

Basic Survivability programming must be removed before the system is upgraded and setting up Survivability. Refer to the IPedge Install manual for detailed information about updating your IPedge system.

Survivability

Survivability is based on the capability of the IPT to send Register messages to two IPedge servers. This makes it possible to provide telephone service in the event that an IPedge server or the link to that server goes down.

The IPT can register to the backup survivability server (Secondary Server) automatically when sever goes down or the linkage between server and IPT is disconnected. Survivability is provided by the following.

- IPT speech path Survivability — If the user is on a peer-to-peer call when the failure occurs the fail-over will occur after the call is finished.
- Fail-over — The IPT can fail-over to the Secondary server by sending a Register message to the Secondary server.
- Fail-back — When the primary server becomes operational, the IPT phones will automatically re-register to the primary) when each IPT has no active call and is not in use by the station user.
- Telephony Service Survivability — The IPedge system is survivability-aware and will automatically selects the appropriate destination server according to IPT Fail-over or Fail back status without complex system data programming or user setting.

Enterprise Manager Survivability

In a multi-node system Enterprise Manager Survivability allows a member server to become the primary server and Enterprise Manager on that server to take the place of the failed or off line primary server.

Only IPedge EC and EM systems can be primary servers. The server configured to be the redundant or fail-over primary server must also be an EC or EM server.

Call Manager Survivability

The survivability feature enables Call Manager to connect to a member server when the primary server is down.

Both VoIP Option/SoftIPT and IPT relies on its connections to the Call Processing module to determine whether or not to switch over, and Call Manager relies on the connection to Net Server to determine whether or not to switch over.

Note: If a component failure such as Net Server module or Call Processing module shutdown takes place instead of the complete server failure, Call Manager and the phone may connect to different IPedge systems. In that case, the user can manually override the survivability to reconnect to the same IPedge system.

Call Manager survivability is supported for the IPedge built-in Net Server. ACD or Unifier based Net Server is not supported.

Messaging Survivability

The IPedge Messaging application can be licensed and configured with a feature called Direct Cluster Networking (DCN). DCN allows the joining of two or more IPedge systems (individually referred to as a Node) into a cluster. These clusters act in unison to maintain the integrity of the messaging database of the entire network. Each node that is configured into the cluster has a copy of the database of the other participating nodes. If one node fails, then when IPedge telephones register into another IPedge system, that is a node participant, all of that user’s greetings and messages are available.

Nodes can be geographically distributed in various configurations. Each node contains the complete database for the entire cluster, and the Messaging application residing on each node only uses the local copy of the database. Each node is identified by a NODE ID. In addition all files, including system greetings, user greetings and messages can be replicated to all nodes (standard cluster) or replicated to a designated subset of nodes (hybrid cluster), depending on cluster size and network capability. Note that all of the nodes in a cluster must be running the same version of the IPedge system software.

Survivability

IPT Survivability operation is automatic. There is no operation required by the station user.

Fail-over

If the primary server connection become unavailable a message will appear for five seconds on the LCD of the IPT (Primary Server Unavailable).

The IPT will attempt to register to the secondary server. The IPT will display: Registering to Secondary Server.

After registering the TCP connection is established: Connecting to Secondary Server. If an error occurs during either of these two steps an error message will be displayed on the third line of the IPT display.

When the IPT is connected to the secondary server the normal DN, Date and Time display is shown. An exclamation mark (!) in the lower right corner of the IPT display indicates connection to the secondary server.

Four-line LCD example shown below.

																	N	O	.	2	0	2	5
A	U	G		0	9		T	U	E	S	D	A	Y						1	0	:	4	6
C	F	-	B	N	A		2	0	2	5	-	3	0	0	0								
	D	I	R																				!

Fail-back

When the primary server connection becomes available a message will appear for five seconds on the LCD of the IPT (Primary Server Available).

The IPT will attempt to register to the primary server. The IPT will display: Registering to Primary Server.

After registering the TCP connection is established: Connecting to Primary Server. If an error occurs during either of these two steps an error message will be displayed on the third line of the IPT display.

When the IPT is connected to the primary server the normal DN, Date and Time display is shown. When the connection to the primary server is re-established the exclamation mark will disappear.

																	N	O	.	2	0	2	5
A	U	G		0	9		T	U	E	S	D	A	Y						1	0	:	4	8
C	F	-	B	N	A		2	0	2	5	-	3	0	0	0								
	D	I	R																				

PROGRAMMING

Survivability requires that the Survivable IPTs be registered in both the primary and secondary survivability IPedge servers.

License

The survivability feature requires an endpoint license for each survivable IPT in the primary server. A survivability license is required for each survivable IPT in the secondary server that IPT will 'fail-over' to. The licenses are:

I-CP-USR-SUR-EP

I-CP-USR-SUR-EC

I-CP-USR-SUR-EM

In order to use the Call Manager survivability feature, the following license is required in the backup node. If the license is not present in the backup node, the Call Manager will not switch to the back up node. In addition, the paired IPT and SoftIPT require the survivability user license on the backup node.

Part number Description:

I-CM-STD1-SUR Call Manager Standard survivability license

I-CM-1-SUR Call Manager Advanced survivability license

I-CM-V1-SUR Call Manager VoIP option survivability license

Upgrade From R1.0

Basic Survivability programming must be removed before the system is upgraded and Survivability is set up.

Basic Survivability programming must be removed before Survivability can be configured.

Survivable Stations

This is automatically programmed in the Station Assignment and Station Survivability program steps. The primary server must have licenses for the IPT stations, the secondary servers must have enough survivability licenses for the stations that can fail-over.

Station Assignment

1. Select **Station > Station Assignment**.
2. Check the Station to be programmed.
3. Click on **Edit** icon.
4. Check-mark the **Survival Station** check box.
5. Select the **Survivability Secondary Server** (the fail-over server) from the pull-down list.
6. Click on **Save** icon.

The station will be created in the secondary server automatically. If the DN already exists in the secondary server an error message will be displayed. The station will not be created on the primary server.

Survivability

1. Select **Station > Survivability**.
2. Select the server to display. The list of survivable stations on the selected server will display.
3. Select the Primary/Secondary Destinations tab. The list of possible secondary servers for the selected primary will display.
4. Select the Configuration Conflicts tab.
5. Select the Configuration Conflict Category. Click on the Detect Conflicts icon. Any conflicts detected will be displayed.

Net Server

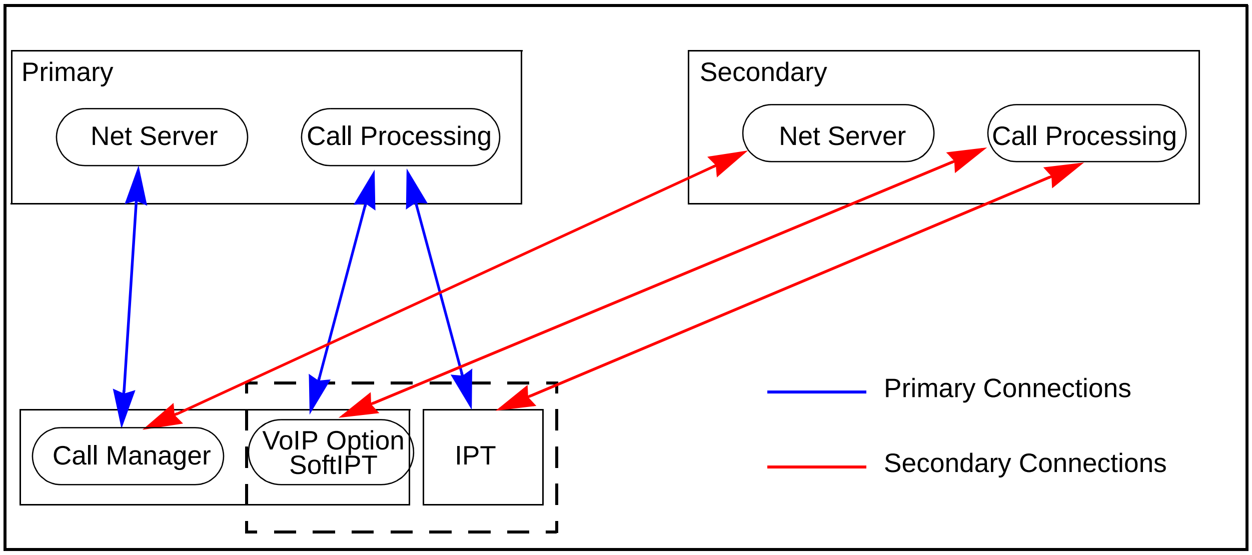
For Call Manager Survivability, ensure that Net Server recognizes the survivable stations.

1. Select **Applications > Net Server > Level 2 Devices**.
2. Click the Synch Table with Switch button
3. Verify the Primary & Secondary Server IP addresses.

CALL MANAGER SURVIVABILITY

Survivability is support for Call Manager with the built-in VoIP option or paired with either a SoftIPT or an IPT. When the IPedge system goes down or the network connection to the IPedge is down, the phone and the Call Manager tries to connect to the secondary server.

Call Manager survivability is supported for the IPedge built-in Net Server. ACD or Unifier based Net Server is not supported.



MESSAGING SURVIVABILITY

IPedge Messaging supports voice mail survivability using a feature called Direct Cluster Networking (DCN). DCN allows joining the Messaging application of two or more IPedge systems (individually referred to as Nodes) into a cluster. This is covered in the Messaging Survivability feature description. Also, refer to the IPedge Messaging Manual.

ENTERPRISE MANAGER SURVIVABILITY

The IPedge system running R1.2 and later software supports Enterprise Manager Survivability. No additional licenses are required. Enterprise Manager Survivability allows an Enterprise Manager member server to take the place of the primary server should the primary server go off-line. Figure 1 shows three IPedge servers in a network. One server is the primary, the other two are member servers. The figure shows how the administration database is configured.

Only IPedge EC and EM systems can be primary servers. The server configured to be the redundant or fail-over primary server must be an EC or EM server.

The primary server database contains the following data:

- Enterprise (Admin users, Permissions, Server tables, etc.)
- EMPA (Enterprise Manager Personal Administration) user data, for example user role, password and preferences like email, GUI theme, locale, etc
- IPedge Call Processing data for each server attached in the network

The member server administration data (Enterprise Manager database) is not used as shown in Figure 1.

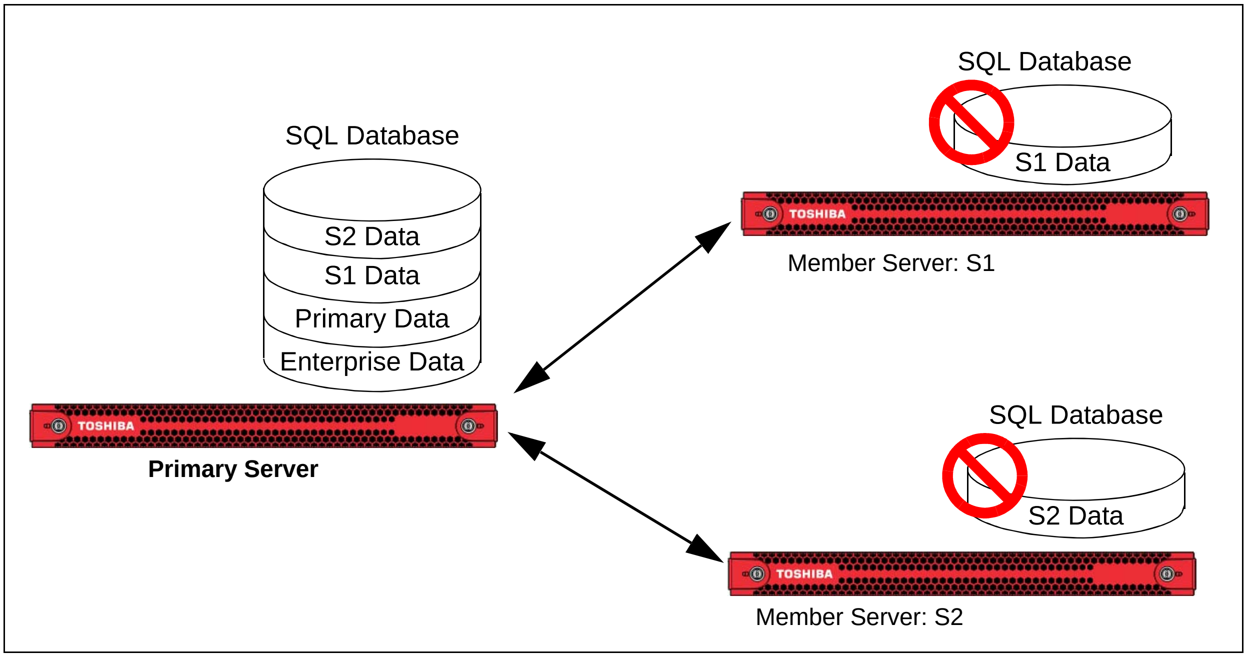


Figure 1 - Enterprise Manager Survivability

To administer the enterprise system shown in Figure 1, the system administrator must login to the primary server. Similarly, EMPA users can only login to the primary server to perform changes to their telephone(s). If a user attempts to login to a member server, Enterprise Manager will block the attempt and instead display an information page requesting user to visit the primary server. If the primary server fails, administrators and EMPA users will not be able to login to the system until the primary server is back online.

Redundant Server Operation

To allow one secondary server to ‘take over’ the administration functions when the primary fails Enterprise Manager Survivability works as follows:

- One server can be selected and designated as a “Redundant server.” This server must be an attached member server.
- The redundant server contains a copy of the Enterprise Manager database that exists on the Primary server. Refer to Figure 2.
- The redundant server database must be kept in synch with the primary server. This means that administration changes (data changes) on the primary server must also be reflected on the same database version existing on the redundant server.
- In case there is a problem with the primary server, the redundant server role will be changed to become the primary server
- Under normal operations the redundant server behaves exactly like a member server, users cannot perform changes by logging into the redundant server before switching the server’s role.

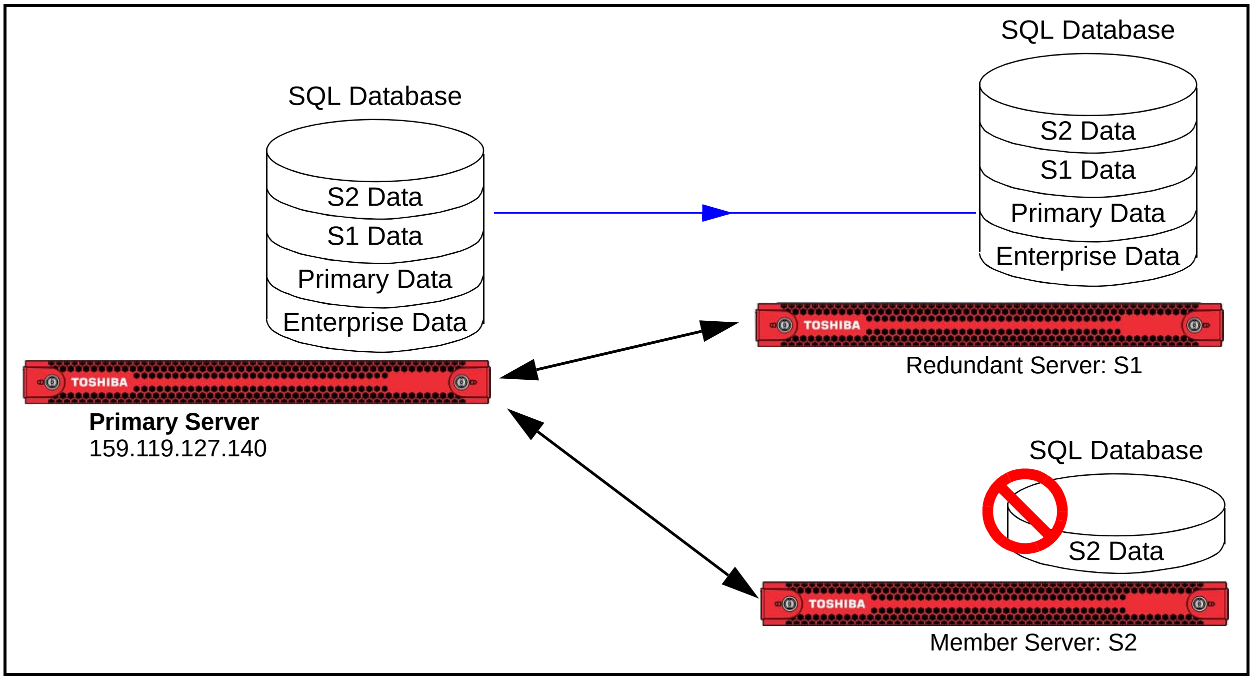


Figure 2 - Switching Servers

Switching from a Member Server to a Primary Server

When a Redundant server is switched to become a Primary, the Administrator must make sure that the old primary server is either configured to be a standalone server or a member. This will ensure that when the old primary is back online and users attempt configuration changes, these changes will be rejected automatically since member servers are no longer assigned to it.

IMPLEMENTATION

Maintaining database integrity and keeping it synchronized between the Primary and the Redundant servers is a key factor in the feature implementation. The SQL replication service will replicate the IPedge call processing database only, other application databases are not replicated. This replication and synchronization is automatic.

CONFIGURING REDUNDANT SERVER

The system allows configuring one redundant server. If the Redundant server is to be moved to another member server, the administrator must remove the configuration from the redundant server first then, configure another server.

Note: Configuring Redundancy causes SQL to restart therefore all call processing will stop in the primary and redundant servers until SQL has restarted. This process will take one to two minutes times the total number of IPedge servers.

Enterprise Manager will test for the following conditions when configuring redundancy

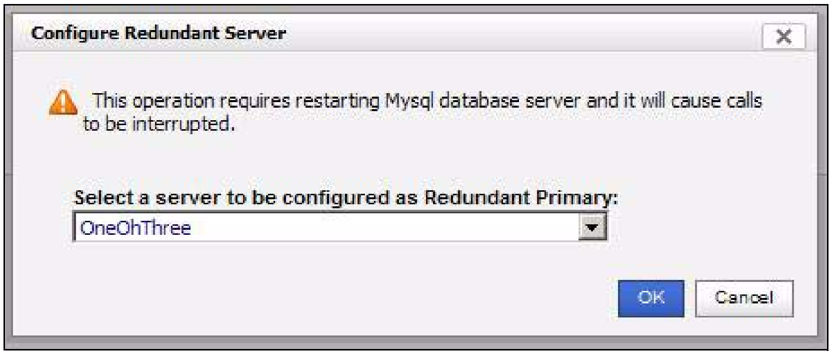
- The Member server selected to be Redundant must be attached and synchronized. Member server must not be hijacked (Enterprise Manager in Primary server thinks it is attached while the member server is detached locally by an administrator)
- The Member server must not be performing Backup or Restore operation
- The Member server must not be performing Program update/rollback operation

If any condition is met, redundancy configuration will fail with the proper message.

Procedure

Procedure to setup a Redundant Primary server.

1. Login to Enterprise Manager.
2. Select **Maintenance > Enterprise Manager Redundancy**.
3. Click on the **Configure Redundant Server** icon.
4. In the dialog box select the member server you want to make the redundant server. Click on **OK**.



Configure Redundant Server

This operation requires restarting Mysql database server and it will cause calls to be interrupted.

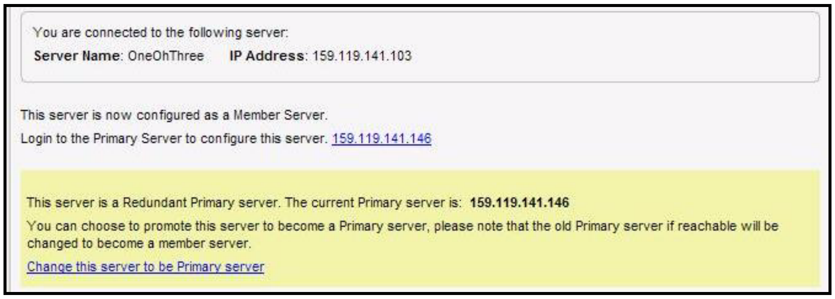
Select a server to be configured as Redundant Primary: OneOhThree

SWITCHING SERVERS

Switching the Redundant Server to become a Primary server must be done manually.

The following are the steps taken to switch the server role.

1. Log into the Redundant server.
2. Click on the link: **Change this server to be the Primary server**.



You are connected to the following server:
Server Name: OneOhThree **IP Address**: 159.119.141.103

This server is now configured as a Member Server.
Login to the Primary Server to configure this server. 159.119.141.146

This server is a Redundant Primary server. The current Primary server is: **159.119.141.146**
You can choose to promote this server to become a Primary server, please note that the old Primary server if reachable will be changed to become a member server.
Change this server to be Primary server

3. Click on **OK** in the dialog box to change the server.

4. The Redundant server will become the Primary server. It will update all of the other members. If the original primary server is online it will be changed into a member.
5. Wait for the Successfully Completed dialog box. Click on **OK**.

Note: At this time Enterprise Manager Redundancy is no longer on.

When a Redundant server is switched to become a Primary, the administrator must make sure that the old Primary is either a member, configure it to be a standalone by deleting server entries, or take the server off-line.

Bring the Failed Server Online

To bring the failed server online:

1. If the restored system was the Primary login to Enterprise Manager on the restored server. Enterprise Manager select **Administration > Enterprise > Servers**. Delete all of the servers in the displayed list.
2. Configure the server as a member. Enter the IP address of the primary. Refer to Chapter 4 of the IPedge Install manual.
3. Login to the Primary server, make the restored server a member of the enterprise with the current primary. Refer to Chapter 4 of the IPedge Install manual.
4. After the database has been synchronized, select **Maintenance > Enterprise Manager Redundancy**.
5. Click on the **Configure Redundant Server** icon.
6. If desired you can now switch the server just brought online to be the Primary.

   Important! Remember to configure a new redundant server.

DELETING REDUNDANT SERVER CONFIGURATION

Use this procedure to remove the Redundant Enterprise Manager server assignment.

1. Login to the Primary server, select **Maintenance > Enterprise Manager Redundancy**.
2. Click on the **Delete Redundant Server Configuration**.
3. In the dialog box warning about SQL database server restart click on **OK**.

Note: Removing Redundancy requires SQL to restart therefore all call processing will stop in the primary and redundant servers until SQL has restarted. This process will take one to two minutes times the total number of IPedge servers.

4. Click on **OK** in the Successfully Completed dialog box.

FEATURE INTERACTION

Backup and Restore

Since Enterprise Manager maintains its data on the primary server, backup and restore is expected to operate as normal, any changes to the Primary data will be replicated to the redundant server.

Program Update

Replication requires both Enterprise Manager databases to be the same, which means it is expected that both Primary and Redundant should have the same Enterprise Manager software version running.

Messaging (Voice Mail)

For information on Messaging survivability refer to Voice Mail Survivability below.

VOICE MAIL SURVIVABILITY WITH MULTI-SITE DIRECT CLUSTER NETWORKING (DCN)

IPedge Messaging supports voice mail survivability by using a feature called Direct Cluster Networking (DCN). DCN allows joining the Messaging application of two or more IPedge systems (individually referred to as Nodes) into a cluster. These clusters act in unison to maintain the integrity of the messaging database of the entire network. Each node configured into the cluster has a copy of the database of the other participating nodes. If one node fails all of the user’s greetings and messages are available when the IPedge telephones register into another node.

Nodes can be geographically distributed in various configurations. Each node contains the complete database for the entire cluster, and the Messaging application residing on each node only uses the local copy of the database. Each node is identified by a NODE ID. In addition all files, including system greetings, user greetings and messages can be replicated to all nodes (standard cluster) or replicated to a designated subset of nodes (hybrid cluster), depending on cluster size and network capability.

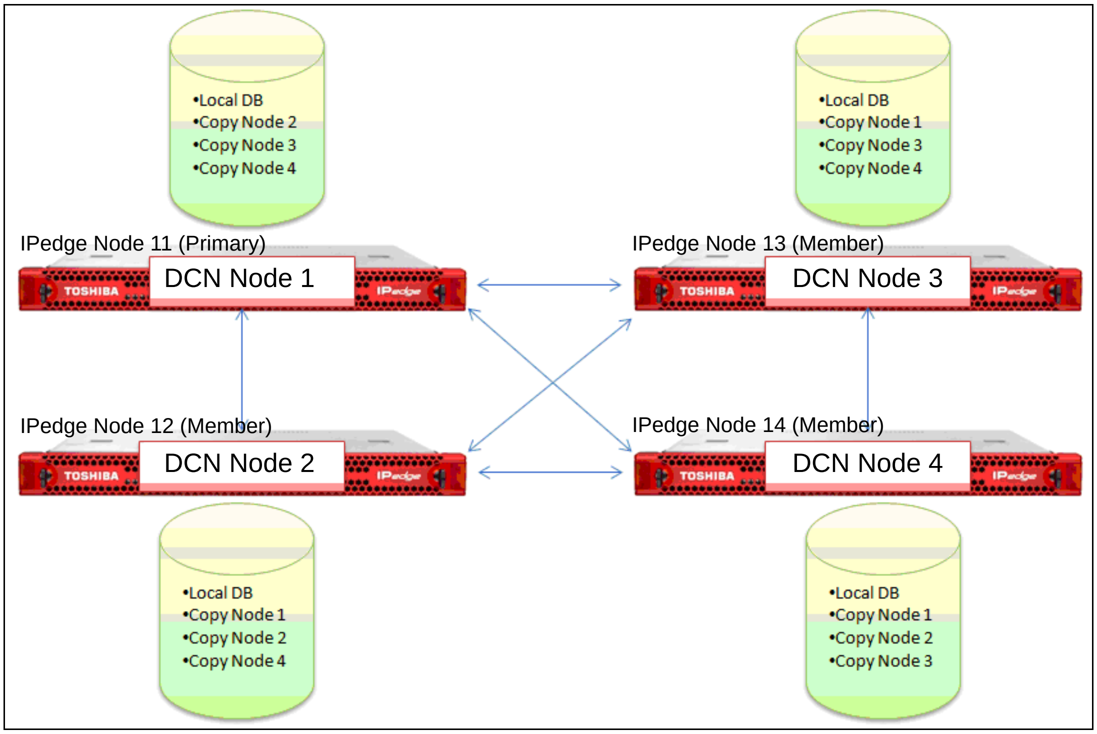


Figure 3 - Four Node System Configuration

Figure 3 illustrates how the DCN stores and synchronizes the clusters database in all systems that are licensed for DCN. Should one node fail, one of the other nodes can be used as a backup mailbox for the surviving IPedge telephones.

There is no license required for the mailboxes replicated in the other nodes.

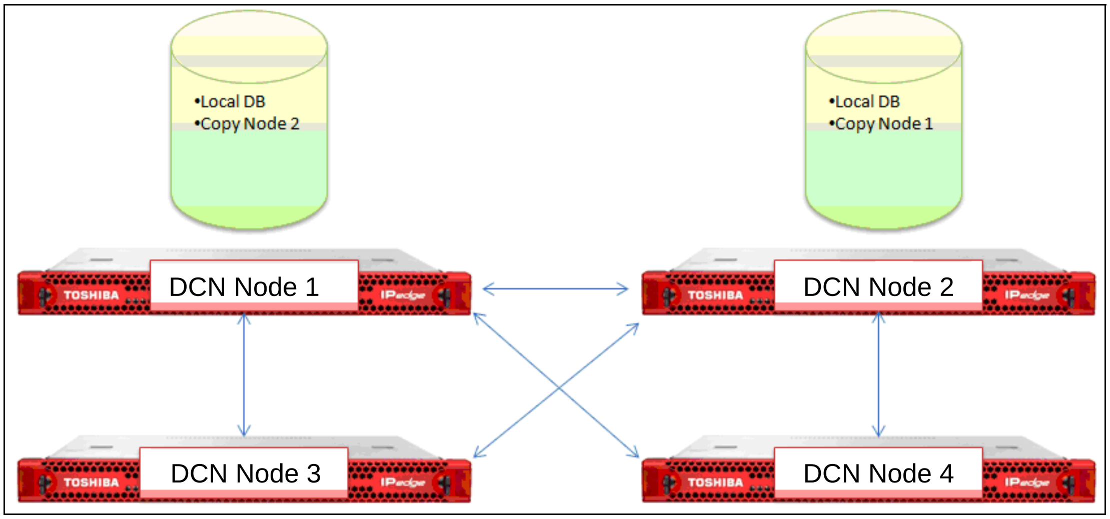


Figure 4 - DCN With Centralized Messaging

Figure 4 shows how DCN can work within a centralized voice mail configuration. Should IPedge Node 11 (DCN node 1) fail, Node 13 can use the replicated mailboxes on Node 12.

FUNCTIONAL CONSIDERATIONS

Although DCN provides a robust voice mail survivability solution, there are some functional considerations that need to be understood and communicated to customer users.

1. If a telephone has a Message Waiting Indicator (MWI) illuminated and the system that supports that telephone should fail the MWI will not be reinstated until another new message is received. The telephone survives over to another system that is in the cluster and has its mailbox intact, but the MW light will not light until a new message is received.
2. The voice mail hunt group pilot number should be the same on the different nodes. If the voice mail hunt group pilot number is different on the different nodes incorrect voice mail forwarding after a node failure will occur. For example, station 201 on IPedge Node 11 (DCN Node 1) is set to system call forward to voicemail hunt group pilot 300. The DNs on IPedge Node 12 (DCN Node 2) are set to system call forward to voicemail hunt group pilot 400. If IPedge Node 11 fails and station 201 re-registers with IPedge Node 12, station 201 will not properly forward to voicemail when a call is presented to it.

Note: The Messaging application must be running on every IPedge system that will run DCN. All of the nodes in a cluster must be running the same version of the IPedge system software.

DCN CONFIGURATION

When setting up a cluster, the original database from one system will be duplicated into the other nodes. Use the Messaging application administrator Site Parameters > Cluster page to define the nodes and copy the database from the original system to the additional nodes. The programming values only become visible after the system is licensed for DCN. The Database includes all information to be replicated (tables, voice messages, greetings, and names).

Note: The DCN Node ID of the IPedge systems in the cluster must start with 1 and be sequential. The IPedge Node ID is not related to the DCN Node ID. The DCN Node ID does not affect the IPedge dialing plan or flexible access codes. Refer to Figure 3.

OPEN NETWORK PORTS

The network communication between nodes to support DCN require the following ports to be open in any firewalls between the nodes.

- 22 TCP (SSH) - It can be disabled during normal runtime. Port 22 must be open to:
  - Create a cluster
  - Add or Remove a node
  - Check Cluster Integrity
  - Upgrade software
- 3306 TCP (SQL)

Important System Requirements

1. Prior to setting up the cluster, verify that each node is licensed for DCN. In Enterprise Manager select **Maintenance > Licensing > License Control**.
2. Verify that license I-MSG-DCN-xx (xx = system type) is present.

Configure the IPedge Nodes

This procedure is used to setup DCN in the Messaging application in every node.

1. In Enterprise Manager select **Application > Webmin**.
2. In Webmin select **System > Startup and Shutdown**.
   - **t3esync**: Only one node should be running esync, set **Yes** only on that node. Set all other nodes to No. (Check-mark then, click on Disable Now and on boot up.")
   - **t3msync**: Only one node should be running msync, set **Yes** only on that node. Set all other nodes to No. (Check-mark then, click on Disable Now and on boot up.")
   - **sshd**: Check-mark then, Check-mark then, click on Start now and on boot up.
3. Select **Application > Messaging**.
4. In the Messaging interface select **Registry > Parameters** Check-mark the box for **DB Sync**, enter a value of 1 to enable then, enter the DCN Node number for the system node you are programming.
5. Scroll down to check-mark **Node Number** then, enter the Node ID number of this node.
6. Click on **Save**.
7. Select **Mailboxes > Properties**.
8. In the **Home Node** field enter the Node ID of this node.
9. Select **Utilities > Database Maintenance**. Scroll down to **House Keeping**. Set the House Keeping Time.
   - Day = **Daily**
   - Time = Select a time of low system activity.
   - Purge Reports = **3**.

   Note: Ensure that the database housekeeping start times are about one hour apart. The schedule should not overlap the regular IPedge system backup the occurs everyday around 0300.
10. Save then, exit the Messaging application.
11. Repeat for each IPedge node.

Create a Cluster

The cluster is setup in the IPedge Primary node only.

First Node

1. In Enterprise Manager select **Applications > Messaging**.
2. Select the Primary node.
3. in the Messaging menu select **Site Parameters > Cluster**.

4. Click on the **Start Cluster Wizard** icon.
5. In the Node ID field enter the DCN node number. The first node is always 1.
6. In the IP Address field enter the IP address of the node you identified in step 5.
7. Click on **Next**.

Add a Node

8. Enter the next DCN node number (DCN node numbers are consecutive).
9. Enter the IP address of this IPedge node.
10. Enter the IPedge username 'admin'.
11. Enter the password for the account 'admin' (the factory default password should have been changed during IPedge server installation (see chapter 4 in the I&M manual). Confirm the admin password.
12. Enter the admin password for this node.
13. Enter the password for the account 'root' (the factory default password should have been changed during IPedge server installation (see chapter 4 in the I&M manual). Confirm the root password.
14. Click on **Next**.
15. If there is another node go to Step 8. If this was the last node click on **Finish**.
16. The wizard will display a list of the nodes and their IP addresses. If the list is correct click on **Create Cluster**. If there is an error click on **Back**.
17. When the cluster has been created the wizard will display a Cluster created successfully message.
18. Restart Messaging service.

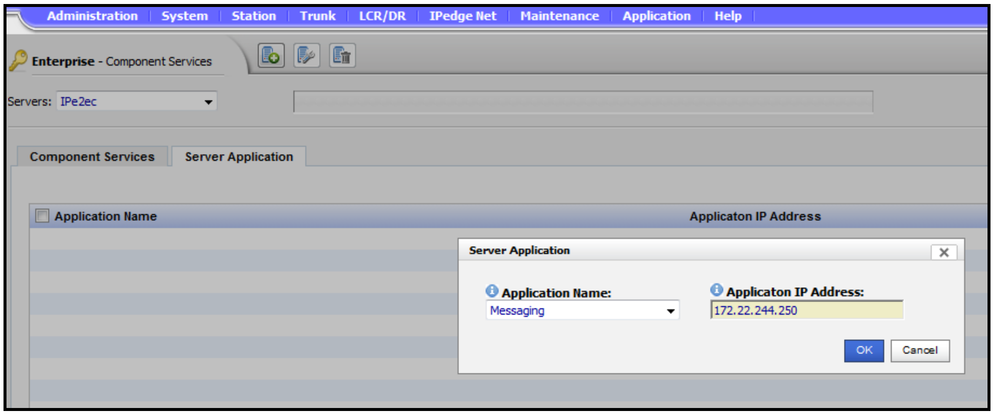
Note: Once the DCN wizard has been run on one of the nodes in the network, it cannot be run on any other nodes in the network. The DCN wizard can only be run again on the same node where the wizard was first run.

Setup Multi-Node Messaging IP Addresses

After the cluster has been created the IP address of each IPedge server must be assigned in the Component Services section of Enterprise Manager. This will allow you to log on to Enterprise Manager on the Primary Node and access the Messaging Application of the Member Node(s).

1. Login to Enterprise Manager on the primary node, select **Administration > Enterprise > Component Services**. Select the Server Application tab.
2. Click on the **New** icon. The Server Application dialog box will open.

3. In the **Application IP Address** field enter the IP address of the IPedge server that will be running that apploicaction. You must enter the IP address, do not enter the 127.0.0.1 loop-back address.

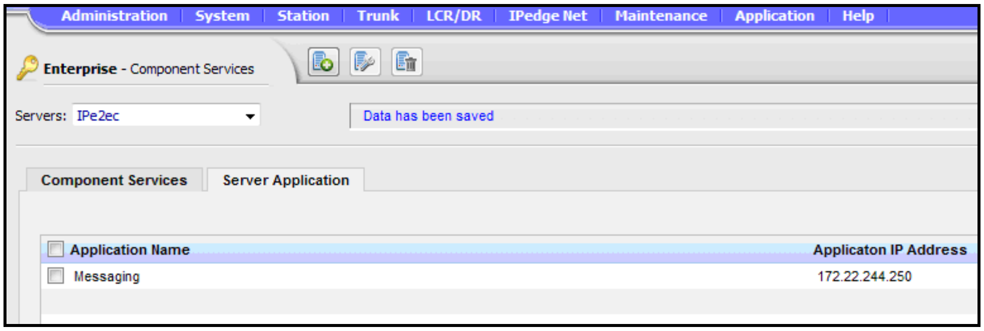


Servers: IPe2ec

Application Name: Messaging

Applicaton IP Address: 172.22.244.250

4. The Messaging application will now be listed in the Component Services.



Servers: IPe2ec

Data has been saved

Application Name	Applicaton IP Address
Messaging	172.22.244.250

5. Repeat steps 2 through 4 for each member server.

Important! Keep in mind that the first time setup of clustering will delete all existing mailboxes on the member node(s).

VERIFY CLUSTER WORKING STATUS

When the Messaging service has restarted on all nodes use the following procedure to verify that the cluster is functioning correctly.

1. Login to Enterprise Manager. Select **Application > Messaging**.
2. Select a node. Start with the Primary IPedge node.
3. In the Messaging screen select **Site Parameters > Cluster**.

4. The screen will show the status of all of the nodes in the cluster except the one you are logged in to.

   The status indicator meaning is shown in the table below.

Color	Meaning	Action
Green	OK - The node is accessible and Operational	None
Red (2)	Database connectivity to the indicated node is successful but the Messaging service is down.	Start Messaging on the indicated node.
Red (1)	No connectivity to the indicated node	1. Verify that the IP address entered for this node is correct 2. Verify that the server is running.
No nodes found	The **Registry > DBsync** parameter is not activated.	Activate the DBsync parameter.

5. Repeat for one other node.
6. Record a department greeting on one node and verify that it is applied to the other nodes.
7. Record a mailbox greeting on one node and verify that it is applied to the other nodes.
8. Leave a message in a mailbox on one node then, access the mailbox on another node. The same message should be there.

Cluster Information

In addition to the status indications detailed in the previous section, the **Site Parameters > Cluster** page allows you to change the database information for each node as well as define the Message Synchronization method between the local node and the other nodes in the cluster using the Automatic Message Synch check-box. The two methods are:

1. Checked — All messages recorded in the local node will be automatically copied to the remote node. The benefit of this method is that there are multiple copies of each message in separate locations. This allows for redundancy and disaster recovery.
2. Unchecked — Messages will not be automatically copied to the remote node. Messages will only be copied as needed, i.e. when a user on the remote node attempts to listen to a message that was recorded on the local node. The benefit of this method is reduced network traffic, as not all messages are copied.

The synchronization method is set per node. This allows for a ‘Hybrid’ Cluster, where some nodes are fully duplicated and others are partially duplicated (messages are duplicated on-demand but database, personal greetings and system greetings are automatically duplicated). A Hybrid cluster is useful for balancing between network traffic limitations and redundancy requirements.

Replicated Files

The table below shows a summary of the data that is replicated and not replicated in the cluster.

Data	Replicated	Not Replicated
PBX parameters		X
Site parameters		X
System Logs		X
Message History Logs		X
Mailbox Properties	X	
Mailbox Greetings/Name	X	
Mailbox Scripts/PIN/Greeting	X	
Messages	X	
Department Settings	X	
Department Greetings	X	
Class Of Service Settings	X	
Reports		X
Registry		X

Verifying Cluster Integrity

While the cluster operates normally, all database records are duplicated across all nodes. To verify this operation login to Enterprise Manager, navigate to the Messaging administration and select **Site Parameters > Cluster** page, click on check **Cluster Integrity** icon.

If records are missing or not updated on any of the nodes, the database will show as NOT synchronized. This may be a result of a network outage or a node that is off-line. Once the node is back on-line, this condition will be automatically corrected. Another option to correct this condition is to re-introduce the node to the cluster (as described in the “Add a Node” on Page -17 section).

SQL Ports And Permissions

All Cluster nodes use SQL on port 3306. The setup process automatically adds all nodes to the allowed hosts in the SQL “user” table.

Mailbox Home Node

Because any mailbox may receive, playback, save or delete a message from any node, Message Waiting Indications and Message Notification may be triggered from any node; depending on where the message was accessed. However, this may cause a problem in some cases. For example:

1. If a Message Waiting Light can only be deactivated by the device that activated it.

2. If only a specific node is attached to the PBX that can trigger MWI for a user.

To overcome these potential issues, a Home Node can be specified in the Mailbox > Parameters page. This will guarantee that MWI would only be activated and deactivated from the Node connected to the preferred PBX (the Node Number that was designated at the time the cluster was created). It would also guarantee that Message Notification attempts will be made from this node. If the Home Node field is set to 0 (default), MWI and Message Notification would be sent from the node in which the mailbox is currently being accessed.

DCN Cluster and Esync Unified Messaging

When using Esync in a DCN environment, only one of the nodes should be running the Esync service and it should be turned off for all other nodes. SMTP messages will be sent from all nodes, however, only one node will synchronize the message status.

DCN Cluster and Msync Unified Messaging

When using Msync in a DCN environment, only one of the nodes should be running the Msync service and it should be turned off for all other nodes.

Add Msync Node

Select **Registry > Msync**. To support the DCN cluster.

To configure click the **Add Msync Node** icon. The primary node displays as 'Node 0.’

The default field entries are:

Messaging Server = Localhost

Message DB = vmuser

Messaging user = gumadmin

Messing Pass = gumAdminPassword

When adding a node input the remote IP address for Messaging Server.

For Messaging DB enter vmuser

For Messaging user enter gumadmin

For Messaging Pass enter gumAdminPassword

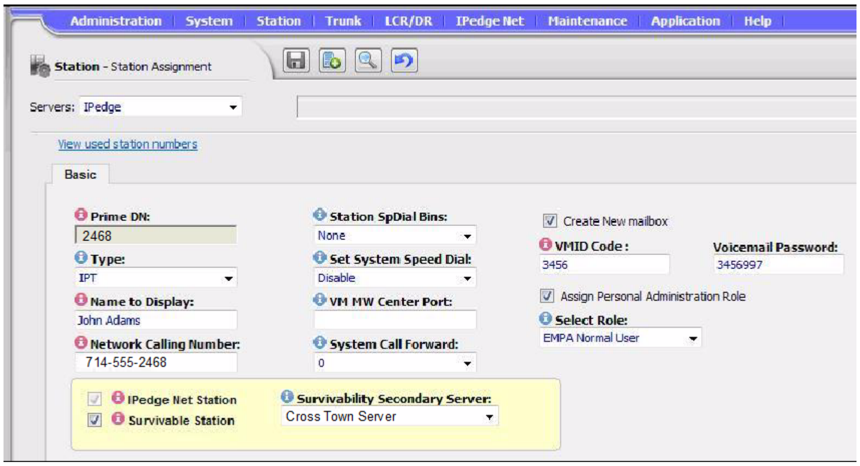
Cluster Housekeeping

The nightly housekeeping routine cleans both database information as well as system specific information. It is recommended to run the housekeeping routine on all nodes in staggered timing. Allow each node enough time to complete before the housekeeping on the next node starts. Refer to “Configure the IPedge Nodes” on Page -16.

Adding Survivability

To add a secondary server to an existing station to make it survivable use the following procedure.

1. In Enterprise Manager select **Station > Assignment**.
2. Select the station to make survivable. Click on the **Edit** icon.
3. Click on the **Survivable Station** check box.
4. Select the Secondary Server.
5. Click on the **Save** icon.
6. Select **Station > IPT Auto Config**.
7. Select the station (step 2).
8. Click on the **Restart IP Phone** icon. This will push the Secondary Server IP address to the IP Telephone.



Servers: IPedge

Prime DN: 2468

Type: IPT

Name to Display: John Adams

Network Calling Number: 714-555-2468

Station SpDial Bins: None

Set System Speed Dial: Disable

VM MW Center Port:

System Call Forward: 0

☑ Create New mailbox

VMID Code : 3456

Voicemail Password: 3456997

☑ Assign Personal Administration Role

Select Role: EMPA Normal User

□ IPedge Net Station

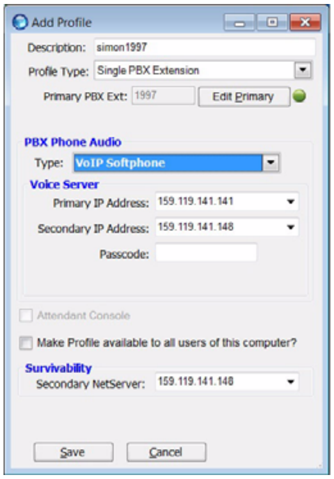
☑ Survivable Station

Survivability Secondary Server: Cross Town Server

Call Manager

A Primary server Profile should be set up in the client’s Call Manager Profile regardless of the survivability feature. Secondary Voice Server and Secondary Net Server is automatically populated. However, it can be overridden.

1. Using Call Manager, from the Main Menu button, click Add New Profile (shown below).
2. Add the description
3. Click Edit Primary
4. Create User and extension, then click OK.



Add Profile

Description: simon1997

Profile Type: Single PBX Extension

Primary PBX Ext: 1997

PBX Phone Audio

Type: VoIP Softphone

Voice Server

Primary IP Address: 159.119.141.141

Secondary IP Address: 159.119.141.148

Passcode:

□ Attendant Console

□ Make Profile available to all users of this computer?

Survivability

Secondary NetServer: 159.119.141.148

CAPACITY

The maximum number of IPTs using the survivability feature in one IPedge server is 1000.

The maximum number of IPTs using the survivability feature in one IPedge network is 6000.

The maximum number of servers in one IPedge network is 128.

Note: The survivability feature requires an endpoint license for each survivable IPT in the primary server. A survivability license is required for each survivable IPT in the secondary server that IPT will 'fail-over' to.

AVAILABILITY

The survivability feature is available on IPedge servers for:

- IP Telephones
- SoftIPT
- Call Manager

CAUTION! The secondary (IPT Failover) IPedge server can not be an EP server. Call Manager, SoftIPT, and IPTs will only fail-over to an EC or EM server.

Messaging Survivability

- Multi-Node IPedge R3.0 and later systems.
- Each node requires a I-MSG-DCN-xx (xx = system type) license.
- The Messaging application must be running on every IPedge system that will run DCN.

Note: All of the nodes in a cluster must be running the same version of the IPedge system software.

RESTRICTION

Does not apply to SIP telephones, telephones via gateways, trunks, IPedge trunks or, SLTs, Door Phones and Paging via gateways.

Interaction for IPT Auto Config and NAT

When the IPT is in factory default setting, the IPT can get the Primary Server and the Secondary Server information from the IPT Auto Config feature if the Server Address is set in the Vender Option on the DHCP server on the WAN side. However if the DHCP server does not support Vender Code, the IPT can not get Primary Server and Secondary Server information. In this case, the user must set Primary Server and Secondary Server information manually before the user connects IPT to IPedge. Refer to the IPT Auto Config feature.

When a user has logged in to the server by User Mobility and the user uses different DN from Station ID registered in the login terminal, Survivability for the login DN does not work. When a user logs into a with a DN different than the assigned DN the IPT Auto Config programming is not changed. Therefore, when the server the user logged in to is down, Survivability works according to the Primary Server and Secondary Server information corresponding to the Station ID. The DN programmed for that station will survive, not the User Mobility (logged-in) DN.

When the Primary Server is placed inside of NAT and the Secondary Server is placed outside of NAT, and the user places the IPT outside of NAT, and the IPT is connected to the Secondary server, the Secondary Server sends both the Primary Server and the Secondary Server information to the IPT and the IPT sets this information. In this case, because the default data of the Primary Server information in Secondary server is a LAN (inside NAT) IP address, the IPT outside NAT will not connect to the Primary Server. To avoid this issue, the user must manually change the Primary Server address in the IPedge database from a LAN IP address to a Public IP address using Enterprise Manager (refer to Case 2 or Case 6 in the diagrams below). The reverse case is the same. When the Secondary Server is placed inside of NAT and the Primary Server is placed outside of NAT, and the user places the IPT outside of NAT, the user must change Secondary Server address from a LAN IP address to a Public IP address (refer to Case 3 or Case 7 in the diagrams below).

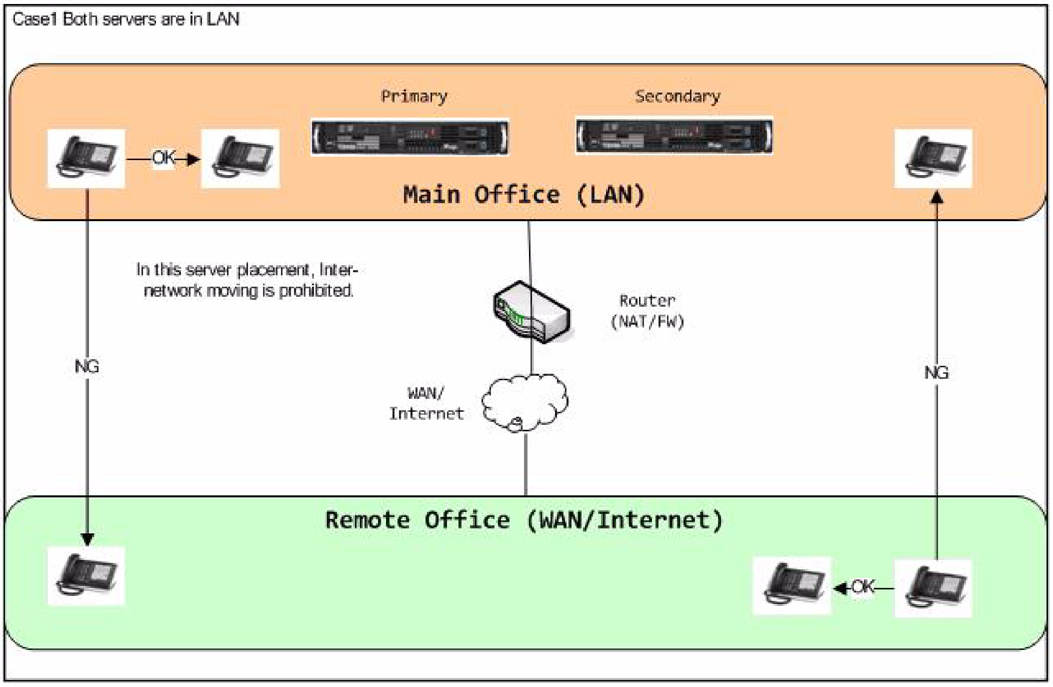
Interaction for IPT Moving and NAT

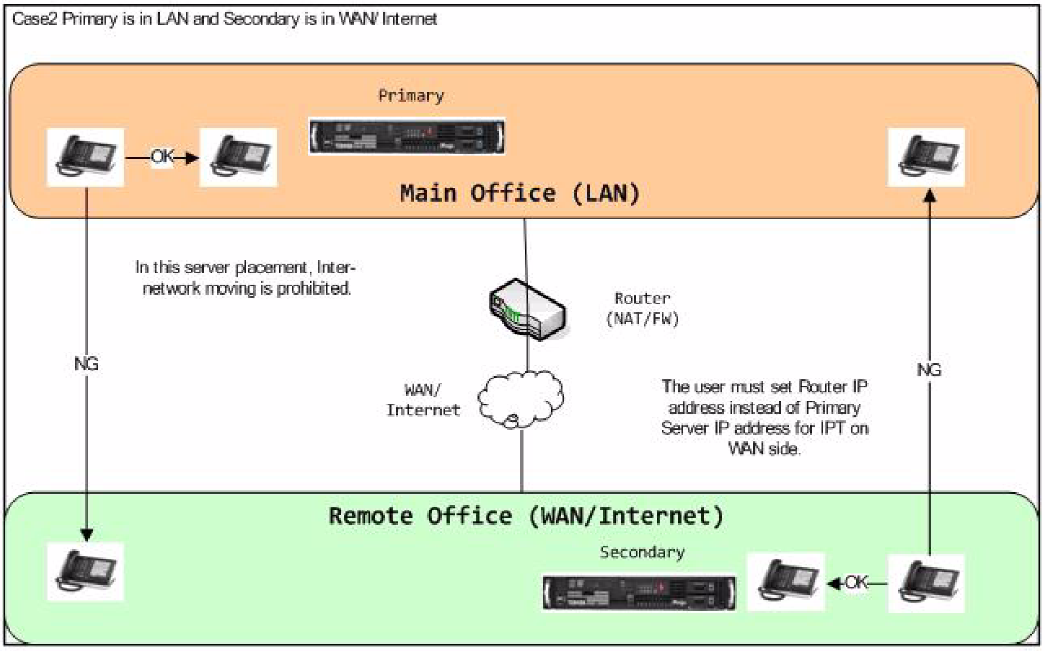
The SoftIPT feature or Transfer Registration feature mean that IPTs have the potential to move a variety of places on the network. When using Survivability under this condition, some restriction about IPT moving will occur. The restriction depends on the placement of Primary Server and Secondary Server (inside of NAT, outside of NAT).

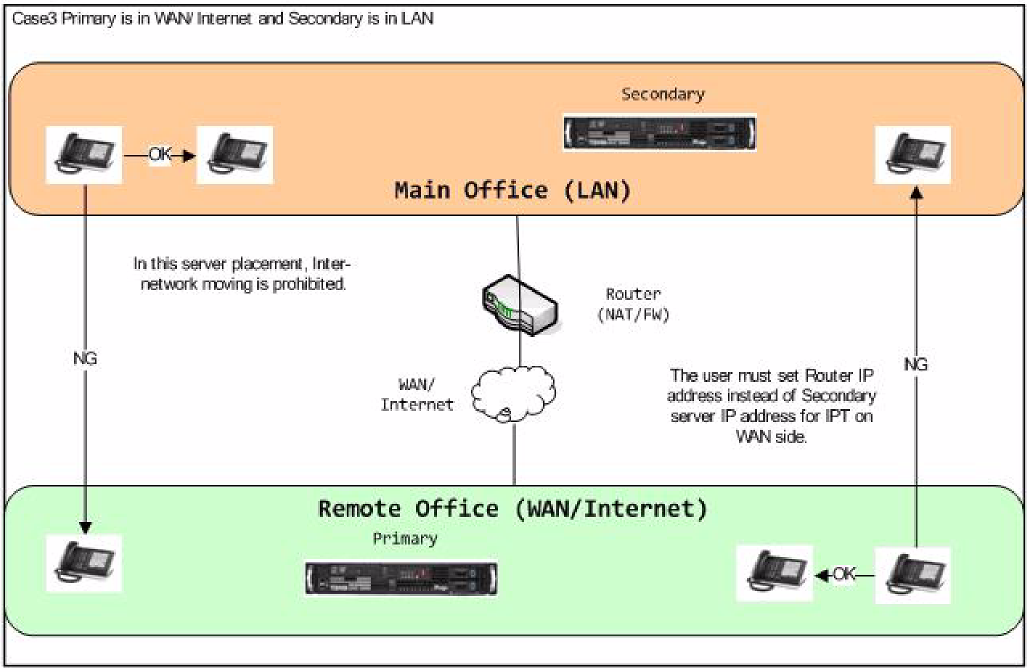
When one terminal moves to a variety of places on the network, like SoftIPT users, the user can not use Survivability feature when the terminal moves from inside the NAT to outside of the NAT or from outside of NAT to inside of NAT except when both the Primary Server and the Secondary Server are placed outside of NAT. (See Case 1 to Case 4)

When multiple terminals log in as same DN from a variety of places on the network, like transfer registration, the user can not use the Survivability feature when the DN moves from inside of NAT to outside of NAT or from outside of NAT to inside of NAT except when both the Primary Server and the Secondary Server are placed the same side (both outside of NAT, or both inside of NAT). (See Case 5 to Case 8)

Example for Soft IPT (one terminal moves a variety of places on the network).

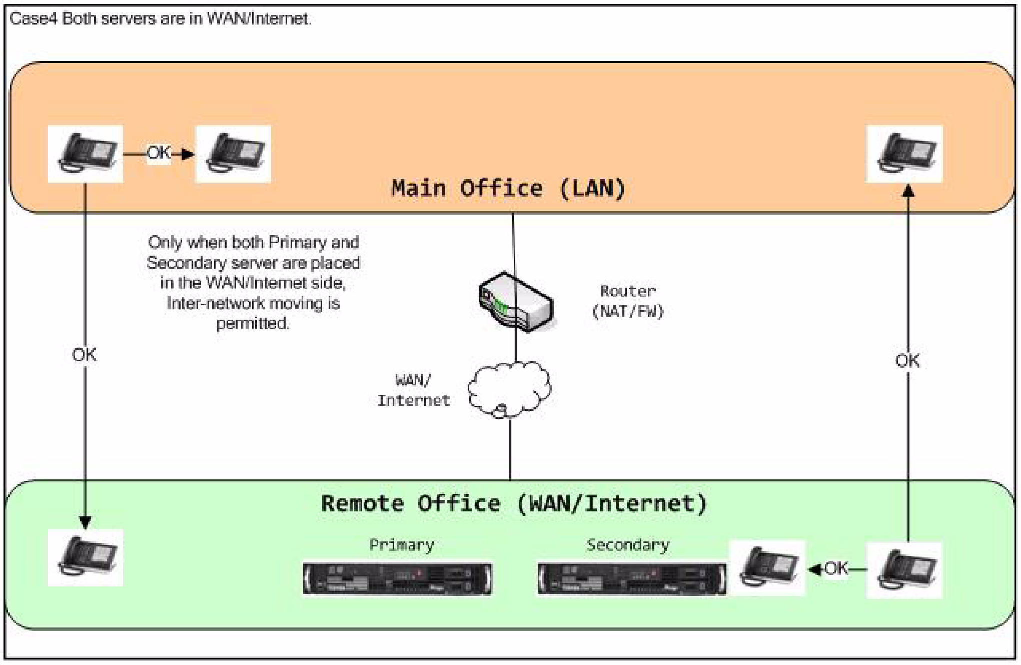

Case1 Both servers are in LAN
Primary
Secondary
OK
Main Office (LAN)
In this server placement, Inter-network moving is prohibited.
Router (NAT/FW)
NG
NG
WAN/ Internet
Remote Office (WAN/Internet)
OK


Case2 Primary is in LAN and Secondary is in WAN/ Internet
Primary
OK
Main Office (LAN)
In this server placement, Inter-network moving is prohibited.
Router (NAT/FW)
NG
NG
WAN/ Internet
The user must set Router IP address instead of Primary Server IP address for IPT on WAN side.
Remote Office (WAN/Internet)
Secondary
OK



Case3 Primary is in WAN/ Internet and Secondary is in LAN

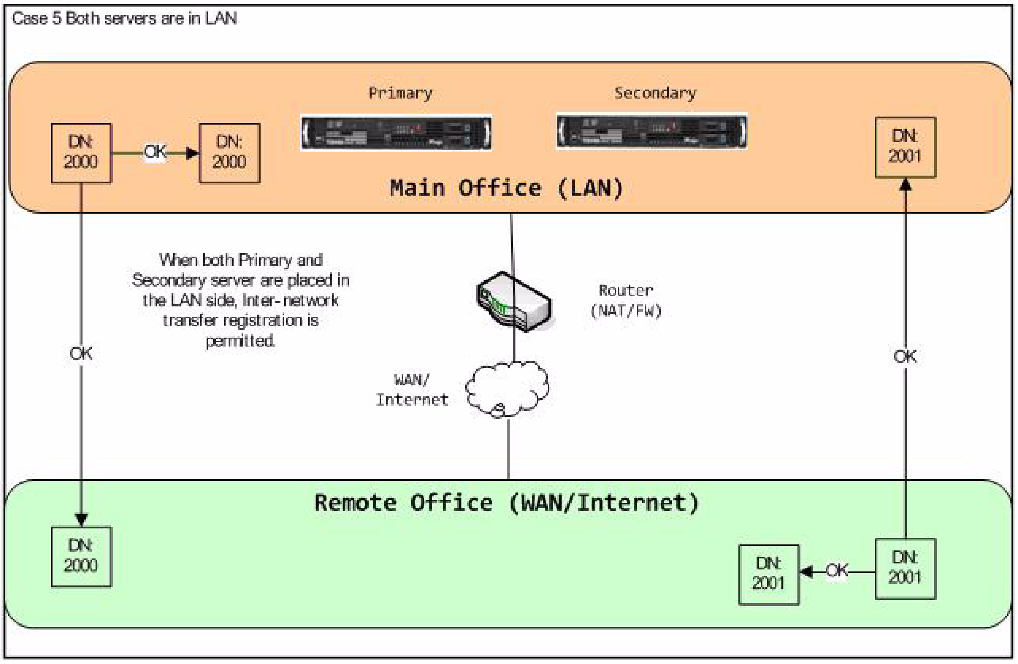
Secondary
OK
Main Office (LAN)
In this server placement, Inter-network moving is prohibited.
Router
(NAT/FW)
NG
NG
WAN/
Internet
The user must set Router IP address instead of Secondary server IP address for IPT on WAN side.
Remote Office (WAN/Internet)
Primary
OK

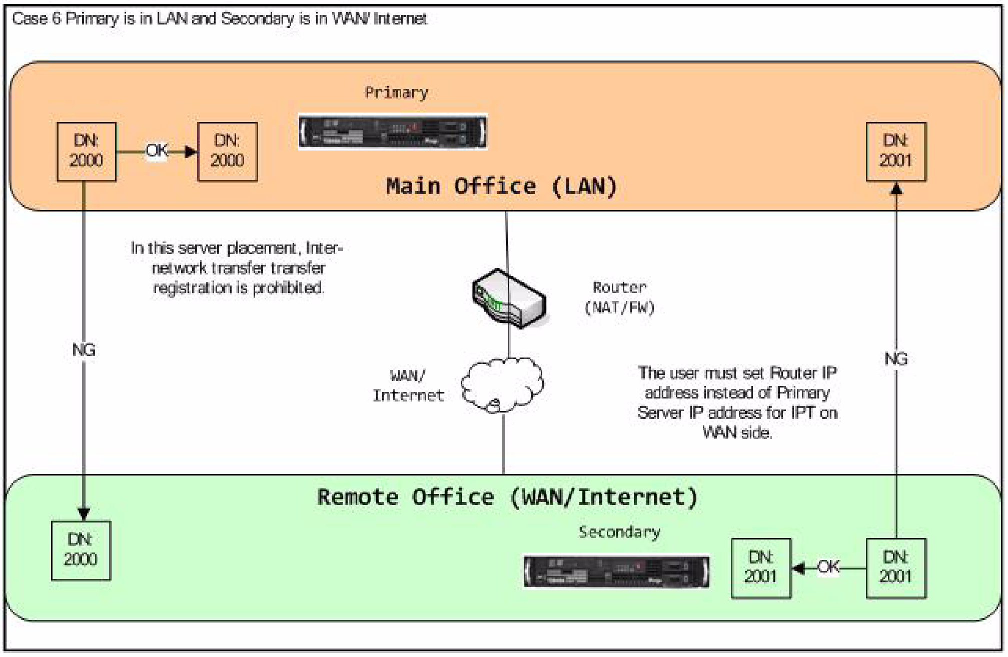


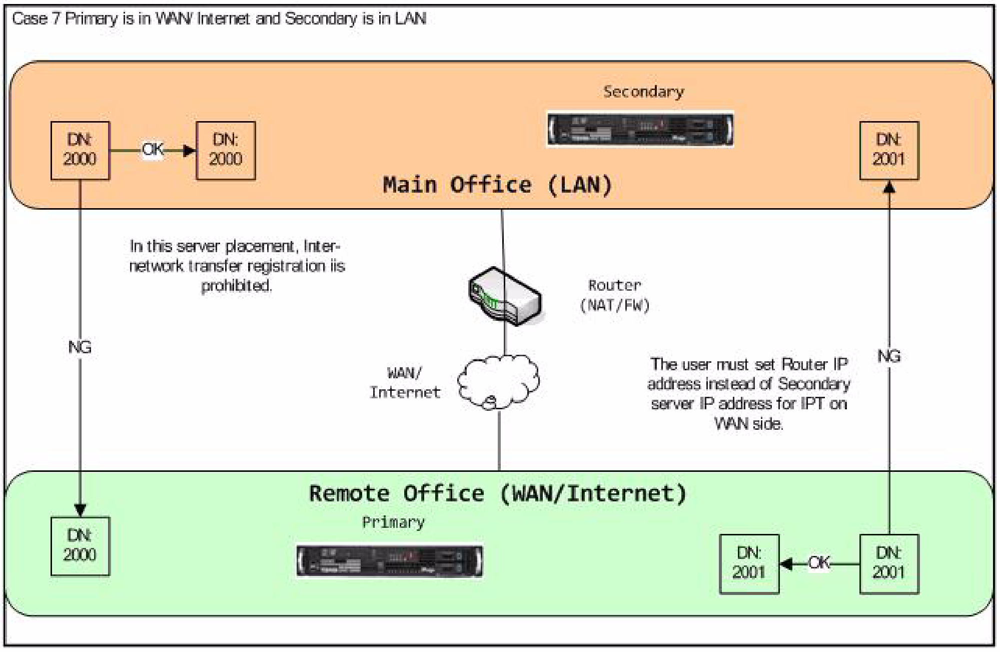
Case4 Both servers are in WAN/Internet.

OK
Main Office (LAN)
Only when both Primary and Secondary server are placed in the WAN/Internet side, Inter-network moving is permitted.
Router
(NAT/FW)
OK
OK
WAN/
Internet
Remote Office (WAN/Internet)
Primary
Secondary
OK

Example for Transfer Registration (multiple IPTs log in as same DN from a variety of places on the network).

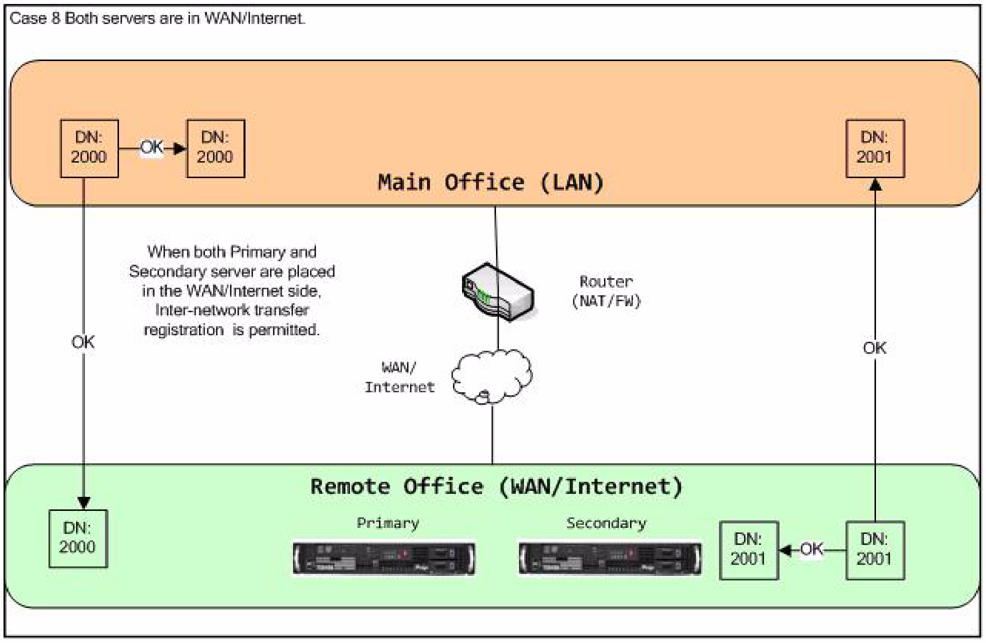

Case 5 Both servers are in LAN
Primary
Secondary
DN: 2000
OK
DN: 2000
DN: 2001
Main Office (LAN)
When both Primary and Secondary server are placed in the LAN side, Inter- network transfer registration is permitted.
Router (NAT/FW)
OK
OK
WAN/ Internet
Remote Office (WAN/Internet)
DN: 2000
DN: 2001
OK
DN: 2001


Case 6 Primary is in LAN and Secondary is in WAN/ Internet
Primary
DN: 2000
OK
DN: 2000
DN: 2001
Main Office (LAN)
In this server placement, Inter-network transfer transfer registration is prohibited.
Router (NAT/FW)
NG
NG
WAN/ Internet
The user must set Router IP address instead of Primary Server IP address for IPT on WAN side.
Remote Office (WAN/Internet)
Secondary
DN: 2000
DN: 2001
OK
DN: 2001



Case 7 Primary is in WAN/ Internet and Secondary is in LAN

Secondary
DN: 2000
OK
DN: 2000
DN: 2001
Main Office (LAN)
In this server placement, Inter-network transfer registration iis prohibited.
Router (NAT/FW)
NG
WAN/ Internet
The user must set Router IP address instead of Secondary server IP address for IPT on WAN side.
NG
Remote Office (WAN/Internet)
Primary
DN: 2000
DN: 2001
OK
DN: 2001



Case 8 Both servers are in WAN/Internet.

DN: 2000
OK
DN: 2000
DN: 2001
Main Office (LAN)
When both Primary and Secondary server are placed in the WAN/Internet side, Inter-network transfer registration is permitted.
Router (NAT/FW)
OK
WAN/ Internet
OK
Remote Office (WAN/Internet)
DN: 2000
Primary
Secondary
DN: 2001
OK
DN: 2001

MESSAGING

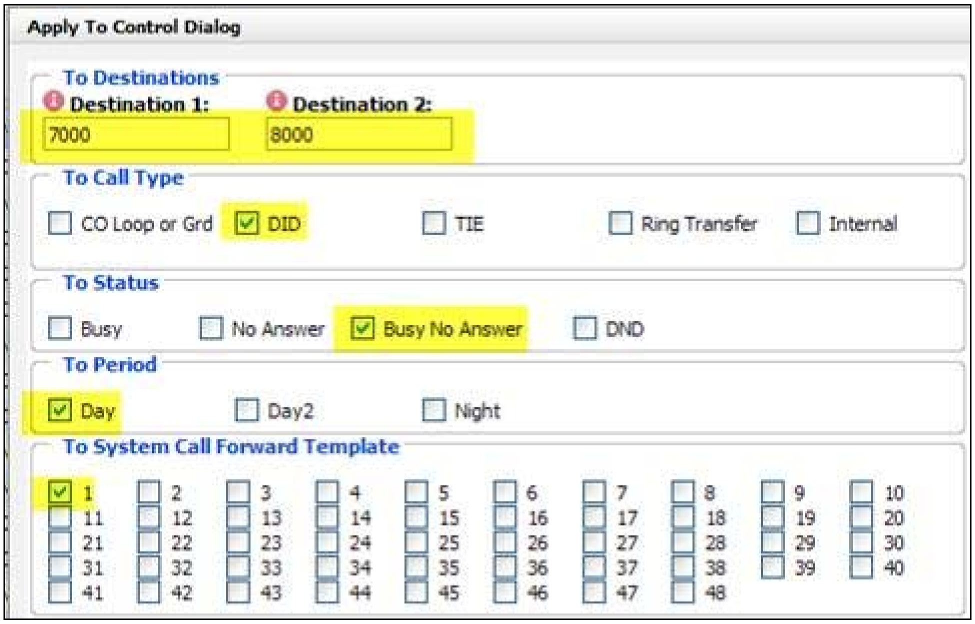
IPedge Messaging survivability is accomplished by setting up Messaging in two system nodes. Calls are sent to Messaging by stations that have set call forwarding to the pilot of the Messaging hunt group.

System call forwarding allows for two destinations to be set. For Messaging Survivability Destination 2 of the call forwarding is set to the Messaging setup in a second system node.

In the example show below the centralized Messaging has pilot number 7000. The ‘fail-over’ node Messaging has pilot number 8000. For this example all stations will have system call forwarding set up as follows.

- Destination 1 is the VM pilot of the central Messaging server (7000).
- Destination 2 is the VM pilot of the fail-over Messaging server (8000).

All phones will forward to 7000, if the system is down it will go to 8000.



Apply To Control Dialog

To Destinations

Destination 1: 7000

Destination 2: 8000

To Call Type

□ CO Loop or Grd ☑ DID □ TIE □ Ring Transfer □ Internal

To Status

□ Busy □ No Answer ☑ Busy No Answer □ DND

To Period

☑ Day □ Day2 □ Night

To System Call Forward Template

☑ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10
□ 11 □ 12 □ 13 □ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20
□ 21 □ 22 □ 23 □ 24 □ 25 □ 26 □ 27 □ 28 □ 29 □ 30
□ 31 □ 32 □ 33 □ 34 □ 35 □ 36 □ 37 □ 38 □ 39 □ 40
□ 41 □ 42 □ 43 □ 44 □ 45 □ 46 □ 47 □ 48

HARDWARE No additional hardware is necessary for this feature.

FEATURE INTERACTION

Table 1 - Survivability Feature Interaction Table

Feature	Interaction
Account Codes	Use the same programming setting for both primary and secondary servers.
Class Of Service	
Day/Night Modes	
DTMF Back Tone	
DTMF Signal Time	
Least Cost Routing (LCR)	
Speed Dial (System/ Station)	
Station CO Line Access	
Tenant Service	
Toll Restriction	
Class Of Service Override	
Emergency ring-down	Survivability is not applied to Emergency ring-down.
Directory Number Presentation	Use the same programming setting for both primary and secondary servers.
Inter-digit Times	
Add-on Module	
Automatic Line Selection	
Continuous DTMF Tone	
Prime DN Button	
Flexible Button Assignment	
Phantom DN Button	
Ringing Assignment	
One Touch Button	• Use the same programming setting for both primary and secondary servers. • Originator server selects the appropriate destination server according to destination IPT fail-over or fail-back status.
Multiple language displays	No special requirements
Delayed Ringing	
Advisory Message	
Distinctive Ringing	
LCD Shift Key	

(Sheet 1 of 8)

Table 1 - Survivability Feature Interaction Table

Feature	Interaction
Automatic Busy Redial (ABR)	ABR or ACB setting is canceled after switch-over.
Automatic Callback (ACB)	
Automatic Campon	• If a switch-over is executed on the camped on destination, the Camped on call is disconnected if there is no other destination. • When switch-over is executed on the campon originator terminal, originator terminal keeps hearing Ring Back Tone.
Call Transfer With Campon	
Call Waiting	
Offhook Campon	
Background Music (BGM) (VIPedge does not support BGM)	• When BGM is invoked in the old server, BGM is stopped if switch-over goes. The customer can hear BGM again by entering BGM invoking feature in the new server. However, the terminal cannot go fail-back to the primary server if it keeps hearing BGM from the secondary server. • The administrator needs to set the same BGM numbers for BGM contents for both primary and secondary server.
Call Forward and System Call Forward	• Use the same programming setting for both primary and secondary server. • Originator server selects the appropriate destination server according to Call Forward destination IPT fail-over or fail-back status. • However, when fail-over or fail-back is executed on the destination IPT but the Roll Book is still not received by the originator server, then the originator server forwards the call to the server, then call may fail (or forward to other terminal if CF is set). After the originator server receives the Roll Book from the new server, the call will forward to the correct destination. • CF remote registration and CF remote cancellation will change the terminal setting when they are in the same server as the invoking terminal. For example, when the IPT-DN: A is registered to the secondary server by survivability and the user tries to changes the CF setting of DN: A by CF remote registration from an IPT in the primary server, the CF setting of DN: A in the primary server will be changed.
Call History	• Call histories in the primary server are not succeeded to the secondary server. • Call histories in the secondary server during switch-over are not succeeded to the primary server.
Call Park Orbits	• Local Parked call in the old server can be retrieved by either other terminals in the old server or terminals in the new server with node ID after switch-over goes, if the old server is still running. • The parked call is handled per the spec of Lost Call Treatment if the terminal in the new server does not go back to the old server.
(Sheet 2 of 8)	

Table 1 - Survivability Feature Interaction Table

Feature	Interaction
Call Transfer Immediate Call Transfer Ring Transfer	When a fail-over or fail-back is executed on the destination IPT but the Roll Book is still not received by the originator server, the originator server will transfer the call to the old server, then the call may fail (or forward to another terminal if CF is set). After the originator server receives the Roll Book from the new server, the call will transfer to the correct destination.
Conference on Hold Consultation Hold Music On Hold Exclusive Hold Line Hold	• If the holing party goes switch-over, it cannot retrieve the held call because it belongs to the new server. • When switch-over is done by network fault during conference, the call is transferred if Consultation holding party or Conference holding party goes switch-over • The held party goes to idle state if the holding party goes switch-over while the held party is hearing MOH. • By network fault, the held call is disconnected and the held party goes switch-over when the held party detects link down and MOH is stopped. • When the holding party is connected via IPedge Net, the held call is disconnected and the held party goes switch-over when the server held party belongs goes down and MOH is stopped • It is not supported to hold a call during Speech Path Survivability.
Conferencing Voice Mail conference	• The conference master is make busy state in the old server even though the speech path is maintained for a while if the conference master detects link down, and after a few seconds the ex-conference master is disconnected. Therefore, the next conference master is chosen from candidates. • If the old server going down is the reason for link down, RTP stream is stopped if media server is chosen in the old server. The conference will continue if the media server in the remote node is chosen.
Direct Inward Dialing (DID)	• Survivability feature is applied if IPT answers DID terminating call. • When fail-over or fail-back is executed on the destination IPT but Roll Book is still not received originator server, originator server transfer the call to old server, then call may fail (or forward to other terminal if CF is set). After originator server receives Roll Book from new server, the call will transfer to correct destination.
Do Not Disturb (DND)	• DND state in the old server is not succeeded to the new server. • When fail-over or fail-back is executed on the IPT-A and old server receives Roll Book from new server, DND state of IPT-A in the old server is ignored. When the user in the old server calls IPT-A, old server ignores IPT-A DND registration status and transfer the call to new server. DND registration status is checked on the new server.
(Sheet 3 of 8)	

Table 1 - Survivability Feature Interaction Table

Feature	Interaction
Enhanced 911 (E911 Interface)	When E911 originator detects link down during the call, E911 originator will be disconnected because RTP stream is stopped by the old server going down. If network fault is the reason, RTP stream might recover if network fault is solved. However, the call is disconnected if E911 originator cannot receive RTP stream within 6 seconds. Internal Notification does not follow destination IPT fail-over or fail-back status. The user must set Internal Notification each node.
Executive Override	The user cannot override the call when destination IPT is registered to other server.
Flexible Numbering Plan	DNs which can go switch-over are set to both primary and secondary server. Feature access codes, park orbits, and so on shall be set the same for both primary and secondary server. Without the same digits, switch-over-station users may be confuse because the correct digits to dial could be different in the backup server.
Group Paging and Emergency Page	• When group paging is done by using media resources in the old server, the originator is disconnected by stopping RTP stream if the old server going down is the reason. RTP stream might recover if a network fault is solved. However, the call is disconnected if originator cannot receive RTP stream within 6 seconds. • Group paging is disconnected if media resources in the remote node are used when paging originator and terminator exist in different server and paging originator is registered to other server by Survivability. • If the old server going down is the reason, destination server detects IPedge Net Keep Alive Timeout and disconnects the call. • If network fault is the reason, old server detects fault make busy on originator terminal and disconnects the call. • If media resources in the remote node are used when paging originator and terminator exist in different node and one of paging terminator is registered to other server by Survivability, only this terminal finish the paging, other terminals continue paging.
Manual Voice Recording	When MVR originator detects link down, the originator is disconnected by stopping RTP stream if the old server going down is the reason.
(Sheet 4 of 8)	

Table 1 - Survivability Feature Interaction Table

Feature	Interaction
Message Waiting	• Message Waiting state in the old server is not succeeded to the new server. • When IPT-A sets MW to IPT-B in the same server of IPT-A and then IPT-A registered to other server by Survivability, or when IPT-A sets MW to IPT-B in the different server of IPT-A and then IPT-A registered to the same server of IPT-B by Survivability, and IPT-B execute MW call back, originator server selects the appropriate destination server according to IPT-A fail-over or fail-back status and clear MW LED when IPT-A answers the call.
Multiple Calling	If network fault is the reason, IPT is temporarily left from the multiple calling group during switch-over. The limitation of belonging to the same local node is the spec of Multiple Calling feature.
Simplified Message Desk Interface (SMDI)	The next call is notified to Voice Mail with node ID + DN from the new server if IPT detects link down during talking with Voice Mail. This means that there is no case to change node ID while talking.
Station Message Detail Record (SMDR)	• There is no assurance to send SMDR message correctly if IPT detects link down during talk. • If the old server going down is the reason, SMDR message is not output. • If network fault is the reason, SMDR message is output, but its talking time is shorter than real talking time because SMDR message is output when the old server detects IPT fault make busy.
Tandem CO Line Connection	• IPT cannot intrude the tandem connection call which IPT hangs up from the conference or transfer the trunk call to the trunk, after switch-over because trunk line button is cleared. The trunk is different for each node. • If the server is running and the station goes switch-over or goes fail-back to the primary server, line buttons do not light but if the user presses these line buttons, the station can barge into the previous tandem connection call.
Tone First/ Voice First and Hands Free Answer Back	Even if the programming is set as “Tone First”, IPT might be called as “Tone First” call after switch-over. Default call type is “Tone First” for the private line call which calls from the old server to IPT in the new server. However it is possible to change call type.
Voice Mail	VMID shall be set as the same in both primary and secondary server. This is to access the same mail box even if switch-over goes.
Call Pickup	After switch-over to the secondary server, the customer needs to enter node ID of the primary server to pick terminating call and held call up in the primary server.
Recall Treatment	In the cases of switch-over in holding, parking, and transferred, the call is forwarded to the Lost Call destination as recall termination cannot be forwarded by Call Forward feature. If there is no Lost Call destination, the call is disconnected.
(Sheet 5 of 8)	

Table 1 - Survivability Feature Interaction Table

Feature	Interaction
Lost Call Treatment	Originator server selects the appropriate destination server according to Lost Call destination IPT fail-over or fail-back status.
Station Hunting	If network fault is the reason, IPT is temporarily left from the station hunting group during switch-over. The limitation of belonging to the same local node is the spec of Station Hunting feature.
DND/Busy Override	The user cannot override the call when destination IPT is registered to other server.
Make Busy	• As system detects the terminal non-existing in 30 seconds and IPT detects link down and go switch-over in 20 seconds, there is 10 seconds for terminal non-existing. During this the new terminating call may be disconnected because the old server does not work for this IPT. • All the servers except fail-over or fail-back destination server detect moving IPT by receiving Roll Book from new server. Before receiving Roll Book (Maximum 5 minutes), when originator server makes the call to moving IPT, the call is terminated to old server and the call may be disconnected by Make Busy. (Or forward to other terminal if CF is set).
Lock Password	• Because Lock Password starts in lock state when IPT goes Make Idle state, IPT keeps lock password state in the new server if IPT goes switch-over in lock state. • Lock key is required to set the same in both primary and secondary server.
Conference Split/Join/Drop	If IPT detects link down because of network fault in split mode, after a few seconds the ex-conference master is disconnected. Therefore, the next conference master is chosen from candidates. The ex-conference master is dropped from the conference, and goes switch-over.
Universal Call Distribution (UCD)	If network fault is the reason, IPT is temporarily left from the UCD group during switch-over. The limitation of belonging to the same local node is the spec of UCD feature.
IP Phone User Mobility	• In the server change in fail-over and fail-back, server connection by automatic logging in is done under following conditions; • Station ID is used the same as the one using in the server change. Cause the IPT to reboot (unplug for 6 seconds or manual program)
Direct Station Selection Key	When the IPT associated with a DSS button registered to another node and the user makes the call by pressing the DSS button, originator server makes the call to its own server and the call may be disconnected by Make Busy. (Or forward to other terminal if CF is set.)
(Sheet 6 of 8)	

Table 1 - Survivability Feature Interaction Table

Feature	Interaction
Release/ Answer Button	• It is needed to set the same programming setting for both primary and secondary server. • The call is not disconnected even if [Release/ Answer] button is pressed during Speech Path Survivability.
Repeat Last Number Dialed	Redial information in the old server is not succeeded to the new server. Either no setting or last redial information in the new server is used.
Speaker Phone ON/OFF	The mode of speaker phone call or handset phone call is not changed even if [SPKR] button is pressed during Speech Path Survivability. And the call is disconnected by pressing [SPKR] button even if the call is in handset phone call.
Volume Control	• The volume is not changed even if either [VOLUP] or [VOLDOWN] button is pressed during Speech Path Survivability. • Volume information in the old server is not succeeded to the new server. Either no setting or last volume information in the new server is used.
Multiple Appearance	During switch-over to the secondary server, IPT follows the setting of multiple appearance in the secondary server. Therefore, it is impossible to indicate secondary appearance on IPTs in the primary server, which are set secondary appearances in the primary server. Multiple appearance is limited and is configured within the node.
Group CO Button and Pooled Line Button	Even if the same trunk number is specified on [GCO] or [Pool] button, calling information to the far end party is different as the actual trunks are different in both primary and secondary server.
Cancel Button	• It is needed to set the same programming setting for both primary and secondary server. • The call is not disconnected even if [Cancel] button is pressed during Speech Path Survivability.
Privacy/Non-privacy	If IPT break into the call by privacy release and then IPT goes switch-over because of the old server down, RTP stream is stopped because Media Server in the old server is used.
Directory Assistance	• Searched name is different between the primary and secondary server because terminals belonging are different. It is impossible to search name in the primary server after IPT goes switch-over to the secondary server. • When the user makes the call from result of searching, originator server selects the appropriate destination server according to destination IPT fail-over or fail-back status.
Call Monitor	• When monitoring party detects link down because of network fault, it can continue the speech path but it cannot stop monitoring. • When monitoring party detects link down because of the old server down, it is disconnected because Media Server in the old server cannot be used so that RTP stream is stopped.
(Sheet 7 of 8)	

Table 1 - Survivability Feature Interaction Table

Feature	Interaction
IPT-Softphone	IPT-Softphone supports the Survivability feature.
Local Date and Time	Time zone information in the old server is not succeeded to the new server.
Overflow	• Because Overflow feature does not support inter-node transfer, the Survivability feature is not supported for Overflow destination. • The terminating call on overflow destination is forwarded to the Lost Call destination if overflow destination goes switch-over to the new server.
Split	• If IPT detects link down because of network fault, after a few seconds the split master is disconnected. Therefore, the call is transferred. • By network fault, the held call is disconnected and the held party goes switch-over when the held party detects link down and MOH is stopped. • The held party is disconnected immediately and goes switch-over if media resource is exhausted and the held party does not hear MOH.
Through Dialing	• When the held party detects link down during through dialing, the call is recalled on the transferring master because the held party cannot enter additional digits. The held party keeps hearing Dial Tone at the new server. • When the transferring party detects link down during through dialing, the call is transferred when terminal fault is detected.
PC-Attendant	Survivability feature is not applied for PC-ATT.
External ACD	• Survivability feature is not applied for External ACD.
Private Networking Over IP	Both the primary and the secondary server are required to connect via IPedge Net.
Network DN Table	• Network DN can be used. • Survivability DN need to be Network DN.
Program Update	After an IPT is restarted by the IPT program update, the IPT tries to connect to the server which ordered IPT to restart.
(Sheet 8 of 8)	