NORTEL NETWORKS

Enterprise Edge 2.0 IP Telephony Configuration Guide

1-800-4 NORTEL
www.nortelnetworks.com

P0911590 Issue 02

Contents

Overview

The Enterprise Edge VoIP Gateway reduces communication costs by routing voice traffic over private Internet Protocol (IP) networks as part of the Enterprise Edge product portfolio. Enterprise Edge uses IP telephony to link multiple sites together using an existing corporate data network. The IP trunks are an important part of the telephony services. IP telephony is transparent to users.

IP telephony involves the conversion of voice from its normal telephony format (continuous analog or digital signal) into a digital packet format transported over an intranet.

IP telephony operates on an installed corporate IP network. IP telephony requires a correctly managed intranet, instead of the internet. The private IP network facilities must have sufficient bandwidth on the private Wide Area Network (WAN) backbone. The Engineering guidelines chapter on page 15 contains information about determining if your corporate IP network can support IP telephony. A keycode controls the number of supported IP ports.

IP telephony uses a Web-based browser for configuration. See the Configuration chapter on page 61 for information about how to configure IP telephony.

The VoIP Gateway supports ITU-H.323v2 gatekeeper operation. The VoIP Gateway allows Enterprise Edge systems to use a central facility for IP address resolution. The VoIP Gateway uses standard Digital Signal Processor (DSP) voice coding. The VoIP Gateway supports compression algorithms (codecs) such as G.711, G.723, and G.729. See Codec types on page 37 in the Engineering guidelines chapter for information about codecs.

The VoIP Gateway monitors the data network and reroutes calls to the conventional circuit-switched voice facilities if Quality of Service (QoS) over the data network decreases. This Fallback to Conventional Circuit-Switched Voice Facilities feature allows the system and installer to determine the acceptable QoS over the data network. The customer can configure QoS parameters according to their requirements. See the Quality of service parameters section on page 10 and Configuration of fallback to conventional circuit-switched facilities section on page 67 in the Configuration chapter for information about configuring the QoS parameters. If the quality is below the expected level of QoS, the conventional circuit-switched voice facilities route is selected until the QoS returns to an acceptable level.

The VoIP Gateway also activates fallback for other cases when a call cannot be completed. Examples include no response from the destination, the remote gateway table is improperly configured, or if there are not enough DSP resources to support the call.

About this document

This guide provides information about the Enterprise Edge VoIP Gateway. This guide is for both guide telecom and datacom engineers who design and install the network. The assumption is that the telecom engineer understands how to engineer the Enterprise Edge product portfolio, and get system voice and fax traffic statistics. The assumption is that the datacom engineer understands the intranet architecture, LAN implementation, tools for collecting and analyzing data network statistics, and data network management systems. The terms installer and administrator used in this document refer to either the telecom or datacom engineer. This guide contains the following chapters:

- Engineering guidelines on page 15
- Engineering checklist on page 55
- Installation on page 57
- Configuration on page 61
- Maintenance on page 69
- Interoperability on page 71

System Functions

Enterprise Edge VoIP Gateway uses IP telephony to provide least cost routing of voice traffic through a corporate intranet. VoIP Gateway provides the following:

- Basic calls with answer and disconnect supervision
- Direct Inward Dial (DID) and Direct Outward Dial (DOD)
- Calling name and number
- VoIP Gateway to M1-ITG capability
- ITU-H.323v2 compatible gateway
- ITU-H.323v2 Gatekeeper interoperability
- Economical bandwidth use through voice compression
- Economical bandwidth use through silence compression
- Quality of Service (QoS) monitoring of gateways
- Circuit-switched voice facilities fallback capability

The core telephony service made available through Enterprise Edge considers the Enterprise Edge VoIP Gateway as a trunk. The IP trunk uses the trunking and routing functionality of the Enterprise Edge product portfolio. The IP trunks are an important part of the Enterprise Edge product portfolio.

VoIP Gateway trunks, are supervised trunks with answer and disconnect supervision. The VoIP Gateway supports voice and fax calls. See the Engineering guidelines chapter on page 15 for more information about fax calls. VoIP Gateway does not support modem calls.

The IP telephony gateway allows communication with other supported gateways and H.323v2 gateways through trunk calls. The IP telephony gateway supports Direct Routed communication. The local gateway performs the address resolution and maintains the remote gateway table.

The ITU-H.323v2 Gatekeeper allows for centralized configuration of IP address information. Two call signaling protocols are available in Enterprise Edge 2.0.

- Direct routed, where Enterprise Edge uses a locally maintained table for IP resolution. The locally maintained table is the remote gateway table. See the Configuration chapter on page 61 for information about the remote gateway table.
- Gatekeeper routed, where Enterprise Edge uses a centralized gatekeeper for address resolution. In this mode, the gatekeeper handles all call control signaling. The remote gateway table is not used.

Dialing plan support

Dialing plan configuration allows the customer to set up the routing tables to route calls to appropriate destinations based on the dialed digits.

Routing codes and the destination code table allow the core telephony services on the Enterprise Edge to direct the use and time of use of trunking facilities for calls. Routing codes are associated with line pools. You can assign more than one routing code to each destination code, depending on factors such as Least Cost Routing.

Enterprise Edge has two main areas of configuration: the destination codes in the core telephony services and the destination digits in the remote gateway configuration table. The destination digits allow VoIP Gateway to route calls to the appropriate intranet destination based on the leading dialed digits. The destination code tables route calls to the appropriate trunks based on the leading dialed digits.

See the Configuration chapter on page 61 for details on configuring destination digits and destination codes.

The dialing plans for all VoIP Gateways connected to the corporate intranet require planning to allow calls between gateways as required.

For more information about Dialing plan support, see Dialing plan section on page 43.

Network Quality of Service

Enterprise Edge VoIP Gateway uses a method like the ITU-T Recommendation G.107, the E-Model, to determine the voice quality. This model evaluates the end-to-end network transmission performance and outputs a scalar rating “R” for the network transmission quality. The packet loss and latency of the end-to-end network determine “R”. The model correlates the network objective measure “R”, with the subjective QoS metric for voice quality, MOS or the Mean Opinion Score.

This model provides an effective traffic building mechanism by activating the Fallback to Circuit-Switched Voice Facilities feature at call set up to avoid quality of service degradation. New calls fall back when the configured MOS values for all codecs are below the threshold.

The model is the reason for compression characteristics of the codecs. Each codec delivers a different MOS for the same network quality.

Network Monitoring

The VoIP Gateway network monitoring function measures the quality of service between the local and all remote gateways on a continuous basis. The network monitoring function exchanges UDP probe packets between all monitored gateways to collect the network statistics for each remote location. All the packets make a round trip from the Sender to Receiver and back to the Sender. From this information, you can calculate the latency and loss in the network for a distinct location.

Note 1: Quality of Service monitoring is not supported for non-Enterprise Edge product locations and must be disabled.

Note 2: The Quality of Service threshold is configurable per remote gateway.

Note 3: Fallback starts for all new originating calls if the QoS of any monitored gateway is below its threshold.

Note 4: The fallback decision is made only at the originating gateway using the QoS thresholds monitored at the originating gateway for the destination gateway.

VoIP Gateway allows for manual configuration of QoS thresholds depending on the customer preference between cost and voice quality. The Engineering guidelines chapter on page 15 provides the guidelines to determine the quality of service that supported for any given network.

Quality of service parameters

Quality of Service is depends on end-to-end network performance and available bandwidth. A number of parameters determine the VoIP Gateway QoS over the data network.

The VoIP Gateway monitoring function can take about 3 mins to respond to marginal changes in the network condition. Fallback can be caused by any of the following reasons:

- Bad network conditions.
- The remote gateway is out of service.
- No network connection.
- Not enough DSP resources available.

Packet loss

Packet loss is the percentage of packets that do not arrive at their destination. Transmission equipment problems, and high delay and congestion can cause packet loss. In a voice conversation, gaps in the conversation represent packet losses. Some packet loss, less than 5%, can be acceptable without audible degradation in voice quality. Sporadic loss of small packets can be more acceptable than less frequent loss of large packets.

Packet delay

Packet delay is the time between when a packet leaves and when a packet arrives at it's destination. The total packet delay time includes fixed and variable delay. Variable delay is the more manageable delay, while fixed delay depends on the network technology. The distinct network routing of packets are the cause of variable delays. The gateway must be as close as possible to the network backbone (WAN) with a minimum number of hops, to minimize packet delay and increase voice quality.

Delay variation (jitter)

The amount of variation in packet delay is otherwise known as delay variations, or jitter. Jitter affects the ability of the receiving gateway to assemble voice packets received at irregular intervals into a continuous voice stream.

Fallback to circuit-switched voice facilities

If the measured Mean Opinion Score (MOS) for all codecs is below the configured threshold for any monitored gateway, the Fallback to Conventional Circuit-switched services activates. This feature reroutes calls to different trunks such as the Public Switched Telephone Network (PSTN) until the network QoS improves. When the QoS meets or exceeds the threshold, calls route over the IP network.

Disable the fallback feature in the Local Gateway Configuration. With the fallback feature disabled, calls move across the IP telephony trunks no matter the QoS. The fallback feature is only active at call setup. A call in progress does not fall back if the QoS degrades.

Calls fallback if there is no response from the destination, an incorrectly configured remote gateway table, or if there are not enough DSP resources available to handle the new call.

Network Performance Utilities

There are two common network utilities, `Ping` and `Traceroute`. These utilities provide a method to measure quality of service parameters. Other utilities used also find more information about VoIP Gateway network performance.

Note 1: Because data network conditions can vary at different times, collect performance data over at least a 24 hour time period.

Note 2: Use performance utilities to measure performance from each gateway to every other gateway.

Ping

`Ping` (Packet InterNet Groper) sends an ICMP (Internet Control Message Protocol) echo request message to a host, expecting an ICMP echo reply which allows for the measurement of a round trip time to a selected host. By sending repeated ICMP echo request messages, percent packet loss for a route can be measured.

Traceroute

`Traceroute` uses the IP TTL (time-to-live) field to determine router hops to a specific IP address. A router must not forward an IP packet with a TTL field of 0 or 1. Instead, a router discards the packet and returns to the originating IP address an ICMP "time exceeded" message.

`Traceroute` uses this mechanism by sending an IP datagram with a TTL of 1 to the selected destination host. The first router to handle the datagram sends back a "time exceeded" message. This message identifies the first router on the route. The `Traceroute` transmits a datagram with a TTL of 2.

Following, the second router on the route returns a "time exceeded" message until all hops are identified. The Traceroute IP datagram has a UDP Port number not likely to be in use at the destination (normally > 30,000). The destination returns a "port unreachable" ICMP packet. The destination host is identified.

`Traceroute` is used to measure round trip times to all hops along a route, identifying bottlenecks in the network.

Codecs

The term codec refers to the voice coding and compression algorithm used by the DSP on the telephony services and the MSPECs. See the *Enterprise Edge Programming Operations Guide* for additional information on DSP and MSPEC resources.

The codec type for a VoIP Gateway call basis is determined at call setup. The originating gateway indicates to the remote gateway which codec types it supports, starting with the selected order of use. The remote gateway, depending on its capabilities, selects one of the codec types and continues with the call. If both ends cannot agree on a codec type, the call fails.

All gateways in the intranet must use the same codec types.

Each gateway is configured with available codecs with the selected order of use. The codecs configuration must reflect available bandwidth on the network. Codec options are between quality compared to bandwidth.

The supported codec types are configured in the Modifying the Local Gateway Configuration table section on page 65. The G.711 codec provides the best audio quality but uses the greatest amount of bandwidth. The G.729 and G.723.1 codecs use less bandwidth, but reduce audio quality. The installer or administrator determines the best option for the user and the available bandwidth on the intranet. For example, if the WAN link cannot support multiple 64 kbit/s calls, G.711 must not be configured as a supported codec.

Enterprise Edge supports and recommends the following order for codec selection:

- G.729
- G.723.1 (6.3 kbit/s or 5.3 kbit/s)
- G.711

The G.729 codec provides the best balance of quality audio plus bandwidth savings.

For more information about codecs, see the Codec types section on page 37.

Silence compression

G.723.1 and G.729, Annex B support Silence compression.

A key to VoIP Gateway's success in business applications is reducing WAN bandwidth use. Beyond speech compression, the best bandwidth reducing technology is silence compression, also known as silence suppression. Silence compression technology identifies the periods of silence in a conversation, and stops sending IP speech packets during those periods. Telco studies show that in a typical telephone conversation, only about 36-40% of a full-duplex conversation is active. When one person talks, the other listens (known as half-duplex). And there are important periods of silence during speaker pauses between words and phrases.

For more information about silence compression, see the Silence compression section on page 38.

Echo cancellation

When a two-wire telephone cable connects to a four-wire PBX interface or a central office (CO) interface, the system uses hybrid circuits to convert between two wires and four wires. Although hybrid circuits are very efficient in their conversion ability, a small percentage of telephony energy is not converted but instead is reflected back to the caller. This is called echo.

For more information about echo cancellation, see the Echo cancellation section on page 40.

Jitter buffer

A major cause to reduced voice quality is IP network packet delay and network jitter. Network delay represents the average length of time for a packet to move across a network. Network jitter represents the differences in arrival time of a packet. Both important in determining voice quality, delay is like the average, jitter is like the standard deviation.

For more information about jitter buffer, see the Jitter buffer section on page 40.

Fax calls

The Enterprise Edge gateways support T.30 Group 3 fax calls. Fax calls automatically use the G.711 codec and require the associated bandwidth.

For more information about fax calls, see the Fax calls section on page 41.

Alarm Notification

Enterprise Edge uses the Unified Manager to record information about its working status.

See the Maintenance chapter on page 69 for additional information.

Engineering guidelines

The engineering guidelines address the design of an IP trunk network for Enterprise Edge VoIP Gateway. The network contains the following:

- Enterprise Edge VoIP gateways
- Gateways attached to LANs
- Corporate intranet connecting the LANs

The guidelines assume that an installed corporate intranet connects the sites of the IP gateways.

Introduction

IP telephony compresses PCM voice and routes the packetized data over an intranet, to provide virtual analog TIE trunks between gateways. As voice traffic flows through at low marginal cost over existing private IP network facilities with available bandwidth on the private Wide Area Network (WAN) backbone, communication costs are lower.

This chapter provides guidelines for correctly designing a network of IP gateways over the corporate intranet. The chapter describes how to qualify the corporate intranet to support an IP network. This chapter indicates which changes ensure the maintenance of the quality of voice services when transferring those services from the PSTN. This chapter also addresses requirements for the successful integration with a customer's existing local area network (LAN). By following these guidelines the installer can configure the IP to ensure the best cost and quality and within a calculated tolerance.

Enterprise Edge IP telephony

Enterprise Edge IP telephony functions on a correctly provisioned and stable LAN. Delay, delay variation or jitter, and packet loss must be minimized end-to-end across the LAN and WAN. The installer must determine the design and configuration of the LAN and WAN that link the IP telephony system. If the intranet exceeds it’s capacity, new calls to the IP telephony fall back to conventional circuit-switched voice facilities to ensure the quality of service for new calls.

Overview

Traditional networks depend on voice services such as LEC and IXC private lines. With Enterprise Edge IP telephony technology, IP telephony selects a new kind of delivery mechanism that uses packet switching over a data network, a corporate intranet. The IP gateway converts a steady-stream digital voice into fixed length IP packets.

Correct design procedures and rules are a must if a corporate network is expected to deliver voice traffic. The intranet introduces limits, delay, delay variation, and error, at levels that are higher than those delivered by voice networks. Delay between a user talking and a listener reduces the performance of conversations, while delay variation and packet errors introduce glitches in conversation. The connection of the IP gateways to the corporate intranet without preliminary evaluation can result in not acceptable degradation in the voice service.

A good design of the network begins with an understanding of traffic, and the network that carries the traffic. There are three preliminary steps where the installer must begin:

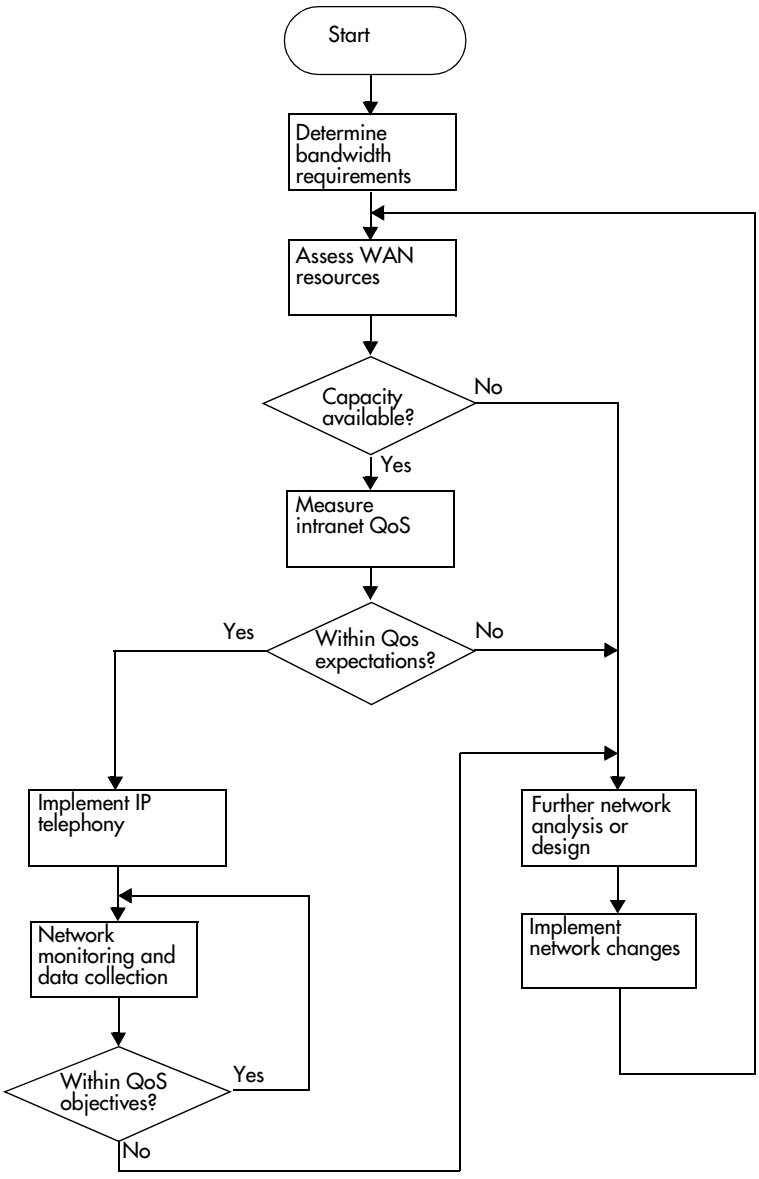
- Determine bandwidth requirements. The installer must determine the amount of traffic that the Enterprise Edge product will route through the IP gateway. This in turn places a traffic load on the corporate intranet. To determine bandwidth requirements, refer to the Enterprise Edge VoIP Gateway bandwidth engineering section on page 17.
- Determine WAN link resources. If there are not enough resources in the corporate intranet to support voice services, the problem is normally because of not enough WAN resources. To determine WAN resources, refer to the Determining WAN link resources section on page 23.
- Measure the existing intranet's QoS. The installer must determine the quality of voice service the corporate intranet can deliver. The Measuring Intranet QoS section on page 27 describes how to measure the delay and error characteristics of an intranet.

After the examination phase, the installer designs and installs the IP telephony network. This design not only includes the IP telephony but can also include making design changes to the intranet.

- The Further network analysis section on page 31 provide guidelines for modifying the intranet.
- The Implementing the network section on page 36 provides guidelines for integrating the IP gateway into the corporate LAN.

Figure 1 IP Telephony network engineering process shows when the design and planning decisions that must occur.

Figure 1 IP Telephony network engineering process



Enterprise Edge VoIP Gateway bandwidth engineering

Traffic controls the network design and the design process starts with the process of getting an IP telephony bandwidth forecast. The bandwidth forecast drives the following:

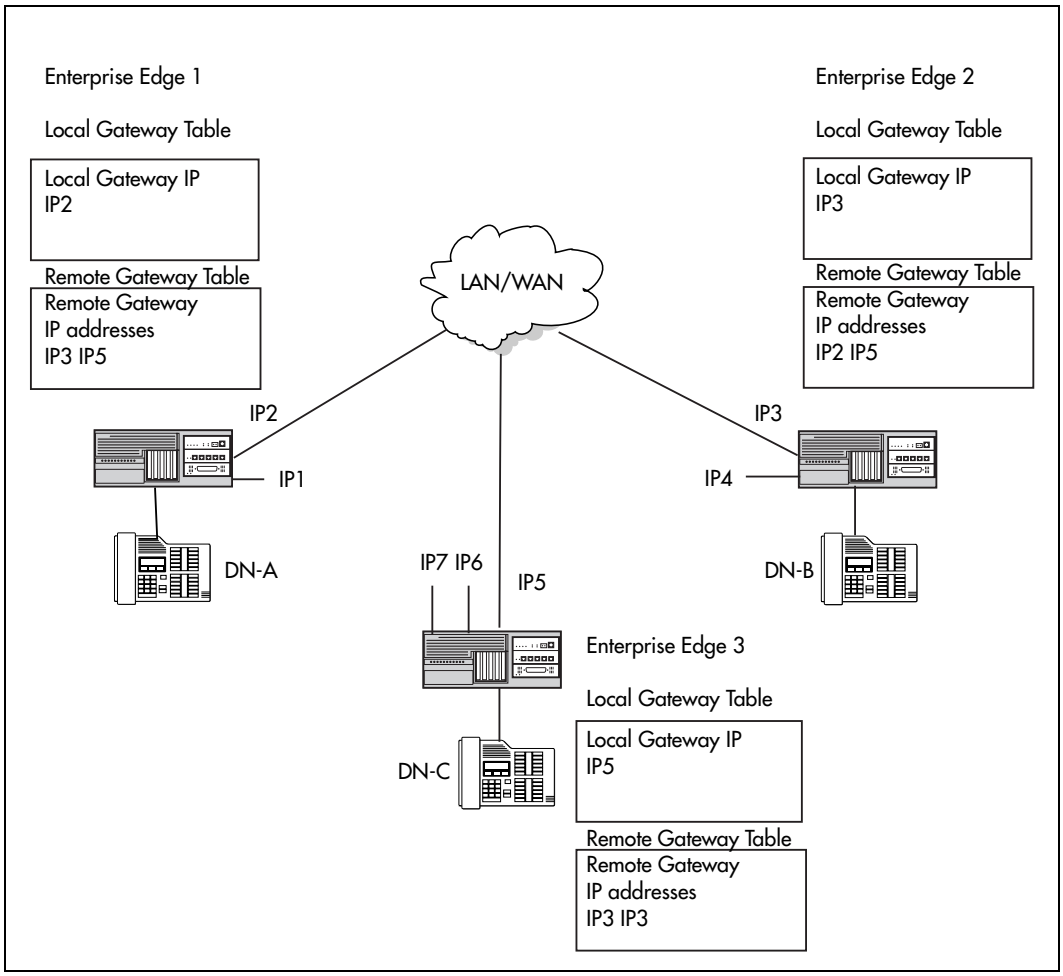
- LAN requirements (LAN must be great enough for the number of calls plus the overhead)
- WAN requirements (WAN must be great enough for the number of calls plus the overhead)

Table 1 LAN and WAN IP bandwidth usage per Enterprise Edge Gateway (loaded to 36 CCS per port per hour) with silence compression on page 20 and Table 2 LAN and WAN IP bandwidth usage per Enterprise Edge Gateway (loaded to 36 CCS per port per hour) without silence compression on page 21 show the bandwidth use for the different codecs. This data assumes that each port is complete to 36 CCS (Centi-call-second). CCS is a channel or circuit occupied for 100 s. The worst case scenario is 100% utilization, or 36 CCS. Engineering the network for worst case numbers ensures that the network can handle peak traffic.

Multiple network interfaces

The Enterprise Edge can have more than one IP address. Figure 2 Multiple network interfaces has three Enterprise Edge systems, each with more than one IP address available. Define the IP address for the VoIP gateway in the Local Gateway table. The other remote gateways use this address to communicate with the Enterprise Edge VoIP Gateway.

Figure 2 Multiple network interfaces



When a user at DN-A calls DN-C, the IP addresses in the Local Gateway and Remote Gateway tables of the each Enterprise Edge systems determine the call routing. The Remote Gateway table of the calling party (EE 1) contains the IP address where the outgoing voice packets are sent (EE 3). The Local Gateway table of EE 1 contains the IP address where EE 3 sends the return voice packets. The Local Gateway table of EE 3 contains the IP address which receives the voice packets from EE 1. The Remote Gateway table of EE 3 contains the IP address where it sends the return voice packets.

There are two methods to set up an IP address.

Method 1

On a routable internal LAN, assign the LAN IP address as the IP address in the Local Gateway table. See the Configuration chapter on page 61 for additional information on entering the Local Gateway IP address.

Method 2

In cases where the LAN is not routable, specify a WAN IP address. If you assign a WAN link as the local gateway IP address and the primary link fails, the VoIP function is lost. See the Configuration chapter on page 61 for additional information on entering the Local Gateway IP address.

For more information, see also the *Enterprise Edge Programming Operations Guide*.

LAN engineering

Engineering the network for worst case numbers indicates the spare bandwidth a LAN must have to handle peak traffic. It is important the LAN be planned to handle the IP telephony traffic using the defined codec, without Ethernet delay or packet loss. The installer or administrator must select one configuration and then set up the LAN so there is more bandwidth than the IP telephony output.

Refer to standard Ethernet engineering tables for passive 10BaseT repeater hubs. Refer to the manufacturer's specification for intelligent 10BaseT layer switches.

Table 1 LAN and WAN IP bandwidth usage per Enterprise Edge Gateway (loaded to 36 CCS per port per hour) with silence compression

Codec Type	Packet duration in ms (payload)	Voice/fax payload in bytes	IP packet in bytes[4]	Ethernet frame bytes[4]	Bandwidth usage on LAN in kbit/s	Bandwidth usage on WAN in kbit/s
G.729[6] (8 kbit/s)	10	10	50	76	60.8	20.0[7]
	20	20	60	86	34.4	12.0
	30	30	70	96	25.6	9.3[7]
G.723.1 (5.3 kbit/s)	30	20	60	86	22.9	8.0
G723.1 (6.3 kbit/s)	30	24	64	90	24.0	8.5

Note 1: LAN data rate is the effective Ethernet bandwidth use.
Note 2: LAN kbit/s = Ethernet frame bytes*8*1000/Frame duration in ms
Note 3: 50% voice traffic reduction due to silence compression; no compression for fax.
Note 4: Overhead of (RTP+UDP+IP) packet over voice packet is 40 bytes; overhead of Ethernet frame over IP packet is 26 bytes.
Note 5: Keep Ethernet bandwidth to support an Interframe gap of at least 12 bytes per frame. This gap is not included in the above bandwidth calculation.
Note 6: IP telephony uses a frame duration of 20 ms for G.729.
Note 7: If interworking with an M1-ITG, other frame durations are supported (configured on the M1-ITG).

Silence compression

If an IP gateway acts as a tandem switch in a network where circuit-switched trunk facilities have a large amount of low audio level, enabling silence compression (also known as Voice Activity Detection) degrades the quality of service, causing broken speech. Under tandem switching conditions, with a large amount of low audio level, disable the silence compression using the IP telephony interface.

With silence compression disabled, the bandwidth use of the LAN/WAN approximately multiplies by two. Table 2 LAN and WAN IP bandwidth usage per Enterprise Edge Gateway (loaded to 36 CCS per port per hour) without silence compression on page 21 shows the full-duplex bandwidth requirements with silence compression disabled.

Fax calls use a G.711 codec which does not support silence compression. Fax calls require 64 kbit/s bandwidth.

For more information about silence compression and fax calls, see the Silence compression on page 38 and the Fax calls section on page 41.

Table 2 LAN and WAN IP bandwidth usage per Enterprise Edge Gateway (loaded to 36 CCS per port per hour) without silence compression

Codec Type	Packet duration in ms (payload)	Voice/fax payload in bytes	IP packet in bytes[4]	Ethernet frame bytes[4]	Bandwidth usage on LAN in kbit/s	Bandwidth usage on WAN in kbit/s
G.711[6] (64 kbit/s)	10	80	240	292	233.6	96[7]
	20	160	400	452	180.8	80
	30	240	560	612	163.2	74.6[7]
G.729[6] (8 kbit/s)	10	10	100	152	121.6	40.0[7]
	20	20	120	172	68.8	24.0
	30	30	140	192	51.2	18.6[7]
G.723.1 (5.3 kbit/s)	30	20	120	172	45.8	16.0
G723.1 (6.3 kbit/s)	30	24	128	180	48.0	17.0

Note 1: LAN data rate is the effective Ethernet bandwidth use.
Note 2: LAN kbit/s = Ethernet frame bytes*8*1000/Frame duration in ms
Note 3: 50% voice traffic reduction due to silence compression; no compression for fax.
Note 4: Overhead of (RTP+UDP+IP) packet over voice packet is 40 bytes; overhead of Ethernet frame over IP packet is 26 bytes.
Note 5: Keep Ethernet bandwidth to support to support an Interframe gap of at least 12 bytes per frame. This gap is not included in the above bandwidth calculation.
Note 6: IP telephony uses a frame duration of 20 ms for G.729 and G.711.
Note 7: If interworking with an M1-ITG, other frame durations are supported (configured on the M1-ITG).

Example 1: LAN engineering – voice calls

Consider a site with four Enterprise Edge IP telephony ports. The Preferred codec is G.729, using a voice payload of 20 ms. Silence compression is enabled.

Given the above, what is the peak traffic in kbit/s that IP telephony will put on the LAN?

With Table 1 LAN and WAN IP bandwidth usage per Enterprise Edge Gateway (loaded to 36 CCS per port per hour) with silence compression on page 20, for calls with silence compression, each port generates 34.4 kbit/s when engaged in a call to another gateway. If all four ports are in use, then the additional load is 137.6 kbit/s.

Example 2: LAN engineering – fax calls

Consider a site with four IP telephony ports. The required codec is G.711, with a voice payload of 20 ms. Silence compression is not used.

With Table 2 LAN and WAN IP bandwidth usage per Enterprise Edge Gateway (loaded to 36 CCS per port per hour) without silence compression on page 21, for calls without silence compression, each fax call generates 180.8 kbit/s. If all four ports are in use for fax calls, then the additional load is 723.2 kbit/s. For more information about fax calls, see the Fax calls section on page 41.

WAN engineering

To get traffic to Wide Area Network (WAN), use the formula: 0.5 x IP packet in bytes x 8 x 1000/payload in ms. The reason for the reduction data rate is because of the type of a duplex channel on a WAN. For example, with G.711 codec, a two-way conversation channel has a rate of 128 kbit/s. However, the same conversation on WAN (for example, a T1) requires a 64 kbit/s channel only, because a WAN channel is a full duplex channel.

Both “talk” and “listen” traffic use a part of the 10 Mbit/s Ethernet channel while a conversation uses a 64 kbit/s (DS0) duplex channel in a T1 or other WAN media.

Example 1: WAN engineering – voice calls

Consider a site with four IP telephony ports. The Preferred codec is G.723.1, 6.3 kbit/s, using a voice payload of 30 ms. Silence compression is enabled.

Given the above, what is the peak traffic in kbit/s that IP telephony will put on the WAN?

With Table 1 LAN and WAN IP bandwidth usage per Enterprise Edge Gateway (loaded to 36 CCS per port per hour) with silence compression on page 20, for silence compression, each port generates 8.5 kbit/s when engaged in a call. If all four ports are in use, then the additional load is 34 kbit/s.

Example 2: WAN engineering – fax calls

Consider a site with four IP telephony ports. The G.711 codec automatically selected, with a voice payload of 20 ms. Silence compression is not used in the G.711 codec.

With Table 2 LAN and WAN IP bandwidth usage per Enterprise Edge Gateway (loaded to 36 CCS per port per hour) without silence compression on page 21, for no silence compression, each port generates 80 kbit/s when engaged in a call. If all four ports are in use, then the additional load is 320 kbit/s.

Determining WAN link resources

For most installations, IP telephony traffic is routed over WAN links within the intranet. WAN links are the most expensive recurring expenses in the network and they often are the source of capacity problems in the network. Different from LAN bandwidth, which is almost free and easily installed, WAN links, especially inter-LATA and international links require time to receive financial approval, provision and upgrade. For these reasons, it is important to determine the state of WAN links in the intranet before installing the IP telephony.

Each voice conversation, (G.729, Annex B codec, 20 ms payload) uses 12 kbit/s of bandwidth for *each* link that moves across in the intranet; a DS0 can support below 5 simultaneous telephone conversations.

Link utilization

The starting point of this evaluation is to get a current topology map and link utilization report of the intranet. A visual inspection of the topology map indicates which WAN links are expected to deliver IP telephony traffic. Also use the `Traceroute` tool (see Measuring Intranet QoS on page 27).

The next step is to find out the current utilization of those links. Note the reporting window that appears in the link utilization report. For example, the link utilization can be an average of a week, a day, or one hour. To be consistent with the dimensioning considerations (see Enterprise Edge VoIP Gateway bandwidth engineering on page 17), get the peak utilization of the trunk. Also, because WAN links are full-duplex that data services show asymmetric traffic behavior, get the utilization of the link representing traffic flowing in the heavier direction.

The third step is to determine the available spare capacity. Enterprise Edge intranets are subject to capacity planning controls that ensure that capacity use remains below some determined utilization level. For example a planning control can state that the utilization of a 56 kbit/s link during the peak hour must not exceed 50%; for a T1 link, the threshold is higher, for example at 85%. The carrying capacity of the 56 kbit/s link can be 28 kbit/s, and for the T1 1.3056 Mbit/s. In some organizations the thresholds can be lower than that used in this example; in the event of link failures, there needs to be spare capacity for traffic to be re-routed.

Some WAN links can be provisioned on top of layer 2 services such as Frame Relay and ATM; the router-to-router link is a virtual circuit, which is subject not only to a physical capacity, but also a “logical capacity” limit. The installer or administrator needs to get the physical link capacity and the QoS parameters. The important QoS parameters are CIR (committed information rate) for Frame Relay, and MCR (maximum cell rate) for ATM.

The difference between the current capacity and its acceptable limit is the available capacity. For example a T1 link used at 48% during the peak hour, with a planning limit of 85% has an available capacity of about 568 kbit/s.

Determining network loading caused by IP telephony traffic

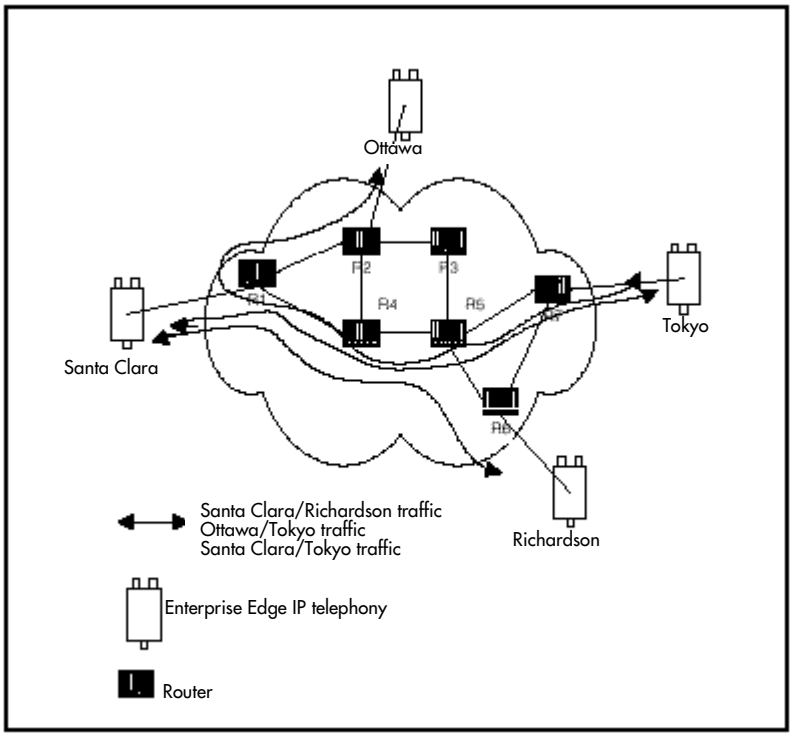
At this point, the installer or administrator has enough information to load the IP telephony traffic on the intranet.

Consider the intranet has the topology as shown Figure 3 Calculating network load with IP telephony traffic on page 24, and the installer or administrator wants to know in advance the amount of traffic on a specific link, R4-R5. Consider there are four IP telephony ports per site.

With the Enterprise Edge VoIP Gateway bandwidth engineering section on page 17 and `Traceroute` measurements, the R4-R5 link is expected to support the Santa Clara/Richardson, Santa Clara/Tokyo and the Ottawa/Tokyo traffic flows. The other IP telephony traffic flows do not route over R4-R5. A peak of eight calls can be made over R4-R5 for the four IP telephony ports per site. R4-R5 needs to support the incremental bandwidth of 8 x 12 = 96 kbit/s.

To complete this exercise, the traffic flow from every site pair needs to be summed to calculate the load on each route and loaded to the link.

Figure 3 Calculating network load with IP telephony traffic



Enough link capacity

Table 3 Link capacity on page 25 sorts the computations so that for each link, the available link capacity is compared against the additional IP telephony load. For example, on link R4-R5, there is capacity (568 kbit/s) to allow for the additional 96 kbit/s of IP telephony traffic.

Table 3 Link capacity

Link		Utilization (%)		Available capacity kbit/s	Incremental IP telephony load		Enough capacity?
End Points	Capacity kbit/s	Threshold	Used		Site pair	Traffic kbit/s	
R1-R2	1536	85	75	154	Santa Clara/ Ottawa Santa Clara/ Tokyo	15.5	Yes
R1-R3	1536						
R2-R3	1536						
R2-R4	1536						
R4-R5	1536	85	48	568	Santa Clara/ Richardson Ottawa/Tokyo Santa Clara/ Tokyo	24	Yes

Some network management systems have network planning modules that determine network flows. These modules provide more detailed and accurate analysis as they can include correct node, link and routing information. They also help the installer or administrator determine network strength by conducting link and node failure analysis. By simulating failures, re-loading network and re-computed routes, the modules indicate where the network can be out of capacity during failures.

Not enough link capacity

If there is not enough link capacity, consider one or more of the following options:

- Use the G.723.1 codec. Compared to the default G.729 codec with 20 ms payload, the G.723.1 codecs use 29% to 33% less bandwidth.
- Upgrade the link's bandwidth.

Other intranet resource considerations

Bottlenecks caused by non-WAN resources do not occur often. For a more complete evaluation consider the impact of incremental IP telephony traffic on routers and LAN resources in the intranet. The IP telephony traffic moves across LAN segments that are saturated, or routers whose CPU utilization is high.

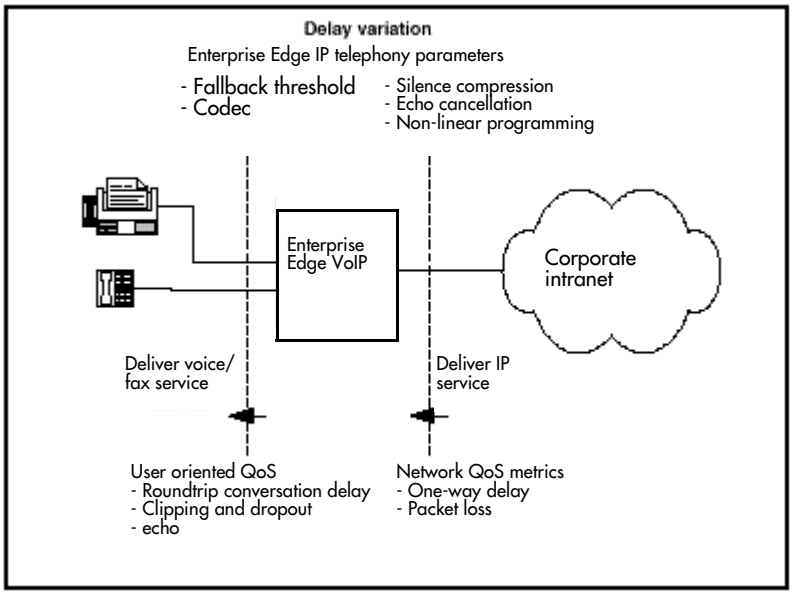
Setting QoS

The users of corporate voice and data services expect these services to meet a level of quality of service (QoS) which in turn affect network design. The purpose is to design and allocate enough resources in the network to meet user needs. QoS metrics or parameters help in meeting the needs required by the user of the service.

There are two interfaces that the installer needs to consider:

- IP telephony interfaces with the end users; voice services made available need to meet user QoS objectives.
- The gateways interface with the intranet; the service provided by the intranet is "best-effort delivery of IP packets," not guaranteed QoS for real-time voice transport. IP telephony translates the QoS objectives set by the end users into IP adjusted QoS objectives. The guidelines call these objectives the intranet QoS objectives.

Figure 4 Relationship between users and services



The IP gateway can monitor the intranet's QoS. In this mode, two parameters, the receive fallback threshold and the transmit fallback threshold control the minimum QoS level of the intranet. Fallback thresholds are set on pair per site basis.

The QoS level is aligned for user QoS metrics that allow to set an acceptable Mean Opinion Score (MOS) level. The administrator can adjust the fallback thresholds to provide acceptable service to the users.

Table 4 Quality of voice service

MOS Range	Qualitative Scale
4.86 to 5.00	Excellent
3.00 to 4.85	Good
2.00 to 2.99	Fair
1.00 to 1.99	Poor

The settings in Table 4 indicate the quality of voice service. IP telephony periodically calculates the prevailing QoS level per site pair based on the measurement of the following:

- one-way delay
- packet loss
- codec

When the QoS level of any remote gateway is below the fallback threshold, all new calls are routed over the standard circuit-switched network.

The computation is taken from the ITU-T G.107 Transmission Rating Model.

Fax is more open to packet loss than the a person's ear; quality starts to degrade when packet loss exceeds 10%. Fax services must be supported with the gateway operating in either the Excellent or Good QoS level. Avoid fax services between site pairs that can guarantee no better than a Fair or Poor QoS level.

Measuring Intranet QoS

Measure the end-to-end delay and error characteristics of the current state of the intranet. These measurements help to set accurate QoS needs when using the corporate intranet to carry voice services.

Measuring end-to-end network delay

The basic tool used in IP networks to get delay measurements is the "`Ping`" program. The `Ping` takes a delay sample by sending an ICMP packet from the host of the `Ping` program to a destination server, and waits for the following:

```
Pinging 10.10.10.15 with 32 bytes of data:
Reply from 10.10.10.15: bytes=32 time=13ms TTL=252
Reply from 10.10.10.15: bytes=32 time=10ms TTL=252
Reply from 10.10.10.15: bytes=32 time=6ms TTL=252
Reply from 10.10.10.15: bytes=32 time=5ms TTL=252
```

The round trip time (rtt) is indicated by the time field

So that the delay sample results match what the gateway experiences, the `Ping` host must be on a correctly working LAN segment on the intranet. The option of destination host is as important, following the same guidelines for the source host.

Set the size of the `Ping` probe packets to 60 bytes to approximate the size of probe packets sent by IP telephony and determine if new calls need to fall back on the circuit-switched voice facilities.

Notice from the `Ping` output the difference of rtt. The repeated sampling of rtt allows you to receive a delay characteristic of the intranet. To get a delay distribution, include the `Ping` tool in a script which controls the frequency of the `Ping` probes, which timestamps and stores the samples in a raw data file.

The file can be analyzed by the administrator using spreadsheet and other statistics packages. The installer can check if the intranet's network management software has any delay measurement modules which can cause a delay distribution measurement for specific site pairs.

Delay characteristics vary depending on the site pair and the time of day. The evaluation of the intranet includes taking delay measurements for each site pair. If there are important changes of traffic in the intranet, include some `Ping` samples during the intranet's peak hour. For a more complete evaluation of the intranet's delay characteristics, get `Ping` measurements over a period of at least a week.

Measuring end-to-end packet loss

The `Ping` program also reports if the packet made its round trip correctly or not. Use the same `Ping` host setup to measure end-to-end errors. Use the same packet size.

Sampling error rate, require taking multiple `Ping` samples (at least 30). An accurate error distribution requires data collection over a greater period of time. The error rate statistic from multiple `Ping` samples is the packet loss rate.

Recording routes

As part of the network evaluation, record routing information for all source destination pairs. Use the `Traceroute` tool to record routing information. A sample of the output of the `Traceroute` tool follows:

```
C:\WINDOWS>tracert 10.10.10.15

Tracing route to 10.10.10.15 over a maximum of 30 hops:

1 3 ms 1 ms <10 ms tftzraf1.ca.nortel.com [10.10.10.1]
2 1 ms 1 ms 1 ms 10.10.10.57
3 7 ms 2 ms 3 ms tcarrbf0.ca.nortel.com [10.10.10.2]
4 8 ms 7 ms 5 ms bcarha56.ca.nortel.com [10.10.10.15]

Trace complete.
```

The `Traceroute` program checks if routing in the intranet is symmetric or not for each source destination pairs. Also, the `Traceroute` program identifies the intranet links used to carry voice traffic. For example, if `Traceroute` of four site pairs gets the results shown Table 5, you can calculate the load of voice traffic per link.

Table 5 Site pairs and routes

Site pair	Intranet route
Santa Clara/Richardson	R1-R4-R5-R6
Santa Clara/Ottawa	R1-R2
Santa Clara/Tokyo	R1-R4-R5-R7
Richardson/Ottawa	R2-R3-R5-R6

Table 6 Computed load of voice traffic per link

Links	Traffic from
R1-R4	Santa Clara/Richardson
R4-R5	Santa Clara/Richardson Santa Clara/Tokyo
R5-R6	Santa Clara/Richardson Richardson/Ottawa
R1-R2	Santa Clara/Ottawa
R1-R4	Santa Clara/Tokyo
R5-R7	Santa Clara/Tokyo
R2-R3	Richardson/Ottawa
R3-R5	Richardson/Ottawa

Adjusting ping measurements

The `Ping` statistics are based on round trip measurements, while the QoS metrics in the Transmission Rating model are one-way. To make the comparison compatible, the delay and packet error `Ping` statistics are halved.

Adjustment for processing

The `Ping` measurements are taken from `Ping` host to `Ping` host. The Transmission Rating QoS metrics are from end user to end user, and include components outside the intranet. The `Ping` statistics for delay needs additional adjustments by adding 140 ms to explain the processing and jitter buffer delay of the gateways.

No adjustment are required for error rates.

If the intranet measurement barely meets the round trip QoS objectives, the one-way QoS is not met in one of the directions of flow. This state can be true when the flow is on a symmetric route caused by the asymmetric behavior of the data processing services.

Late packets

Packets that arrive outside of the window allowed by the jitter buffer are discarded. To determine which `Ping` samples to ignore, calculate the average one-way delay based on all the samples. Add 300 ms to that amount. This amount is the maximum delay. All samples that exceed this one-way delay maximum are considered late and are removed from the sample. Calculate the percentage of late packets, and add that percentage to the packet loss statistic.

Measurement procedure

The following procedure is an example of how to get delay and error statistics for a specific site pair during peak hours.

Program a script to run the `Ping` program during intranet's peak hours, repeatedly sending a series of 50 `Ping` requests. Each `Ping` request generates a summary of packet loss (with a granularity of 2%), and for each successful probe that made its roundtrip, that many *rtt* samples.

For a strong network there must be at least 3000 delay samples and 60 packet loss samples. Have the raw output of the `Ping` results stored in a file. Determine the average and standard deviation of *one-way delay* and *packet loss*.

Repeat this for each site pair. At the end of the measurements, the results are as shown in Table 7.

Table 7 Delay and error statistics

Destination pair	Measured one-way delay (ms)		Measured packet loss (%)		Expected QoS level	
	Mean	Mean+σ	Mean	Mean+σ	Mean	Mean+σ
Santa Clara /Richardson	171	179	2	2.3	Good	Good
Santa Clara /Ottawa						
Santa Clara /Tokyo						
Richardson/ Ottawa						
Richardson/ Tokyo						
Ottawa/Tokyo						

Other measurement considerations

The `Ping` statistics described above measure the intranet before IP telephony installation. The measurement does not take into consideration the expected load provide by the IP telephony users.

If the intranet capacity is tight and the IP telephony traffic important, the installer or administrator must consider making intranet measurements under load. Apply load using traffic generator tools; the amount of load must match the IP telephony offered traffic estimated in the Enterprise Edge VoIP Gateway bandwidth engineering section on page 17.

Decision: does the intranet meet IP telephony QoS needs?

The end of the measurement and analysis is a good indicator if the corporate intranet can deliver acceptable voice and fax services. The Expected QoS level column in Table 7 indicates to the installer or administrator the QoS level for each site pair with the data.

To provide voice and fax services over the intranet, keep the network within a Good or Excellent QoS level at the Mean+σ operating area. Fax services must not travel on routes that have "Fair" or "Poor" QoS levels.

If QoS levels of some or all routes fall short of being “Good”, the installer or administrator needs to evaluate options and costs for upgrading the intranet. Further network analysis on page 31 provides guidelines for reducing *one-way delay*. The evaluation often requires a link upgrade, a topology change, or implementation of QoS in the network.

The installer or administrator can opt for keeping costs down, and accept a Fair QoS level for the time for a selected route. A calculated trade-off in quality requires the installer or administrator monitor the QoS level, reset needs with the end users, and respond to user feedback.

Further network analysis

This section describes actions possible actions to examine the sources of delay and error in the intranet. This section and Implementing QoS in IP networks on page 34 discuss several methods for reducing one-way delay and packet loss. The key methods are:

- Reduce link delay
- Reducing hop count
- Adjust the jitter buffer size
- Setting IP telephony QoS objectives.

Components of delay

End-to-end delay is the result of many delay components. The major components of delay are as follows:

Propagation delay

Propagation delay is the result of the mileage and the medium of links moved across. Within a country, the one-way propagation delay over terrestrial lines is under 18 ms. Within the U.S., the propagation delay from coast-to-coast is under 40 ms. To estimate the propagation delay of long-haul and trans-oceanic circuits, use the rule of thumb of 1 ms per 100 terrestrial miles.

If a circuit goes through a satellite system, estimate each hop between earth stations to adds 260 ms to the propagation delay.

Serialization delay

The serialization delay is the time it takes to transmit the voice packet one bit at a time over a WAN link. The serialization delay depends on the voice packet size and the link bandwidth, and is the result of the following formula:

$$\text{serialization delay in ms} = 8 \times \frac{\text{IP packet size in bytes}}{\text{link bandwidth in kbit/s}}$$

Queuing delay

The queuing delay is the time it takes for a packet to wait in the transmission queue of the link before it is serialized. On a link where packets are processed in a first come first served order, the average queuing time in ms and is the result of the following formula:

$$\text{queuing time in ms} = p \times p \times \frac{\text{average packet size in bytes}}{(1-p)(\text{link speed in kbit/s})}$$

Note: where p is the link utilization level.

The average size of intranet packets carried over WAN links generally is between 250 and 500 bytes. Queueing delays can be important for links with bandwidth under 512 kbit/s, while with higher speed links they can allow higher utilization levels.

Routing and hop count

Each site pair takes different routes over the intranet. The route taken determines the number and type of delay components that add to end-to-end delay. Sound routing in the network depends on correct network design.

Reduce link delay

In this and the next few sections, the guidelines examines different ways of reducing one-way delay and packet loss in the network.

The time taken for a voice packet to queue on the transmission buffer of a link until received at the next hop router is the link delay. Methods to reduce link delays are:

- Upgrade link capacity to reduce the serialization delay of the packet, but more so, reduces the utilization of the link, reducing the queueing delay. Before upgrading a link, the installer or administrator must check both routers connected to the link for the upgrade and ensure correct router configuration guidelines.
- Change the link from satellite to terrestrial to reduce the link delay by on the order of 100 to 300 ms.
- Put into operation a priority queueing rule.
- Identify the links with the highest use and the slowest traffic. Estimate the link delay of these links using `Traceroute`. Contact your service provider for help with improving your QoS.

Reducing hop count

To reduce end-to-end delay can, reduce hop count, especially on hops that move across WAN links. Some of the ways to reduce hop count include:

- Improve meshing. Add links to help improve meshing, adding a link from

router1 to router4 instead of having the call routed from router1 to router2 to router3 to router4 reducing the hop count by two.

- Router reduction. Join co-located gateways on one larger and more powerful router.

Adjust the jitter buffer size

The parameters for the voice jitter buffer directly affect the end-to-end delay and audio quality. IP telephony dynamically adjusts the size of the jitter buffer to adjust for jitter in the network. The installer or administrator sets the starting point for the jitter buffer.

Lower the jitter buffer to decrease one-way delay and provide less waiting time for late packets. Late packets that are lost are replaced with silence. Quality decreases with lost packets. Increase the size of the jitter buffer to improve quality when jitter is high.

IP telephony fax calls use a fixed jitter buffer that does not change the hold time over the duration of the call. Fax calls are more prone to packet loss. In conditions of high jitter, increase delay (through the use of a deeper jitter buffer). To allow for this increase, IP telephony provides a separate jitter buffer setting for fax calls.

Reduce packet errors

Packet errors in intranets correlate to congestion in the network. Packet errors are high because the packets are dropped if they arrive faster than the link can transmit. Identify which links are the most used to upgrade removes a source of packet errors on a distinct flow. A reduction in hop count provides for less occurrences for routers and links to drop packets.

Other causes of packet errors not related to delay are as follows:

- Bad link quality
- Overloaded CPU
- Saturation
- LAN saturation
- Limited size of Jitter buffer

If the underlying circuit has transmission problems, high line error rates, outages, or other problems, the link quality is bad. Other services such as X.25, frame relay or ATM can affect the link. Check with your service provider for information.

Find out what the router’s threshold CPU utilization level is, and check if the router conforms to the threshold. If a router is overloaded, the router is continuously processing intensive tasks. Process intensive tasks prevent the router from forwarding packets. Reconfigure or upgrade the router.

Routers can be overloaded when there are too many high capacity and high traffic links configured on it. Ensure that routers are configured to vendor guidelines.

Saturation refers to too many packets on the intranet. Packets can be dropped on improperly planned or damaged LAN segments.

Packets that arrive at the destination late are not placed in the jitter buffer and are lost packets. See Adjust the jitter buffer size section on page 33.

Routing issues

Routing problems cause not needed delay. Some routes are better than other routes. The Traceroute program allows the user to detect routing anomalies and to correct these problems.

Possible high delay differences causes are:

- routing instability
- wrong load splitting
- frequent changes to the intranet
- asymmetrical routing

Implementing QoS in IP networks

Corporate intranets developed to support data services. Accordingly, normal intranets are designed to support a set of QoS objectives dictated by these data services.

When an intranet takes on a real-time service, users of that service set additional QoS objectives in the intranet; some of the targets can be less controlled compared with the targets set by current services, while other targets are more controlled. For intranets not exposed to real-time services in the past but now need to deliver IP telephony traffic, QoS objectives for delay can set an additional design restriction on the intranet.

One method is to subject all intranet traffic to additional QoS restrictions, and design the network to the strictest QoS objectives. A exact plan to the design improves the quality of data services, although most applications cannot identify a reduction of, say, 50 ms in delay. Improvement of the network results in one correctly planned for voice, but over planned for data services.

Another plan is to consider using QoS mechanisms in the intranet, the purpose of which is to provide a more cost-effective solution to engineering the intranet for non-homogenous traffic types.

Traffic mix

This section describes what QoS mechanisms work with the IP telephony, and with what new intranet-wide results if done.

Before putting into operation QoS mechanisms in the network, determine the traffic mix of the network. QoS mechanisms depend on the process and ability to determine traffic (by class) so as to provide different services.

With an intranet designed only to deliver IP telephony traffic, where all traffic flows are equal priority, there is no need to consider QoS mechanisms. This network can have one class of traffic.

In most corporate environments, the intranet is supporting data and other services. When planning to provide voice services over the intranet the installer determine the following:

- Are there existing QoS mechanisms? What kind? IP telephony traffic must take advantage of established mechanisms if possible.
- What is the traffic mix? If the IP telephony traffic is small compared to data traffic on the intranet, then IP QoS mechanisms can do. If IP telephony traffic is a large amount, data services can be hit if those mechanisms are biased toward IP telephony traffic.

TCP traffic behavior

Most of corporate intranet traffic is TCP-based. Different from UDP, that has no flow control, TCP uses a sliding window flow control mechanism. Under this design TCP increases its window size, increasing throughput, until congestion occurs. Congestion results in packet losses, and when that occurs the throughput decreases, and the whole cycle repeats.

When multiple TCP sessions flow over few congestion links in the intranet, the flow control algorithm can cause TCP sessions in the network to decrease at the same time, causing a periodic and synchronized surge and ebb in traffic flows. WAN links can appear to be overloaded at one time, and then followed by a period of under-utilization. There are two results:

- bad performance of WAN links
- IP telephony traffic streams are unfairly affected

Enterprise Edge Router QoS Support

In Enterprise Edge, the VoIP gateway and the router are in the same box. The Enterprise Edge router performs QoS and priority queuing to support VoIP traffic. The router supports VoIP in the following two ways:

- In a DiffServ network, Enterprise Edge acts as a DiffServ edge device and performs packet classification, prioritization, and marking. The router performs admission control for H.323 flows based on the WAN link bandwidth and

utilization. When received, the WAN link marks the H.323 flows as Premium traffic and places the flows in the high priority queue.

Note: Differentiated Service (DiffServ) is a QoS framework standardized by IETF.

- In a non DiffServ or legacy network, the router manages the WAN link to make sure Premium VoIP packets have high priority in both directions when crossing a slow WAN link.

Implementing the network

LAN engineering

To minimize the number of router hops between the systems, connect the gateways to the intranet, ensuring there is enough bandwidth on the WAN links shorter routes. To prevent division of the constant bit-rate IP telephony traffic from bursty LAN traffic, and make easier the end-to-end Quality of Service engineering for packet delay, jitter, and packet loss, place the gateway and the LAN router near the WAN backbone.

With supported codecs through the IP telephony network set to G.729, G.723.1 6.3 kbit/s, G.723.1 5.3 kbit/s, and G.711, ensure that up to 8 ports share the same 10BaseT LAN collision domain.

For the deployment of a mixed codec IP telephony, refer to Table 1 LAN and WAN IP bandwidth usage per Enterprise Edge Gateway (loaded to 36 CCS per port per hour) with silence compression on page 20 to estimate the amount of LAN bandwidth used.

Setting the Quality of Service threshold for fallback routing

Configure the Quality of Service thresholds for fallback routing in the IP telephony Manager application. Configure a threshold for both the receive fall back threshold (Rx) and the transmit fall back threshold (Tx). The available thresholds are: Excellent, Good, Fair, and Poor.

Table 8 Sample Mean Opinion Score to qualitative scale

MOS Range	Qualitative Scale
4.86 to 5.00	Excellent
3.00 to 4.85	Good
2.00 to 2.99	Fair
1.00 to 1.99	Poor

Set the MOS values using the lowest number matching to the required threshold. You can adjust the MOS values to fine tune the fallback scale.

IP telephony settings

Codec types

The term codec refers to the voice coding and compression algorithm used by the DSP on the telephony services and the MSPECs. See the *Enterprise Edge Programming Operations Guide* for additional information on DSP and MSPEC resources.

Determine the codec type for a VoIP Gateway call basis at call setup. The originating gateway indicates to the remote gateway which codec types it supports, starting with the selected order of use. The remote gateway, depending on its capabilities, selects one of the codec types and continues with the call. If both ends cannot agree on a codec type, the call fails.

All gateways in the intranet must use the same codec types.

Configure each gateway with available codecs with the selected order of use. The codecs configuration must reflect available bandwidth on the network. Codec options are between quality compared to bandwidth.

The supported codec types are configured in the Modifying the Local Gateway Configuration table section on page 65. The G.711 codec provides the best audio quality but uses the greatest amount of bandwidth. The G.729 and G.723.1 codecs use less bandwidth, but reduce audio quality. The installer or administrator determines the best option for the user and the available bandwidth on the intranet. For example, if the WAN link cannot support multiple 64 kbit/s calls, G.711 must not be configured as a supported codec.

Enterprise Edge IP Telephony supports and recommends the following order for codec selection:

- G.729
- G.723.1 6.3 kbit/s or 5.3 kbit/s
- G.711

The G.729 codec provides the best balance of quality audio plus bandwidth savings.

G.729

The G.729 codec is the default and Preferred codec for IP telephony. The G.729 codec provides near toll quality with a low delay. This codec uses compression to 8 kbit/s. Enterprise Edge VoIP Gateway supports G.729 with silence compression, per Annex B.

G.723.1

The G.723.1 codec uses the smallest amount of bandwidth. This codec uses the greatest compression, 5.3 kbit/s or 6.3 kbit/s.

The G.723.1 codec uses a different compression method than the G.729 codec. The G.723.1 method uses more DSP resources. Each MSPEC supports one G.723.1 call. A G.711 call can run in the same MSPEC as a G.723.1 call. See the *Enterprise Edge Programming Operations Guide* for additional information.

If the G.723.1 codec is the only possible codec for a call, a trunk can not be available for the call if there are not enough DSP resources available. All VoIP Gateway facilities can appear to be in use, although there are DSP resources available for calls using other codec types.

Because most gateways support the G.711 codec, configure G.711 as a supported codec. The G.711 codec does not compress audio or fax. The G.711 codec supports two IP trunks on each MSPEC. See the *Enterprise Edge Programming Operations Guide* for additional information.

G.711

This codec delivers “toll quality” audio at 64 kbit/s. This codec is best for speech because it has the smallest delay, and is very strong to channel errors. However, the G.711 codec uses the largest bandwidth. North America uses G.711 μ-LAW and international markets use G.711 A-LAW.

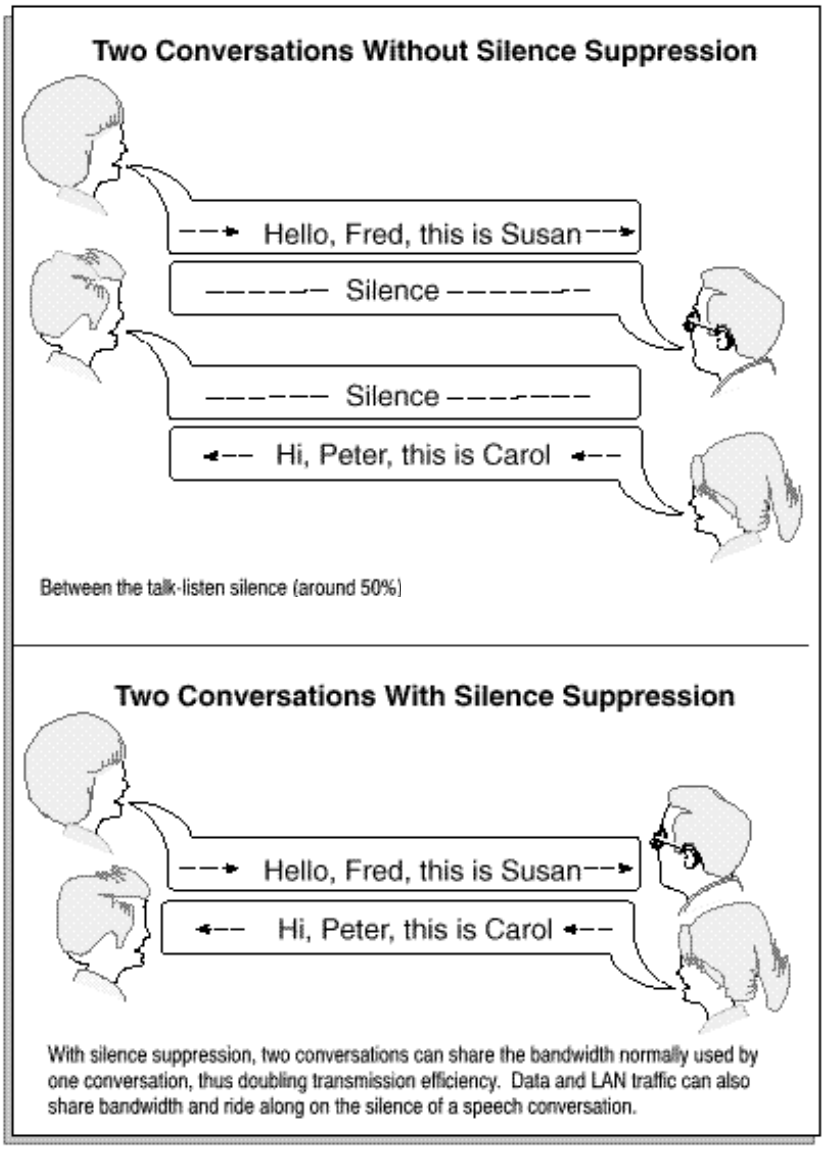
Silence compression

G.723.1 and G.729, Annex B support Silence compression.

A key to VoIP Gateway’s in business applications is reducing WAN bandwidth use. Beyond speech compression, the best bandwidth reducing technology is silence compression, also known as silence suppression. Silence compression technology identifies the periods of silence in a conversation, and stops sending IP speech packets during those periods. Telco studies show that in a typical telephone conversation, only about 36-40% of a full-duplex conversation is active. When one person talks, the other listens (known as half-duplex). And there are important periods of silence during speaker pauses between words and phrases.

By applying silence compression, full duplex bandwidth use is reduced by the same amount, releasing bandwidth for other voice/fax or data communications. Figure 5 Silence compression shows how silence compression allows two conversations to fit in the bandwidth otherwise used by one. This 50% bandwidth reduction develops over a 20-30 second period as the conversation switches from one direction to another.

Figure 5 Silence compression



To provide a more natural sound, comfort noise is added at the destination gateway during the silent periods to calls where silence compression is active. Silence compression can cause a sensed degradation in audio quality. Silence compression can be disabled. With silence compression disabled, the bandwidth use of the LAN/WAN approximately multiplies by two.

If an IP gateway acts as a tandem switch in a network where circuit-switched trunk facilities have a large amount of low audio level, enabling silence compression degrades the quality of service, causing broken speech. Under tandem switching conditions, with a large amount of low audio level, disable the silence compression using the IP telephony interface.

Fax calls use a G.711 codec which does not support silence compression. Fax calls require 64 kbit/s bandwidth. For more information about fax calls, see the Fax calls section on page 41.

Echo cancellation

When a two-wire telephone cable connects to a four-wire PBX interface or a central office (CO) interface, the system uses hybrid circuits to convert between two wires and four wires. Although hybrid circuits are very efficient in their conversion ability, a small percentage of telephony energy is not converted but instead is reflected back to the user. This is called echo.

If the user is near the PBX or CO switch, the echo comes back so quickly it cannot be detected. However, if the delay is more than about 10 ms, the user can hear an echo. To prevent this occurrence, gateway vendors include special code in the DSPs that listens for the echo signal and subtracts it from the listener's audio signal.

Echo cancellation is important for gateway vendors because the IP network delay can be 40–50 ms, so the echo from the far-end hybrid can be important at the near end. Far-end echo cancellation removes this.

Echo cancellation can cause broken speech in conversations in a low audio conversation. Although echo cancellation can be disabled, it is not recommended.

Non-linear processing

Non-linear processing (NLP) is part of echo cancellation. It improves echo cancellation by reducing remaining echo. NLP mutes background noise during periods of far-end silence and prevents additional comfort noise from occurring. Some listeners find muted background noise a problem. NLP can be disabled to prevent this, but with the trade-off of increased heard echo.

Jitter buffer

A major cause to reduced voice quality is IP network packet delay and network jitter. Network delay represents the average length of time for a packet to move across a network. Network jitter represents the differences in arrival time of a packet. Both important in determining voice quality, delay is like the average, jitter is like the standard deviation.

To allow for differences in arrival time of a packet and continue to produce a steady out-going stream of speech, the far-end gateway does not play out the speech when the first packet arrives. Instead, it holds it for a some time in part of its memory called the jitter buffer, and then plays it out. The amount of this hold time is the measure of the jitter buffer, for example, a 50 ms hold time indicates a 50 ms jitter buffer.

As the network delay (total time, including codec processing time) exceeds about 200 ms, the two speakers increasingly use a half-duplex communications mode, where one speaks, the other listens and pauses to make sure the speaker is done. If the pauses are ill timed, they end up "stepping" on each other's speech. This is the problem that occurs when two persons speak over a satellite telephony connection. The result is a reduction in voice quality.

When a voice packet is delayed and does not arrive at the far-end in time to fit into the voice stream going out of the far-end gateway, it is discarded, and the previous packet is replayed. If the scenario occurs often, or twice in a row, the listener hears reduced voice quality.

The jitter buffer hold time adds to the delay, so if the network has high jitter, the effect is a long delay in the voice stream. For example, a network can have an average delay of 50 ms and a variability of 5 ms. The network is said to have 5 ms of jitter, a low figure. The jitter buffer hold time is only 5 ms, so the network total delay is 55 ms.

If a network has a low average delay of 15 ms, but 10% of the time the delay goes out to a 100 ms, while 90% of the time the delay is a brief 4 ms, the jitter buffer is 100 ms and the total network delay is 115 ms, a long delay. Network jitter can be more important than average delay in many VoIP Gateway applications.

VoIP Gateway voice calls use an adaptive jitter buffer that changes the hold time over the duration of the call. The installer or administrator configures the maximum hold time.

VoIP Gateway fax calls use a fixed jitter buffer that does not change the hold time over the duration of the call. Fax calls are more prone to packet loss. In conditions of high jitter, increased delay (through the use of a deeper jitter buffer) is preferred. To adapt, VoIP Gateway provides a separate jitter buffer setting for fax calls.

The voice jitter buffer parameters directly affect the end-to-end delay and audio quality. IP telephony dynamically adjusts the size of the jitter buffer to adjust for jitter in the network. The installer or administrator sets the starting point for the jitter buffer.

Fax calls

The Enterprise Edge gateways support T.30 Group 3 fax calls. Fax calls automatically use the G.711 codec and require the associated bandwidth.

As the gateway does not know in advance that a call carries a fax transmission, it first establishes a voice channel. The voice channel can use G.729 or G.723.1 audio compression. When detecting the answering fax machine’s CED tone, the terminating gateway performs the following operations:

- Starts the procedure to revert the speech path to a G.711, 64 Kbit/s clear channel.
- Disables the adaptive jitter buffer feature.
- Sets the hold time for the jitter buffer to the value indicated in the Local Gateway settings to improve late IP packet tolerance.

The answering fax machine must produce its CED tone within 15 s of connection. The terminating gateway turns off CED tone detection after 15 s to prevent false tone detection during a voice call.

This method sets the following restrictions:

- Interoperability with other IP gateways. A terminating gateway must support CED fax tone detection, and start the procedure as described in previous paragraphs. An originating gateway must support the H.323 Request Mode procedure, but does not need to detect fax tones. The originating gateway must additionally be capable of supporting the large G.711 packets used for fax transmission.
- In order for the gateways to revert to a G.711 clear channel, the terminating fax machine must issue a CED tone when answering the call. Manually started fax transmissions, where the user at the terminating end first talks with the originating user before setting the terminating fax to receive the document, are not supported.
- Fax machines allow a maximum round trip delay of 1200 ms. Media processing in the two gateways introduces a round trip delay of approximately 300 ms, and the delay caused by the jitter buffer. If a 250 ms jitter buffer is used, IP latency must never exceed (1200 - (300 + (2 x 250))) = 400 ms round trip delay, or approximately 200 ms one way.

Fallback threshold

Fallback threshold has two parameters, the receive fallback threshold (Rx) and the transmit fallback threshold (Tx), set on a per site pair basis.

The Setting QoS section on page 26 and Measuring Intranet QoS section on page 27 describe the process to determine the appropriate QoS level for operating the voice network. Site pairs can have very different QoS measurements, either because some traffic flows are local, while other traffic flows are inter-continental. The installer or administrator can consider setting a higher QoS level for the local sites compared to the international sites, keeping cost of international WAN links down.

Normally, set the fallback threshold in both directions to the same QoS level. In site pairs where the applications are so that one direction of flow is more important, the installer or administrator can set up asymmetric QoS levels.

Enterprise Edge uses routes to determine which outgoing facilities to use. A given destination code can have an alternate route configured. The alternate route is used if the main route is not available to process calls. For example, calls use the alternate route if all lines in the line pool are busy. See the *Enterprise Edge Programming Operations Guide* for more information.

IP trunks can use this capability. Unique to IP trunks is the ability to take advantage of the QoS monitoring capability that is part of IP telephony. If fallback functionality enabled, any QoS damage in the intranet which causes any monitored remote gateway to exceed its threshold results in the configuration of an alternate route (if configured). Until the QoS improves, IP trunks are all considered busy.

Enable QoS monitoring for the required destination in the Modifying the Remote Gateway Configuration table on page 66. To prevent a few bad sites from starting fallback, disable the QoS monitoring for remote gateways which have QoS problems until solved.

Set the Tx and Rx thresholds (MOS numbers) for the remote gateway with the required QoS level as indicated in the Modifying the Remote Gateway Configuration table on page 66.

The fallback threshold algorithm considers a fixed IP telephony delay of 140 ms. This delay is based on the default settings and its delay monitoring probe packets. The fallback mechanism does not adjust when the parameters are modified from their default values. Users can sense a lower quality of service than the QoS levels at fallback thresholds when:

- Delay variation in the intranet is important. If the standard deviation of one-way delay is like the jitter buffer maximum delay, it means that there is a group of packets that arrive late to be used by the gateway in the playout process.
- The jitter buffer is increased. The real one-way delay is greater than that estimated by the delay probe.
- The codec is G.711. The voice packets formed by this codec are larger (120 to 280 bytes) than the delay probe packets (60 bytes). This means there is a greater delay felt per hop. If there are low bandwidth links in the path, then the one-way delay is higher both in terms of average and variation.

Dialing plan

The dialing plan determines the digits used to make and receive calls over the IP telephony. Because all the gateways attached to the intranet must work together, the installer and administrator ensures the control of the configuration of all gateways, including the dialing plan and codec selections. A local gateway at one location is a remote gateway from another location and reversed.

IP telephony supports wildcards through the best match algorithm. All calls which do not have a specific match in the Modifying the Remote Gateway Configuration table on page 66 route through the generic IP address.

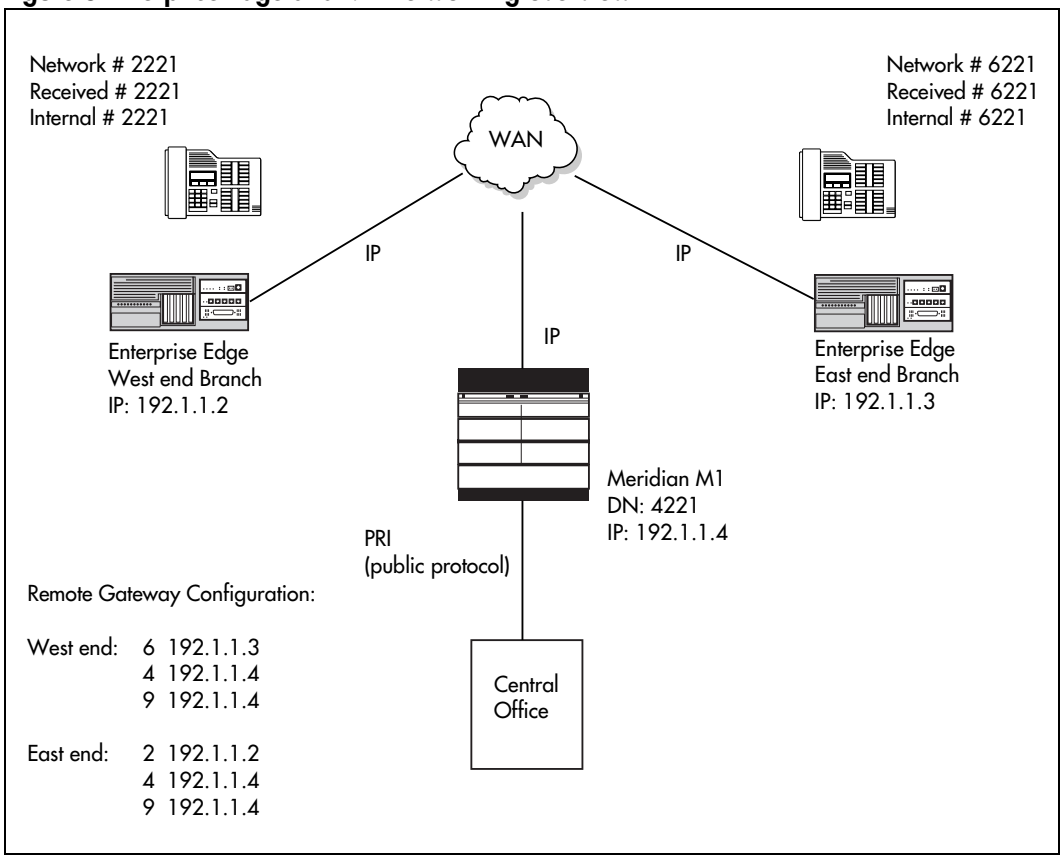
IP telephony and M1 networking

This example shows a private network made of one central Meridian 1, and two smaller sites with Enterprise Edge systems connected over IP trunks through a corporate IP network. This example can represent a large head office (with the Meridian 1) connected to several smaller branch offices.

In this network, only the head office has trunks connected to the public network. The branch offices access the public network using IP trunks to the head office. This configuration allows to save costs and to join together public access trunks. Users at all three locations access the public network by dialing ‘9’, followed by the public number. For example, a user in the west end branch can dial 9-555-1212 (for a local call) or 9-1-613-555-1212 (for a long distance call). These public calls routes to the Meridian 1 by the Enterprise Edge’s routing table. Routing tables at the Meridian 1 select an appropriate public facility for the call.

Private network calls are done by dialing a 4-digit private network DN. For example, if a user in the west end branch calls a user in the east end branch within the private network, they dial 6221.

Figure 6 Enterprise Edge and M1 networking overview



If the quality of the IP trunk connection during initial call setup rates as poor, Enterprise Edge finds an alternate route to complete the call (fallback) based on the programming definitions in the routing table. In this example, if the quality of the IP connection is poor during the call setup phase, the call can fail. For an example of fallback programming, refer to the section, Toll bypass with VoIP telephony on page 47.

Note: Enterprise Edge IP telephony requires a keycode. After entering the keycode for Enterprise Edge IP Telephony, perform a warm reset by following the procedure in the Maintenance chapter of the *Enterprise Edge Programming Operations Guide*.

In Table 9 Private and public network routing (West End to East End office), private network routing information appears in gray. Public network routing information appears in white.

The Call Managers examine the dialed digits and route the call to the matching IP address.

Table 9 Private and public network routing (West End to East End office)

Heading	Parameter	Setting
West End office:		
Trunk/Line Data	Line 241	Target line
	Received #	2221
Line Access	Set 2221	L241:Ring only
	Line pool access	Line pool A
To Head office (M1):		
Service/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	None
To East End:		
Service/Routing Service	Destination Code	6
	Normal route	001
	Absorb	None
To Public Network:		
Service/Routing Service	Route	002
	Use	Pool A
	External #	(leave blank)
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	None
East End office:		
Trunk/Line Data	Line 241	Target line
	Received #	6221
Line Access	Set 6221	L241:Ring only
	Line pool access	Line pool A

To Head Office: (M1)

Heading	Parameter	Setting
Service/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	None
To West End:		
Service/Routing Service	Destination Code	2
	Normal route	001
	Absorb	None
To Public Network:		
Service/Routing Service	Route	002
	Use	Pool A
	External #	(leave blank)
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	None

In this example, outgoing public network calls dialed from a Enterprise Edge route to the Meridian M1, and the Meridian M1 is responsible for seizing a public trunk. For this reason, the ‘9’ prefix remains in the number passed to the Meridian 1.

Note: For IP trunks, ensure the programming selection is Line Pool A.

Set the Private Network Access Code to ‘9’ on each Enterprise Edge system to ensure the algorithm for outgoing IP calls include this additional digit.

The Meridian M1 must identify incoming 2xxx and 6xxx DID calls, and route the call over IP trunks to either the East or West end offices.

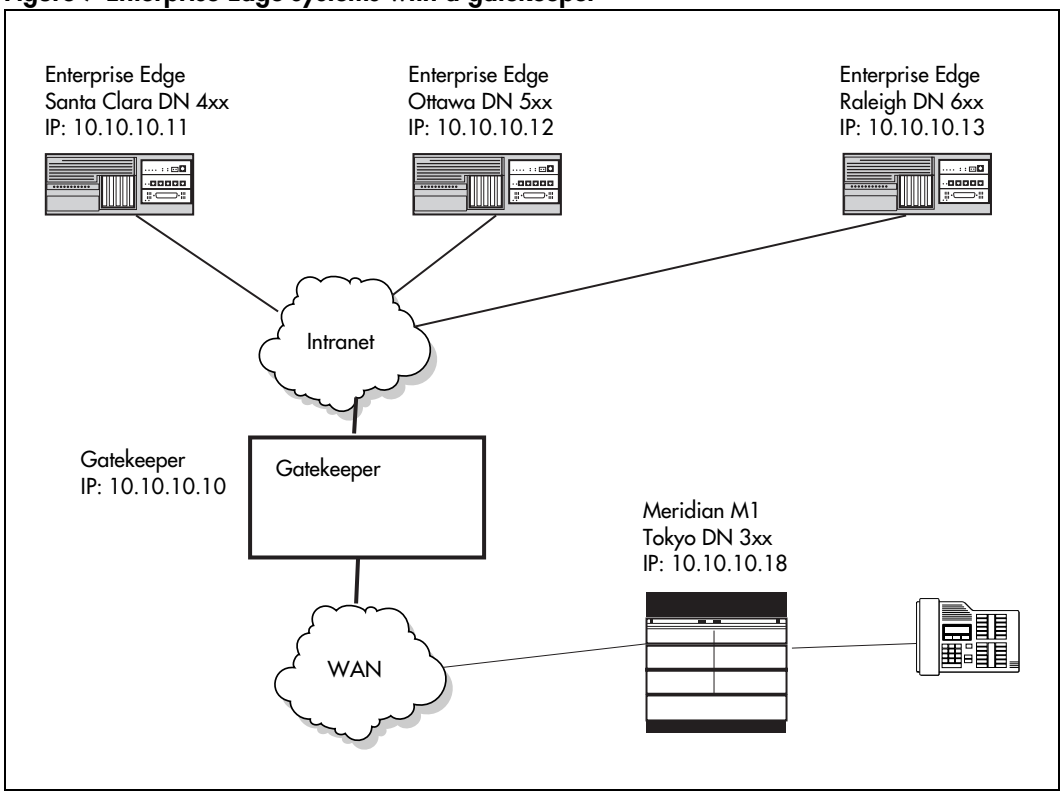
The Meridian M1 must identify numbers starting with ‘9’ as public numbers, when the numbers are dialed by Meridian M1 users or by Enterprise Edge Solution users.

Enterprise Edge and a Gatekeeper

Enterprise Edge supports the use of an ITU-H.323 gatekeeper. A gatekeeper is a third party software installed on a server to centralize IP address configuration information. Each port on the network receives an aliasname. Instead of having remote gateway tables on each Enterprise Edge system, the gatekeeper contains the remote gateway table. The aliasname is linked to an IP address by the gatekeeper. If an IP address changes, only the gatekeeper need updating as the aliasname remains the same.

See the gatekeeper's software documentation for information about changing IP addresses.

Figure 7 Enterprise Edge systems with a gatekeeper



A user in Tokyo at DN300 dials DN400. The least cost routing is over the internet. The Tokyo Meridian M1 connects to the destination IP address in its remote gateway table for DN4xx. That address is the gatekeeper. The gatekeeper identifies DN4xx as a Santa Clara DN. The gatekeeper performs address resolution from the Santa Clara aliasname to the IP address 10.10.10.11. The call connects to the Santa Clara Enterprise Edge, routed to DN400.

Toll bypass with VoIP telephony

This example shows a private network with one Enterprise Edge system in Toronto and one system in Ottawa, connected over IP trunks through a corporate IP network.

Each system has a PRI trunk to the Central Office, and IP trunks to the other system. Calls arrive from Toronto to the Ottawa and the Ottawa public network over IP trunks with fallback to the PRI trunks when IP trunks are overflowed. This configuration allows for reduced costs, using the corporate IP network when possible, bypassing toll charges and other charges when using the public network.

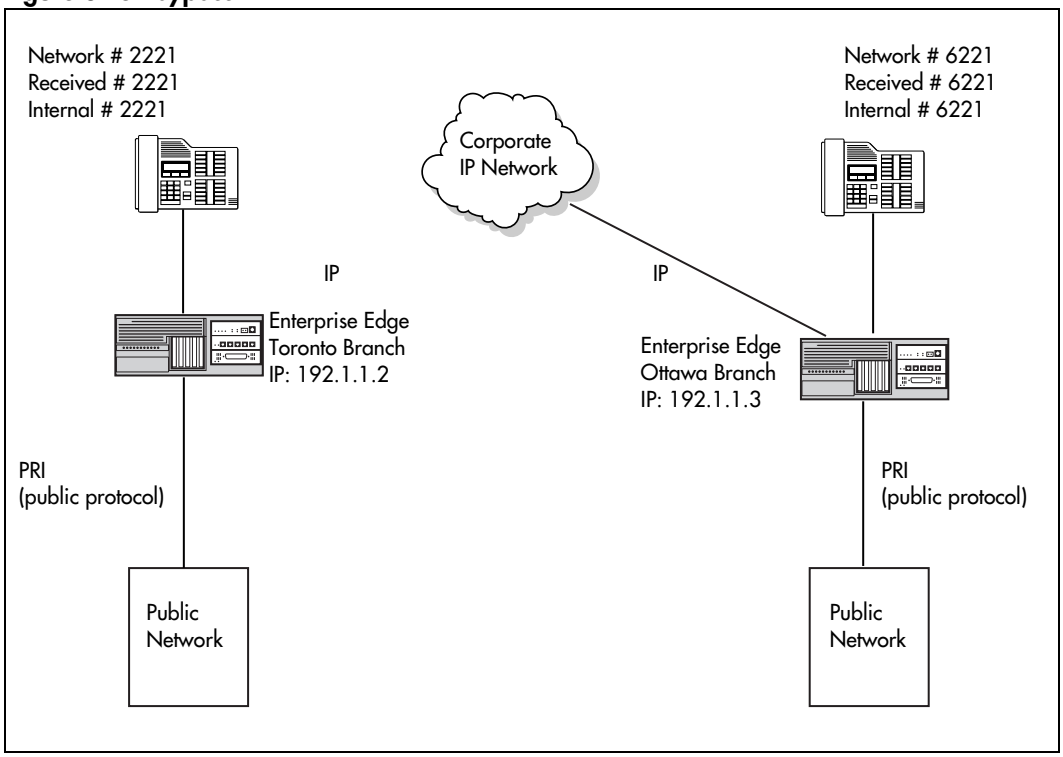
Note: When a call gets rerouted over the PSTN as a result of congestion, the user can see a prompt "Expensive route." The warning indicates that toll charges can apply to this call.

Users at both locations access the public network by dialing ‘9’ , followed by the public number. For example, a user in Toronto can dial 9-555-1212 (for a local call), or 9-1-613-555-1212 (for a long distance call to Ottawa). Local calls can go to the Central Office over PRI trunks. Long distance calls to Ottawa can go over IP trunks; the Ottawa system can tandem these calls to the local Central Office over PRI trunks.

Private network calls are done by dialing a 4-digit private network DN. For example, if a user in the west end branch calls a user in the east end branch within the private network, they dial 6221.

Note: Enterprise Edge IP telephony requires a keycode. After entering the keycode for Enterprise Edge IP Telephony, perform a warm reset by following the procedure in the Maintenance chapter of the *Enterprise Edge Programming Operations Guide*.

Figure 8 Toll bypass



The Call Manager at the Toronto office examines the dialed digits and determines the call can be routed to the IP address matching to the Ottawa office. The Ottawa office receives the call, sees that the leading digit(s) match its Private Network Access Code, and uses a destination code to route the call over its public trunks to the PSTN.

This is a common example with only calls to the 613 Area Code routed by the Ottawa node. In a real world configuration, it can be a consideration to handle Area Codes that are ‘close’, for example Montreal: 514.

In Table 10 Private and public network routing (Toronto to Ottawa office) on page 49, private network routing information appears in gray. Public network routing information appears in white.

Table 10 Private and public network routing (Toronto to Ottawa office)

Heading	Parameter	Setting
Toronto office:		
Lines/Trunk/Line Data	Line 241	Target line
	Received #	2221
Terminals & Sets/Line Access	Set 221	L241:Ring only
	Line pool access	Line pool A Line pool PRI-A
Calls to Ottawa office:		
Services/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
Services/Routing Service	Route	002
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Private
Services/Routing Service	Destination Code	6
	Schedule 4	001
	Absorb	None
	Normal route	002
	Absorb	None
Calls to Ottawa Public Network:		
Services/Routing Service	Route	003
	Use	Pool A
	External #	(leave blank)
	DN type	Public
	Route	004
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Public
	Destination Code	91613
	Normal route	004
	Absorb	1
	Schedule 4	003
	Absorb	None

Heading	Parameter	Setting
To Public Network:		
Services/Routing Service	Destination Code	9161A
	Normal route	004
	Absorb	1
	Destination Code	916A
	Normal route	004
	Absorb	1
	Destination Code	91A
	Normal route	004
	Absorb	1
	Destination Code	9A
	Normal route	004
	Absorb	1
Ottawa office:		
Trunk/Line Data	Line 241	Target line
	Received #	6221
Line Access	Set 6221	L241:Ring only
	Line pool access	Line pool A Line pool PRI-A
To Toronto office:		
Services/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
	Route	002
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Private
	Destination Code	2
	Normal route	002
	Absorb	None
	Schedule 4	001
	Absorb	None
To Toronto Public Network:		
Services/Routing Service	Route	003
	Use	Pool A
	External #	(leave blank)
	DN type	Public

Heading	Parameter	Setting
Services/Routing Service	Route	004
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Public
	Destination Code	91416
	Normal route	004
	Absorb	1
	Schedule 4	003
	Absorb	None
To Public Network:		
Services/Routing Service	Destination Code	9141A
	Normal route	004
	Absorb	1
	Destination Code	914A
	Normal route	004
	Absorb	1
	Destination Code	91A
	Normal route	004
	Absorb	1
	Destination Code	9A
	Normal route	004
	Absorb	1

The impact on the configuration on each node are:

- each node must have the Private Network Access Code set to the value 9.
- each node must have destination codes that match the Private Network Access Code plus digits matching to calls terminating in the local PSTN. For example, if the Private Network Access Code is ‘9’, the node in Ottawa can require a destination code of ‘91613’. In the same way, Toronto can require the following destination code: 91416.

Note: For IP trunks, ensure the programming selection is Line Pool A.

To allow for fallback to PRI trunks when the IP trunks are overflowed, you must program the following Routing service settings:

- Set the start and end times for Sched 4 to 1:00 to allow IP calls can 24 hours a day.
- Program the Sched 4 Service setting to Auto and enable overflow routing by changing the Overflow setting to Y (Yes).
- Define a control set for all sets on the system that make calls over IP trunks. See the *Enterprise Edge Programming Operations Guide* for more information.

Program Remote Packages so that the IP trunks in Pool A can access the lines in Pool PRI-A in a toll bypass plan. A Remote Package is a set of capabilities associated with an incoming trunk. The default package is fully restricted, so to change the restrictions, configure a new Remote Package for each trunk. For example, you give package 01 access to pool PRI-A and you assign package 01 to all IP trunks. For more information, see the *Enterprise Edge Programming Operations Guide*.

Core telephony services configuration

IP telephony ports represent private IP trunking facilities by the core telephony services.

The core telephony services require configuration to enable calls to use IP telephony ports as IP trunks. The user indicates the required destination by dialing digits. The dialing plan determines the digits required to reach each destination.

The user dials a destination code configured to select a fixed route which in turn, selects a line pool. A line pool is a group of trunk facilities. This configuration process allows the administrator to determine the use of facilities. IP trunks are one of many possible facilities that used to optimize communication functionality.

With this information, Direct Inward Dial (DID) and Direct Outward Dial (DOD) services are provided.

IP trunks are a point-to-multipoint facility, different from analog TIE trunks, which are a point-to-point facility. When IP trunk is selected through the dialed digits, its endpoint is not determined. The remote gateway configuration on IP telephony provides the final address resolution. To ensure functionality, the installer and administrator need to ensure that the core telephony services configuration, such as planning the destination codes with the IP telephony remote gateway configuration. If the leading dialed digits which are passed to the IP gateway during call setup do not match the IP telephony remote gateway configuration, the call fails.

The installer and administrator need to understand the core telephony services. See the *Enterprise Edge Programming Operations Guide* for more information.

See the Configuration chapter on page 61 for more information about core telephony services set up and configuring the remote gateway.

Post-installation network measurements

The design process is continuous, even after implementation of the IP telephony and commissioning of voice services over the network. Network changes – in real IP telephony traffic, general intranet traffic patterns, network controls, network topology, user needs and networking technology – can make a design no longer valid or non-compliant with QoS objectives. Review designs against prevailing and trended network conditions and traffic patterns, every two to three weeks at the start, and after, four times a year.

When operating IP telephony services, a customer's organization must have or include processes to monitor, analyze, and perform design changes to the IP telephony and the corporate intranet. These processes ensure that both networks continue to conform to internal quality of service standards and that QoS objectives are always met.

Setting IP telephony QoS objectives

The installer or administrator needs to state the design objective of IP telephony, the purpose of which sets the standard for evaluating compliance to meeting users' needs. When IP telephony is first installed, set the design objectives based on the work done in Measuring Intranet QoS on page 27.

The QoS objective is to ensure that for each destination pair, the mean+σ of *one-way delay* and *packet loss* is below a threshold value so that calls between those site pairs have a accurate QoS level. The graphs in Setting QoS on page 26, with the QoS measurements, can help the installer or administrator determine what threshold levels are appropriate. The Table 11 IP telephony QoS objectives describes examples of IP telephony QoS objectives:

Table 11 IP telephony QoS objectives

Site pair	Enterprise Edge IP telephony QoS objective	Fallback threshold setting
Santa Clara/ Richardson	Mean (one-way delay) + σ(one-way delay) < 120 ms Mean (packet loss) + σ(packet loss) < 0.3%	Excellent
Santa Clara/Ottawa	Mean (one-way delay) + σ(one-way delay) < 150 ms Mean (packet loss) + σ(packet loss) < 1.1%	Excellent

In following design cycles, the QoS objective is reviewed and improved, based on data collected from monitoring of intranet QoS. Having decided on a set of QoS objectives, the installer or administrator determines the planning threshold. The planning thresholds are based on the QoS objectives. These thresholds used to trigger the network implementation decisions when the prevailing QoS is within range of the affected values. This gives time for implementation processes to follow through. The planning thresholds can be set 5% to 15% below the QoS objectives, depending on the implementation lag time.

Intranet QoS monitoring

To monitor the one-way delay and packet loss statistics, install delay and route monitoring tools such as `Ping` and `Traceroute` on the LAN of each gateway site. See Measuring Intranet QoS on page 27 for guidelines describing the implementation of `Ping` hosts, the use of scripting, and information about other delay monitoring tools. Delay monitoring tool runs continuously, adding probe packets to each gateway about every minute. The load generated by the probe packets is not considered a large amount. At the end of the month, the hours with the highest one-way delay are indicated; within those hours, the packet loss and standard deviation statistics can be calculated.

At the end of the month, the administrator can analyze each gateway's QoS based on information described in Table 12 Gateway QoS objectives.

Table 12 Gateway QoS objectives

Site pair	One-way delay Mean+σ (ms)		Packet loss Mean+σ (ms)		Peak hour traffic		Carried traffic		QoS objective
	Last period	Current period	Last period	Current period	End	Start	End	Start	
Santa Clara/ Richardson									
Santa Clara/ Ottawa									
etc.									

Declines in QoS can be correlated with increasing IP telephony traffic, and intranet health reports to locate the sources of delay and error in the network. Steps can be taken to strengthen the intranet.

User feedback

Qualitative feedback from users helps confirm if the QoS settings match what end users sense. The feedback can come from a Helpdesk facility, and can include information such as time of day, origination and destination points, and a description so the service degradation.

Engineering checklist

How do you determine if you have enough available bandwidth on your private network (intranet)?

Before installing Enterprise Edge VoIP Gateway, test your intranet:

- Use a terminal on the intranet to test network capability.
- Use the guidelines to determine if you have enough bandwidth.
- Choose the codec settings
- Determine the dialing plan for VoIP Gateway
- Determine if the VoIP Gateway uses a ITU-H.323 gatekeeper.

For further information, refer to the Engineering guidelines chapter and the Interoperability chapter.

Installation

Before configuration of the Enterprise Edge IP Telephony install the following hardware and software components. See the *Enterprise Edge Programming Operations Guide* for information about installing these components.

- Enterprise Edge product software
- Keycode – software key that allows IP telephony – refer to the Systems operations chapter, Software keys section, in the *Enterprise Edge Programming Operations Guide*.
- Media Services Card (MSC) – contains the Central Processing Unit (CPU) and the MSPEC slots – refer to the Hardware Description chapter in the *Enterprise Edge Programming Operations Guide*.
- Media Services Processing Expansion Cards (MSPEC) – plug into the MSC to provide additional resources – refer to the Hardware Description chapter in the *Enterprise Edge Programming Operations Guide*.

Installation flowchart

Figure 9 Configuring the local gateway installation flowchart and Figure 10 Configuring the remote gateway installation flowchart show how to install a local gateway and how to add a remote gateway.

Configuring a local gateway

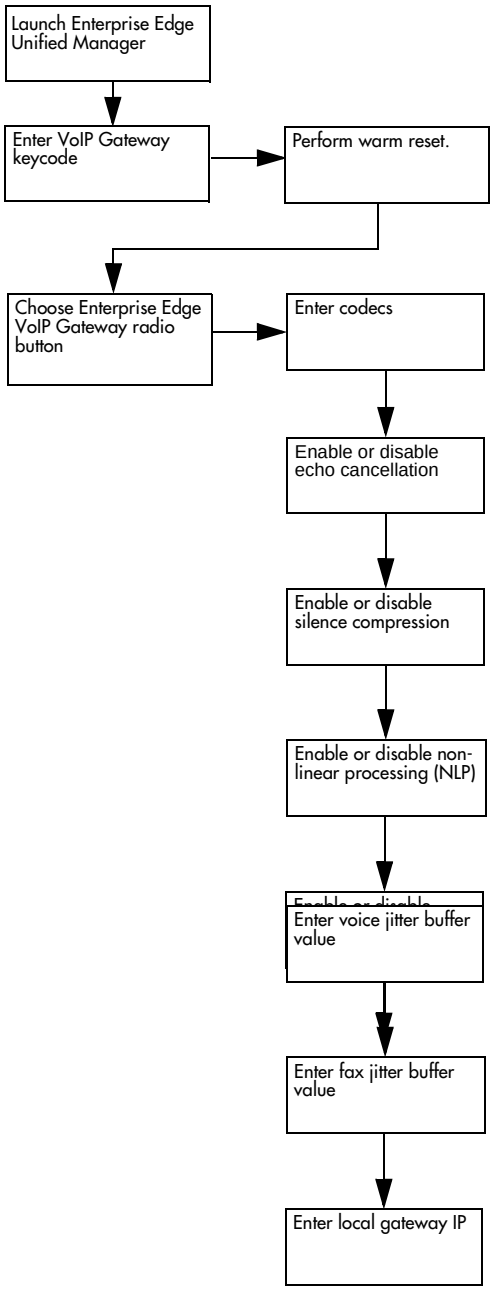
The installer sets the characteristics of the local gateway. These characteristics determine the bandwidth and QoS requirements for all calls over IP telephony.

- Launch Enterprise Edge Unified Manager:
  - — Enter the Enterprise Edge VoIP Gateway keycode.
  - — Perform a warm reset by following the procedure in the Maintenance chapter of the *Enterprise Edge Programming Operations Guide*.
- Select the Enterprise Edge VoIP Gateway radio button:
  - — Enter the codecs.
  - — Enable or disable echo cancellation.
  - — Enable or disable non-linear processing.
  - — Enable or disable silence compression.
  - — Enable or disable fallback.
  - — Enter the voice jitter buffer value.

— Enter the fax jitter buffer value.

— Enter the local gateway IP.

Figure 9 Configuring the local gateway installation flowchart



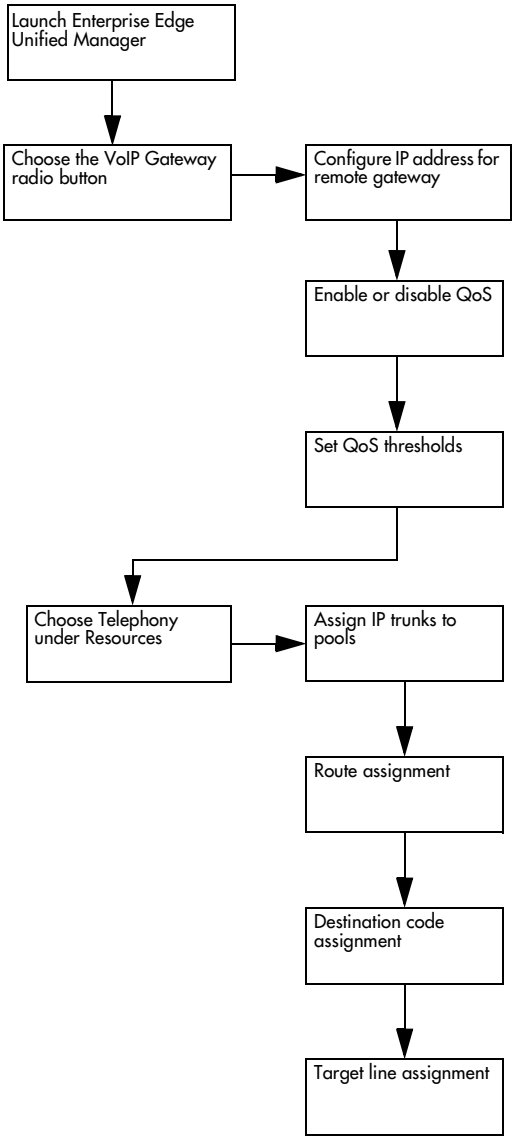
Configuring a remote gateway

Figure 10 Configuring the remote gateway installation flowchart contains the steps for configuring a remote gateway. The installer adds information about each remote gateway.

- Launch Enterprise Edge Unified Manager.

- Select the VoIP Gateway radio button.
  - — Configure IP address for remote gateway and dialed digits needed to call that gateway.
  - — Enable or disable QoS.
  - — Set QoS thresholds.
- Select Telephony under Resources.
  - — Assign IP trunks to pools.
  - — Route assignment.
  - — Destination code assignment.
  - — Target line assignment.

Figure 10 Configuring the remote gateway installation flowchart



Fallback to normal circuit-switched services configuration

If the measured Mean Opinion Score (MOS) exceeds the configured threshold for any monitored gateway, the fallback to normal circuit-switched services is triggered. This feature reroutes calls to other trunks such as PSTN, until the network QoS improves to exceed the configured threshold.

IP trunks on the core telephony services use routes to determine which outgoing facilities to use. A given destination code can have an alternate route configured. This alternate route is used if the main route is not available to process calls. For example, the alternate route is used if all the lines in a line pool are busy. See the Systems Operation chapter of the *Enterprise Edge Programming Operations Guide*. See Dialing plan section.

IP trunks also use this capability. One capability unique to IP trunks takes advantage of the QoS monitoring that is part of IP Telephony. With fallback to normal circuit-switched facilities enabled in the local gateway configuration, calls route to the circuit-switched facilities if the QoS is below the permitted threshold.

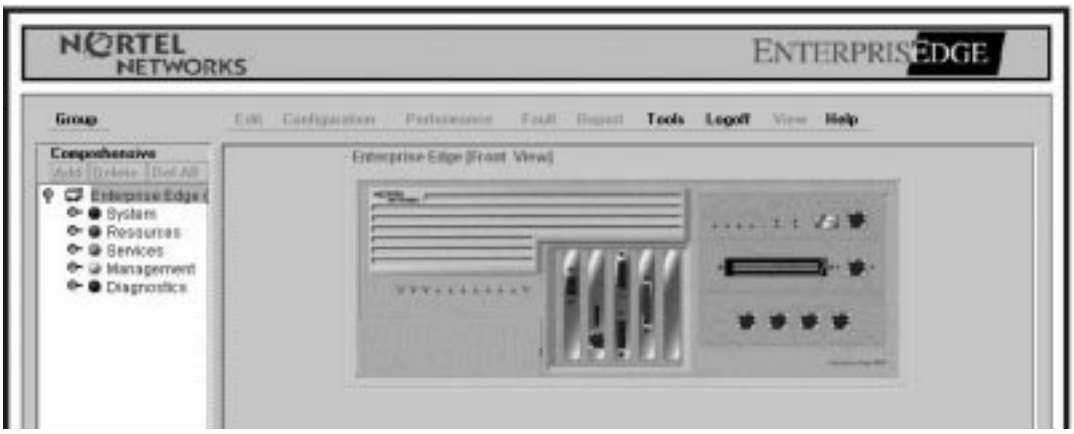
The installer configures fallback as follows:

- Launch the Unified Manager.
- Select the IP Telephony radio button.
  - — Enable fallback in the local gateway configuration.
  - — Enable QoS monitoring for the required destinations in the remote gateway configuration.
  - — Set the Tx and Rx thresholds (MOS numbers) for the required QoS.
- Launch Enterprise Edge Unified Manager.
  - — Configure all alternate routes for the IP trunks.

Configuration

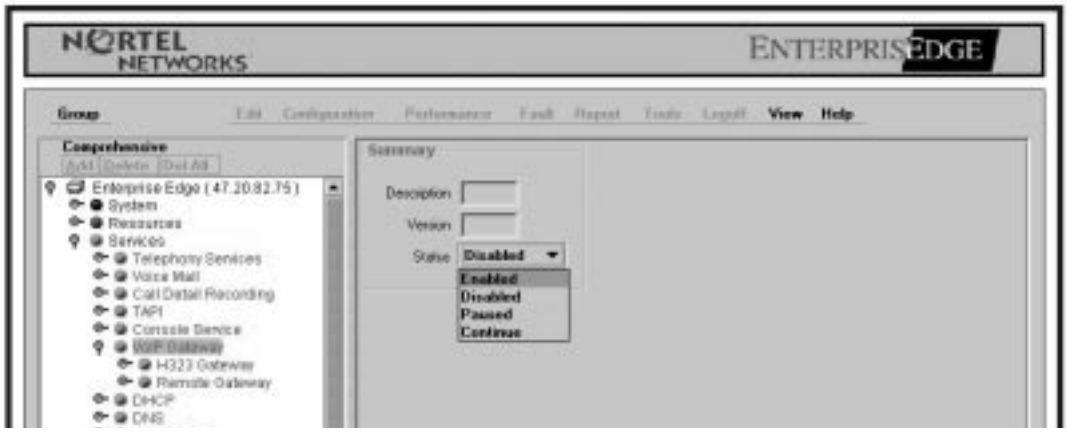
Enterprise Edge VoIP Gateway uses a menu-driven interface for operations, administration and maintenance (OA&M). The interface includes a display, pull-down menus, dialog windows, status bars, page contents, and data. A radio button provides access to the interface from the Enterprise Edge Unified Manager shell.

Figure 11 Enterprise Edge Unified Manager



The IP telephony main menu is part of the Services menu. When you click on IP Telephony to access the sub-menus in the interface, the IP telephony version appears as Figure 12.

Figure 12 Enterprise Edge VoIP Gateway display



The interface allows the administrator to modify the following areas:

- Local gateway
- Remote gateways

User Interface Overview

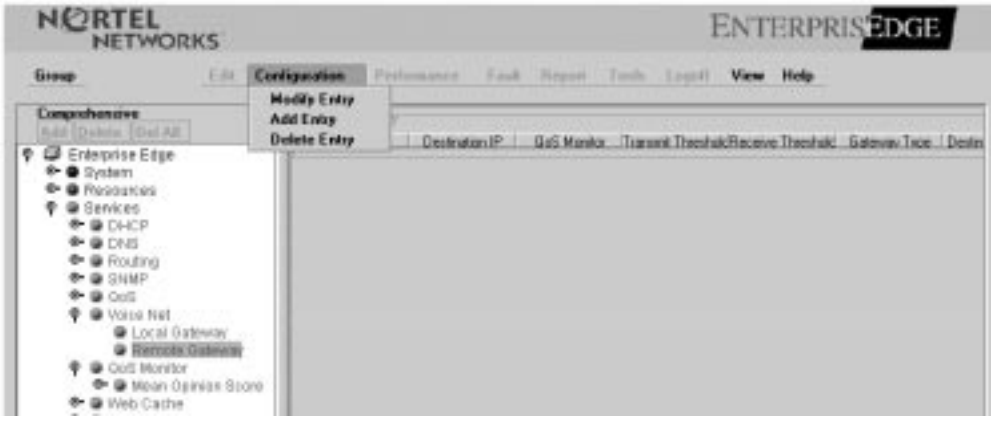
Use the following steps to modify an entry:

1. Select the item, click on the radio button to open the Enterprise Edge IP Gateway menu.

Figure 13 Unified Manager selection list

2. Select an item from the Unified Manager menu. The right hand side of the manager displays a pull-down menu bar and the current information for the selected item.

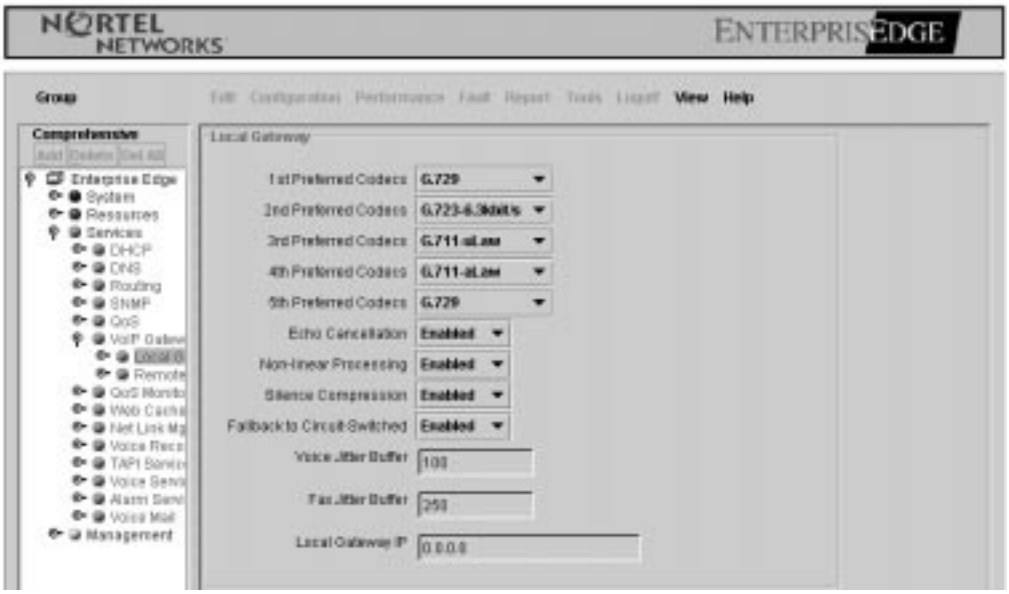
Figure 14 Unified Manager with pull-down menu and sample information



3. Highlight an entry to modify it.

4. Use the pull-down menu bar to select the operation. A dialog box opens.

Figure 15 Sample dialog box - sample display - new screen cap to be provided



5. Perform the operation.

The menus for all of the possible selection from the IP Telephony web browser are the same. The menu headers are:

- Configuration
- View
- Help

Configuration contains options that allow the administrator to modify the table and the highlighted entries. The options available in this pull-down menu depend on the table selected for modification.

Local Gateway Configuration

These settings apply to all calls no matter the IP destination. Settings include the Preferred order of codecs, echo cancellation state, silence compression state, and jitter buffer settings.

Codecs reduce bandwidth use by reducing the amount of information sent between gateways.The G.7XX series of codecs are standards defined by the International Telecommunications Union (ITU). Different codecs have different QoS and compression properties. The compression properties can affect heard audio quality while saving bandwidth. The installer or administrator configures the supported codecs.

Refer to the Codec types section on page 37 for more information about selecting a codec.

Table 13 Sample Local Gateway Configuration

Parameters	Settings
Supported Codecs	G.729 G.723.1 6.3 kbit/s or 5.3 kbit/s G.711
Echo Cancellation	Enabled
Non-linear processing	Enabled
Silence Compression	Enabled
Fallback to Circuit-switched	Enabled
Voice Jitter Buffer	100
Fax Jitter Buffer	250
Local Gateway IP	
Gatekeeper IP address	00.00.00.00
Call signaling	Direct/GatekeeperRouted/ GatekeeperResolved
Aliasname	Alias assigned to the local gateway

The Local Gateway Configuration menu contains the following are fields:

- The Supported Codecs field indicates the supported codecs. A pull-down menu allows the installer or administrator to modify the list.
- The Echo Cancellation field indicates Echo cancellation. A pull-down menu allows the installer or administrator to select enabled or disabled.
- The Non-linear processing field indicates Non-linear processing. A pull-down menu allows the installer or administrator to select enabled or disabled.
- The Silence Compression field indicates Silence compression. A pull-down menu allows the installer or administrator to select enabled or disabled.
- The Fallback to Circuit-switched field has a pull-down menu that allows the installer or administrator to select enabled or disabled.
- The Voice Jitter Buffer field displays the maximum size of the voice Jitter buffer. The installer or administrator enters a numeric value between 20 and 200. The recommended maximum is 100.
- The Fax Jitter Buffer field displays the maximum size of the fax Jitter buffer. The installer or administrator enters a numeric value between 20 and 500. The recommended value is 250.
- The Local Gateway IP displays the IP address used by the local gateway and the remote gateways of other VoIP systems. See the Multiple network interfaces section page 18 for more information.
- The Gatekeeper IP displays the IP address of the gatekeeper. Set the field to none or enter the IP address of the gatekeeper. When the installer or administrator enters an IP address, the gateway registers with the gatekeeper at this address on port 1719.

- The Call Signaling field displays the selected IP address conversion process and the installer or administrator enters one of the following options:
  - — Direct: gateway resolves IP addresses locally, using the remote gateway table
  - — GatekeeperRouted: gateway sends call signaling messages to the gatekeeper to use the gatekeeper's remote gateway table to resolve the IP address.
  - — GatekeeperResolved: not supported.
- The Aliasname field contains a text string that identifies the Enterprise Edge gateway to the gatekeeper. The gatekeeper matches dialed DNs with aliasnames as part of the dialing plan for the network.

Modifying the Local Gateway Configuration table

The pull-down menu Configuration contains the Modify Entry option.

The Modify Entry option allows the administrator to change the settings for the supported codecs, non-linear processing, silence compression, and the jitter buffers. Echo cancellation cannot be disabled. If the administrator selects an entry, and selects the Modify Entry option, a dialog box appears. The dialog box allows the administrator to select a new value.

The Modify Entry option allows the administrator to change the order of the Preferred codecs through a set of five dialog boxes. Each dialog box contains a list of the supported codecs and a none option. The administrator selects from the list for each of the five boxes, and the result of the information appears in the Supported Codecs field.

Stop and restart the gateway to change the configuration to the new settings. Select **VoIP Gateway** from the Unified Manager menu, then select the **Status** pull-down menu. Click on **Disabled**, then click on **Enabled**. The new configuration is active when the status returns to **Up**. Changes to the Local Gateway Configuration table only begin on the next call. Calls in progress are not affected.

Remote Gateway Configuration

The Remote Gateway Configuration menu manages the Remote Gateway Configuration table.

The gateway configuration table contains the IP address, destination digits, and QoS threshold for each remote gateway. The gateway configuration table allows QoS monitoring to be enabled or disabled for each IP destination. A pull-down menu allows the administrator to modify the table.

Table 14 Sample Remote Gateway Configuration

Name	IP	Destination Digits	QoS Monitor	QoS Tx Threshold	QoS Rx Threshold
Toronto	10.10.10.1	61	Disabled	5.00	5.00
Santa Clara	10.192.5.2	6265 61408	Enabled	4.35	4.00
Montreal	10.192.5.5	6852 61514	Enabled	3.23	4.80
Calgary	10.192.5.6	6775 61406	Disabled	5.00	5.00

The Remote Gateway Configuration menu contains the following are fields:

- The Name field contains the name connected with the IP address. Ensure this name is correct before pressing the **Save** button. When saved, the name cannot be changed.
- The IP field contains the IP address or the machine name of the destination gateway. If the machine name is used, disable QoS. Only enter an IP address or machine name one time in the Remote Gateway Configuration table.
- The Destination Digits field contains the leading dialed digits that indicate which calls route to this remote gateway. Separate groups of dialed digits with a space. See the Dialing plan section on page 43. IP Telephony uses the best match algorithm to determine call destinations.
- The QoS Monitor field indicates the status of QoS monitor for the destination.
- The QoS Tx Threshold and QoS Rx Threshold indicate the minimum QoS required for traffic to route over the IP Telephony to or from the defined destination. Valid thresholds are between 0 and 5.00.

Modifying the Remote Gateway Configuration table

The pull-down menu Table contains the following options:

- Add Entry
- Delete Entry
- Modify Entry

The Add Entry option allows the administrator to add a new entry to the Remote Gateway Configuration table. If the administrator highlights an entry on the existing table, and selects the Add Entry option, a dialog box appears. Insert the new entry at the end of the table. Enable or disable the QoS monitor for each entry with the radio button.

The Delete Entry option allows the administrator to delete an entry from the Remote Gateway Configuration table. If the administrator highlights an entry on the existing table, and selects the Delete Entry option, a dialog box appears. The dialog box asks the administrator to confirm either or not to delete an entry. The Delete Entry option is not available when there is no entry on the existing table highlighted.

The Modify Entry option allows the administrator to change the information in an entry. The administrator highlights an entry on the existing table and selects the Modify Entry option. A dialog box allows changes to entry information. A default button restores the information to the settings shown in the table.

Core telephony services configuration

Launch the Enterprise Edge Unified Manager and configure the following:

1. Put the IP trunks into a line pool. IP Telephony ports are IP trunks. Start with Line 01, to a maximum of Line 08 (depending on the keycode entered).

2. Configure a route which uses the line pool linked with the IP trunks. For IP trunks, do not add or absorb because the IP telephony gateway receives the dialed digits as dialed.

3. Enter a destination code which uses the route configured above. Ensure the destination code is the identical to the destination digits in the Remote Gateway Configuration. See the Remote Gateway Configuration section on page 65.

The above procedure ensures Direct Outward Dial (DOD) calls go to a remote gateway.

To receive Direct Inward Dial (DID) calls, configure DID lines, also called target lines, on the core telephony services. The full dialed number passes from the originating to the destination gateway during call setup. The destination gateway processes the dialed number to determine which DID line can terminate the call.

For private networking, the call terminates at a terminal at the destination gateway. Configure target lines which match to the dialed digits to complete private networking. For a description of target lines and DID, see the *Enterprise Edge Programming Operations Guide*.

For toll bypass, the DID calls can terminate on an outgoing PSTN trunk. To do this, configure additional destination codes. These destination codes point to line pools which contain PSTN trunks. For information about line pools, see the *Enterprise Edge Programming Operations Guide.*

Configuration of fallback to conventional circuit-switched facilities

If the measured Mean Opinion Score (MOS) for all codecs is below the configured threshold for any monitored gateway, the Fallback to Conventional Circuit-switched services activates. This feature reroutes calls to different trunks such as the Public Switched Telephone Network (PSTN) until the network QoS improves. When the QoS meets or exceeds the threshold, calls route over the IP network.

With the fallback feature disabled, calls move across the IP telephony trunks no matter the QoS. The fallback feature is only active at call setup. A call in progress does not fall back if the QoS degrades.

Calls fallback if there is no response from the destination, an improperly configured remote gateway table, or if there are not enough DSP resources available to handle the new call.

IP trunks on the core telephony services use routes to determine which outgoing facilities to use. A given destination code can have an alternate route configured. The alternate route is used if the main route is not available to process calls. For example, if all the lines in a line pool are busy.

IP trunks also use this capability. One capability unique to IP trunks takes advantage of the QoS monitoring that is part of IP telephony. If fallback to conventional circuit-switched facilities is enabled in the Local Gateway Configuration, calls route to the circuit-switched facilities if the QoS is below the acceptable threshold.

The installer configures fallback as follows:

1. Launch Unified Manager and select the IP Telephony radio button.

2. Enable fallback in the Local Gateway Configuration.

3. Enable QoS monitoring for the required destination in the Remote Gateway Configuration.

4. Set the Tx and Rx thresholds (MOS numbers) for the required QoS.

5. Configure all alternate routes for the IP trunks.

Maintenance

Quality of Service Monitor

The Quality of Service Monitor is a software that monitors the quality of the IP channels every 15 seconds. The QoS Monitor determines the quality of the intranet based on threshold tables for each codec. If the QoS Monitor determines that a threshold has been exceeded, the QoS Monitor, if enabled, will trigger fallback to conventional circuit-switched systems.

Quality of Service Status

The QoS Status displays the current network quality described as a Mean Opinion Score (MOS) for each IP destination. A pull-down menu allows the administrator to view the MOS mapping. A sample QoS Monitor follows.

IP	QoS Monitor	G.729		G.711		G.723.1 6.3 kbit/s		G.723.1 5.3 kbit/s	
		Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx
47.192.5.2	Enabled	4.50	4.50	4.00	4.30	4.75	4.70	4.80	4.90
47.192.5.6	Disabled	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Using the QoS Monitor pull-down View menu

The View menu contains the following option:

- Refresh

The Refresh option updates the display with the most current values.

Operational Statistics

IP Telephony uses the Unified Manager to record information about its operation.

The administrator accesses the Unified Manager from the Start menu. See the software documentation for more information about the events and the viewer.

Backup and Restore Procedures

IP Telephony uses the backup and restore procedures in the *Enterprise Edge Programming Operations Guide*.

Interoperability

Enterprise Edge IP Telephony is compatible with the ITU-T H.323v2 standards.

IP Voice supports H.323v2 Direct-routed gateway capabilities. Enterprise Edge IP Telephony 2.0 is compatible with H.323 gatekeepers such as Radvision and the Inca M10.

First, IP Telephony only interworks with itself and the M1-ITG. The M1-ITG is an H.323v2 gateway. We expect future releases to support H.323 products from other vendors.

Interoperability considerations

Enterprise Edge IP Telephony interoperates with M1-ITG and Microsoft NetMeeting. Enterprise Edge IP Telephony interoperates with any H.323v1 or H.323v2 compliant gateway that conforms to the specifications in the following table.

Fax calls are only supported between Enterprise Edge Gateways.

Table 15 Engineering specifications

Capacity	1 to 8 ports
Voice Compression	G.723.1 MP-MLQ, 6.3 kbit/s or ACELP, 5.3 kbit/s G.729 CS-ACELP, 8 kbit/s (supports plain, Annex A and Annex B) G.711 PCM, 64 kbit/s u/A-law
Silence compression	G.723.1 Annex A G.729 Annex B
Echo cancellation	48 ms tail delay
In-band signalling	DTMF (TIA 464B) Call progress
Speech path setup methods	H.323v1slowStart media negotiation H.323v2 fastStart
End-to-end DTMF signaling	digits 0-9, # and *, fixed duration tones only

Table 16 Supported voice payload sizes

Codec	Receive/transmit to M1-ITG	Receive/transmit to others
G.711	Up to 30 ms in 10 ms increments. 10, 20, or 30 ms per ITG's indication	20 ms
G.723.1	30 ms	30 ms
G.729	Up to 30 ms in 10 ms increments. 10, 20, or 30 ms per ITG's indication	20

Asymmetrical media channel negotiation

By default, the Enterprise Edge IP Telephony gateway supports G.729, G.723.1, G.711 μ-law and G.711 A-law audio media encoding. Because NetMeeting does not support the H.323 fastStart call setup method, NetMeeting can choose a different media type for its receive and transmit channels. Enterprise Edge IP Telephony gateway does not support calls with different media types for the receive and transmit channels and immediately hangs up a call taken with asymmetric audio channels. The party on the Enterprise Edge switch hears a treatment from the switch (normally a reorder tone). The party on the NetMeeting client losses connection.

To solve this problem, in NetMeeting, under the **Tools**, **Options**, **Audio**, **Advanced**, check **Manually configure compression settings**, and ensure that the media types are in the same order as shown in the Enterprise Edge local gateway configuration table. Table 17 lists the names used by the Enterprise Edge local gateway table and the matching names in NetMeeting.

Table 17 Name comparison

Enterprise Edge local gateway table	MS NetMeeting
G.723.1 6.3 Kbit/s	MS G.723 6400 bit/s
G.723.1 5.3 Kbit/s	MS G.723 5333 bit/s
G.711 μ-law	CCITT μ-law
G.711 A-law	CCITT A-law

No feedback busy station

The Enterprise Edge VoIP gateway considers the voice over IP connection as the equivalent of an MF trunk. The Enterprise Edge VoIP gateway provides call progress tones in-band to the user. On calling a busy station through the gateway, the gateway plays a busy tone to the user. As NetMeeting does not support fastStart, no speech path is opened to the user before the call connects. In this distinct design, the user on the NetMeeting station does not hear a busy signal from the gateway.

Glossary

Backbone	A network's major transmission path, handling high-volume, high-density traffic.
Bandwidth	A measure of information carrying capacity available for a transmission medium, shown in bits per second. The greater the bandwidth, the more information sent in a given amount of time.
Bridge	LAN equipment providing interconnection between two networks using the same addressing structure. A bridge filters out packets that remain on one LAN and forwards packets for other LANs.
CBQ	Class Based Queuing
CD-ROM	Compact Disk - Read Only Memory
CDP	Coordinated Dialing Plan
CO	Central Office
Codec	Equipment or circuits that digitally code and decode voice signals
Communications Protocol	A set of agreed-upon communications formats and procedures between devices on a data communication network.
CPU	Central Processing Unit
Data Communications	Processes and equipment used to transport signals from a data processing device at one location to a data processing device at another location.
DID	Direct Inward Dialing
DN	Directory Number
DOD	Direct Outward Dialing
DSP	Digital Signal Processor
E&M	E&M is a type of analog trunk that detects line disconnect.
Enbloc	All dialed digits sent in a single expression.
Full-duplex transmission	Simultaneous two-way separate transmission in both directions.
G.711	A codec that delivers "toll quality" audio at 64 kbit/s. This codec is best for speech because it has small delay, and is very resillient to channel errors.
G.729	A codec that provides near toll quality at a low delay. Uses compression to 8 kbit/s (8:1 compression rate). The G.729 codec allows the Enterprise Edge IP Telephony to support only four VoIP ports.
G.723.1	A codec that provides the greatest compression, 5.3 kbit/s or 6.3 kbit/s. Normally indicated for multimedia applications such as H.323 videoconferencing. Allows connectivity to Microsoft-based equipment.
GUI	Graphical User Interface
H.323	The ITU standard for multimedia communications over an IP network. Enterprise Edge IP Telephony supports H.323.
Hub	Center of a star topology network or cabling system.
IP	Internet Protocol
ITG	IP Telephony Gateway

ITU	International Telecommunications Union
kbit/s	kilobits per second. Thousands of bits per second.
LAN	Local Area Network
Latency	The amount of time it takes for a discrete event to occur.
M1-ITG	Meridian 1 - Internet Telephony Gateway
Mbit/s	Megabits per second. Millions of bits per second.
Modem	Device that converts serial data from a transmitting terminal to an analog device for transmission over a telephone channel. Another modem converts the signal to serial digital data for the receiving terminal.
MOS	Mean Opinion Score
MSC	Media Services Card
Noise	Random electrical signals, generated by circuit components or by natural interruptions, that damage communications.
OA&M	Operations, Administration and Maintenance
Packet	Group of bits transmitted as a complete package on a packet switched network.
Packet switched network	A telecommunications network based on packet switching technology. A link is busy for the duration of the packets.
PEC	Processing Expansion Card
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTP	Real Time Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol. Protocol for routing and reliable message delivery.
Terminal	Device capable of sending or receiving data over a data communications channel.
Throughput	Indicator of data handling ability. Measures data processed as output by a computer, communications device, link, or system.
Topology	Logical or physical arrangement of nodes or stations.
Voice Compression	Method of reducing bandwidth by reducing the number of bits required to transmit voice.
VoIP	Voice over Internet Protocol.
WAN	Wide Area Network
WRED	Weighted Random Early Detection

Index

V