IXC Overview

The Unified ICM Enterprise Edition software requires access to the IntereXchange Carrier intelligent call routing network to perform pre-routing. Each interexchange carrier offers intelligent network services that allow customer-premises equipment to participate in network-level call routing. The Unified ICM software uses a Cisco Network Interface Controller (NIC) to connect to one or more networks.

Specifically, this chapter helps you to complete the following tasks:

- Choose one or more carriers. Cisco supports network interfaces with several carriers. You can use one or more carriers with the Unified ICM software.

- Choose the types of network link fault tolerance to apply. Apply fault tolerance in the network interface and the links to the carrier intelligent network.

- Order intelligent network service. After you review the requirements for your specific Cisco NIC, order intelligent network service and work with the carrier and Cisco to bring the service on line.

ICM Software and IXC Interaction

The Network Interface Controller (NIC) is the interface between the Unified ICM software and the IXC intelligent network. The NIC uses network control links to communicate with the IXC network. These links are typically offered as part of the carrier intelligent network service.

Cisco provides a NIC to interface with the specific carrier network. For example, if you have TIM service, your Unified ICM system is equipped with a Cisco-supplied TIM NIC. If you use both AT&T and TIM as carriers, your Unified ICM system is equipped with AT&T and TIM NICs. The following figure shows the interaction between the IXC network and the Unified ICM NIC.

Figure 1: Network Interface Controller
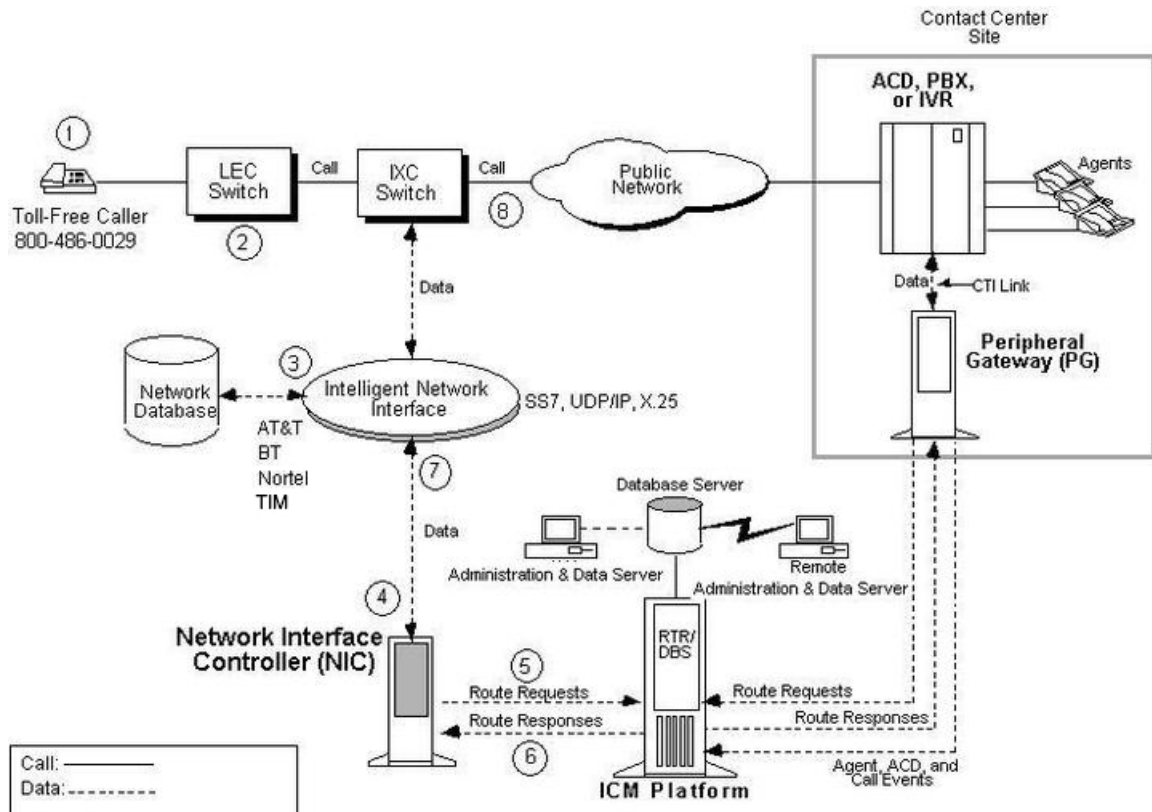
You can implement a Unified ICM Network Gateway for Sigtran networks. The Unified ICM Network Gateway is implemented as a separate node on the Unified ICM signaling access network. When this node is implemented, you can install the NIC software on the CallRouter server. For Sigtran networks, you can deploy a Sigtran Gateway on either the CallRouter server or a separate machine; the NIC software is installed on the CallRouter server. However, the INAP Sigtran gateway must be installed on a separate server.

The circled numbers in the preceding diagram show the specific flow of messages to and from the NIC within the Unified ICM software and the IXC network. The following sections explain the message flow.

Toll-Free Caller

As shown in the preceding figure, the flow of messages between the network and the Unified ICM begins when a caller dials a toll-free number (1).

LEC-to-IXC

The Local Exchange Carrier (LEC) determines which interexchange carrier (IXC) is providing transport for that particular number and forwards the call to the IXC switch (2).

Network Query

The IXC switch holds the call momentarily while it queries a network database to determine where to route the call (3).

ICM NIC

The network database forwards the query to the NIC and requests an intelligent routing decision (4).

Unified ICM CallRouter Process

The NIC software process receives the request, translates it into a standard format, and forwards it to the Unified ICM CallRouter process (5)

Best Destination Address Returned

The Unified ICM software selects the appropriate call routing script, assesses the skills and current real-time status of agents throughout the contact center network, and returns the best destination address back to the NIC (6).

IXC Network

The NIC sends the destination address to the IXC network (7).

Connecting Call

The network instructs the originating IXC switch to connect the call to the destination specified by the Unified ICM software (8). The total time the carrier takes to connect the call varies. However, the additional time the Unified ICM software adds to process the route request is typically less than half a second.

Supported Carrier Connections

The following table summarizes the basic supported carrier connections and their corresponding Unified ICM software routing client (NIC) and network transport protocol.

Table 1: Interexchange Carrier Connections

Routing Client	Connection to ICM
AT&T	AT&T Network (AT&T Sigtran)
CRSP	Call Routing Service Protocol (UDP)
GKTMP	Gatekeeper GKTMP interface (TCP/IP) **Note** Deprecated in release 10.
ICRP	Intelligent CallRouter Protocol (UDP)

Routing Client	Connection to ICM
INCRP	NAM/ICM Gateway Call Routing Protocol interface (UDP) **Note** Deprecated in release 10.
MCI	MCI Network (TCP/IP)
Nortel	INAP (Sigtran)
NTL	NTL Network (TCP/IP)
SS7IN	ITU (Sigtran)
Unisource INAP	INAP (Sigtran)
TIM	INAP (Sigtran)
CWC	INAP (Sigtran)

SPRINT network interface

Network Interface	Hardware (For Signaling Access Networks)	
SPRINT network interface	3 (5 if simplexed) x Eiconcard:	
	PCI 2.2	S94 V2 • Motorola Freescale 852 T @ 98 MHz • 16 MB SDRAM • Bus Type: PCI 2.2 64bit / 66 MHz (3.3 V)
	PCIe (PCI Express)	S94 PCI Express • Motorola Freescale 852 T @ 98 MHz • 16 MB SDRAM • PLX 8111 Express Interface • Bus Type: Single lane PCIe 1.0a 2.5Gbit/Sec • Two VHSI connectors
	• 5 (10 if simplexed) x VHSI V.35 DCE cable (Eicon #300-076) • Eiconcard Connections for Windows V6R9	

Fault Tolerance to NICs

You may already have a strategy for fault tolerance for some parts of the Unified ICM system. For example, you may have decided to use a duplexed, distributed Unified ICM central controller and duplexed PGs at each call center. It is just as important to apply fault tolerance to the NICs and intelligent network access links. Without a connection to the carrier's intelligent network, the Unified ICM system cannot perform pre-routing. If these links are lost, calls are typically routed according to the default routing plans set up in the carrier network.

✎

| **Note** | For more information on Unified ICM system fault tolerance, see the for more information. |

Goal of NIC Fault Tolerance

The goal in applying NIC fault tolerance is to add levels of protection that successively eliminate single points of failure.

Cisco requires an order of importance to follow when choosing the types of fault tolerance to apply in the carrier network-to-ICM system connection:

- First, use **redundant links** from the Cisco NIC to the carrier's intelligent network.

- Next, if you have redundant links, provision those links on **diverse facilities**. This adds another level of fault tolerance to your network connection.

- For NICs that run on the Unified ICM CallRouter platform, the NIC processes are duplexed when the CallRouter is duplexed.

  The types of NIC fault tolerance you apply have a bearing on the number of links you need to provision for IXC intelligent network access.

Link Redundancy

Cisco requires that you configure redundant links to the IXC network. In other words, rather than having a single link from the NIC to the IXC intelligent network, provision two links. Having just one link to the IXC network represents a single point of failure (that is, an area or node in the system that, should it fail, can cause the system to stop routing calls).

By using redundant links, you increase the reliability of the IXC network connection and add an important level of fault tolerance to the system. The following figure shows a simplexed Unified ICM central controller and NIC with redundant links to the IXC network.

Figure 2: Redundant Links
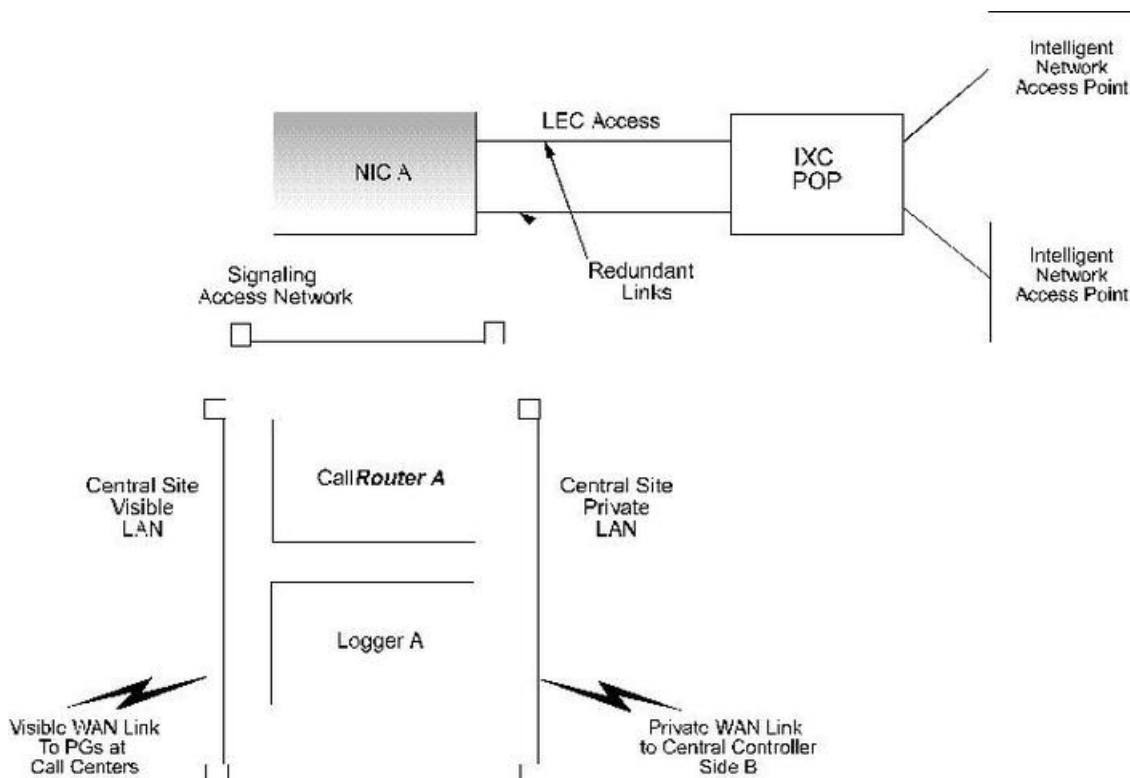
In the preceding figure, single points of failure still exist because the NIC, CallRouter, and Logger are simplexed. The simplexed central controller and NIC configuration are shown here only as an example. This type of simplexed configuration is used only for non-critical systems that can tolerate potentially long interruptions in service (for example, in lab or demo systems).

The major IXCs support redundant links to their intelligent networks. Contact your carrier for more information on access link options.

Route Diversity

For even more protection against network outages, Cisco requires that the network links are provisioned on diverse network facilities. By having diverse links, you further reduce the risk that another single point of failure (in this case, the failure of a circuit) could cause you to lose the connection to the IXC network. For example, you might provision one access link on one T1 circuit and provision the other access link on a different T1 circuit. By having diverse links, you protect against network failures in which an entire circuit is lost.

The following figure shows a simplexed Unified ICM system with redundant links and route diversity:

Figure 3: Redundant Links and Route Diversity
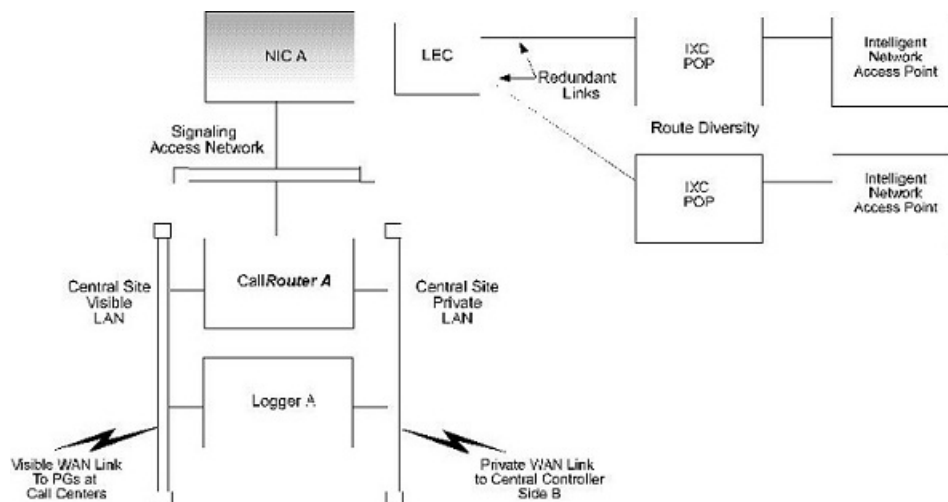
This example provides more fault tolerance by protecting against circuit failure or the loss of an IXC Point Of Presence (POP). Although the NIC is at one location, the redundant links connect to two different POPs. If one IXC POP is taken out of service (for example, in the event of a natural disaster), one link can still access the IXC network through the other POP.

The major carriers provide options for route diversity. Check with your carrier to discuss having the links handled by different POPs. You need to make sure that both the IXC and the Local Exchange Carrier (LEC) are using diverse circuits. Your LEC may impose some limitations on link diversity from the NIC to the IXC POP (that is, over the "last mile"). These limitations often depend on whether the call center is located in a metropolitan or rural area.