



viaIP ECS

Technical Overview

NOTICE

© 2001 RADVISION Ltd. All intellectual property rights in this publication are owned by RADVISION Ltd. and are protected by United States copyright laws, other applicable copyright laws and international treaty provisions. RADVISION Ltd. retains all rights not expressly granted.

No part of this publication may be reproduced in any form whatsoever or used to make any derivative work without prior written approval by RADVISION Ltd.

No representation of warranties for fitness for any purpose other than what is specifically mentioned in this guide is made either by RADVISION Ltd. or its agents.

RADVISION Ltd. reserves the right to revise this publication and make changes without obligation to notify any person of such revisions or changes. RADVISION Ltd. may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this publication, it is furnished under a license agreement included with the product as a separate document. If you are unable to locate a copy, please contact RADVISION Ltd. and a copy will be provided to you.

Unless otherwise indicated, RADVISION registered trademarks are registered in the United States and other territories. All registered trademarks recognized.

For further information contact RADVISION or your local distributor or reseller.

viaIP ECS version 2.0, October, 2001

CONTENTS

Introduction

1 *ECS Overview*

What's In This Chapter	7
What is the ECS?	7
ECS Environment	8
What the ECS Provides	9

2 *Gatekeepers*

What's In This Chapter	17
H.323 Recommendation	17
H.323 Gatekeepers	18
Gatekeeper Procedures	19
Call Establishment	19
Routing H.225.0 Call Signaling Channels	20
Routing H.245 Control Channels	23
Call Termination	23
Support of Endpoints without RAS Capabilities	24

Contacting RADVISION

INTRODUCTION

Designed for next-generation communications networks by the voice and video over IP (V²oIP) experts, RADVISION's viaIP multi-function platform is the most flexible and cost-effective solution for deploying IP-centric voice, video and data communications. The viaIP solutions are built around RADVISION's award-winning industry standard H.323 technology and provide the scalability and proven interoperability needed to deliver enhanced services for converged networks.

The viaIP product family is the ideal solution for businesses, educational communities and government agencies in need of IP videoconferencing to bolster organizational efficiency. Likewise, viaIP enables carriers and service providers to offer customers an industry-leading videoconferencing solution that integrates gatekeeper intelligence, multimedia gateway, multipoint conferencing and data collaboration into a single platform tailored to the organization's networking needs.

This document is a technical overview of the ECS.

1

ECS OVERVIEW

WHAT'S IN THIS CHAPTER

This chapter introduces you to the following:

- What is the ECS?
- ECS Environment
- What the ECS Provides

WHAT IS THE ECS?

The RADVISION viaIP Enhanced Communication Server (ECS) is a simple-to-use, ITU-T H.323 version 2-compliant gatekeeper application that is essential for the management of IP telephony and multimedia communication networks. The viaIP ECS runs on the asNT-10 board in the viaIP platform, or as standalone software on the Windows NT or Windows 2000 operating systems.

Designed with the network manager in mind, viaIP ECS provides complete functionality for defining and controlling voice and video traffic management over IP networks. Network managers can configure, monitor and manage the activities of registered network users. Managers can set policies and control network resources such as bandwidth usage to ensure optimal implementation.

This flexible and scalable gatekeeper application can accommodate the growing needs of a continuously expanding networking environment. The ECS supports up to 500 calls and 3000 registrations according to the license purchased. It is designed to provide the necessary performance for high call volume carrier-class networks.

This chapter describes the ECS environment and its unique features.

ECS ENVIRONMENT

The ECS system consists of three main entities:

- An ECS application that works together with the underlying RADVISION software—the Gatekeeper Core, H.341 MIB Stack and the H.323 Protocol Stack.
- A web server together with a web browser.
- SNMP Services.

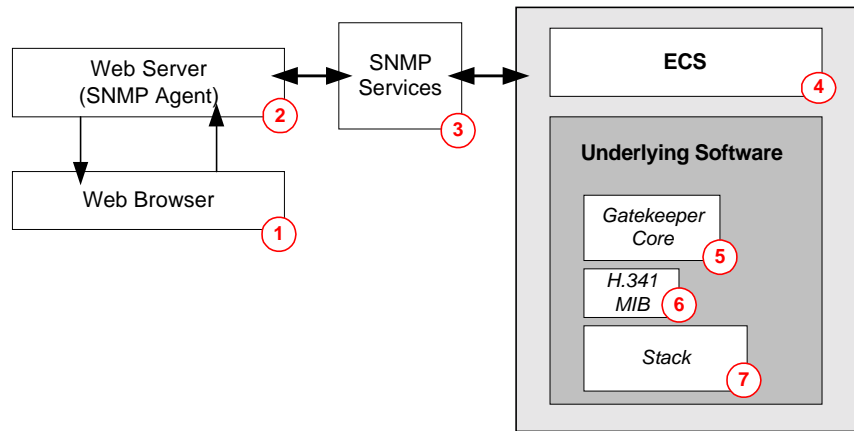


Figure 1-1 The ECS Environment

Each numbered component in the ECS environment performs a specific activity. The flow of information between components is as follows:

1. A user interacts with the ECS via a web browser.
2. The browser sends and receives data (via HTTP) to a web server, which is an SNMP agent.
3. The web server sends and receives data to and from the ECS using SNMP services.
4. The ECS processes the data.
5. The Gatekeeper Core manages the gatekeeper activities.
6. The H.341 MIB manages the MIB data.
7. The Stack manages the sending and receiving of H.323 messages.

WHAT THE ECS PROVIDES

The ECS is a fully compliant H.323 version 2 gatekeeper and provides all the functionality described in the H.323 Recommendation.

BUILT-IN POLICIES

In addition to the standard gatekeeper capabilities, a set of built-in policies¹ enables the ECS to provide the following enhanced functionality:

- Admission Control
- Address Translation
- Direct and Routed Modes
- Call acceptance
- Polling mechanism (IRQ)
- Call Authorization
- Bandwidth Management

ENHANCED SERVICES

The ECS has many features that provide enhanced communication facilities and services. These include:

- A web interface for configuring and administering the ECS.
- CDR for customized billing solutions.
- MIB support.
- H.450 Forwarding and Transfer Supplementary Services.
- Cisco Proxy support.
- RAI/RAC support, line hunting and conference hunting.
- LDAP support.
- Online logging.
- Resolution of unrecognized aliases.

1. See *Gatekeeper Procedures* in the *Gatekeepers* chapter.

What the ECS Provides

WEB INTERFACE

The viaIP Administrator provides a single point of entry that allows you to configure the ECS and any other element of the viaIP system. You can also monitor and control video conferences hosted by a viaIP MCU, using the viaIP Conference Control interface.

CDR

The ECS builds Call Detail Records (CDRs) in a simple text format that can be used as input to third party billing programs or other software.

MIB SUPPORT

A Management Information Base (MIB) is a formal description of a set of network objects that can be managed using SNMP. The format of the MIB is defined as part of SNMP. All other MIBs are extensions of this basic MIB. MIB-I refers to the initial MIB definition. MIB-II is the current definition. SNMPv2 includes MIB-II and adds some new objects.

Standard operations are requested or performed on a system via a management agent by management clients. The management agent accesses the requested information and returns it to the requesting client.

The H.323 MIB extension is described in the ITU-T Draft Recommendation H.341 (May 1999), Multimedia Management Information Base for H.323v2.

MIB NODES WITHIN ECS

The ECS supports the H.341 standard node for Registration, Admission and Signaling (RAS). This node contains three tables, one for each of the RAS parameters.

The ECS MIB tree also includes a unique 903 node. The 903 node contains an extension node called Private RADVision Gatekeeper MIB which allows the addition of a fourth parameter to the standard H.341 RAS node. The SNMP agent in the ECS implements the parameters of the H.341 extension.

H.450 FORWARDING AND TRANSFER

A service is the collective set of operations that are carried out to perform a Supplementary Service process as defined in the H.450.x Recommendations. The ECS defines two types of services: Call Forwarding and Call Transfer.

A service is created when:

- A Q.931 message containing an H.450 APDU¹ arrives across the network.
- The suitable condition for performing a service is implemented.

The protocols that support Supplementary Services are specified in a number of ITU-T Recommendations starting from H.450.1 and up, as each new Supplementary Service is defined. The ITU-T Recommendations relevant to the Supplementary Services supported by the ECS are defined below.

Note Full details about the H.450.x Recommendations are available in the appropriate ITU-T Recommendations.

H.450.1

Recommendation H.450.1 defines the signaling protocol between H.323 entities for the control of Supplementary Services. The generic functional protocol defined in the Recommendation H.450 provides the means of exchanging signaling information for the control of Supplementary Services over a LAN. This recommendation does not control any Supplementary Services but rather provides generic services to specific Supplementary Services Control entities. The generic functional protocol operates in conjunction with the Call Signaling Protocol defined in H.225.0. The protocol provides mechanisms for the support of Supplementary Services that may relate to existing H.323 calls, or are entirely independent of any existing H.323 calls.

H.450.2

Recommendation H.450.2 describes the procedures and the signaling protocol for the Call Transfer Supplementary Service in H.323 networks. The Call Transfer Supplementary Service enables user A to transform an existing call (from user A to user B) into a new call between user B and a user C, selected by user A.

H.450.3

Recommendation H.450.3 specifies the Call Diversion Supplementary Services which comprise the Call Forwarding Unconditional (CFU), Call Forwarding Busy (CFB), Call Forwarding No Reply (CFNR) and Call Deflection services, all of which are applicable to various basic services supported by H.323 endpoints. The Call Diversion Supplementary Services apply during call establishment, providing a diversion of an incoming call to another destination endpoint before the call is established. They apply to point-to-point calls.

-
1. APDUs convey a sequence of H.450 messages from the caller to the receiver and back. The APDU sequence is an octet string and it is conveyed in the User-user information element of Q.931. The APDUs of H.450 are transparent to Q.931; the Q.931 does not know the structure of H.450 APDUs, nor does it analyze the string.

What the ECS Provides

CISCO PROXY SUPPORT

The Cisco Proxy is a device that acts as a gateway and relays H.323 data between H.323 zones. A Proxy registers with an ECS, thereby becoming part of the zone of that ECS. The Proxy isolates endpoints of different zones by concealing their addresses. The only addresses that are revealed are those of the ECS and Proxy. During Call Setup, the ECS applications in each zone obtain address information from each other. The Proxies use the address information from the ECS to route the call between zones. In this way, endpoints in different zones cannot see each other directly. They only see the Proxy address of each other.

The Proxy and ECS can be configured in the **Neighbors** tab to manage endpoint-to-endpoint security when the network firewall does not support Dynamic Access Control.

RAI/RAC, LINE HUNTING AND CONFERENCE HUNTING

The Resource Available Indication/Resource Available Confirmation (RAI/RAC) function of the ECS manages load balancing on the network.

RAI/RAC messages are exchanged between the ECS and a gateway to determine whether the gateway is available to receive calls. A gateway sends a RAI message to notify the ECS of the current availability of the gateway for each H-series protocol. The ECS responds with a RAC message to acknowledge receipt of a RAI message.

If the gateway is unavailable, the ECS routes the call to an alternative available gateway.

LINE HUNTING

A gateway supports a list of prefixes (services). When a gateway is unavailable to receive a call, this means that it cannot accept calls with the particular prefix in question. The ECS activates the Line Hunting function and searches for a gateway which is free to accept calls with this prefix.

When the ECS receives an indication from a gateway in the RAI message that the gateway is almost at maximum capacity, the ECS marks the services of that gateway as “almost out of resources”. During the first round of Line Hunting, the ECS ignores this gateway when searching for the indicated gateway service.

If the ECS cannot find a gateway which can accept a call with a specific prefix in this first round of searching, the ECS can return to the first gateway it checked and begin a second round of searching for an available gateway. In this second round, the ECS ignores the “almost out of resources” flag and tries *all* gateways in searching for a gateway to take the call. If the ECS does not find a service provider (an available gateway) in the second round of searching, the call is refused.

CONFERENCE HUNTING

The ECS supports Conference Hunting. The purpose of Conference Hunting is to maintain conferences and ignore Line Hunting where necessary.

RADVISION MCU calls consist of a service prefix followed by a password (or conference ID). In order to create a conference, all calls with the same password (or conference ID) have to be directed to the same MCU. If a password (or conference ID) is new, Conference Hunting takes place in *all* MCUs in the zone.

When the ECS receives a call with the same prefix as an existing call, the ECS directs the new call to the same service provider (MCU) as the existing call. If the service provider refuses the call, the ECS does not attempt Line Hunting. This scenario also overrides RAI indications.

For example, prefix 78 is configured to be of Conference Hunting type. Assume a call is made to this prefix with the number 78111. If another call with the same number (78111) is made, the gatekeeper will direct the second call to the same MCU. If the MCU refuses to accept the call, Line Hunting does not take place.

CONFIGURATION

There is no need to configure RAI/RAC.

LDAP SUPPORT

The Lightweight Directory Access Protocol (LDAP) is a protocol for accessing online directory services. LDAP is both an information model and a protocol for querying and manipulating the model.

A special RADVISION LDAP client Plug-in that is part of the ECS is used for retrieving information from a dedicated LDAP server, for permitting or denying service, or for routing calls.

The LDAP Plug-in defines some entry structures, sets user and gatekeeper information in these structures, and stores them in an LDAP server. The information thus stored in the LDAP server is then used by the ECS Plug-in for address resolution.

ONLINE LOGGING

The ECS provides an online window containing all ECS logging information.

What the ECS Provides

RESOLUTION OF UNRECOGNIZED ALIASES

The ECS resolves unrecognized aliases (aliases that are not in the ECS registration database) by sending an LRQ first to the LDAP server, then to a DNS server, then to the Neighbor Gatekeepers that appear in the **Neighbors** tab, and finally by using multicast. To instruct the ECS to send an LRQ to each of these destinations, you must configure each destination separately. You can also configure the ECS to send an LRQ simultaneously to all the destinations listed above.

When the **Dial Plan** field in the **Basics** section of the **Settings** tab is set to **Version 2**, the **Hierarchy** tab replaces the **Neighbors** tab. In such cases the ECS sends an LRQ to the Neighbor Gatekeepers that appear in the **Neighbors** section of the **Hierarchy** tab instead of to the Neighbor Gatekeepers that appear in the **Neighbors** tab.

LDAP server

To instruct the ECS to send LRQ messages to the LDAP server, check the **Locate endpoints** option in the **LDAP** section of the **Settings** tab.

DNS server

To instruct the ECS to send LRQ messages to a DNS server, check the **Enable DNS queries** option in the **DNS** section of the **Settings** tab.

Neighbor Gatekeepers

To instruct the ECS to resolve unrecognized aliases by sending a Location Request message (LRQ) to the Neighbor Gatekeepers that appear in the **Neighbors** tab, check the **Use the following Neighbor Gatekeepers to resolve unrecognized aliases** option in the **Neighbors** tab.

To instruct the ECS to resolve unrecognized aliases by sending a Location Request message (LRQ) to the Neighbor Gatekeepers that appear in the **Neighbors** section of the **Hierarchy** tab, check the **Use the following Neighbor Gatekeepers to resolve unrecognized aliases** option in the **Neighbors** section of the **Hierarchy** tab.

Multicast

To instruct the ECS to resolve unrecognized aliases by using multicast to send a Location Request message (LRQ) to other gatekeepers, check the **Use multicast to resolve unrecognized aliases** option in the **Basics** section of the **Settings** tab. This may be in addition to using unicast.

All destinations simultaneously

To instruct the ECS to resolve unrecognized aliases by sending a Location Request message (LRQ) to all LRQ policy destinations simultaneously, check the **Search for out-of-zone aliases simultaneously in all sources** option in the **Advanced** section of the **Settings** tab.

What the ECS Provides

2

GATEKEEPERS

WHAT'S IN THIS CHAPTER

The ECS is an H.323 gatekeeper. This chapter introduces you to the following:

- H.323 Recommendation
- H.323 Gatekeepers
- A typical H.323 network topology

This chapter is optional and has been provided to give a better understanding of what H.323 gatekeepers are. This knowledge is not essential for working with the ECS but it may assist you in making better decisions when configuring the ECS. Therefore, you should read this chapter if you are not familiar with H.323 gatekeepers or you wish to make the most of ECS gatekeeper functionality.

H.323 RECOMMENDATION

H.323 is an umbrella recommendation of the International Telecommunications Union (ITU-T) that specifies the complete architecture and operation of real-time multimedia communications over packet networks. H.323 is very broad in scope, including both stand-alone devices and embedded personal computer technology. It defines models of interaction for both endpoint-to-endpoint and multipoint conferences.

In the document that details Recommendation H.323, references are made to other standards including *H.225.0* and *H.245*. *H.225.0* specifies the procedures and messages applicable to gatekeepers, including the *RAS* protocol for Registration, Admission and Status. *H.225.0* also includes the *Q.931* protocol for Call Signaling, consisting of Setup, Teardown and Disengage. *H.225.0* also refers to *H.245*.

H.323 Gatekeepers

H.245 provides signaling for the proper operation of the H.323 terminal, including capabilities exchange, opening and closing of logical channels together with a full description of these channels, mode preference requests, flow control messages, and general commands and indications. H.245 signaling is established between two endpoints, an endpoint and an MCU, or an endpoint and a gatekeeper. For each call in which the endpoint participates, the endpoint establishes exactly one H.245 Control channel. This channel uses the messages and procedures of Recommendation H.245.

All messages that are exchanged between two or more H.323 entities use the Abstract Syntax Notation One (ASN.1) language. ASN.1 is a language for describing the complex data structures independently from the underlying hardware. ASN.1 is a standard developed by the ITU-T and is described in Recommendations X.680-X.694.

H.323 GATEKEEPERS

A gatekeeper is at the heart of the H.323 network. Gatekeepers manage the H.323 entities that are capable of receiving or initiating calls. These entities—terminals, gateways and multiple control units (MCUs)—are called *endpoints*. Each gatekeeper has a zone. An endpoint that registers with a gatekeeper becomes part of the zone of that gatekeeper. The main function of the gatekeeper within its zone is to provide call control services for its endpoints. Gatekeeper functions include:

- Address resolution, by translating LAN aliases for endpoints to transport address.
- Admissions control for authorizing network access.
- Bandwidth management.
- Network management (in Routed Mode).

The viaIP ECS supports all the mandatory requirements stated in H.323. The ECS also supports additional functions necessary for effective advanced audio/video conferencing in networks.

GATEKEEPER PROCEDURES

The H.323 Recommendation specifies *procedures* that define the standard operational characteristics and behavior of a gatekeeper in a network. These procedures describe the steps needed to fulfill a policy or provide a service. *Messages* enable the procedures to accomplish what the policies or services need to do. The ECS implements standard H.323 gatekeeper procedures according to the specification of the RAS and the Call Signaling protocols.

The H.323 Recommendation also states that certain functionality can be built into a gatekeeper, based on standard gatekeeper procedures. Policies that are built into the ECS provide the basic framework for fundamental gatekeeper behavior and also establish Default Policies for certain procedures, such as how to control a zone.

CALL ESTABLISHMENT

Calls are established on the RAS channel, which is the unreliable (UDP) channel for Registration, Admission and Status messages, as described below.

GATEKEEPER DISCOVERY

Call establishment starts with Gatekeeper Discovery, which is an automatic procedure that occurs before a conference starts. In Gatekeeper Discovery, both endpoints look for a gatekeeper with which to register by multicasting a Gatekeeper Discovery Request message (GRQ). Upon receiving a GRQ message, the gatekeeper either returns a Gatekeeper Confirm message (GCF) with the transport address of the RAS channel of the gatekeeper, or if the gatekeeper does not want the endpoint to register with it, the gatekeeper returns a Gatekeeper Reject message (GRJ).

Gatekeeper Discovery allows the endpoint-gatekeeper association to change over time. The advantage of this procedure is two-fold:

- Administrative overhead is lower, since there is no need to configure individual endpoints.
- An existing gatekeeper can be replaced without the need to manually reconfigure all of the affected endpoints.

The gatekeeper does not maintain an internal database based on the Discovery procedure since the requesting endpoint is not obliged to register with this specific gatekeeper at a later time.

GATEKEEPER REGISTRATION

After discovering gatekeepers, both endpoints then register with a gatekeeper using the Registration Request message (RRQ). In this process each endpoint joins a *zone* and informs the gatekeeper of its transport and alias addresses, such as names or phone numbers. Registration occurs before any calls are attempted and may occur periodically, or once, such as during endpoint power-up.

The gatekeeper is capable of receiving registrations from endpoints with multiple transport addresses, such as gateways or MCUs. Upon receiving an RRQ message from an endpoint, the gatekeeper responds with either a Registration Confirm message (RCF) or a Registration Reject message (RRJ).

LOCATION REQUEST

An endpoint or gatekeeper can request the location of another endpoint using its alias name by sending a Location Request message (LRQ), and the gatekeeper replies with a Location Confirm message (LCF) containing the resolved address for the alias name.

ADMISSION REQUEST

When a user places a call from an endpoint, the endpoint starts by requesting admission from the gatekeeper using an Admission Request message (ARQ). The gatekeeper can accept by sending an Admission Confirm message (ACF), or deny the request by sending an Admission Reject message (ARJ). If the call is accepted, the endpoint sends a Q.931 Setup message to the remote party. The remote party that receives the Setup message then requests admission from its gatekeeper by sending an ARQ. If the call is accepted, the Q.931 Call Signaling process is completed when, in the Q.931 Connect message, an endpoint receives a reliable transport address to which to send the control messages. H.245 message negotiation then follows. It is at this stage that an endpoint can request additional bandwidth by sending a Bandwidth Request message (BRQ) to its gatekeeper.

ROUTING H.225.0 CALL SIGNALING CHANNELS

The Call Signaling channel is a reliable TCP channel for carrying H.225.0 Call Signaling messages, as discussed above. This section discusses the methods for passing Call Signaling messages between two endpoints.

ROUTED AND DIRECT MODES

The two methods for passing Call Signaling messages between two endpoints are:

- *Direct Mode* which passes Call Signaling messages directly between two endpoints.
- *Routed Mode* which routes Call Signaling messages, and possibly H.245 messages, between two endpoints via the gatekeeper.

During the initial Admission Procedure, a parameter in the ACF message specifies the mode in which the gatekeeper should be set for the specific requested call. The Default Policy for all calls, excluding calls to a supported prefix of a gateway, can be defined by the gatekeeper administrator using the zone properties configuration.

DIRECT MODE FLOW

Figure 2-1 shows the flow of RAS and Call Signaling messages in Direct Mode.

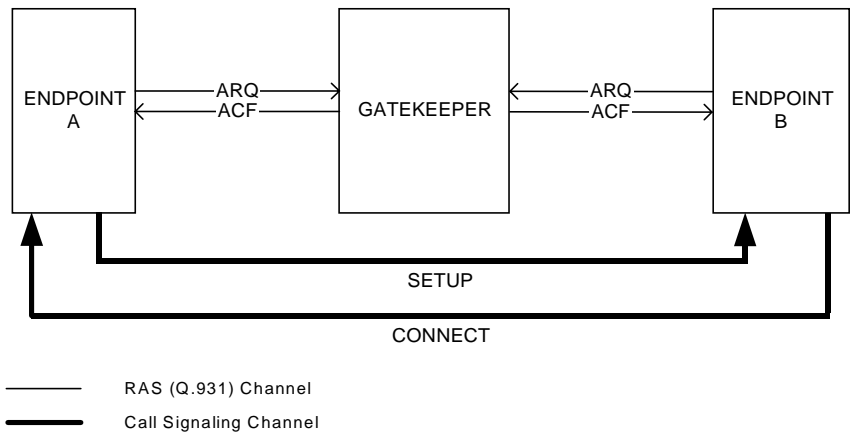


Figure 2-1 Direct Call Signaling

ROUTED MODE FLOW

Figure 2-2 shows the flow of RAS and Call Signaling messages in Routed Mode. In this case, the gatekeeper keeps the Call Signaling channel open while routing the call for the duration of the call. The H.245 Control channel is established directly between the two endpoints.

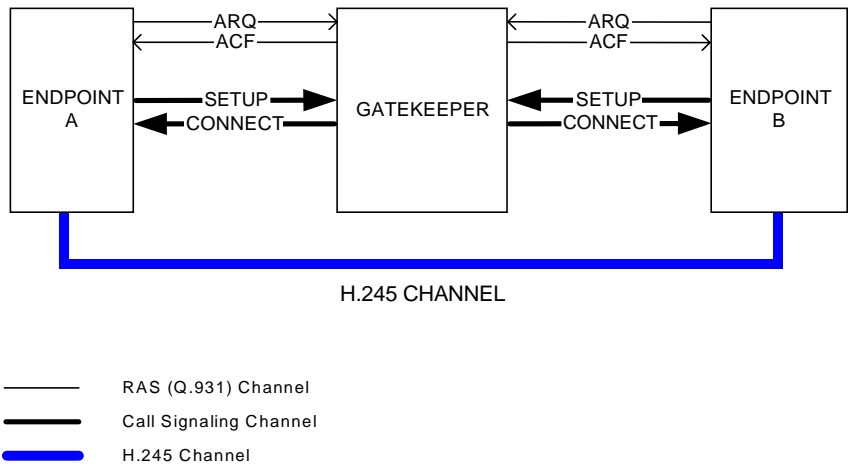


Figure 2-2 Routed Call Signaling

ROUTING H.245 CONTROL CHANNELS

In addition to the Call Signaling routing mode, the gatekeeper can route H.245 Control channels. To establish a H.245 routed call, the gatekeeper administrator can define an H.245 routed mode as a Default Policy for all calls. *Figure 2-3* shows H.245 routed Call Signaling.

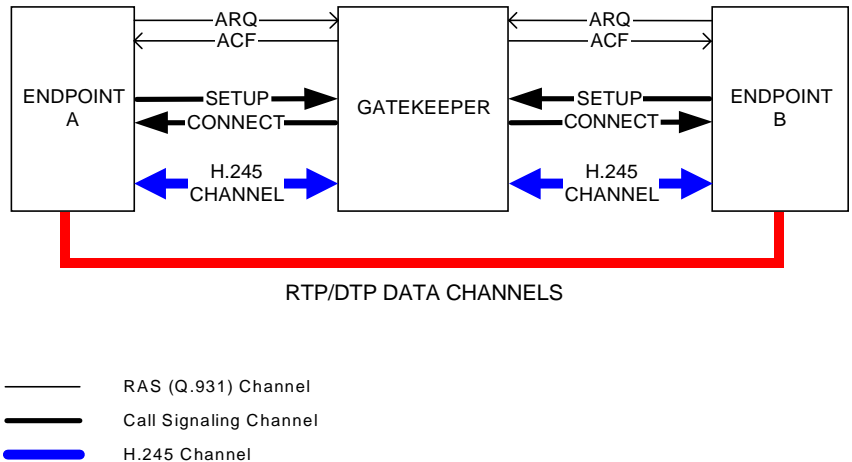


Figure 2-3 H.245 Routed Call Signaling

CALL TERMINATION

A call can be terminated in a number of ways, as described below.

DISENGAGE REQUEST

To terminate a call, both endpoints send a Disengage Request message (DRQ) to inform the gatekeeper that a call is being terminated. The gatekeeper can accept or reject this request.

UNREGISTRATION REQUEST

An alternative to a Disengage Request message is an Unregistration Request message (URQ). Either an endpoint or a gatekeeper can unregister an endpoint.

ENDPOINT-INITIATED UNREGISTRATION

When the gatekeeper receives a URQ message from a valid endpoint, the gatekeeper views the request details and can either accept or reject the request.

GATEKEEPER INITIATED UNREGISTRATION

The gatekeeper uses the H.323 polling mechanism (IRQ/IRR), or the Time To Live message (TTL) sent by the endpoint, for detecting endpoints that went offline without performing Unregistration. When the gatekeeper detects that an endpoint is not active, the gatekeeper initiates a URQ message.

SUPPORT OF ENDPOINTS WITHOUT RAS CAPABILITIES

The gatekeeper partially supports endpoints that do not support RAS. You can predefine aliases for these endpoints with the gatekeeper. The gatekeeper stores these aliases as dynamic data and thus can route calls to these endpoints.

The gatekeeper also gives services to calls from endpoints that do not support RAS, by relating to these calls as out-of-zone calls. In this case, the gatekeeper does not give the endpoint predefined permission to services or predefined distances, and it does not forward calls to the endpoint. However, the gatekeeper allows these endpoints to access services defined as public for out-of-zone endpoints.

CONTACTING RADVISION

For more information, please visit our website or contact a RADVISION sales representative at:

Europe/Middle East

24 Raul Wallenberg
Tel Aviv, Israel 69719
Tel: +972-3-645-5220
Fax: +972-3-647-6669

**infointernational@
radvision.com**

USA

575 Corporate Drive
Mahwah, NJ 07430
Tel: (201) 529-4300
Fax: (201) 529-3516

info@radvision.com

Asia Pacific

Suite F, 17/F China Overseas Bldg.
139 Hennessy Road
Wanchai, Hong Kong
Tel: +852-2801-4070
Fax: +852-2801-4071

apacinfo@hk.radvision.com

