UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Q.812

(02/2004)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE Q: CONMUTACIÓN Y SEÑALIZACIÓN

Interfaz Q3

Perfiles de protocolo de capa superior para las interfaces Q y X

Recomendación UIT-T Q.812

RECOMENDACIONES UIT-T DE LA SERIE Q

CONMUTACIÓN Y SEÑALIZACIÓN

SEÑALIZACIÓN EN EL SERVICIO MANUAL INTERNACIONAL	Q.1–Q.3
EXPLOTACIÓN INTERNACIONAL SEMIAUTOMÁTICA Y AUTOMÁTICA	Q.4–Q.59
CLÁUSULAS APLICABLES A TODOS LOS SISTEMAS NORMALIZADOS DEL UIT-T	Q.100–Q.119
ESPECIFICACIONES DE LOS SISTEMAS DE SEÑALIZACIÓN N.° 4, 5, 6, R1 Y R2	Q.120–Q.499
CENTRALES DIGITALES	Q.500–Q.599
INTERFUNCIONAMIENTO DE LOS SISTEMAS DE SEÑALIZACIÓN	Q.600–Q.699
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN N.° 7	Q.700–Q.799
INTERFAZ Q3	**Q.800–Q.849**
SISTEMA DE SEÑALIZACIÓN DIGITAL DE ABONADO N.° 1	Q.850–Q.999
RED MÓVIL TERRESTRE PÚBLICA	Q.1000–Q.1099
INTERFUNCIONAMIENTO CON SISTEMAS MÓVILES POR SATÉLITE	Q.1100–Q.1199
RED INTELIGENTE	Q.1200–Q.1699
REQUISITOS Y PROTOCOLOS DE SEÑALIZACIÓN PARA IMT-2000	Q.1700–Q.1799
ESPECIFICACIONES DE LA SEÑALIZACIÓN RELACIONADA CON EL CONTROL DE LLAMADA INDEPENDIENTE DEL PORTADOR	Q.1900–Q.1999
RED DIGITAL DE SERVICIOS INTEGRADOS DE BANDA ANCHA (RDSI-BA)	Q.2000–Q.2999

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T Q.812

Perfiles de protocolo de capa superior para las interfaces Q y X

Resumen

Esta Recomendación proporciona los perfiles de protocolo de capa superior (5-7) para las interfaces Q y X, definidas en las Recomendaciones UIT-T de la serie M.3000.

Orígenes

La Recomendación UIT-T Q.812 fue aprobada el 13 de febrero de 2004 por la Comisión de Estudio 4 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Recomendación UIT-T Q.812

Perfiles de protocolo de capa superior para las interfaces Q y X

1 Alcance

La presente Recomendación define las características de los perfiles de protocolo de las interfaces Q y X, definidas en las Recomendaciones UIT-T de la serie M.3000. Las interfaces soportarán la transferencia de datos bidireccional para la gestión de sistemas de telecomunicaciones.

Aunque se reconoce la necesidad de la funcionalidad de seguridad, este tema no se aborda a fondo en la presente Recomendación y queda en estudio. Es posible que los usuarios deban utilizar mecanismos al margen de la presente Recomendación para atender a sus necesidades específicas de seguridad. Puede darse el caso de que los mecanismos de seguridad elegidos dependan de la configuración de red que se utilice.

La Recomendación define:

– los perfiles de servicios de capa;

– los perfiles de protocolos de capa;

– los perfiles de servicios y protocolos de aplicación;

– los requisitos de conformidad que debe satisfacer una implementacion de esta interfaz.

La Recomendación no define:

– la estructura ni el significado de la información de gestión que se transmite mediante la serie de protocolos;

– la manera de efectuarse la gestión de resultas de los intercambios de protocolos de aplicación;

– las interacciones resultantes de la utilización de los protocolos de capa de aplicación.

Los perfiles indicados en la presente Recomendación son acordes con los perfiles normalizados internacionales equivalentes.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[1] ISO/CEI/TR 10000-1:1995, *Information technology – Framework and taxonomy of International Standardized Profiles – Part 1: General principles and documentation framework*.

[2] Recomendación UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico*.

[3] Recomendación UIT-T M.3010 (2000), *Principios para una red de gestión de las telecomunicaciones*.

[4] Recomendación UIT-T X.224 (1995) | ISO/CEI 8073:1997, *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo para proporcionar el servicio de transporte en modo con conexión*.

[5] Recomendación UIT-T X.225 (1995) | ISO/CEI 8327-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo de presentación con conexión: Especificación del protocolo*, más enmienda 1 (1997), *Mejoras del rendimiento*.

[6] ISO/CEI ISP 11183-1:1992, *Information technology – International Standardized Profiles AOM1n OSI Management – Management Communications – Part 1: Specification of ACSE, presentation and session protocols for the use by ROSE and CMISE*.

[7] Recomendación UIT-T X.216 (1994) | ISO/CEI 8822:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Definición del servicio de presentación*.

[8] Recomendación UIT-T X.226 (1994) | ISO/CEI 8823-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo de presentación con conexión: Especificación del protocolo*.

[9] Recomendación UIT-T X.209 (1988), *Especificación de las reglas básicas de codificación de la notación de sintaxis abstracta uno (NSA.1)*.

ISO/CEI 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*.

[10] Recomendación UIT-T X.680 (1994) | ISO/CEI 8824-1:1995, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica*.

[11] Recomendación UIT-T X.681 (1994) | ISO/CEI 8824-2:1995, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de objetos de información*.

[12] Recomendación UIT-T X.682 (1994) | ISO/CEI 8824-3:1995, *Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de constricciones*.

[13] Recomendación UIT-T X.683 (1994) | ISO/CEI 8824-4:1995, *Tecnología de la información – Notación de sintaxis abstracta uno: Parametrización de las especificaciones de la notación de sintaxis abstracta uno*.

[14] Recomendación UIT-T X.208 (1988), *Especificación de la notación de sintaxis abstracta uno (NSA.1)*.

ISO/CEI 8824:1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)*.

[15] ISO/CEI 9545:1994, *Information technology – Open Systems Interconnection – Application Layer structure*.

[16] Recomendación UIT-T X.217 (1995) | ISO/CEI 8649:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Definición de servicio para el elemento de servicio de control de asociación*.

[17] Recomendación UIT-T X.227 (1995) | ISO/CEI 8650-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo con conexión para el elemento de servicio de control de asociación: Especificación de protocolo*.

[18] Recomendación UIT-T X.219 (1988), *Operaciones a distancia: Modelo, notación y definición del servicio*.

ISO/CEI 9072-1:1989, *Information processing systems – Text communication – Remote operations – Part 1: Model, notation and service definition*.

[19] Recomendación UIT-T X.229 (1988), *Operaciones a distancia: Especificación del protocolo*.

ISO/CEI 9072-2:1989, *Information processing systems – Text communication – Remote operations – Part 2: Protocol specification*.

[20] Recomendación X.710 del CCITT (1991), *Definición del servicio común de información de gestión para aplicaciones del CCITT*.

ISO/CEI 9595:1991, *Information technology – Open Systems Interconnection – Common management information service definition*.

[21] Recomendación X.711 del CCITT (1991), *Especificación del protocolo común de información de gestión para aplicaciones del CCITT*.

ISO/CEI 9596-1:1991, *Information technology – Open Systems Interconnection – Common management information protocol – Part 1: Specification*.

[22] ISO/CEI ISP 11183-3:1992, *Information technology – International Standardized Profiles AOM1n OSI Management – Management Communications – Part 3: CMISE/ROSE for AOM11 – Basic Management Communications*.

[23] ISO/CEI ISP 11183-2:1992, *Information technology – International Standardized Profiles AOM1n OSI Management – Management Communications – Part 2: CMISE/ROSE for AOM12 – Enhanced Management Communications*.

[24] ISO/CEI ISP 10607-1:1995, *Information technology – International Standardized Profiles AFTnn – File Transfer, Access and Management – Part 1: Specification of ACSE, Presentation and Session protocols for the use of FTAM*.

[25] ISO 8571-1:1988, *Information processing systems – Open Systems Interconnection – File Transfer, Access and Management – Part 1: General introduction*.

[26] ISO 8571-2:1988, *Information processing systems – Open Systems Interconnection – File Transfer, Access and Management – Part 2: Virtual Filestore Definition*.

[27] ISO 8571-3:1988, *Information processing systems – Open Systems Interconnection – File Transfer, Access and Management – Part 3: File Service Definition*.

[28] ISO 8571-4:1988, *Information processing systems – Open Systems Interconnection – File Transfer, Access and Management – Part 4: File Protocol Specification*.

[29] Recomendación UIT-T X.500 (1997) | ISO/CEI 9594-1:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Visión de conjunto de conceptos, modelos y servicios*.

[30] Recomendación UIT-T X.501 (1997) | ISO/CEI 9594-2:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos*.

[31] Recomendación UIT-T X.511 (1997) | ISO/CEI 9594-3:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Definición de servicio abstracto*.

[32] Recomendación UIT-T X.518 (1997) | ISO/CEI 9594-4:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Procedimientos para operación distribuida*.

[33] Recomendación UIT-T X.519 (1997) | ISO/CEI 9594-5:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Especificaciones de protocolo*.

[34] Recomendación UIT-T X.520 (1997) | ISO/CEI 9594-6:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Tipos de atributos seleccionados*.

[35] Recomendación UIT-T X.521 (1997) | ISO/CEI 9594-7:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Clases de objetos seleccionadas*.

[36] Recomendación UIT-T X.509 (1997) | ISO/CEI 9594-8:1998, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marco de autenticación*.

[37] Recomendación UIT-T X.880 (1994) | ISO/CEI 13712-1:1995, *Tecnología de la información – Operaciones a distancia: Conceptos, modelo y notación*.

[38] Recomendación UIT-T X.881 (1994) | ISO/CEI 13712-2:1995, *Tecnología de la información – Operaciones a distancia – Realizaciones de interconexión de sistemas abiertos: definición de servicio del elemento de servicio de operaciones a distancia*.

[39] Recomendación UIT-T X.830 (1995) | ISO/CEI 11586-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de capas más altas: Sinopsis, modelo y notación*.

[40] ISO/CEI ISP 10607-3:1995, *Information technology – International Standardized Profiles AFTnn – File Transfer, Access and Management – Part 3: AFT11 – Simple File Transfer Service (unstructured)*.

[41] Recomendación UIT-T X.214 (1995) | ISO/CEI 8072:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Definición del servicio del transporte*.

[42] Recomendación UIT-T X.882 (1994) | ISO/CEI 13712-3:1995, *Tecnología de la información – Operaciones a distancia: Realizaciones de interconexión de sistemas abiertos: Especificación de protocolo del elemento del servicio de operaciones a distancia*.

[43] Recomendación X.800 del CCITT (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

ISO/CEI 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

[44] Recomendación UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad para las capas superiores*.

[45] Recomendación UIT-T Q.811 (2004), *Perfiles de protocolo de capa inferior para las interfaces Q y X*.

[46] Recomendación UIT-T Q.814 (2000), *Especificación de un agente interactivo de intercambio electrónico de datos*.

[47] Recomendación UIT-T Q.815 (2000), *Especificación de un modelo de seguridad para la protección del mensaje completo*.

[48] IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet Standard Management Framework*.

[49] IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*.

[50] IETF RFC 3412 (2002), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*.

[51] IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications*.

[52] IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

[53] IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

[54] IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.

[55] IETF RFC 3417 (2002), *Transport Mappings for the Simple Network Management Protocol (SNMP)*.

[56] IETF RFC 3584 (2003), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*.

[57] IETF RFC 2578 (1999), *Structure of Management Information Version 2 (SMIv2)*.

[58] IETF RFC 3430 (2002), *Simple Network Management Protocol (SNMP) over Transmission Control Protocol (TCP) Transport Mapping*.

[59] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

[60] ISO/CEI ISP 10608-1:1992, *Information technology – International Standardized Profile TAnnnn – Connection-mode Transport Service over Connectionless-mode Network Service – Part 1: General overview and subnetwork-independent requirements*.

[61] ISO/CEI ISP 10609-1;1992, *Information technology – International Standardized Profiles TB, TC, TD and TE – Connection-mode Transport Service over connection-mode Network Service – Part 1: Subnetwork-type independent requirements for Group TB*.

[62] CORBA GIOP Specification, Chapter 15 of *The Common Object Request Broker: Architecture and Specification*, Revision 2.3, Object Management Group (OMG Doc. Number: Formal/98-12-01).

[63] CORBA Security Service Specification, Chapter 15 of *CORBA services: Common Object Services Specification*, Object Management Group (OMG Doc. Number: Formal/98-12-17).

[64] Recomendación UIT-T M.3030 (2002), *Marco para un lenguaje de marcaje en telecomunicaciones*.

3 Definiciones

En esta Recomendación se definen los términos siguientes.

3.1 perfil normalizado internacional (ISP, *international standardized profile*): Documento armonizado objeto de acuerdo internacional en el que se identifica una norma o grupo de normas, junto con las opciones y los parámetros, necesarios para desempeñar una función o conjunto de funciones [1].

3.2 agente interactivo (IA, *interactive agent*) (Rec. UIT-T Q.814): El IA soporta el intercambio de transacciones de intercambio de datos electrónicos (UN/EDIFACT o ASC X12 EDI) entre entidades pares. El IA actúa como una interfaz entre su usuario directo (normalmente un traductor EDIFACT/ASC X12 EDI o un módulo de seguridad) y la seguridad de la capa de transporte. Se pueden considerar diversos planteamientos de implementación que varían desde una simple API (interfaz de programa de aplicación) hasta un programa independiente. El IA se describe en la Rec. UIT-T Q.814 y el módulo de seguridad se describe en la Rec. UIT-T Q.815.

3.3 seguridad de la capa de transporte (TLS, *transport layer security*) (Rec. UIT-T Q.814): El protocolo de seguridad de la capa de transporte (TLS) proporciona una opción de privacidad en las comunicaciones. El protocolo permite que las aplicaciones cliente/servidor comuniquen en una

forma diseñada para evitar escuchas, alteraciones e intrusiones. El protocolo TLS también proporciona una fuerte autenticación par e integridad de flujo de datos.

3.4 reglas de codificación distinguida (DER, *distinguished encoding rules*) (Rec. UIT-T X.690): Las DER para ASN.1 son un subconjunto de las reglas de codificación básica (BER, *basic encoding rules*) y proporcionan exactamente una forma de representar cualquier valor ASN.1 como una cadena de octetos. Las DER están destinadas a aplicaciones en las que solo se precisa una única codificación de cadenas de octetos, lo que es el caso cuando se codifica un mensaje ASN.1 para su transporte por TLS. Las DER se describen en la Rec. UIT-T X.690. En este perfil se tiene que emplear el método de longitud definida para construir los mensajes IA.

3.5 protocolo de transferencia de agente interactivo (IATP, *interactive agent transfer protocol*) (Rec. UIT-T Q.814): El protocolo IATP se utiliza entre agentes interactivos pares que desean intercambiar transacciones/mensajes de intercambio de datos electrónicos con protocolos de control de transmisión o protocolos de Internet utilizando la seguridad de la capa de transporte. El IATP se describe en la Rec. UIT-T UIT-T Q.814.

3.6 traductor de intercambio de datos electrónicos (EDI, *electronic data interchange*) (Rec. UIT-T Q.814): Módulo o programa de soporte lógico de ordenador que traduce formatos y representaciones de datos privados en/hacia formatos normalizados y representaciones de datos normalizados tales como los especificados por ISO 9735 o ANSI ASC X12.

4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

ACSE Elemento de servicio de control de asociación (*association control service element*)

AE Entidad de aplicación (*application entity*)

APDU Unidad de datos de protocolo de aplicación (*application protocol data unit*)

ASE Elemento de servicio de aplicación (*application service element*)

ASN.1 Notación de sintaxis abstracta uno (*abstract syntax notation one*)

ASO Objeto de servicio de aplicación (*application service object*)

BER Reglas básicas de codificación (*basic encoding rules*)

CCITT Comité Consultivo Internacional Telegráfico y Telefónico

CEI Comisión Electrotécnica Internacional

CF Función de control (*control function*)

CLNS Servicio de capa de red sin conexión (*connectionless-mode network layer service*)

CMIP Protocolo común de información de gestión (*common management information protocol*)

CMISE Elemento de servicio común de información de gestión (*common management information service element*)

CONS Servicio de capa de red con conexión (*connection-mode network layer service*)

CORBA Arquitectura de intermediario de petición de objetos común (*common object request broker architecture*)

COTS servicio de transporte con conexión (*connection-mode transport service*)

DAP Protocolo de acceso al directorio (*directory access protocol*)

DER Reglas de codificación distinguida (*distinguished encoding rules*)

DSA	Agente de sistema de directorio (*directory system agent*)
DUA	Agente de usuario de directorio (*directory user agent*)
EDI	Intercambio electrónico de datos (*electronic data interchange*)
EDIFACT	Intercambio electrónico de datos para administración, comercio y transporte (*electronic data interchange for administration, commerce and transport*)
FTAM	Transferencia, acceso y gestión de ficheros (*file transfer, access and management*)
GULS	Seguridad genérica de capa superior (*generic upper layer security*)
IA	Agente interactivo (*interactive agent*)
IATP	Protocolo de transferencia de agente interactivo (*interactive agent transfer protocol*)
IDL	Lenguaje de definición de interfaz (*interface definition language*)
IETF	Grupo de tareas especiales de ingeniería en Internet (*Internet engineering task force*)
IP	Protocolo Internet (*Internet protocol*)
IPSec	Arquitectura de seguridad para el protocolo IP (*security architecture for the IP protocol*)
ISO	Organización internacional de normalización (*international organization for standardization*)
ISP	Perfil normalizado internacional (*international standardized profile*)
NBS	Oficina nacional de normas (*National Bureau of Standards*)
NCMS	Subprotocolo de gestión de conexión de red (*network connection management subprotocol*)
NE	Elemento de red (*network element*)
OS	Sistema de operaciones (*operations system*)
OSI	Interconexión de sistemas abiertos (*open systems interconnection*)
PDU	Unidad de datos de protocolo (*protocol data unit*)
RCD	Red de comunicación de datos
RFC	Petición de comentarios (*request for comments*)
RGT	Red de gestión de telecomunicaciones
ROS	Servicio de operaciones a distancia (*remote operations service*)
ROSE	Elemento de servicio de operaciones a distancia (*remote operations service element*)
SACF	Función individual de control de asociación (*single association control function*)
SMASE	Elemento de servicio de aplicación de gestión de sistemas (*systems management application service element*)
SNMP	Protocolo simple de gestión de red (*simple network management protocol*)
SPDU	Unidad de datos de protocolo de sesión (*session protocol data unit*)
TCP	Protocolo de control de transmisión (*transmisión control protocol*)
TLS	Seguridad de la capa de transporte (*transport layer security*)
tML	Lenguaje de marcaje en telecomunicaciones (*telecommunications markup lenguaje*)
UDP	Protocolo de datagrama de usuario (*user datagram protocol*)
UIT	Unión Internacional de Telecomunicaciones

UIT-T Unión Internacional de Telecomunicaciones – Sector de Normalización de las Telecomunicaciones

USM Modelo de seguridad basado en el usuario (*user-based security model*)

5 Especificaciones de protocolo de capa superior para el paradigma OSI

5.1 Introducción a las especificaciones de protocolo de capa superior para el paradigma OSI

Los servicios y protocolos de comunicación definidos en esta Recomendación están de acuerdo con el modelo de referencia de interconexión de sistemas abiertos (OSI, *open systems interconnection*) [2].

Los protocolos de las diferentes capas se basan en Recomendaciones UIT-T y/o Normas ISO, especificaciones CORBA de OMG y especificaciones de protocolo de Internet del IETF.

En la presente Recomendación se definen tres tipos de perfiles de protocolo:

– perfil de protocolo de capa superior para servicios de clase interactiva;

– perfil de protocolo de capa superior para servicios de clase orientada a ficheros;

– especificación de protocolo de capa superior para servicios de directorio.

Los tres perfiles de protocolo pueden aplicarse a aplicaciones que utilizan la RCD, que se define en la Rec. UIT-T M.3010 [3].

La interfaz Q se define para tratar de conectar los dispositivos de mediación a los sistemas de operaciones (OS, *operations systems*), los adaptadores Q a los OS, los NE a los OS y los OS a los OS a través de una RCD. La interfaz X se define para conectar las RGT de dos Administraciones.

Se añadirán otros ASE en los perfiles de protocolo identificados a medida que se desarrollen nuevos requisitos.

5.2 Especificación de protocolo de capa superior para servicios de clase interactiva

En la figura 1 se ilustra la pila de protocolos del perfil de protocolo de capa superior para los servicios de clase interactiva. El perfil para los conjuntos de funciones RGT correspondientes al SMASE de clase interactiva de servicios puede especificarse como parte de las Recomendaciones en que se definen los modelos y servicios de información.

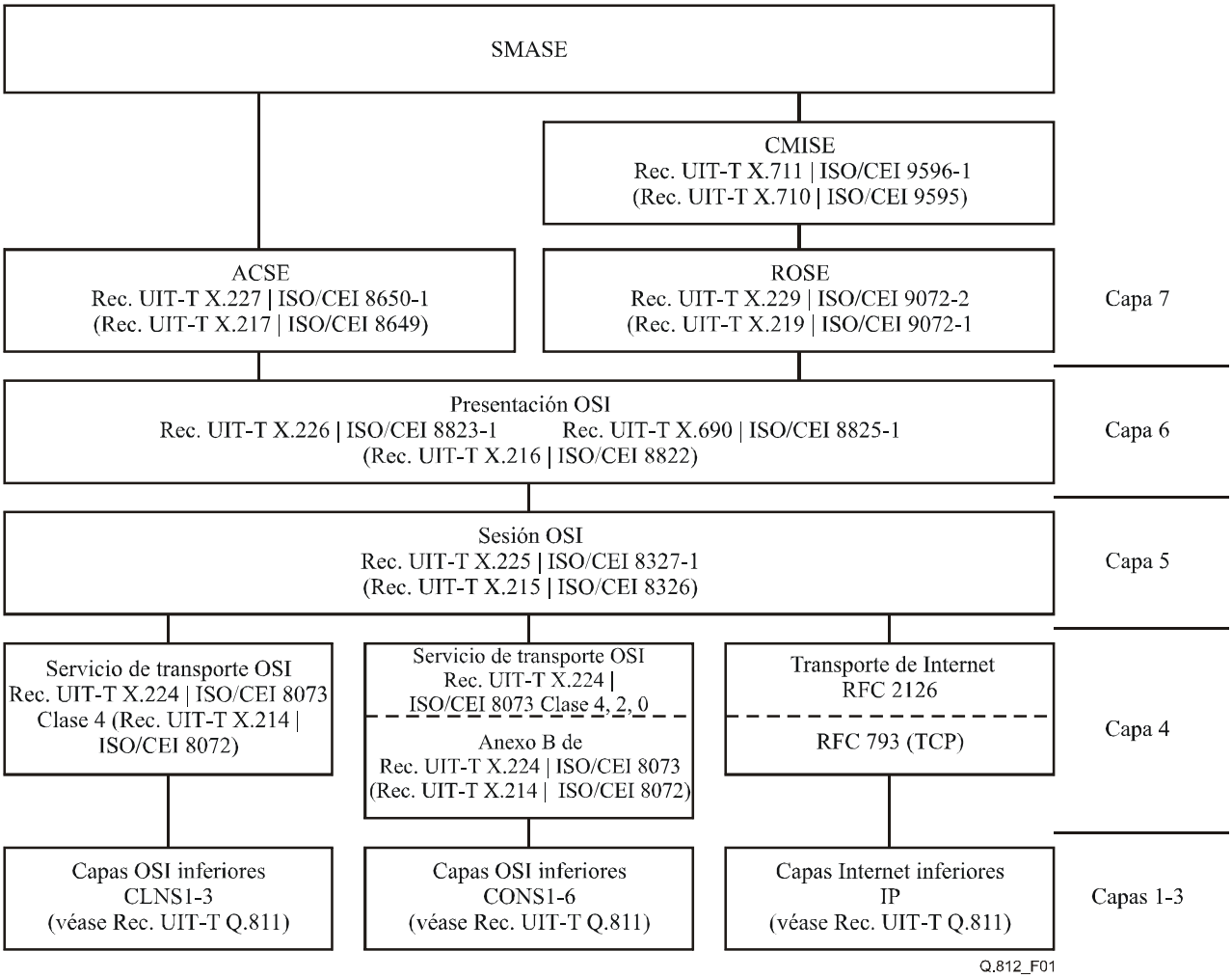

Figura 1/Q.812 – Pila de protocolos del perfil de protocolo de capa superior para servicios de clase interactiva para el paradigma OSI

5.3 Especificación de protocolo de capa superior para servicios de clase orientada a ficheros

En la figura 2 se ilustra la pila de protocolos del perfil de protocolo de capa superior para servicios de clase orientada a ficheros.

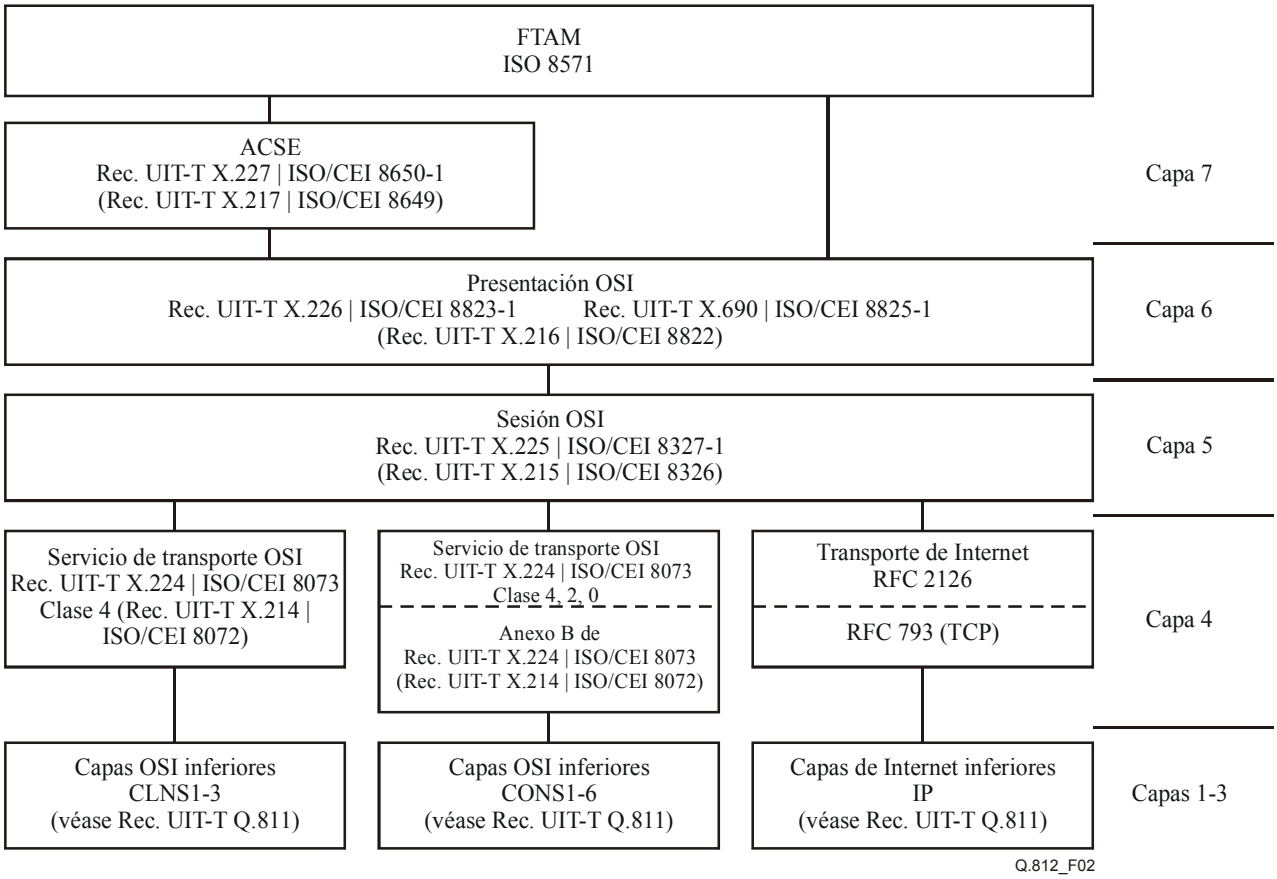

Figura 2/Q.812 – Pila de protocolos del perfil de protocolo de capa superior para servicios de clase orientada a ficheros para el paradigma OSI

5.4 Especificación de protocolo de capa superior para servicios de directorio

En la figura 3 se ilustra la pila de protocolos del perfil de protocolo de capa superior para servicios de directorio.

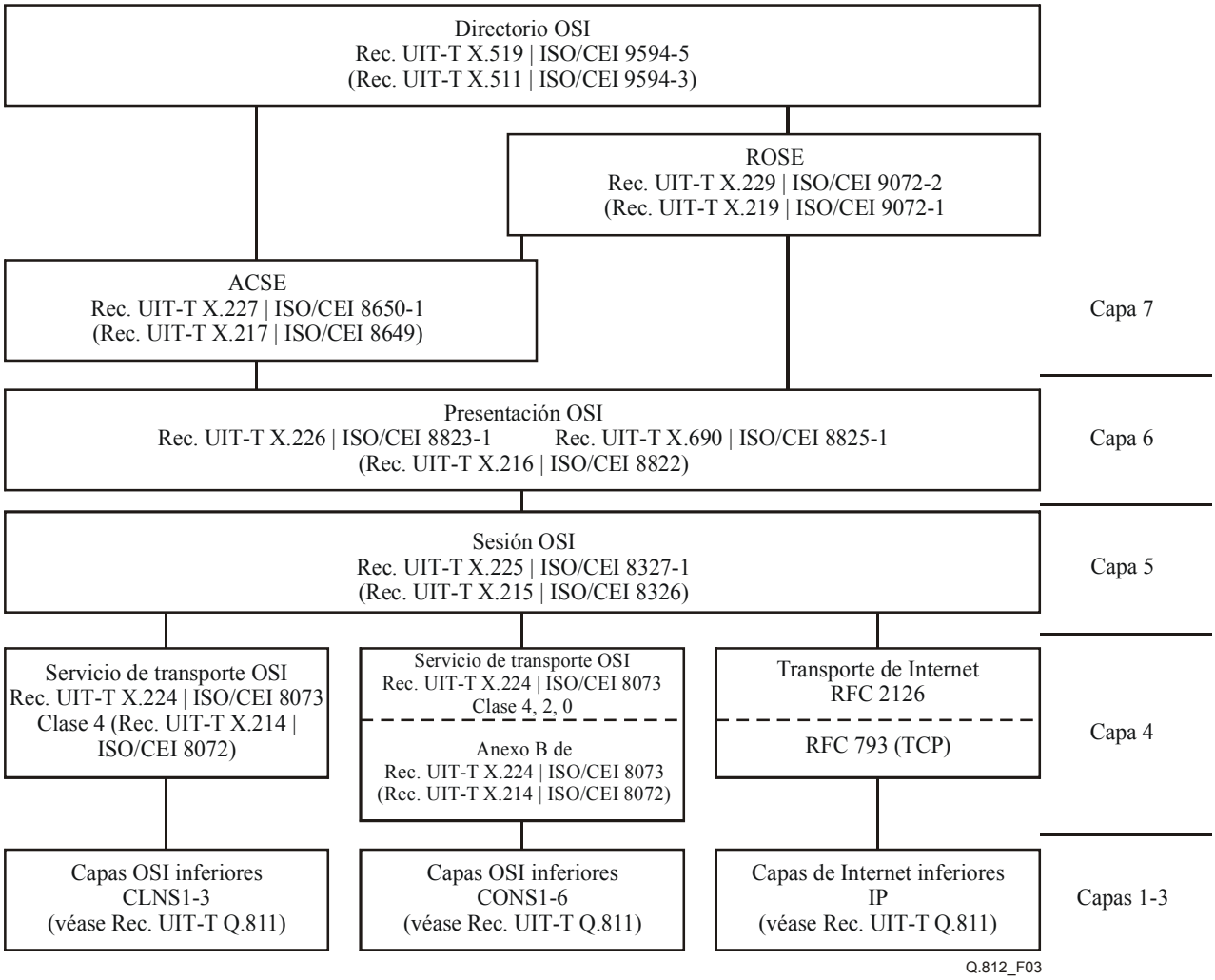

Figura 3/Q.812 – Pila de protocolos del perfil de protocolo de capa superior para servicios de directorio en el paradigma OSI

5.5 Especificación de protocolo de capa superior para servicios de almacenamiento y retransmisión

Los protocolos de capa superior que han de utilizarse para los servicios de almacenamiento y retransmisión (por ejemplo, para intercambiar información formateada EDI) quedan en estudio.

6 Especificación de protocolo de capa superior para servicios de clase interactiva que utilizan el paradigma OSI

6.1 Perfiles de capa de transporte

6.1.1 Perfil de capa de transporte para CLNS1, CLNS2 y CLNS3

Esta cláusula define el perfil de capa de transporte para su utilización con CLNS1, CLNS2 y CLNS3 como se define en la Rec. UIT-T UIT-T Q.811 [45].

6.1.1.1 Perfil de servicio

Es obligatorio para el servicio de red sin conexión que el servicio de transporte sea conforme a la Rec. UIT-T X.214 | ISO/CEI 8072 [41].

6.1.1.2 Perfil de protocolo

La operación del protocolo de transporte sobre el servicio de capa de red sin conexión (CLNS, *connectionless-mode network layer service*), descrito en la Rec. UIT-T X.213 | ISO/CEI 8348, utilizará los elementos de la Rec. UIT-T X.224 | ISO/CEI 8073 [4], operación de clase 4 sobre el CLNS. También aplican aquí las cláusulas 6.1.2.1.2, 6.1.2.1.3, 6.1.2.1.4, 6.1.2.2.4, 6.1.2.2.6, 6.1.2.2.7 y 6.1.2.2.8 del protocolo de transporte de perfil CONS1.

6.1.1.3 Clase de servicio

Es obligatorio el soporte de la operación de clase 4 de la Rec. UIT-T X.224 | ISO/CEI 8073 [4].

6.1.1.4 Atributos de la capa de transporte

Los atributos de la capa de transporte para la operación de clase 4 sobre el servicio de capa de red sin conexión será el que se muestra en el cuadro 1.

Cuadro 1/Q.812 – Atributos de la capa de transporte [para su uso con el servicio de capa de red en modo sin conexión (CLNS)]

Atributo	Gama	Valor por defecto
TPDU máxima (octetos)	128, 256, 512, 1024 (2048, 4096, 8192 opcional)	(128)
TSAP-ID (nota 1)	Hasta 32 octetos	–
Clase de servicio	4	–
Clase preferida	4	–
Clase alternativa	Ninguna	–
Datos acelerados	No utilización	–
Opciones:		
Parámetros de seguridad	Optativo	–
Numeración TPDU de datos (nota 2)	Normal, ampliada	(Normal)
Suma de verificación (nota 3)	Utilización, no utilización	(No utilización)
Parámetros:		
T1 – Tiempo de retransmisión	0,25-64 segundos (nota 4)	(8)
N – Retransmisiones	2-15	(2)
L – Referencia vinculada	1-256 segundos	(32)
I – Tiempo de inactividad	2-512 segundos	(64)

NOTA 1 – Algunos sistemas pueden necesitar identificadores de punto de acceso al servicio de transporte (TSAP-ID). Sin embargo, todos los sistemas deberán poder generar TSAP-ID llamados en las TPDU de CR poder recibir TSAP-ID llamantes y llamados en las TPDU de CR y CS, respectivamente.

NOTA 2 – Se implementará la opción de formato ampliado. La no utilización de esta opción será negociable. El contestador atenderá cuando sea posible la petición del iniciador. La negociación de algo distinto de lo solicitado sólo se producirá en condiciones anormales; por ejemplo, en caso de grave congestión si así lo determina el implementador. Los iniciadores deberán poder operar en el modo confirmado por el contestador.

NOTA 3 – Para la TPDU de CR se requiere suma de verificación. Un requisito adicional es que todas las implementaciones soporten la "no utilización" negociada de suma de verificación. Los iniciadores pedirán la "no utilización" de la suma de verificación y los contestadores darán su acuerdo.

NOTA 4 – El temporizador T1 de la capa de transporte debe ser siempre mayor que el temporizador T1 de la capa de enlace.

6.1.2 Perfil de la capa de transporte para CONS1, CONS2, CONS3 y CONS5

Esta cláusula define el perfil de capa de transporte para su utilización con CONS1, CONS2, CONS3, CONS4 y CONS5 como se define en la Rec. UIT-T Q.811 [45].

6.1.2.1 Perfiles de servicio

Los perfiles de protocolo descritos en esta Recomendación proporcionan a las capas OSI superiores el servicio de transporte en modo con conexión (COTS, *connection-mode transport service*) que se define en la Rec. UIT-T X.214 | ISO/CEI 8072 [41].

6.1.2.1.1 Subdivisión

Los contestadores pueden rechazar conexiones de red que pudieran imponer una restricción innecesaria a su capacidad de establecer conexiones de red salientes. Para evitar la repetición de tentativas fallidas durante la subdivisión, los iniciadores se abstendrán de pedir conexiones de red adicionales para una conexión de transporte inmediatamente después de haber sido rechazada una conexión de red. El tiempo que ha de transcurrir antes de pedir nuevas conexiones de red queda en estudio.

6.1.2.1.2 Negociación de la calidad de servicio

La negociación de la calidad de servicio cae fuera del alcance de esta Recomendación. Si no se soporta la negociación de la calidad de servicio, se ignorará la recepción de los parámetros "caudal", "tasa de errores residuales", "prioridad" y "retardo de tránsito" en las TPDU de CR y CC.

6.1.2.1.3 Negociación del tamaño de las TPDU

La interoperabilidad se logra haciendo que el iniciador proponga uno de los tamaños de TPDU del conjunto especificado en el cuadro 2, y que el contestador seleccione el más adecuado, entre 128 y el tamaño propuesto. Las reglas para la negociación del tamaño de la TPDU a utilizar en un caso de comunicación determinado se especifican en la Rec. UIT-T X.224 | ISO/CEI 8073 [4].

La elección del tamaño de la TPDU es un asunto de implementación de carácter local.

6.1.2.1.4 Negociación de la protección

La negociación de la protección cae fuera del alcance de esta Recomendación. Si no se soporta la negociación de la protección, se ignorará la recepción de los parámetros de protección en cualesquiera TPDU de CR y CC.

6.1.2.2 Perfil de protocolo

Es obligatorio que, para el servicio de red en modo conexión, la capa de transporte cumpla la Rec. UIT-T X.224 | ISO/CEI 8073 [4] aplicables a la utilización del servicio de capa de red en modo con conexión (CONS, *connection-mode network layer service*).

6.1.2.2.1 Clase de servicio

Las clases 4, 2 y 0 se soportarán, como se muestra en el cuadro 2, en los países que necesiten las características de clase 4 de la capa de transporte. Las reglas de conformidad de la Rec. UIT-T X.224 | ISO/CEI 8073 [4] exigen que se soporten asimismo de las clases 0 y 2 cuando se especifica clase 4. Con el equipo existente y en los países que no necesiten la clase 4, es obligatorio soportar la clase 0 y la clase 2 es facultativa.

Los valores por defecto formarán parte de la oferta del vendedor. Es decir, si el usuario no especifica otra cosa, los parámetros por defecto serán los suministrados inicialmente. El usuario podrá modificarlos posteriormente dentro de la gama especificada.

Además de los especificados en la Rec. UIT-T X.224 | ISO/CEI 8073 [4] el equipo cumplirá el requisito siguiente: si un contestador recibe como clase alternativa "ninguna", responderá con la clase preferida. Las reglas para los contestadores se especifican en el cuadro 3.

Se facilitarán opciones de usuario para designar las clases preferida y alternativa (véase el cuadro 3/X.224 | ISO/CEI 8073 [4]). Cuando se soportan todas las clases, la preferida para la conexión es la clase 4.

Cuadro 2/Q.812 – Atributos de la capa de transporte [para servicios de red en modo conexión (CONS)]

Atributo	Gama	Valor por defecto
TPDU máxima (octetos)	128, 256, 512, 1024 (2048, 4096, 8192 opcional)	(128)
Clase de servicio	4, 2, 0	
Clase preferida	4, 2, 0	(4)
Clase alternativa	4, 2, 0, ninguna	(Ninguna)
Datos acelerados	No utilización	
Opciones para clase 4		
Numeración TPDU de datos (nota 2)	Normal, ampliada	(Normal)
Opciones para clase 2		
Numeración TPDU de datos (nota 2)	Normal, ampliada	(Normal)
Control de flujo	Explícito	
Parámetros para clase 4		
T1 – Tiempo de retransmisión	0,25-64 segundos (nota 4)	(8)
N – Retransmisiones	2 (otros valores, en estudio)	
L – Referencia vinculada	1-256 segundos	(32)
I – Tiempo de inactividad	2-512 segundos	(64)

NOTA 1 – Algunos sistemas pueden necesitar identificadores de punto de acceso al servicio de transporte (TSAP-ID, *transport service access point identifier*). Sin embargo, todos los sistemas deberán poder generar TSAP-ID llamados en las TPDU de CR poder recibir TSAP-ID llamantes y llamados en las TPDU de CR y CS, respectivamente.

NOTA 2 – Se implementará la opción de formato ampliado. La no utilización de esta opción será negociable. El contestador atenderá cuando sea posible la petición del iniciador. La negociación de algo distinto de lo solicitado sólo se producirá en condiciones anormales; por ejemplo, en caso de grave congestión si así lo determina el implementador. Los iniciadores deberán poder operar en el modo confirmado por el contestador.

NOTA 3 – Para la TPDU de CR se requiere suma de verificación. Un requisito adicional es que todas las implementaciones soporten la "no utilización" negociada de suma de verificación. Los iniciadores pedirán la "no utilización" de la suma de verificación y los contestadores darán su acuerdo.

NOTA 4 – El temporizador T1 de la capa de transporte debe ser siempre mayor que el temporizador T1 de la capa de enlace.

Cuadro 3/Q.812 – Respuestas válidas correspondientes a las clases preferida y alternativa propuestas en la TPDU de CR

Clase preferida	Clase alternativa			
	0	2	4	Ninguna
0	No válida	No válida	No válida	Clase 0
2	Clases 0, 2	Clase 2	No válida	Clase 2
4	Clases 0, 2, 4	Clases 2 ó 4	Clase 4	Clases 2 ó 4

6.1.2.2.2 Identificación de protocolo

Para la identificación de protocolo de capa de transporte se utilizarán los procedimientos especificados en el anexo B de la Rec. UIT-T X.224 | ISO/CEI 8073 [4] y la Rec. UIT-T X.264 | ISO/CEI 11570. Deben seguirse los convenios para la identificación de protocolos que figuran en la Rec. UIT-T X.263 | ISO/CEI TR 9577. La selección de códigos no especificados en las normas mencionadas queda en estudio. La ausencia de datos de usuario de llamada en una petición de

llamada o en un paquete de aceptación de llamada de la Rec. UIT-T X.25 y de ISO/CEI 8208 indica la actuación de los procedimientos de capa de transporte de la Rec. UIT-T X.224 | ISO/CEI 8073 [4].

6.1.2.2.3 Atributos

El cuadro 2 resume los atributos de la capa de transporte a utilizar con el CONS. La elección de valores dentro de las gamas requerida y opcional depende de las características de los mensajes.

NOTA – La necesidad de soportar mensajes de alta prioridad que requieren bajo retardo de tránsito en una conexión de transporte determinada debe quedar reflejada en los parámetros de calidad de servicio pedidos cuando se establece la conexión de transporte. Una entidad de transporte adecuadamente implementada no debe multiplexar mensajes de alta prioridad que requieran bajo retardo de tránsito si no pueden proporcionar la calidad de servicio solicitada. Como este detalle es de implementación, no está sujeto a normalización.

6.1.2.2.4 Datos de usuario en las TPDU de petición de conexión y confirmación de conexión

Los datos de usuario en las TPDU de petición y confirmación de conexión son opcionales en la Rec. UIT-T X.224 | ISO/CEI 8073 [4]. Ningún usuario del servicio de transporte los enviará; todas las implementaciones de protocolos estarán preparadas para recibirlos y todas ellas podrán ignorarlos, es decir, no provocarán una desconexión.

6.1.2.2.5 TPDU de error de clase 0

Si se ha negociado la clase de transporte 0, puede utilizarse en cualquier momento la unidad de datos de protocolo de transporte de error (ER-TPDU, *error transport protocol data unit*) y, a su recepción, hará falta que el destinatario desconecte la conexión de red y, por extensión, la conexión de transporte.

6.1.2.2.6 Parámetros de TPDU de CR desconocidos

Se ignorará todo parámetro desconocido recibido en cualquier TPDU de CR.

Cuando se soporten todas las clases, la clase preferida al iniciar una TPDU de CR será la clase 4.

Si un contestador recibe como clase alternativa "ninguna", es obligatoria una negociación implícita.

6.1.2.2.7 Valores no válidos de parámetros de TPDU de CR conocidos

Los parámetros conocidos con longitudes válidas pero con valores no válidos en una CR de TPDU se tratarán como se indica en el cuadro 4.

Cuadro 4/Q.812 – Parámetros de TPDU

Parámetro	Acción
TSAP ID	Enviar TPDU de DR
Tamaño de TPDU	Ignorar parámetro, utilizar valor por defecto
Versión	Ignorar parámetro, utilizar valor por defecto
Suma de control	Descartar TPDU de CR
Clases de protocolo alternativo	Error de protocolo

6.1.2.2.8 Parámetro de opciones adicionales

Se ignorarán los bits no reconocidos o no aplicables de las "opciones adicionales".

6.1.2.2.9 Subprotocolo de gestión de conexión de red (NCMS)

La utilización del subprotocolo de gestión de conexión de red (NCMS, *network connection management subprotocol*), tal como se define en el anexo B de la Rec. UIT-T X.224 |

ISO/CEI 8073 [4] es opcional. Las implementaciones que soporten el NCMS deberán poder comunicarse con aquéllas que no lo soporten.

6.1.3 Perfil ISO TP0/TPC/IP para su utilización con el servicio IP

Esta cláusula define el perfil de protocolo de transporte para su utilización con el paradigma OSI cuando se utiliza el servicio IP de capa inferior definido en la Rec. UIT-T UIT-T Q.811 [45].

– Para la parte superior de la capa 4 – STD0035 "Servicio de transporte ISO en la parte superior del TCP (Versión 3)", marzo de 1997. (Incluye RFC 2126.) Este documento define como proporcionar los servicios de transporte TP0, ISO por TCP.

– Para la parte inferior de la capa 4 – STD0007 "Protocolo de control de transmisión", septiembre de 1981 (incluye RFC 793).

Hay que destacar que STD0035 (RFC 2126) implementa el protocolo ISO TP0 además de TCP/IP, pero no del protocolo de red ISO/UIT-T. Puesto que se utiliza el protocolo de transporte de clase 0 en la conexión TCP/IP, consigue la misma funcionalidad que la clase 4 de transporte. Por lo tanto, las capas de niveles superiores ISO/UIT-T (todas las entidades de sesión, presentación y aplicación) pueden funcionar totalmente sin conocer el hecho de que están funcionando en una red TCP/IP.

6.2 Capa de sesión

6.2.1 Definición del servicio

La capa de sesión se ajusta a la definición de servicio de la Rec. UIT-T X.215 | ISO/CEI 8326.

Los valores por defecto formarán parte de la oferta del vendedor; es decir, a menos que el usuario especifique otra cosa, los parámetros por defecto serán los valores iniciales suministrados. Posteriormente pueden ser modificados por el usuario dentro de una gama especificada.

Entre la ISO y el UIT-T se ha planteado un conflicto en cuanto a los valores de código para el número de subsecuencia y confirmación del control de flujo. Cabe esperar que este problema se resuelva como se especifica en ISO/CEI 8073 [4].

6.2.1.1 Unidades funcionales

Se requieren dos unidades funcionales (FU, *functional units*) de capa de sesión en esta Recomendación:

1) Núcleo.

2) Dúplex.

6.2.2 Especificación de protocolo

La capa de sesión cumple la definición de protocolo de la Rec. UIT-T X.225 | ISO/CEI 8327-1 [5]. Las opciones y los valores de parámetros específicos que deben ser soportados para la aplicación de gestión de sistemas de telecomunicaciones se especifican en ISO/CEI ISP 11183-1 [6].

6.2.2.1 Datos de usuario

La máxima longitud de los datos de usuario de sesión será de 10 240 octetos. Esta restricción implica que no es necesario soportar las SPDU aceptación de desbordamiento (OA, *overflow accept*) y desbordamiento de datos de conexión (CDO, *connect data overflow*). Los valores del parámetro "selector de sesión" tendrán una longitud máxima de 16 octetos.

6.3 Capa de presentación

6.3.1 Definición del servicio

Es obligatorio que la capa de presentación se ajuste a los servicios y protocolos especificados en la Rec. UIT-T X.216 | ISO/CEI 8822 [7].

6.3.1.1 Unidades funcionales

En la presente Recomendación es necesaria una unidad funcional (FU) de capa de presentación:

– Núcleo.

6.3.2 Especificación del protocolo

Es obligatorio que la capa de presentación se ajuste a los protocolos especificados en la Rec. UIT-T X.226 | ISO/CEI 8823-1 [8] (modo normal). Las opciones y los valores de parámetros específicos que deben soportarse para la aplicación de gestión de sistemas de telecomunicaciones se especifican en ISO/CEI ISP 11183-1 [6].

6.3.3 Reglas de codificación para la sintaxis de transferencia

Se aplicarán las reglas de codificación definidas en la Rec. UIT-T X.209 | ISO/CEI 8825 [9] para derivar la sintaxis de transferencia de las unidades de datos de protocolo de aplicación (APDU, *application protocol data units*). Se utilizará ASN.1 [10] a [13] OBJECT IDENTIFIER [joint-iso-itu-t asn1 (1) basic-encoding (1)] como el valor del nombre de sintaxis de transferencia. El valor máximo de un rótulo de codificación básico ASN.1 que requiere tratamiento para su conformidad con esta Recomendación es 16 383. Éste es el mayor entero sin signo que puede representarse con 14 bits. Por tanto, los octetos del identificador constarán de un octeto inicial y hasta dos octetos más, ocupando así un máximo de tres octetos. Además, el mayor número de octetos del componente "octetos de contenido" de una codificación de valores de datos ASN.1 que necesita tratamiento para su conformidad con esta Recomendación es de 4 294 967 295. Éste es el mayor entero sin signo que puede representarse con 32 bits. De aquí que en la codificación en "forma larga", los octetos de longitud consten de un octeto inicial y hasta cuatro octetos más, ocupando así un máximo de cinco octetos. (Obsérvese que esta restricción no se aplica al caso de codificaciones de "longitud indefinida".)

6.4 Capa de aplicación

La presentación de unidades de datos de protocolo de capa de aplicación se describe utilizando la notación de sintaxis abstracta uno (ASN.1, *abstract syntax notation one*), que se define en la Rec. UIT-T X.208 | ISO/CEI 8824 [14].

6.4.1 Arquitectura de la capa de aplicación

Es obligatorio que la capa de aplicación se ajuste a la arquitectura de la capa de aplicación descrita en ISO/CEI 9545 [15].

Se utilizarán los conceptos de entidad de aplicación (AE, *application entity*), invocación de entidad de aplicación, objeto de servicio de aplicación (ASO, *application service object*), función de control (CF, *control function*) y contexto de aplicación (AC, *application context*) para describir la relación entre ROSE, ACSE, CMISE y SMASE.

6.4.2 Elemento de servicio de control de asociación

6.4.2.1 Definición del servicio

La descripción del servicio ACSE se detalla en la Rec. UIT-T X.217 | ISO/CEI 8649 [16]. Todos los servicios ACSE definidos (véase el cuadro 5) son obligatorios. El valor del parámetro de modo de A-ASOCIACIÓN será "normal".

6.4.2.2 Especificación de protocolo

La especificación de protocolo para ACSE se ajustará a la Rec. UIT-T X.227 | ISO/CEI 8650-1 [17]. Las cinco APDU (véase el cuadro 5) especificadas en la norma son obligatorias. Las opciones y los valores de parámetros específicos que habrán de soportarse para la

aplicación de gestión de sistemas de telecomunicaciones de clase interactiva se especifican en ISO/CEI ISP 11183-1 [6].

Cuadro 5/Q.812 – Servicios ACSE y APDU asociadas

Servicio ACSE	APDU asociadas	Servicio P conexo
A-ASOCIACIÓN	AARQ, AARE	P-CONEXIÓN
A-LIBERACIÓN	RLRQ, RLRE	P-LIBERACIÓN
A-ABORTO	ABRT	P-U-ABORTO
A-P-ABORTO	(Ninguna)	P-P-ABORTO

6.4.2.3 Utilización de la SACF para el control de asociación

Por definición, la CF debe controlar las interacciones entre los ASE y/o los ASO en los ASO contenedores en ISO/CEI 9545 [15] con DAM 1.

Por tanto, controla el establecimiento, liberación y aborto de asociación en relación con las reglas definidas en el contexto de aplicación disponible para la asociación.

De este modo, permite la utilización conjunta de varios ASE en la misma asociación.

6.4.2.4 Nombre de sintaxis abstracta

El nombre de sintaxis abstracta ACSE tiene OBJECT IDENTIFIER tipo ASN.1. Para identificar la definición de sintaxis abstracta ACSE se utilizará el valor siguiente:

```
{
joint-iso-itu-t association-control (2)
abstract-syntax (1) apdu's (0) version (1)

}
```

6.4.3 Operaciones a distancia

6.4.3.1 Definición del servicio

El elemento de servicio de operaciones a distancia (ROSE, *remote operations service element*) será un elemento de servicio obligatorio. La descripción de los servicios ROSE se detalla en la Rec. UIT-T X.219 | ISO/CEI 9072-1 [18]. Todos los servicios ROSE definidos (véase el cuadro 6) son obligatorios.

6.4.3.2 Especificación de protocolo

La especificación de protocolo para ROSE se ajustará a la Rec. UIT-T X.229 | ISO/CEI 9072-2 [19]. Las cuatro APDU especificadas en la norma (véase el cuadro 6) son obligatorias. Además se requiere la posibilidad de soportar el origen y recepción correctos del elemento de protocolo de identificación vinculada.

El requisito especificado en el cuadro 6 conlleva la clase de asociación 3 en ROSE.

Cuadro 6/Q.812 – Servicios ROSE y APDU asociadas

Servicio ROSE	APDU asociadas	Servicio subyacente conexo
RO-INVOCACIÓN	ROIV	P-DATOS
RO-RESULTADO	RORS	P-DATOS
RO-ERROR	RORE	P-DATOS
RO-RECHAZO-U	RORJ	P-DATOS
RO-RECHAZO-P	RORJ	P-DATOS

6.4.4 Información de gestión común

Las aplicaciones de gestión de la red utilizarán el elemento de servicio común de información de gestión (CMISE, *common management information service element*).

6.4.4.1 Definiciones de los servicios

La descripción de los servicios CMISE se detalla en la Rec. UIT-T X.710 | ISO/CEI 9595 [20]. En el cuadro 7 se da una relación de los servicios CMISE.

Las unidades funcionales selección de múltiples objetos, filtro, respuesta múltiple y obtención cancelación, que se definen en la Rec. UIT-T X.710 | ISO/CEI 9595 [20], son opcionales. Su utilización depende de la aplicación. Durante el establecimiento se negociará la utilización o no de las unidades funcionales.

No es necesario soportar la unidad funcional de servicio extendido definida en la Rec. UIT-T X.710 | ISO/CEI 9595 [20] para la conformidad con la presente Recomendación, y se negociará, en el establecimiento de asociación, su no utilización.

Cuadro 7/Q.812 – Servicios CMISE

Servicio	Tipo
M-INFORME-EVENTO	Confirmado/no confirmado
M-OBTENCIÓN	Confirmado
M-FIJACIÓN	Confirmado/no confirmado
M-ACCIÓN	Confirmado/no confirmado
M-CREACIÓN	Confirmado
M-SUPRESIÓN	Confirmado
M-OBTENCIÓN-CANCELACIÓN	Confirmado

6.4.4.2 Especificación de protocolo

Las implementaciones soportarán las operaciones definidas en la Rec. UIT-T X.711 | ISO/CEI 9596-1 [21], que son requeridas por aplicaciones específicas. Todos los parámetros obligatorios definidos en la Rec. UIT-T X.711 | ISO/CEI 9596-1 [21], para las operaciones requeridas son parámetros obligatorios en esta Recomendación. Las opciones y los valores de parámetros específicos que habrán de soportarse se especifican en ISO/CEI ISP 11183-3 [22] en lo que concierne a la gestión de sistemas de telecomunicaciones básicos y en ISO/CEI ISP 11183-2 [23] para la gestión de sistemas de telecomunicaciones mejorados.

6.4.4.3 Sintaxis abstracta

El nombre de sintaxis abstracta para el CMISE es {joint-iso-ccitt ms(9) cmip(1) abstract syntax(4)}.

6.5 Soporte de seguridad para aplicaciones interactivas

En lo que concierne a la interfaz X, el soporte para los servicios de control de acceso y autenticación es obligatorio. Tratándose de la interfaz Q, el soporte de estos servicios es facultativo. El servicio de autenticación será soportado utilizando la unidad funcional de autenticación especificada en el ACSE. El o los mecanismo(s) que habrá(n) de utilizarse en la práctica para la interfaz X quedan en estudio.

El servicio de control de acceso será soportado recurriendo al parámetro de control de acceso definido en las operaciones CMIP. La sintaxis para este parámetro depende del mecanismo de que se trate concretamente y queda en estudio. Cuando se definan los mecanismos específicos, se

incluirá una sintaxis abstracta adicional en que se defina la sintaxis del control de acceso en el conjunto de contextos de definición (DCS, *definition context set*) para el protocolo de presentación.

7 Especificación de protocolo de capa superior para funciones de clase orientada a ficheros que utilizan el paradigma OSI

Los perfiles de cada capa son los mismos que se describen en la cláusula 6; esta cláusula sólo documenta las diferencias requeridas para soportar la FTAM.

7.1 Capa de sesión

7.1.1 Perfil de servicio

7.1.1.1 Unidades funcionales

Se requieren cuatro unidades funcionales (FU) de capa de sesión en esta Recomendación:

1) Núcleo.
2) Dúplex.
3) Sincronización menor.
4) Resincronización.

7.1.2 Perfil de protocolo

Las opciones y los valores de parámetros específicos que habrán de soportarse para los servicios de transferencia de ficheros se especifican en ISO/CEI ISP 10607-1 [24].

7.2 Capa de presentación

7.2.1 Definición del servicio

Es obligatorio que la capa de presentación sea acorde con los servicios especificados en la Rec. UIT-T X.216 | ISO/CEI 8822 [7].

7.2.1.1 Unidades funcionales

En la presente Recomendación se requiere una unidad funcional (FU) de capa de presentación:

– Núcleo.

7.2.2 Especificación de protocolo

Es obligatorio que la capa de presentación sea acorde con los protocolos especificados en la Rec. UIT-T X.226 | ISO/CEI 8823-1 [8] (modo normal). Las opciones y valores de parámetros específicos que habrán de soportarse para la aplicación de gestión de sistemas de telecomunicaciones se especifican en ISO/CEI ISP 11183-1 [6].

7.2.3 Reglas de codificación para la sintaxis de transferencia

Se aplicarán las reglas de codificación definidas en la Rec. UIT-T X.209 | ISO/CEI 8825 [9] para obtener la sintaxis de transferencia aplicable a las unidades de datos de protocolo de aplicación (APDU, *application protocol data unit*). El IDENTIFICADOR DE OBJETO ASN.1 [joint-iso-itu-t asn1 (1) basic-encoding (1)] se utilizará como el valor aplicable al nombre de sintaxis de transferencia. El valor máximo de un rótulo de codificación básica ASN.1 con el que habrá de trabajarse a los efectos de la conformidad con la presente Recomendación es 16 383. Éste es el mayor número entero sin signo que puede representarse con 14 bits. De ahí que los octetos del identificador deban consistir en un octeto inicial y hasta dos octetos más, lo cual ocuparía un máximo de tres octetos. Por otra parte, el número mayor de octetos que puede haber en el componente "octetos de contenido" de una codificación de valores de datos ASN.1 con el que hay que trabajar a los efectos de la conformidad con la presente Recomendación es 4 294 967 295. Éste

es el mayor número entero sin signo que puede representarse con 32 bits. Por esta razón, en la codificación de "forma larga", los octetos de longitud deben consistir en un octeto inicial y hasta cuatro octetos más, con lo cual se ocuparía un máximo de cinco octetos. (Hay que señalar que esta restricción no se aplica a las codificaciones de "longitud indefinida".)

7.3 Perfil de capa de aplicación

7.3.1 Arquitectura de la capa de aplicación

Tiene que suministrarse la descripción del ACSE y la FTAM como parte de la arquitectura de la capa de aplicación.

7.3.2 Transferencia, acceso y gestión de ficheros

7.3.2.1 Perfil de servicio

La clase de servicio de fichero obligatoria es la clase de transferencia de ficheros.

En esta clase son obligatorias las siguientes unidades funcionales:

– la unidad funcional núcleo;
– ambas unidades funcionales lectura y escritura;
– la unidad funcional gestión limitada de ficheros;
– la unidad funcional agrupamiento;
– y, en el servicio interno de fichero, la unidad funcional recuperación y opcionalmente la unidad funcional reiniciación.

7.3.2.2 Perfil de protocolo

Las unidades funcionales del protocolo de ficheros son equivalentes a las unidades funcionales del servicio sustentado antes descrito.

Las unidades funcionales conservadas y sus PDU asociadas se enumeran en el cuadro 8.

Este protocolo de ficheros supone los servicios de sesión descritos en 7.1.1.1 con los siguientes detalles:

– la unidad funcional recuperación o reiniciación implica el uso del servicio de sesión sincronización menor;
– la unidad funcional reiniciación implica la adición al servicio de sesión sincronización menor del servicio de sesión resincronización.

Cuadro 8/Q.812 – Unidades funcionales de FTAM y PDU asociadas

Nombre	Unidades funcionales
Petición F-INICIALIZACIÓN	Núcleo
Respuesta F-INICIALIZACIÓN	Núcleo
Petición F-TERMINACIÓN	Núcleo
Respuesta F-TERMINACIÓN	Núcleo
Petición F-P-ABORTO	Núcleo
Petición F-U-ABORTO	Núcleo
Petición F-SELECCIÓN	Núcleo
Respuesta F-SELECCIÓN	Núcleo
Petición F-DESELECCIÓN	Núcleo
Respuesta F-DESELECCIÓN	Núcleo
Petición F-CREACIÓN	Gestión de fichero limitada
Respuesta F-CREACIÓN	Gestión de fichero limitada
Petición F-SUPRESIÓN	Gestión de fichero limitada
Respuesta F-SUPRESIÓN	Gestión de fichero limitada
Petición F-ATRIBUCIÓN-LECTURA	Gestión de fichero limitada
Respuesta F-ATRIBUCIÓN-LECTURA	Gestión de fichero limitada
Petición F-APERTURA	Lectura, escritura
Respuesta F-APERTURA	Lectura, escritura
Petición F-CIERRE	Lectura, escritura
Respuesta F-CIERRE	Lectura, escritura
Petición F-LECTURA	Lectura
Petición F-ESCRITURA	Escritura
Petición F-FIN-DATOS	Lectura, escritura
Petición F-FIN-TRANSFERENCIA	Lectura, escritura
Respuesta F-FIN-TRANSFERENCIA	Lectura, escritura
Petición F-CANCELACIÓN	Lectura, escritura
Respuesta F-CANCELACIÓN	Lectura, escritura
Petición F-GRUPO-COMIENZO	Agrupamiento
Respuesta F-GRUPO-COMIENZO	Agrupamiento
Petición F-GRUPO-FIN	Agrupamiento
Respuesta F-GRUPO-FIN	Agrupamiento
Petición F-RECUPERACIÓN	Recuperación
Respuesta F-RECUPERACIÓN	Recuperación
Petición F-REARRANQUE	Rearranque
Respuesta F-REARRANQUE	Rearranque

7.3.2.3 Sintaxis abstracta

Los nombres de la sintaxis abstracta para FTAM son los siguientes:

{iso standard 8571 abstract syntax(2) ftam-fadu(2)}

{iso standard 8571 abstract syntax(2) ftam-pci(1)}

{iso standard 8571 abstract syntax(2) unstructured-text(3)}

{iso standard 8571 abstract syntax(2) unstructured-binary(4)}

7.3.2.4 Soporte de tipos de documentos

La naturaleza de las estructuras de fichero que han de transferirse exige el uso de tipos de documentos adecuados.

Se adoptan tres tipos de ficheros:

– ficheros binarios no estructurados;

– ficheros de texto no estructurados;
– ficheros ordenados secuencialmente (estos ficheros se componen de una secuencia de registros sin posibilidad de tener acceso directo a un determinado registro, estando cada registro compuesto por campos de tipo diferente).

Por tanto, son obligatorios tres tipos de documentos:

– texto no estructurado FTAM de ISO (FTAM.1);
– binario no estructurado FTAM de ISO (FTAM.3);
– fichero secuencial NBS (NBS-6).

FTAM.1 y FTAM.3 son admitidos por el modelo de fichero jerárquico FTAM definido en ISO 8571-2 [26], limitado por el conjunto de constricciones no estructuradas.

NBS-6 es admitido por el modelo de fichero jerárquico FTAM definido en ISO 8571-2 [26], limitado por el conjunto de constricciones categóricas secuenciales.

7.4 Soporte de seguridad para servicios FTAM

El soporte del servicio de autenticación es obligatorio en el caso de la interfaz X. En lo que concierne a la interfaz Q, el soporte de estos servicios es facultativo. El servicio de autenticación debe soportarse utilizando la unidad funcional de autenticación especificada en el ACSE. El mecanismo o los mecanismos que habrán de utilizarse realmente para la interfaz X quedan en estudio.

El soporte de seguridad para los servicios FTAM en la RGT queda en estudio.

8 Especificación de protocolo de capa superior para servicios de directorio que utilizan el paradigma OSI

Los perfiles para cada capa son los mismos que los descritos en la cláusula 6; esta cláusula solo indica las diferencias necesarias para el soporte de directorio.

8.1 Capa de sesión

8.1.1 Definición de los servicios

Esta capa es acorde con la definición de los servicios en la Rec. UIT-T X.215 | ISO/CEI 8326.

8.1.1.1 Unidades funcionales

En la presente Recomendación se estipulan las dos unidades funcionales siguientes de capa de sesión:

a) Núcleo
b) Dúplex.

8.1.2 Especificación de protocolo

La capa de sesión es acorde con la definición de protocolo dada en la Rec. UIT-T X.225 | ISO/CEI 8327-1 [5].

8.1.3 Datos de usuario

Los DUA serán capaces de enviar APDU de petición de cualquier tamaño hasta 32 767 (32k – 1) octetos de longitud. Los DSA serán capaces de aceptar y procesar APDU de petición de operación de cualquier tamaño hasta 32 767 octetos de longitud. Los DSA serán capaces de enviar APDU de respuesta de cualquier tamaño hasta 262 143 (256k – 1) octetos de longitud. Los DSA serán capaces de aceptar y procesar APDU de respuesta de cualquier tamaño hasta 262 143 octetos de longitud y de enviar APDU de petición de cualquier tamaño hasta 32 767 octetos de longitud.

8.2 Capa de presentación

8.2.1 Definición del servicio

El servicio de presentación se define en la Rec. UIT-T X.216 | ISO/CEI 8822 [7].

El ACSE es el único usuario de los servicios P-CONEXIÓN, P-LIBERACIÓN, P-U-ABORTO y P-P-ABORTO del servicio de presentación.

El ROSE es el único usuario del servicio P-DATOS del servicio de presentación.

No se utiliza el contexto de presentación por defecto, la restauración del contexto y la gestión del contexto.

8.2.2 Especificación de protocolo

Es obligatorio que la capa de presentación sea acorde con los protocolos especificados en la Rec. UIT-T X.226 | ISO/CEI 8823-1 [8] (modo normal).

8.3 Capa de aplicación

8.3.1 Arquitectura de la capa de aplicación

Es obligatorio que la capa de aplicación sea acorde con la arquitectura de la capa de aplicación esbozada en las Recomendaciones UIT-T de la serie X.500.x | ISO/CEI 9594 [29] a [36].

8.3.2 Sintaxis abstractas de protocolo de directorio

El tipo ASN.1 del que se derivan los valores de las sintaxis abstractas se especifica utilizando los tipos parametrizados de ROS {DAP-InvokeIDSet **|** DAP-Invokable **|** DAP-Returnable **|** DSP-InvokeIDSet **|** DSP-Invokable **|** DSP-Returnable}, Bind {dSABind **|** directoryBind} y Unbind {dSAUnbind **|** directoryUnbind}, que se definen en la Rec. UIT-T X.880 | ISO/CEI 13712-1 [37].

La sintaxis abstracta del DAP se denomina directoryAccessAbstractSyntax. La sintaxis abstracta del DSP se denomina directorySystemAbstractSyntax.

8.3.3 Contextos de aplicación de directorio

El contexto de aplicación del DAP se denomina directoryAccessAC. El contexto de aplicación del DSP se denomina directorySystemAC.

8.3.4 Elemento de servicio de control de asociación

La sintaxis abstracta del ACSE, acse-abstract-syntax, se requiere para el DAP y el DSP.

El ACSE soporta el establecimiento, la liberación y el aborto de una asociación-aplicación entre un par de elementos de asociación. Las asociaciones entre un DUA y un DSA pueden ser establecidas únicamente por el DUA. Una asociación establecida sólo puede ser liberada por el iniciador.

8.3.4.1 Definición del servicio

El servicio ACSE se describe detalladamente en la Rec. UIT-T X.217 | ISO/CEI 8649 [16].

Los servicios RO-VINCULACIÓN y RO-DESVINCULACIÓN son los únicos usuarios de los servicios A-ASOCIACIÓN y A-LIBERACIÓN del ACSE. El proceso de aplicación es el usuario de los servicios A-ABORTO y A-P-ABORTO del ACSE.

8.3.4.2 Especificación de protocolo

La especificación de protocolo para el ACSE debe ser conforme a la Rec. UIT-T X.227 | ISO/CEI 8650-1 [17].

8.3.5 Operaciones a distancia

8.3.5.1 Definición del servicio

El ROSE será un elemento de servicio obligatorio. El servicio ROSE se describe detalladamente en la Rec. UIT-T X.881 | ISO/CEI 13712-2 [38].

Los ASE de directorio son los usuarios de los servicios RO-INVOCACIÓN, RO-RESULTADO, RO-ERROR, RO-RECHAZO-U y RO-RECHAZO-P del ROSE.

8.3.5.2 Especificación de protocolo

El DAP y el DSP son los protocolos de directorio utilizados para proporcionar comunicaciones entre dos procesos de aplicación.

8.4 Soporte de seguridad para servicios de directorio

En la Rec. UIT-T X.509 | ISO/CEI 9594-8 [36] se define un marco para el suministro de servicios de autenticación por el directorio a sus usuarios. El soporte de seguridad para los servicios de directorio en la RGT queda en estudio.

Los protocolos de capa superior que han de utilizarse para los servicios de almacenamiento y retransmisión (por ejemplo, para intercambiar información formateada EDI) quedan en estudio.

En esta Recomendación se especifica soporte parcial para los requisitos de seguridad a través de las interfaces Q3 y X. Para soportar servicios de seguridad tales como la integridad, la confidencialidad y el no rechazo de datos y la gestión de información de seguridad (por ejemplo, procedimientos y protocolos de gestión claves) será preciso aplicar las Recomendaciones sobre seguridad genérica de capa superior (Recomendaciones UIT-T de la serie X.830). Las directrices para utilizar la GULS en las aplicaciones se especifican en el anexo A/X.830 | ISO/CEI 11586-1 [39]. Los detalles de utilización de la GULS en las clases interactiva y de transferencia de ficheros de las aplicaciones RGT quedan en estudio.

9 Conformidad para el paradigma OSI

Los requisitos referentes a las cuestiones a las que no se hace referencia concretamente en la presente Recomendación serán acordes con los ISP indicados a continuación:

– Transporte:
  - Para CLNS1 (véase la Rec. UIT-T Q.811 [45]) la capa de transporte cumplirá los requisitos independientes del tipo de subred de la ISO/CEI ISP 10608-1 [60].
  - Para CLNS2 (véase la Rec. UIT-T Q.811 [45]) la capa de transporte cumplirá la ISO/CEI ISP 10608-1 [60].
  - Para CLNS3 (véase la Rec. UIT-T Q.811 [45]) la capa de transporte cumplirá los requisitos independientes del tipo de subred de la ISO/CEI ISP 10608-1 [60].
  - Para CONS1 (véase la Rec. UIT-T Q.811 [45]) la capa de transporte cumplirá la ISO/CEI ISP 10609-1 [61] modificada por el cuadro II.1.
  - Para CONS6 (véase la Rec. UIT-T Q.811 [45]) la capa de transporte cumplirá la ISO/CEI ISP 10609-1 [61].
  - Para ISO TP0/TCP/IP la capa de transporte de pilas cumplirá la clase 0 de RFC 2126.
– Las capas de sesión, presentación y ACSE para servicios de clase interactiva serán acordes con ISO/CEI ISP 11183-1 [6].
– La sesión, la presentación y el ACSE para los servicios de clase orientada a ficheros serán acordes con ISO/CEI ISP 10607-1 [24].

– El CMIP utilizado en el perfil de servicios de clase interactiva será acorde con ISO/CEI ISP 11183-3 [22] en el caso de los servicios básicos y con ISO/CEI ISP 11183-2 [23], en el caso de los servicios mejorados. Las aplicaciones pueden sobrepasar la dimensión de 10K de la APDU especificada en AOM-12, en caso de requerirse un tamaño mayor.

– El perfil FTAM corresponderá a ISO/CEI ISP 10607-3 [40].

10 Perfil de protocolo para servicios basados en la CORBA

10.1 Alcance del perfil del protocolo CORBA

Las aplicaciones de la RGT especificadas que utilizan IDL interoperarán según las disposiciones de este perfil de protocolo CORBA.

10.2 Panorama del perfil para servicios basados en la CORBA

En la figura 4 se ilustra la pila de protocolos del perfil para servicios basados en la CORBA.

A través de este perfil se puede tener acceso a los servicios de la RGT que tienen interfaces orientadas al objeto y especificadas conforme a IDL ODP (Rec. UIT-T X.920).

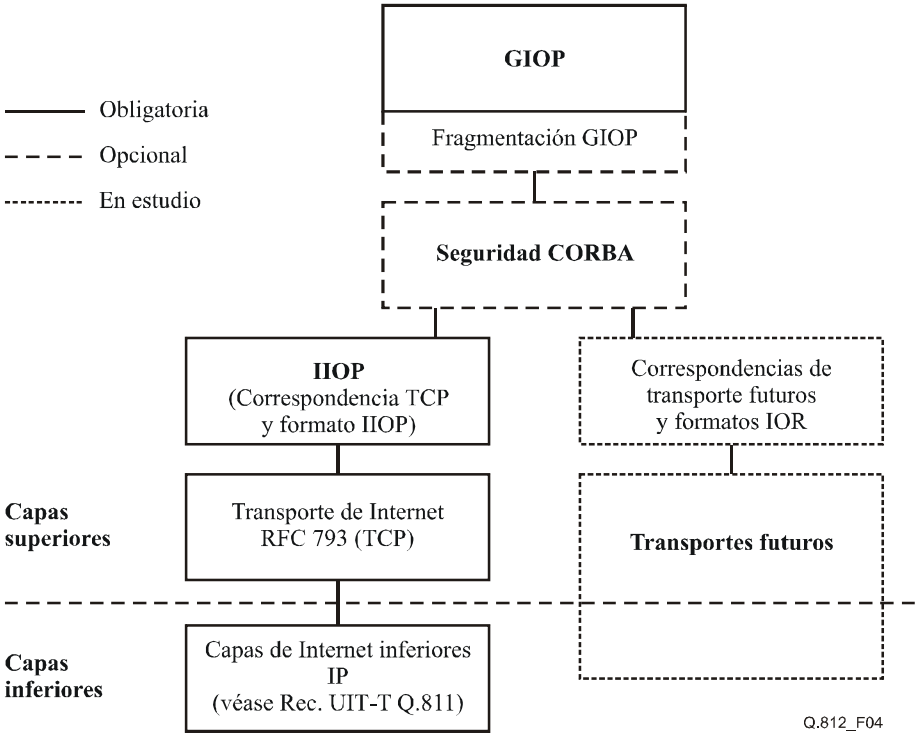

Figura 4/Q.812 – Pila de protocolos de servicios basados en la CORBA de capa superior GIOP

Para soportar el nivel 1 y niveles superiores de CSI, se debe utilizar el protocolo SECIOP dentro de este perfil. Para el soporte del nivel 0 de CSI, se puede utilizar interoperabilidad SSL de seguridad CORBA como una alternativa a SECIOP dentro de este perfil. Los sistemas que soportan seguridad CORBA deben también soportar el formato versión 1.1 del perfil IIOR.

Si se requiere fragmentación de la aplicación, se utilizará entonces la versión 1.1 de GIOP o una versión posterior con este perfil.

Las correspondencias de GIOP con transportes diferentes de TCP quedarán en estudio.

NOTA – Las correspondencias de GIOP con perfiles de transporte requieren la especificación de un formato del perfil referencia de objetos interoperable (IOR, *interoperable object reference*), asociado con ese perfil de transporte, así como la especificación de cómo se utilizan servicios vinculantes del perfil de transporte.

10.3 Definición de servicio

Los servicios que utilizan CORBA deben tener especificadas interfaces orientadas a objeto que utilizan IDL OMG (Rec. UIT-T X.920).

NOTA – Los sistemas basados en CORBA pueden utilizar vinculaciones de lenguaje de programación normalizadas para tener acceso a objetos CORBA.

10.4 Especificación de protocolo GIOP

Las versiones 1.0, 1.1 y 1.2 del protocolo GIOP se deben aplicar como se especifica en [CORBA GIOP Specification]. Todos los sistemas que actúan como servidores CORBA deben soportar al menos GIOP 1.0.

Los servidores que soportan las versiones 1.1 ó 1.2 de GIOP también deben soportar mensajes de procesamiento con todas las versiones de GIOP anteriores.

10.5 Especificación del protocolo IOP de seguridad

Todos los sistemas que requieren la utilización de servicios de seguridad CORBA deben soportar la versión 1.1 de GIOP o una versión posterior.

Todos los sistemas que requieren la utilización de seguridad CORBA deben soportar el "Protocolo IOP de seguridad" o la "Interoperabilidad SSL de seguridad CORBA", como se define en [CORBA Security Service Specification].

10.6 Especificación del protocolo IIOP

Para interfuncionamiento, todos los sistemas CORBA deberán soportar el protocolo de correspondencia IIOP de GIOP con servicios de capa inferior TCP/IP, como se especifica en [CORBA GIOP Specification].

Los servidores indicarán su soporte a GIOP mediante la publicación de referencias de objetos interoperables (IOR) que incluyen un perfil IOR de Internet (IIOR, *Internet IOR*) con la versión de perfil IIOP fijada en el nivel más elevado de la versión de protocolo GIOP soportado por el sistema que actúa como servidor. El formato del perfil IIOR es el que se especifica en [CORBA GIOP Specification].

10.7 Perfil del protocolo TCP/IP para utilización con IIOP

IIOP está diseñado para ser utilizado con protocolos de capa inferior basados en TCP/IP.

Esta cláusula define un perfil de protocolo para utilización como protocolo de capa inferior RGT para sistemas basados en la CORBA que utilizan IIOP. Este perfil se basa en la utilización de protocolos Internet definidos por el Grupo de tareas especiales de ingeniería en Internet (IETF, *Internet Engineering Task Force*). El modo como se pueden referenciar estos documentos en la presente Recomendación queda en estudio. La pila de protocolos utiliza lo siguiente:

- Para la capa 4 – STD0007 "Protocolo de control de transmisión", septiembre de 1981. (Incluye RFC 793.)
- Para la capa 3 e inferiores se utiliza el perfil de protocolo especificado en la Rec. UIT-T Q.811 [45].

Otras correspondencias de protocolo de capa inferior para GIOP quedarán en estudio.

11 Perfil de protocolo para servicios basados en EDI/EDIFACT

11.1 Alcance del perfil de protocolo EDI/EDIFACT

Las aplicaciones RGT que tienen definiciones de interfaz X para su uso en la capa de gestión de servicio tienen que poder interoperar de conformidad con las disposiciones de este perfil de protocolo. Esta Recomendación define el perfil para el agente interactivo de comunicaciones electrónicas (IA, *interactive agent*) y las capas de funcionalidad asociadas. El protocolo para el propio IA está descrito en la Rec. UIT-T Q.814. La interfaz par a par IA soportará la transferencia de datos bidireccional casi en tiempo real entre entidades pares.

La modelización del perfil global descrito aquí se ha realizado a partir del modelo de interconexión de sistemas abiertos (OSI) de siete capas, es decir, las capas de perfiles se describen en términos de capa de transporte (4), capa de sesión (5), capa de presentación (6) y capa de aplicación (7).

El IA descrito a continuación proporciona servicios de capa cinco (5). Las restantes capas, cuatro, seis y siete proporcionan funcionalidad que interactúa directa o indirectamente con el IA. Este perfil describe la interacción y responsabilidades de cada una de estas cuatro capas.

11.2 Resumen de las capas

Consúltese la figura 5 para lo que sigue.

11.3 Perfil de protocolo TCP/IP para su utilización con IA

El IA está diseñado para su uso con protocolos de capa inferior basados en TCP/IP.

Esta cláusula define un perfil de protocolo para su uso como protocolo de capa inferior RGT para IA. Este perfil está basado en la utilización de protocolos de Internet definidos por el Grupo de tareas especiales de ingeniería en Internet (IETF). La forma en que se puede hacer referencia a estos documentos en la presente Recomendación queda en estudio. La pila de protocolo utiliza lo siguiente:

- Para la capa 4 – STD0007 "Protocolo de control de transmisión", septiembre de 1981. (Incluye RFC 793.)
- Para la capa 3 e inferiores se utiliza el perfil de protocolo IP especificado en la Rec. UIT-T Q.811 [45].

11.4 Perfil de protocolo TLS para su utilización con IA

La capa 4 proporciona seguridad a la capa de transporte y servicios de transporte que utilizan el protocolo de control de transmisión (TCP, *transmission control protocol*).

El mecanismo de transporte especificado por el agente interactivo (IA) precisa una sesión TLS individual. Esta sesión puede ser persistente o puede ser establecida o reanudada para cada mensaje. La comunicación es básicamente en un sentido, del cliente al servidor. El mensaje de estado IA es un mecanismo que permite a entidades pares intercambiar errores y otros tipos de información de control de flujo. Las entidades pares pueden definir códigos de mensaje específicos que no se incluyen en esta Recomendación. TLS proporciona intercambios y transferencias seguros entre entidades TLS pares. TLS también proporciona integridad de flujo de datos, autenticación de entidad par y, opcionalmente, privacidad.

11.5 Perfil IA

El IA realiza la funcionalidad de capa de sesión. El IA soporta la permuta de transacciones de cambio de datos electrónicos (EDIFACT/ASC X12 EDI/cadena general) entre entidades pares. El IA soporta este intercambio sobre la seguridad de capa de transporte (TLS, *transport layer security*). Las funciones de capa de sesión proporcionadas por el IA incluyen el establecimiento,

gestión y clausura de sesiones de comunicaciones entre entidades pares. El IA realiza también la conversión de nombres de receptores EDIFACT/ASC X12 EDI en direcciones de red y gestiona la sesión TLS de capa de transporte. Al final de una sesión, el IA determinará si debe cerrar una sesión o mantenerla en un estado en el que pueda reanudarse.

La interfaz de acuerdo de servicio IA está definida en la frontera entre el IA y su usuario directo.

El protocolo que soporta el intercambio de mensajes IA se denomina protocolo de transferencia de agente interactivo (IATP, *interactive agent transfer protocol*) y está definido en la Rec. UIT-T Q.814.

11.6 Módulo de seguridad para el perfil de protección de mensajes completos

La funcionalidad de este módulo de seguridad es optativa en función de las necesidades de seguridad de la transacción. Sin embargo, si se precisan servicios de seguridad de mensajes completos, se aplicarán los procedimientos de la Rec. UIT-T Q.815. Los mensajes seguros se transfieren entre módulos de seguridad que proporcionan tanto no repudio de origen y de destino como integridad de mensaje.

El módulo de seguridad genera o valida los campos de seguridad correspondientes y realiza la codificación o decodificación necesaria en función de si se está enviando o recibiendo, respectivamente.

El flujo de mensajes entre el traductor EDI y el IA puede o no precisar servicios de seguridad. El caso en el que se aplican mejoras de seguridad a un mensaje se describe en la figura 5.

El módulo de seguridad no es sensible al contenido de los mensajes que provienen del traductor EDI o del IA.

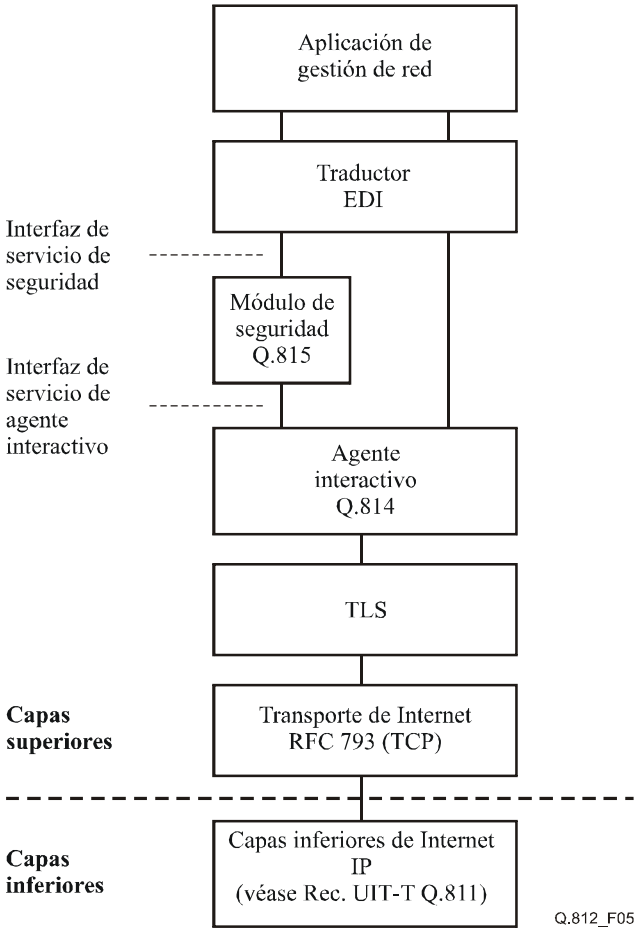

Figura 5/Q.812 – Pila de protocolo de servicios basados en EDI/EDIFACT de capa superior

11.7 Protocolo de traductor EDI/EDIFACT

El protocolo EDI/EDIFACT contiene la aplicación de usuario que utiliza los servicios del agente interactivo y, opcionalmente, el módulo de seguridad.

Un traductor/pasarela EDIFACT/ASC X12 EDI es un servicio de aplicación que proporciona una combinación de traducciones de formatos de datos y de funciones de intercambio de datos para datos de mensajes de transacción electrónica.

Un traductor/pasarela EDIFACT/ASC X12 EDI intercambia datos de transacción hacia y desde aplicaciones de gestión de red mediante formatos de datos intermedios. Traduce estos datos hacia y desde formatos de datos EDIFACT/ASC X12 EDI definidos externamente utilizando correspondencias de traducción.

12 Perfil de protocolo para el paradigma SNMP

El paradigma SNMP se muestra en la figura 6. La versión 3 del marco de gestión de Internet se describe en IETF RFC 3410. Este marco consiste de un lenguaje de definición de datos [57], definiciones de información de gestión, una definición de protocolo [54], seguridad [52] y [53] y administración [51]. El protocolo se ejecuta en primer lugar en UDP [55] pero también se puede ejecutar en TCP [58]. En [56] se describe la coexistencia con versiones anteriores de SNMP.

Cuando se despliega SNMP, la versión 3 es la versión preferida. Versiones anteriores del marco de gestión de Internet se pueden securizar utilizando IPSec [59].

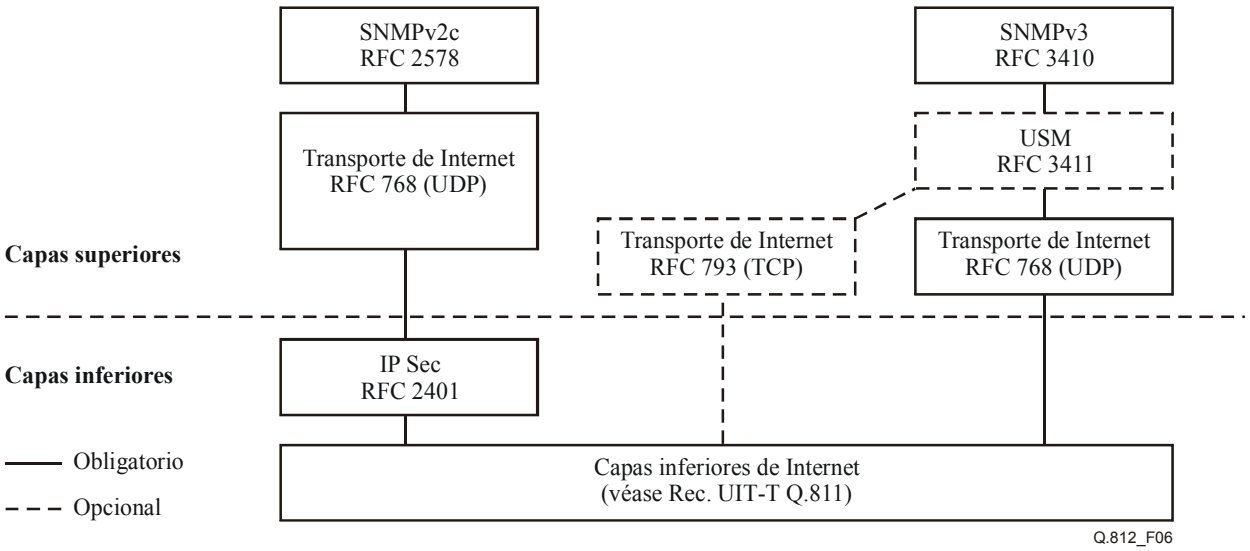

Figura 6/Q.812 – Perfil de protocolo para el paradigma SNMP

13 Perfil de protocolo para el paradigma de lenguaje de marcaje en las telecomunicaciones (tML)

Está en estudio un perfil protocolo para soportar la utilización de información de gestión codificado tML [64].

Apéndice I

Directrices para la utilización de la gestión alomórfica

I.1 Introducción

El presente apéndice trata de orientar a quienes desarrollan gestores y agentes del protocolo común de información de gestión (CMIP, *common management information protocol*) respecto a la utilización del alomorfismo. El alomorfismo es un concepto poderoso, cuyo valor aumenta al irse implementando las redes de gestión de las telecomunicaciones (RGT). El alomorfismo se puede utilizar para abordar el tema de cómo añadir capacidades nuevas a implementaciones existentes de gestor y agente de RGT. A medida que evolucionan los requisitos y se amplían los modelos para dar satisfacción a los mismos, se pueden elaborar programas informáticos del sistema de gestión que aprovechen el alomorfismo de manera que no haga falta rehacer dichos programas sino hasta que se necesiten las nuevas características del modelo.

En el presente apéndice se trata de explicar cómo hacer frente al comportamiento alomórfico en implementaciones de sistemas de gestor y agente. Se aclara aquí la descripción del alomorfismo que figura en la Rec. UIT-T X.720 | ISO/CEI 10165-1. Los gestores en particular han de estar al corriente del alomorfismo para beneficiarse de él. Incluso si un gestor no tiene previsto utilizarlo, deberá tener una capacidad mínima de conexión en interfaz con los agentes que sí lo implementen. El gestor, por ejemplo, debe soportar el atributo alomorfos y tener la posibilidad de construir filtros utilizando alomorfos frente a la clase real del atributo clase de objeto (objectClass).

En el presente apéndice se examinan los temas relacionados con el alomorfismo de cada operación CMIP desde la perspectiva tanto del gestor como del agente. A continuación se analizan asuntos relativos a las notificaciones del CMIP, de nuevo desde la perspectiva del gestor y del agente. Se hacen después algunas consideraciones a propósito de las pilas de protocolos y las

implementaciones. El apéndice concluye respondiendo a algunas de las cuestiones que se plantean a menudo en relación con el alomorfismo.

En el análisis que sigue, se utiliza la frase "si el agente soporta el alomorfismo", frase que se ha de interpretar como "si el agente soporta el alomorfismo para un ejemplar específico", porque es posible que un agente soporta revisiones de algunas clases de objeto y no de otras. En sentido estricto, incluso dos ejemplares de una misma clase pueden diferir en lo que se refiere al soporte del alomorfismo, si bien, en el presente análisis, se considera que una implementación como ésa sería un caso extremo y poco frecuente. Lo mismo cabe decir a propósito del lado gestor, en donde una versión específica de un sistema de gestor puede reconocer múltiples definiciones para algunas clases básicas y no para otras. Las decisiones respecto a la inclusión de las diferentes versiones se toman en función de objetivos empresariales (que quedan fuera del alcance del presente apéndice).

I.1.1 Visión de conjunto

alomorfismo es la capacidad que tiene un objeto gestionado, que es un ejemplar de una determinada clase de objetos gestionados, de ser gestionado como miembro de una o más clases de objetos gestionados. El alomorfismo permite que ejemplares de una clase de objetos gestionados – a la que se hace referencia como clase ampliada – representen ejemplares de otra clase de objetos gestionados, la clase alomórfica.

Cuando se ejemplifica una clase ampliada, la clase real (véase la Rec. UIT-T X.720 | ISO/CEI 10165-1) del objeto almacenado en el atributo clase de objeto (objectClass) es la clase ampliada. Se amplía con respecto a otra clase de objetos gestionados, que es su clase de objetos gestionados compatible. La clase real es aquella de la que el objeto gestionado es un ejemplar. Una clase alomórfica de un objeto gestionado es una clase de objetos gestionados distinta de la clase de objetos gestionados real; sin embargo, puede ser gestionada como un ejemplar de esa clase. Un objeto gestionado puede ser alomórfico para una o más clases compatibles (es decir, ejemplares de la clase ampliada pueden ser gestionados como ejemplares de la clase de objetos gestionados compatible). En otras palabras, las expresiones "clase alomórfica" y "clase de objetos gestionados compatible" se pueden utilizar como sinónimos. Cuando un agente crea un objeto gestionado que soporta el alomorfismo, se incluye el lote alomórfico (allomorphicPackage) (definido como un lote condicional en la clase tope de la Rec. UIT-T X.721 | ISO/CEI 10165-2). El lote contiene el atributo alomorfos. Este atributo obtención solamente (GET-Only) es un atributo conjunto de valores y contiene los identificadores de objeto de las clases que ese objeto puede representar (es alomórfico con ellas). El atributo clase de objeto (objectClass) tiene un valor de la clase efectivamente utilizada al crear este ejemplar.

La idea básica que subyace en el alomorfismo consiste en que la clase ampliada soporta todas las capacidades de las clases con las que es alomórfica. Puede soportar también clases adicionales. La clase ampliada puede ser una subclase de las clases con las que es alomórfica, pero esto no es un requisito necesario. A todos los efectos, la clase se comporta como la clase que realmente es, lo que significa que el gestor puede recibir información que no figure en la clase alomórfica. Por ejemplo, si la clase ampliada tiene atributos nuevos, una operación de obtención de todo promovida por el gestor dará como resultado los valores de esos atributos. El tratamiento de asuntos de este tipo requiere que el gestor sepa que se está aplicando gestión alomórfica. En la Rec. UIT-T X.724 | ISO/CEI 10165-6 se definen cuadros de conformidad de objetos gestionados a utilizar por las implementaciones tanto de agente como de gestor. Se recomienda el empleo de esos cuadros para identificar la lista de alomorfos soportados, a fin de determinar los niveles de interoperabilidad.

En las cláusulas que siguen se analizan las diversas interacciones entre gestor y agentes que aplican la gestión alomórfica. En la Rec. UIT-T X.720 | ISO/CEI 10165-1 se analiza además la interoperabilidad limitada, cuando no se cumplen por completo las reglas de compatibilidad. El presente apéndice sólo se refiere a aquellas situaciones en las que las reglas de compatibilidad definidas de acuerdo con la Rec. UIT-T X.720 | ISO/CEI 10165-1 sí se cumplen, para soportar el alomorfismo (véase 5.2.3.2/X.720 | ISO/CEI 10165-1).

I.2 Operaciones CMIP

En esta cláusula se analiza el alomorfismo en relación con las operaciones CMIP, m-Creación, m-Obtención, m-Fijación, m-acción y m-Supresión. No se ha determinado que el alomorfismo tenga repercusión alguna en la operación m-Obtención-Cancelación.

I.2.1 Creación de objetos gestionados

Un objeto gestionado lo crea el gestor emitiendo una petición de creación explícita en la interfaz, o bien se crea de manera automática dentro del sistema de agente. A continuación se analiza cada una de estas opciones. Es preciso que la estructura y el atributo de denominación se seleccionen con cuidado. Los asuntos relativos a la denominación se examinan más adelante, en una subcláusula aparte.

I.2.1.1 Creación explícita – Cometido de gestor

Caso 1: El gestor emite una petición de creación CMIP proporcionando en la clase de objetos gestionados un valor y un conjunto de valores de atributo apropiados para esa clase. El gestor suministra el nombre efectivo del nuevo objeto. La acción resultante en el agente es una de las definidas en los casos a, b y c de I.2.1.2 Creación explícita – Cometido de agente. Si la respuesta es tal como se define en el caso c, el gestor debe ser capaz de ignorar atributos desconocidos incluidos como consecuencia de la creación de una clase ampliada.

Caso 2: El gestor emite una petición de creación CMIP proporcionando en la clase de objetos gestionados un valor y un conjunto de valores de atributo apropiados para esa clase. El gestor suministra el valor del atributo vinculación de nombres. La acción resultante en el agente es una de las definidas en los casos a, b y d de I.2.1.2 Creación explícita – Cometido de agente. Si la respuesta es tal como se define en el caso d, el gestor debe ser capaz de ignorar los atributos desconocidos incluidos como resultado de la creación de una clase ampliada.

Caso 3: El gestor especifica la clase sin un nombre específico en el campo de la ejemplificación o un valor para el atributo vinculación de nombres. La acción resultante en el agente es una de las definidas en los casos a, b y e de I.2.1.2 Creación explícita – Cometido de agente. Si la respuesta es tal como se define en el caso e, el gestor debe ser capaz de ignorar los atributos desconocidos incluidos como resultado de la creación de una clase ampliada.

Caso 4: El gestor especifica una clase y pide que sea una copia de otro objeto, es decir, con objeto de referencia. Dependiendo del valor de la clase, es posible cualquiera de los tres casos anteriores.

I.2.1.2 Creación explícita – Cometido de agente

Caso a: El agente reconoce la clase de objetos gestionados en la petición y la soporta como clase real. En este caso, la clase de objetos gestionados pedida se crea sin que intervenga el alomorfismo. La creación tiene éxito o no dependiendo de las condiciones asociadas con el comportamiento y los valores de atributo suministrados por el gestor. El agente utiliza el nombre suministrado en el anterior caso 1 o asigna un nombre (para ello utiliza la regla de vinculación de nombres del caso 2, o bien lo genera internamente en base a la definición del esquema).

Caso b: El agente no soporta la clase pedida ni como una clase real soportada ni como un alomorfo. La clase de objetos gestionados proporcionada en la petición no es reconocida. La petición de creación es rechazada con la indicación de error "no existe esa clase de objetos". Se trata de un fallo normal de creación de una clase desconocida.

Caso c: El agente soporta el alomorfismo y crea una clase que es una clase ampliada con el nombre suministrado por el gestor. Se supone aquí que el nombre proporcionado por el gestor sigue las reglas de estructuración (vinculación de nombres) para la clase ampliada [la misma clase superior o clase superior ampliada, el mismo nombre distinguido relativo (RDN, *relative distinguished name*)]. Si esta condición no se cumple, fallará la creación. Si la creación tiene éxito, el agente responde indicando el valor de la clase real en el campo de clase de objetos gestionados y todos los atributos

que correspondan a la clase real. El objeto se crea de acuerdo con el comportamiento de la clase ampliada. Si el sistema de agente proporciona interoperabilidad (véase 5.2.3.1/X.720 | ISO/CEI 10165-1), el agente incluye el atributo alomorfos con el valor de la clase indicado en la petición de creación. Si el sistema de gestor proporciona interoperabilidad (véase 5.2.3.2/X.720 | ISO/CEI 10165-1), el gestor puede examinar el atributo alomorfos y determinar si la clase de objetos pedida es alomórfica con la clase real.

Caso d: El agente soporta el alomorfismo y crea una clase que es una clase ampliada con la vinculación de nombres suministrada por el gestor. Se supone aquí que la vinculación de nombres proporcionada es válida para la clase ampliada. A menudo esto es verdad si la clase ampliada es una subclase y las directrices para la definición de objetos gestionados (GDMO, *guidelines for the definition of managed objects*) incluyen la cláusula "WITH SUBCLASSES" (con subclases) para la vinculación de nombres. La respuesta, cuando la creación tiene éxito, es la misma que en el caso c. Si la vinculación de nombres no es válida para la clase ampliada (por ejemplo, se puede incluir comportamiento adicional en una vinculación de nombres diferente para la clase ampliada incluso si la estructura y el atributo de denominación son los mismos), la creación fallará. Se señala que si el gestor recibe una indicación de error por valor no válido del atributo vinculación de nombres sin más información, dicha indicación no ayudará a resolver el problema. Desde la perspectiva del gestor, la petición es una petición de clase y la vinculación de nombres es válida. Puesto que la clase ampliada requiere un comportamiento diferente, el agente no puede utilizar la vinculación de nombres. Es por esto por lo que se recomienda que no se suministre el atributo vinculación de nombres en la petición de creación.

Caso e: El agente soporta el alomorfismo y crea una clase con un nombre apropiado seleccionado por él (para el caso 3 de I.2.1.1: Creación explícita – Cometido de gestor). El nombre asignado puede ser comprendido o no por el gestor, dependiendo de la definición de la vinculación de nombres elegida. Cualquier otra información en las respuestas sería la misma que en el caso c.

En todos los casos anteriores, cuando el gestor no suministra un valor para un atributo y existe un valor por defecto, el valor de ese atributo se elige de acuerdo con la clase de objetos creada. En los casos c, d y e, esto puede dar lugar a que el gestor reciba valores para atributos que sólo existen en la clase ampliada. Es posible que el gestor no comprenda estos tipos y ha de tener la posibilidad de hacer caso omiso de los mismos sin que se produzca una interrupción de la asociación. Se señala que el gestor quizá desee tomar medidas de gestión adicionales para que quede constancia de que está encontrando agentes alomórficos (por ejemplo, registrar cronológicamente la información no comprendida).

Además de los valores por defecto de los atributos, pueden diferir las limitaciones impuestas al valor inicial, los valores permitidos y los valores requeridos de la clase alomórfica y la clase ampliada. En I.4 se dan más detalles al respecto.

I.2.1.3 Resumen de creación explícita

El cuadro que sigue presenta de manera resumida los diversos casos examinados de creación explícita del cometido de gestor y el cometido de agente, indicando si se admite o no el alomorfismo.

Cometido de gestor	**Cometido de agente con alomorfismo**	
	Soportado	No soportado
Caso 1	Casos a, b, c	Casos a, b
Caso 2	Casos a, b, d	Casos a, b
Caso 3	Casos a, b, e	Casos a, b
Caso 4	Casos a, b, c, d, e	Casos a, b

I.2.1.4 Creación automática – Cometido de agente

El agente puede crear un objeto gestionado internamente e informar a los gestores de la creación mediante la notificación de creación de objeto.

Caso 1: Se supone implementación por el agente de la clase ampliada y comportamiento alomórfico. Además de todos los atributos correspondientes a la clase creada, en el objeto gestionado creado se incluye el atributo alomorfos que contiene todas las clases de objetos alomórficos (compatibles). El agente envía una notificación de creación del nuevo objeto.

En este caso, el agente envía a continuación una notificación a todos los gestores utilizando la notificación de creación de objeto que contiene la clase real. Se incluyen en ella todos los atributos de la clase referenciada en el campo de la clase de objetos gestionados de la notificación de creación. Lo que comprende el atributo alomorfos.

Se señala que los valores por defecto utilizados son coherentes con la clase creada.

Caso 2: El agente sólo implementa la clase ampliada y no manifiesta alomorfismo para las clases compatibles. En este caso, la notificación de creación de objeto contiene sólo la información correspondiente a la clase ampliada y no está presente el atributo alomorfos. Para ese entorno, se recomienda que el sistema gestor proporcione la interoperabilidad con independencia de si se requieren o no características adicionales. El rechazo de la notificación no será de utilidad en un entorno práctico de RGT.

I.2.1.5 Creación automática – Cometido de gestor

El gestor recibe la notificación de creación de objeto con el atributo alomorfos y una clase ampliada en el campo de clase de objetos gestionados. La aplicabilidad de los casos descritos en **a** a **d** al caso 1 anterior depende de si el gestor admite o no el alomorfismo.

Caso a: El gestor tiene conocimiento de la clase ampliada y no se necesita el atributo alomorfos porque el gestor no tiene que efectuar gestión alomórfica. Todas las características asociadas con el reconocimiento o no de los valores y los identificadores de atributo son los mismos cuando no se utiliza alomorfismo.

Caso b: El gestor no reconoce el valor de la clase de objetos gestionados indicado en la notificación. Si el gestor comprende el identificador del atributo alomorfos, antes de pasar por alto la notificación como información no reconocida, deberá examinar el valor del atributo alomorfos para determinar si puede llevar a cabo la gestión utilizando uno de los valores de dicho atributo. Esto significa que al menos uno de los valores de la clase de objetos del atributo alomorfos es reconocido por el gestor. El gestor debe ignorar todos los atributos no reconocidos como pertenecientes a la clase alomórfica.

Caso c: El gestor no reconoce el valor de la clase de objetos gestionados y no ha implementado la capacidad de reconocer el identificador del atributo alomorfos. En tal caso, el gestor no puede gestionar el objeto creado automáticamente. Si la notificación de creación se envía con una confirmación, el gestor puede dar una respuesta indicadora de error para señalar que el objeto es desconocido.

Caso d: El gestor no reconoce el valor de la clase de objetos gestionados indicado en la notificación. El gestor comprende el atributo alomorfos; sin embargo, no reconoce ninguna de las clases de dicho atributo. En este caso, el resultado es el mismo que en el caso c. No es posible que este gestor gestione el objeto creado automáticamente.

El agente envía una notificación utilizando la clase real sin el atributo alomorfos (el agente no soporta el alomorfismo). Lo que corresponde al anterior caso a.

Caso e: El gestor comprende la clase ampliada y el comportamiento es como en el caso a anterior. La ausencia del atributo alomorfos es irrelevante y el gestor puede gestionar el objeto creado automáticamente.

Caso f: El gestor no reconoce la clase ampliada. El gestor no podrá gestionar este objeto ya que el agente no soporta el atributo alomorfos. Lo cual es cierto tanto si el gestor soporta el alomorfismo como si no lo soporta.

I.2.1.6 Resumen de creación automática

El cuadro que sigue presenta de manera resumida la relación entre los casos de gestor y agente.

Caso de agente	Caso de gestor
1	a, b, c, d
2	e, f

I.2.2 Operación obtención

La operación obtención se puede lanzar con un conjunto explícito de identificadores de atributo, una lista vacía o una lista faltante. A continuación se introduce en los dos casos (la lista vacía y la lista faltante se tratan del mismo modo) una nueva diferenciación de función de si la clase de objetos gestionados de la petición es la clase real o una clase alomórfica para el agente. Se señala que hay un identificador de objeto especial (42) que puede utilizar el gestor en la petición para referirse a la clase real del objeto gestionado sin tener que especificarla.

I.2.2.1 Cometido de gestor

Caso 1: El gestor emite una petición de obtención con una clase que no es la clase real del objeto sino uno de los alomorfos soportados por el agente. La lista de identificadores de atributo incluida es la apropiada para esa clase alomórfica. La respuesta recibida será de acuerdo con los casos a, b o c que se describen más adelante. Si el gestor soporta la interoperabilidad, una respuesta satisfactoria del caso b recibida con una clase diferente será reconocida como respuesta válida. De otro modo, el gestor rechazará la respuesta (rechazo ROSE y no del CMIP).

Caso 2: El gestor emite una petición de obtención con una clase que es la clase real o el identificador de objeto especial que implica la clase real. La lista de atributos pedida puede ser o no la apropiada para esa clase. Esto se debe a que, ya sea condicionalmente o utilizando el identificador de objeto especial, el gestor puede incluir atributos no disponibles para la clase implementada. La respuesta recibida será de acuerdo con el caso d que se describe más adelante.

Caso 3: El gestor emite su petición especificando una clase y un nombre de objeto gestionado y sin lista de atributos. La respuesta recibida depende del valor de la clase, de si el agente soporta o no el alomorfismo y del método de interoperabilidad. La respuesta recibida será de acuerdo con los casos e, f o g que se describen más adelante. Si la respuesta del caso f o el caso g contiene atributos que no comprende, el gestor hace caso omiso de los mismos.

Caso 4: El gestor emite su petición especificando una clase soportada por el agente y el nombre de un objeto gestionado o el identificador de objeto especial examinado más arriba y un nombre. No incluye la lista de atributos. La respuesta recibida será de acuerdo con el caso h que se describe más adelante. El gestor deberá hacer caso omiso de los atributos que no sean reconocidos cuando la clase indicada en la respuesta difiera de la que él reconoce (como resultado de utilizar el identificador de objeto especial).

I.2.2.2 Cometido de agente

Caso a: El agente soporta el alomorfismo y reconoce el nombre del objeto gestionado. La clase de objeto gestionado indicada en la respuesta concuerda con uno de los valores del atributo alomorfos. El agente responde con los valores de los atributos pedidos y la clase, que en la petición puede estar o no incluida. Si la clase está incluida, se recomienda que se utilice en la respuesta el valor de la clase real. De esta manera es posible una respuesta uniforme y coherente con independencia de que la petición sea de un único objeto o de múltiples objetos aplicando delimitación. Se prevé además

que el parámetro clase de objetos gestionados indicado en una respuesta CMIP corresponda al valor del atributo clase de objeto (objectClass).

Caso b: El agente no soporta el alomorfismo pero reconoce el nombre del objeto gestionado. El agente puede devolver una indicación de error ("no existe esa clase de objeto" o "conflicto de ejemplificación de clase") o responder con los valores del atributo (el agente proporciona interoperabilidad). Se recomienda este último comportamiento. El campo de la clase se puede dejar vacío o llenarlo con la clase real. Si no se reconocen ni la clase ni el nombre, se genera una respuesta de error (no existe ese ejemplar de objeto o no existe esa clase de objeto).

Caso c: El agente no soporta el alomorfismo y no comprende el valor de la clase o el nombre indicado en la petición. Se devuelve una indicación de error "no existe esa clase de objeto o ese ejemplar de objeto".

Caso d: El agente reconoce la clase y el nombre con independencia de si soporta o no el alomorfismo (esto corresponde al caso 2 en el que el gestor pide que se utilice una clase que sea compatible y no la clase ampliada incluso aunque tenga conocimiento de la clase ampliada, o al caso sencillo en que tanto el gestor como el agente sólo tienen conocimiento de una clase). El agente responde con valores de atributos (incluidas indicaciones de error si los atributos pedidos no son los adecuados para esa clase o no han sido implementados como consecuencia de la condicionalidad). Se puede prescindir del campo de la clase o incluir la clase efectiva.

Caso e: El agente reconoce la clase y el nombre indicado en la petición (con independencia de si se soporta o no el alomorfismo) y devuelve todos los valores e identificadores de atributos de ese objeto. En la respuesta se pueden omitir la clase y el nombre.

Caso f: El agente soporta el alomorfismo. El valor de la clase indicado en la respuesta no concuerda con el valor de la clase real incluso aunque el nombre corresponda a uno de los objetos contenidos en el sistema. La clase corresponde a un valor del atributo alomorfos. Si el agente proporciona interoperabilidad, responde sólo con el valor de los atributos apropiados para la clase pedida. Si el valor de la clase está indicado en la respuesta (no es preciso incluir la clase o el nombre), se utiliza la clase real (véase más arriba una explicación de este mismo tema). Si el gestor proporciona interoperabilidad, el agente devuelve todos los atributos incluidos en el objeto. Si el valor de la clase que figura en la petición no corresponde a ninguno de los valores del atributo alomorfos, el agente devuelve una indicación de error "no existe esa clase de objetos" al gestor. Se señala que, para proporcionar la interoperabilidad, es recomendable que tanto el agente como el gestor aporten algunas capacidades: el agente soportando el alomorfismo y el gestor ignorando la información desconocida.

Caso g: El agente no soporta el alomorfismo. La clase pedida no es reconocida pero se dispone de un objeto con ese nombre. El agente puede responder con una indicación de error "no existe esa clase de objeto" o con todos los atributos correspondientes a esa clase. Incluso aunque no se requiera que la respuesta incluya la clase ni la ejemplificación cuando se pida un único objeto, se recomienda que, en este caso, se incluyan la clase real y el nombre. De esta manera se informa al gestor de que la clase real es una clase ampliada de la clase compatible que él comprende.

Caso h: La clase pedida corresponde a la clase real en el agente o la clase real se utiliza porque la petición contenía el valor de identificador de objeto especial. Con independencia de si se soporta o no el alomorfismo, se devuelven todos los valores de atributos correspondientes a la clase realmente implementada para ese objeto suponiendo que el agente reconoce el nombre. Los campos de clase y nombre pueden estar o no presentes en la respuesta. Se recomienda no obstante que, en este caso, se incluyan la clase real y el nombre cuando en la respuesta se utilice el identificador de objeto especial. Si el nombre no es reconocido, se devuelve una indicación de error "no existe ese ejemplar de objeto".

I.2.2.3 Resumen de la operación OBTENCIÓN

El cuadro que sigue muestra de manera resumida la relación entre los casos de gestor y agente.

Caso de gestor	Caso de agente
1	a, b, c
2	d
3	e, f, g
4	h

I.2.3 Operación fijación

La operación fijación se puede lanzar con diferentes operadores. La sustitución se puede especificar con un valor concreto o indicando "fijación al valor por defecto". El valor por defecto de un atributo dependerá de la clase real. En una clase se puede especificar un atributo con un conjunto de valores permitidos y un conjunto de valores requeridos. Los valores requeridos deben ser un subconjunto de, o un conjunto igual a, los valores permitidos. La clase ampliada no debe aumentar los valores permitidos, pero puede eliminar algunos de ellos mientras no figuren en el conjunto de valores requeridos (véase la figura I.1). El no soporte de un valor permitido se autoriza en la clase ampliada o en la clase compatible en tanto en cuanto dicho valor no figure en la lista de valores requeridos. Así pues, con gestión alomórfica, cuando se dé un valor permitido para el alomorfo que no esté incluido en la clase ampliada, podrá ser rechazado sin que ello suponga un quebrantamiento del comportamiento alomórfico (garantizado para soportar todos los valores de la clase compatible; sin embargo, si el valor no figura en el conjunto permitido de la clase compatible, no será soportado ya que la lista no se puede ampliar).

I.2.3.1 Cometido de gestor

Caso 1: El gestor emite una petición de fijación con una clase, un nombre y el valor o los valores de los atributos (operador sustitución/adición o eliminación). La clase del objeto no es la clase real en el agente sino una clase compatible. Si se recibe una respuesta (sólo si la petición fue confirmada), serán válidos los casos a, b o c que se describen más adelante. Si el gestor soporta la interoperabilidad, una respuesta satisfactoria del caso b recibida con una clase diferente será reconocida como respuesta válida. De otro modo, el gestor rechazará la respuesta (un rechazo ROSE y no del CMIP).

Caso 2: El gestor emite una petición de fijación con una clase que es la clase real o el identificador de objeto especial que implica la clase real. El valor o los valores de los atributos (operador sustitución/adición o eliminación) pueden ser o no los apropiados para ese ejemplar. Esta alternativa de posibilidades se debe a la condicionalidad o a que, al utilizar el identificador de objeto especial, el gestor puede estar proporcionando valores apropiados para la clase compatible. Si se recibe una respuesta (sólo si la petición fue confirmada), será válido el caso d que se describe más adelante.

Caso 3: El gestor emite su petición especificando una clase, un nombre y la sustitución por un valor por defecto para uno o más atributos. La respuesta, si se recibe, depende del valor de la clase, de si el agente soporta o no el alomorfismo y del método de interoperabilidad. Será una respuesta de los casos e, f o g que se describen más adelante. La respuesta recibida puede indicar valores por defecto para los atributos diferentes de los asociados con la clase pedida. El gestor deberá reconocer estos valores porque la clase real en el agente es diferente.

Caso 4: El gestor emite su petición especificando una clase soportada por el agente, un nombre o el identificador de objeto especial examinado más arriba y un nombre y la sustitución por un valor por defecto para uno o más atributos. La respuesta, si se recibe, será de acuerdo con el caso h que se describe más adelante.

I.2.3.2 Cometido de agente

Caso a: El agente soporta el alomorfismo y reconoce el nombre del objeto gestionado. La clase de objeto gestionado indicada en la petición concuerda con uno de los valores del atributo alomorfos. El agente efectúa la modificación de esos atributos (suponiendo que existan y que los valores proporcionados sean válidos). Si la petición es confirmada, el agente responde con un acuse de recibo o los valores modificados. En este último caso, el valor del campo de clase (si está presente) es la clase real (véase más arriba una explicación para obtención). Si los atributos o valores proporcionados en la petición no son válidos, se devuelve una indicación de error o de éxito parcial (error de fijación de lista).

Caso b: El agente no soporta el alomorfismo pero reconoce el nombre del objeto gestionado. Es posible que el agente no efectúe la modificación pedida en base al no reconocimiento de la clase. Si la petición no fue confirmada, el gestor desconoce el resultado a menos que lance una operación de obtención. Considérese el caso en que se requiere una respuesta. Si el agente efectuó la operación (de manera satisfactoria o no) su respuesta puede ser una indicación de error ("no existe esa clase de objeto" o "conflicto de ejemplar de clase"), una confirmación indicando éxito o una indicación de error con éxito parcial. No es preciso que los campos de clase y nombre figuren en la respuesta. Si están presentes, se recomienda que incluyan la clase real para informar al gestor de cuál es la clase implementada. Si no se reconocen ni la clase ni el nombre, se genera una respuesta de error (no existe esa ejemplificación de objeto o no existe esa clase de objeto).

Caso c: El agente no soporta el alomorfismo y no comprende el nombre indicado en la petición. Se devuelve una indicación de error "no existe esa clase de objeto" o "no existe ese ejemplar de objeto".

Caso d: El agente reconoce la clase y el nombre con independencia de si soporta o no el alomorfismo (esto corresponde al caso 2 en el que el gestor pide que se utilice una clase que sea compatible y no la clase ampliada incluso aunque tenga conocimiento de la clase ampliada, o al caso sencillo en el que tanto el gestor como el agente sólo tienen conocimiento de una clase). El agente efectúa la modificación de esos atributos (suponiendo que existan y que los valores proporcionados sean válidos). Si la petición es confirmada, el agente responde con un acuse de recibo o los valores modificados. En este último caso, no es preciso que los campos de clase y nombre figuren en la respuesta. Si están presentes, el valor de campo de clase es la clase real (la misma explicación que en obtención). Si los atributos o los valores proporcionados en la petición no son válidos, se devuelve una indicación de error o de éxito parcial (error de fijación de lista).

Caso e: El agente reconoce la clase y el nombre de la petición (con independencia de si se soporta o no el alomorfismo) y efectúa la operación. La respuesta, si hace falta, puede ser un acuse de recibo, una indicación de error porque no hay valor por defecto definido o el valor modificado (el valor por defecto especificado para esa clase).

Caso f: El agente soporta el alomorfismo. El valor de la clase indicado en la petición no concuerda con el valor de la clase real incluso aunque el nombre corresponda a uno de los objetos contenidos en el sistema. La clase corresponde a un valor del atributo alomorfos. Si el agente proporciona interoperabilidad, efectúa la modificación de acuerdo con el valor por defecto para la clase real o detecta un error (por ejemplo, ausencia del valor por defecto definido para alguno de los atributos). Responde con un acuse de recibo o el valor por defecto asignado o una indicación de error con éxito parcial. No es necesario que incluya los campos de clase y nombre en la respuesta. Si el valor de la clase se incluye en la respuesta, ello significa que se trata de la clase real (véase la explicación en obtención). Si el valor de la clase que figura en la respuesta no corresponde a ninguno de los valores del atributo alomorfos, el agente devuelve una indicación de error "no existe esa clase de objeto" al gestor.

Caso g: El agente no soporta el alomorfismo. La clase pedida no es reconocida pero se dispone de un objeto con ese nombre. El agente puede efectuar la operación sustituyendo la clase real por los

valores por defecto apropiados o puede rechazar la petición. Si la petición fue confirmada y el agente rechaza la petición, el agente responde con una indicación de error "no existe esa clase de objeto" o "conflicto de ejemplificación de clase". Si efectúa la operación de manera satisfactoria, se devuelve un acuse de recibo o una indicación de éxito con los valores modificados. Los valores devueltos son los apropiados para la clase real. Incluso aunque no sea necesario que la respuesta incluya la clase y la ejemplificación para petición de objeto único, se recomienda que, en este caso, se incluyan la clase real y el nombre. De esta manera se informa al gestor de que la clase real es una clase ampliada de la clase compatible que él comprende (el gestor proporciona interoperabilidad). Si se efectúa la modificación con éxito parcial, se envía una indicación de error. La utilización del campo de clase es la misma que en caso de éxito.

Caso h: La clase pedida corresponde a la clase real en el agente o la clase real se utiliza porque la petición contenía el valor de identificador de objeto especial. Con independencia de si se soporta o no el alomorfismo, el agente sustituye con valores por defecto todos los valores correspondientes a los identificadores de atributo en la petición (suponiendo que todos los atributos de la petición sean soportados por el agente). Si efectúa la operación de manera satisfactoria, se devuelve un acuse de recibo o una indicación de éxito con los valores modificados. Incluso aunque no se requiera que la respuesta incluya la clase ni la ejemplificación para la petición de objeto único, se recomienda que, en este caso, se incluyan la clase real y el nombre cuando se utilice identificador de objeto especial en la petición. Si el nombre no se reconoce, se devuelve una indicación de error "no existe ese ejemplar de objeto".

I.2.3.3 Resumen de la operación OBTENCIÓN

El cuadro que sigue muestra de manera resumida la relación entre los casos de gestor y agente.

Caso de gestor	Caso de agente
1	a, b, c
2	d
3	e, f, g
4	h

I.2.4 Operación acción

La operación acción de cualquier clase específica puede incluir argumento y respuestas con parámetros tanto obligatorios como opcionales. Si en el argumento de la clase real hay parámetros requeridos que no forman parte de la clase compatible, dichos parámetros han de tener valores por defecto asociados. Incluso aunque la Rec. UIT-T X.720 | ISO/CEI 10165-1 permita la adición de los parámetros requeridos en la información de la acción, no es posible especificar ésta utilizando la notación de plantilla sin crear una nueva acción. No obstante, el requisito se puede especificar mediante el comportamiento. Esto es así porque sólo las etiquetas de los parámetros se pueden utilizar para potenciar una especificación de acción. Por ello, la acción original tiene un campo ANY DEFINED BY (cualquiera definido por) (o una clase de objeto de información de la Rec. UIT-T X.681 | ISO/CEI 8824-2) y se potencia con la etiqueta de la plantilla de parámetros en otra clase (o creando un objeto de información). Si los campos requeridos se han de añadir a una acción, el único procedimiento disponible consiste en definir una acción nueva, que tenga un registro diferente. En otras palabras, las plantillas no soportan que una acción se derive de otra acción añadiendo campos nuevos que son obligatorios en una especificación ASN.1 formal.

I.2.4.1 Cometido de gestor

Caso 1: El gestor emite una petición de acción con una clase, un nombre y el valor o los valores de los parámetros del argumento de acción (si está presente). La clase del objeto no es la clase real en el agente sino una clase compatible. Si se recibe una respuesta (sólo si la acción se definió como

confirmada), serán válidos los casos a, b o c que se describen más adelante. Si el gestor soporta la interoperabilidad, una respuesta satisfactoria de los casos a y b recibida con una clase diferente y campos adicionales en la respuesta de acción será reconocida como respuesta válida. De otro modo, el gestor rechazará la respuesta (un rechazo ROSE y no del CMIP).

Caso 2: El gestor emite una petición de acción con una clase que es la clase real o el identificador de objeto especial que implica la utilización de la clase real. Es posible que no todos los campos incluidos sean los apropiados para esa clase. Si se recibe una respuesta (sólo si la petición fue confirmada), será válido el caso d que se describe más adelante.

I.2.4.2 Cometido de agente

Caso a: El agente soporta el alomorfismo y reconoce el nombre del objeto gestionado. La clase de objeto gestionado indicada en la petición concuerda con uno de los valores del atributo alomorfos. El agente efectúa la acción de acuerdo con su clase real utilizando los parámetros suministrados en la petición. Se señala que si hacen falta algunos campos adicionales para efectuar la acción, deben estar disponibles valores por defecto ya que no serán suministrados por el gestor. Si la petición es confirmada, la respuesta del agente depende de si la acción se llevó a cabo de manera satisfactoria y de si el agente proporciona interoperabilidad. No es necesario que la respuesta incluya la clase y el nombre en este caso en el que se hace referencia a un único objeto. Si la operación no tiene éxito, se devuelve una indicación de error. El agente puede incluir la clase real para informar al gestor de cuál es la clase implementada o la clase pedida (clase alomórfica). Si la acción tiene éxito, el agente responde con un acuse de recibo (una confirmación de que la acción se efectuó de manera satisfactoria) porque la definición de la acción no incluye ningún campo para la respuesta, o bien se produce la respuesta de la acción con los campos apropiados. El agente puede optar entre uno de los dos métodos de respuesta siguientes. Si el agente proporciona interoperabilidad, puede incluir sólo los campos apropiados para la clase pedida y no las adiciones para la clase real. En este caso, se puede omitir el valor del campo de clase. En el segundo método, se supone que el gestor proporciona interoperabilidad. La respuesta puede incluir campos adicionales que no figuraban en la acción para la clase indicada en la respuesta (es posible que se hayan incluido nuevas plantillas de parámetros para el campo de ampliación o que se apliquen las reglas de extensibilidad en ASN.1). Se recomienda incluir en el campo de clase la clase real para que el gestor se entere de cuál es la clase implementada.

Caso b: El agente no soporta el alomorfismo pero reconoce el nombre del objeto gestionado y la acción es válida para su clase real. Es posible que el agente no efectúe la acción pedida en base al no reconocimiento de la clase indicada en la petición (diferente de la clase real). Si la definición de la clase indica no confirmada, el gestor desconoce si la acción tuvo éxito o no. Dependiendo del tipo de acción, el efecto de la misma puede ser deducido más adelante (por ejemplo, realizando una operación de obtención). Considérese el caso en que la acción es confirmada. Si el agente efectuó la acción (de manera satisfactoria o no) puede devolver una indicación de error ("no existe esa clase de objeto" o "conflicto de ejemplar de clase"), una confirmación indicando éxito, una indicación de error específico (si existe alguno) definido para esa acción o un error CMIP genérico. La acción se efectúa de acuerdo con la clase real. No es preciso que los campos de clase y nombre figuren en la respuesta. Si están presentes, se recomienda que incluyan la clase real para informar al gestor de cuál es la clase implementada. Si no se reconocen ni la clase ni el nombre, se genera una respuesta de error (no existe ese ejemplar de objeto).

Caso c: El agente no soporta el alomorfismo y no reconoce el nombre indicado en la respuesta. Se devuelve una indicación de error "no existe esa clase de objeto" o "no existe ese ejemplar de objeto".

Caso d: El agente reconoce la clase y el nombre con independencia de si soporta o no el alomorfismo (esto corresponde al caso 2 en el que el gestor pide que se utilice una clase que sea compatible y no la clase ampliada incluso aunque tenga conocimiento de la clase ampliada admitiendo así la interoperabilidad proporcionada por el gestor, o al caso sencillo en el que tanto el

gestor como el agente sólo tienen conocimiento de una clase). El agente efectúa la acción de acuerdo con su clase real con independencia de si la petición contenía la clase alomórfica o el identificador de objeto especial. El resultado de la acción puede ser satisfactorio o puede ser un error. Si la acción no estaba definida como acción confirmada, no se genera ninguna respuesta. Si la acción se lleva a cabo con éxito o se produce un error, se emite la indicación de resultado apropiada o una respuesta de error. Si la acción tiene éxito, la respuesta se genera de acuerdo con la definición de la clase real. Si se utiliza el identificador de objeto especial, se recomienda incluir el valor de clase de la clase real incluso aunque no se requieran los campos de clase y nombre en el caso de objeto único.

I.2.4.3 Resumen de la operación ACCIÓN

El cuadro que sigue muestra de manera resumida la relación entre los casos de gestor y agente.

Caso de gestor	Caso de agente
1	a, b, c
2	d

I.2.5 Operación supresión

La operación supresión se define con dos opciones: supresión de los objetos contenidos y supresión no permitida a menos que se supriman todos los objetos contenidos. Para la operación de supresión se ha de tener en cuenta lo siguiente: que con independencia de la clase, es el nombre lo que ha de ser reconocido porque dos ejemplificaciones de la misma clase pueden tener nombres diferentes y/o comportamiento diferente (en base a la vinculación de nombre utilizada para ejemplificar el objeto).

I.2.5.1 Cometido de gestor

Caso 1: El gesto emite una petición de supresión con una clase y un nombre. La clase del objeto no es la clase real en el agente sino una clase compatible. Para la respuesta serán válidos los casos a, b o c que se describen más adelante. Si el gestor soporta la interoperabilidad, una respuesta satisfactoria de los casos a y b recibida con una clase diferente será reconocida como respuesta válida. De otro modo, el gestor rechazará la respuesta (un rechazo ROSE y no del CMIP). Como se ha indicado antes, no sirve el envío de un rechazo (no se recomienda por tanto) y el gestor deberá proporcionar un cierto nivel de interoperabilidad.

Caso 2: El gestor emite una petición de supresión con una clase que es la clase real o el identificador de objeto especial que implica la utilización de la clase real. La respuesta indicada en el caso d descrito más adelante es una respuesta válida.

I.2.5.2 Cometido de agente

Caso a: El agente soporta el alomorfismo y reconoce el nombre del objeto gestionado. La clase de objeto gestionado indicada en la petición concuerda con uno de los valores del atributo alomorfos. El agente suprime el objeto suponiendo que son aceptables las condiciones para la supresión de acuerdo con la vinculación de nombres utilizada para ese ejemplar. Si la supresión no se efectúa, se genera un error. Si la supresión tiene éxito, el agente responde con un acuse de recibo (una confirmación de que la supresión se llevó a cabo de manera satisfactoria). No es necesario que la respuesta incluya la clase y el nombre en este caso en que se hace referencia a un único objeto. Se recomienda incluir en el campo de clase la clase real para que el gestor se entere de cuál es la clase implementada (es posible que esto no le sirva al gestor ya que el objeto se suprime, a diferencia de las operaciones anteriores).

Caso b: El agente no soporta el alomorfismo pero reconoce el nombre del objeto gestionado. Es posible que el agente no suprima el objeto en base al no reconocimiento de la clase ("no existe esa clase de objeto" o "conflicto de ejemplar de clase"). Si el agente efectúa la supresión en base al

nombre del objeto (suponiendo que se cumplen las demás condiciones para la supresión), se devuelve un acuse de recibo. Si la supresión no es posible (no se cumplen las condiciones), se devuelve una indicación de error. En cualquier caso, no es necesario incluir la clase y el nombre del objeto. Se recomienda incluir la clase real (es posible que esto no le sirva al gestor ya que el objeto se suprime, a diferencia de las operaciones anteriores).

Caso c: El agente no soporta el alomorfismo y no reconoce el nombre que figura en la petición. Se devuelve una indicación de error "no existe esa clase de objeto" o "no existe ese ejemplar de objeto".

Caso d: El agente reconoce la clase y el nombre con independencia de si soporta o no el alomorfismo (esto corresponde al caso 2 en el que el gestor pide la utilización de una clase que sea compatible y no la clase ampliada incluso aunque tenga conocimiento de la clase ampliada soportando así la interoperabilidad proporcionada por el gestor, o al caso sencillo en el que tanto el gestor como el agente sólo tiene conocimiento de una clase). El agente suprime el objeto suponiendo que son aceptables las condiciones para la supresión de acuerdo con la vinculación de nombres utilizada para ese ejemplar. Si la supresión no se efectúa, se genera un error. Si la supresión tiene éxito, el agente responde con un acuse de recibo (una confirmación de que la supresión se realizó de manera satisfactoria). No es necesario que la respuesta incluya la clase y el nombre en este caso en que se hace referencia a un único objeto. Se recomienda incluir en el campo de clase la clase real (si se utilizó el identificador de objeto especial; de no ser así, el gestor y el agente hacen la misma interpretación del valor de la clase) para que el gestor se entere de cuál es la clase implementada (es posible que esto no le sirva al gestor ya que el objeto se suprime, a diferencia de las operaciones anteriores).

I.2.5.3 Resumen de la operación SUPRESIÓN

El cuadro que sigue muestra de manera resumida la relación entre los casos de gestor y agente.

Caso de gestor	Caso de agente
1	a, b, c
2	d

I.3 Notificación CMIP

Las notificaciones son mucho más sencillas que las operaciones mencionadas en la cláusula anterior. La notificación puede ser enviada en modo confirmado o en modo no confirmado. Si se envía en modo no confirmado, el gestor puede hacer caso omiso de lo que recibe porque no se reconoce algo de lo siguiente: la clase, el nombre, el tipo de evento o cualquiera de los campos de información del evento. Siempre es posible utilizar RO-Rechazo, pero se envía a nivel de ROSE y no es reconocido por el CMIP. De todos modos, el envío de una indicación de rechazo no proporciona la interoperabilidad de las RGT.

I.3.1 Cometido de gestor

Caso a: El gestor comprende la clase, el nombre, el tipo de notificación y algunos de los parámetros de información del evento. El gestor hace caso omiso de los parámetros desconocidos.

Caso b: El gestor no proporciona interoperabilidad. No comprende la clase. El gestor deberá hacer caso omiso de la notificación. Puede optar por enviar una indicación de rechazo.

Caso c: El gestor comprende el nombre, el tipo de notificación y algunos de los parámetros de información del evento. El gestor no comprende la clase. Puede hacer caso omiso de la notificación o determinar que la clase es una clase ampliada e ignorar los parámetros desconocidos (si el gestor proporciona interoperabilidad). De otro modo, el gestor puede enviar una indicación de rechazo.

Caso d: El gestor no reconoce la clase ni el nombre (en este caso es posible que el no reconocimiento de otros parámetros de la notificación no tenga importancia). El gestor deberá hacer caso omiso de la notificación.

I.3.2 Cometido de agente

Caso 1: El agente soporta el alomorfismo. Si el agente proporciona interoperabilidad, la notificación puede incluir en el campo de clase un valor del atributo alomorfos y toda la información del evento (con independencia de si los parámetros son aplicables o no a la clase alomórfica). Normalmente, se prevé que el agente utilizará la clase real porque por lo general desconoce cuál es el alomorfo que debería utilizarse en el informe de evento. Si la notificación es confirmada, se aplican los anteriores casos a, b o c.

Caso 2: El agente no soporta el alomorfismo. El agente emite la notificación utilizando la clase real y los parámetros pertinentes para esa notificación. Son válidos los anteriores casos a, b, c o d.

I.3.3 Resumen de NOTIFICACIÓN

El cuadro que sigue muestra de manera resumida la relación entre los casos de gestor y agente.

Caso de gestor	Caso de agente
a	1, 2
b	1, 2
c	1, 2
d	2

I.4 Asuntos relativos a la implementación

I.4.1 Asuntos relacionados con la pila de protocolos

En repetidas ocasiones, durante el análisis del alomorfismo, se ha indicado la exigencia de que el gestor pueda hacer caso omiso de las sintaxis ASN.1 (bien de los atributos de la clase ampliada únicamente o bien sólo de las notificaciones de la clase ampliada). Por lo general, estas sintaxis no son las que han sido implementadas en el gestor (ya que el gestor trata de llevar a cabo una gestión alomórfica). Para que el gestor prescinda de esas sintaxis de manera satisfactoria, se ha de permitir que pasen a través de la pila de protocolos sin interrumpir la asociación. A ello contribuyen los protocolos de la capa de presentación. La capa de presentación tiene normalmente la obligación de abortar las asociaciones si se recibe una PDU desconocida (véase 6.4.4.3/X.226 | ISO/CEI 8823-1). Sin embargo, en 7.5/X.711 (CMIP) se especifica que el CMIP resuelve todas las sintaxis ANY DEFINED BY OBJECT IDENTIFIER (cualquiera definido por identificador de objeto). En 7.5/X.711 se indica lo siguiente:

> El correspondiente valor de descriptor de objeto ASN.1 será "CMIP-PCI".
>
> Esta sintaxis abstracta se define para incluir todos los tipos de datos resueltos por las producciones ANY DEFINED BY X, donde X es de tipo OBJECT IDENTIFIER.

I.4.2 Valores permitidos y valores requeridos

La relación entre los valores de atributos de las clases alomórficas y las clases ampliadas es similar a la relación entre las superclases y sus subclases. Los valores requeridos de la clase alomórfica deben ser un subconjunto de los valores requeridos de la clase ampliada. A su vez, los valores requeridos de la clase ampliada deben ser un subconjunto de los valores permitidos de la clase alomórfica. Por último, los valores permitidos de la clase ampliada deben ser un subconjunto de los valores permitidos de la clase ampliada. En la figura I.1 se ilustran estas relaciones.

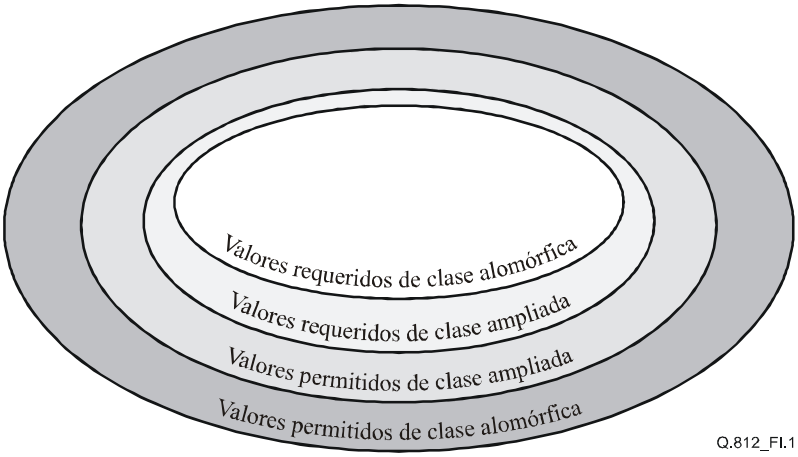

Figura I.1/Q.812 – Relación entre valores permitidos y valores requeridos

NOTA – Al desarrollar el modelo se han de respetar las reglas anteriores, pero su aplicación práctica puede ser difícil. Un ejemplo al respecto es el paquete de circuitos y el paquete de circuitos multipuerto definidos en la Rec. UIT-T M.3100. Los valores permitidos del estado de disponibilidad se redujeron a uno solo, mientras que la experiencia práctica indicaba que eran necesarios otros valores. Por ello se eliminó esa restricción en el paquete de circuitos multipuerto. Sin embargo, la versión nueva del paquete de circuitos podría no ser una subclase del paquete de circuitos porque los valores permitidos no pueden ser ampliados y, en sentido estricto, no pueden ser alomórficos. Incluso aunque la ejemplificación de una clase ampliada tenga un valor de atributo fuera de la gama permitida para la clase compatible, el sistema gestor puede proporcionar un cierto nivel de interoperabilidad. Deberá poder codificar la sintaxis ASN.1 del atributo.

I.4.3 Valor inicial

La especificación de una clase de objetos gestionados puede incluir valores iniciales para cero o más atributos. A diferencia de lo que ocurre con los valores por defecto, con valores iniciales, la petición de creación fallará si el valor indicado en la petición es distinto del valor inicial especificado. Si el valor no está presente, el agente proporciona el valor inicial especificado. Una clase ampliada puede especificar un valor inicial para un determinado atributo distinto del correspondiente a la clase compatible. Cuando el agente cree el objeto gestionado, se utilizará el valor inicial apropiado para la clase real. Así pues, de manera similar el caso de los atributos con valores por defecto que se examina en I.2.1.2, el gestor puede recibir valores para atributos que difieran de los asociados con la clase de objetos que figura en la petición. Se recomienda que, cuando se definan valores iniciales para un atributo, el gestor no indique el valor en la petición de creación. De esta manera se evitará el posible rechazo de la petición porque el valor inicial indicado no es el apropiado para la clase real.

I.4.4 Filtrado en un único objeto

Cuando se efectúa una petición con filtrado, y suponiendo que el agente haya reconocido la petición (con las condiciones indicadas más arriba), se plantean los siguientes casos:

Caso 1: El filtro tiene todos los atributos que reconoce y han sido implementados para el objeto. El funcionamiento del filtro no resulta afectado.

Caso 2: El filtro tiene atributos no implementados por el agente para ese objeto porque son condicionales o porque corresponden a la nueva versión del objeto. La condición que se comprueba para cualquier atributo es equivalente a (el atributo existe y el valor cumple la condición establecida). Esa parte del filtro deberá tomar el valor de verdadero para que los agentes sean sencillos con independencia de la clase implementada. Si el atributo especificado en el filtro es clase de objeto (objectClass) y el valor que se ha de comparar es el de la clase compatible, los objetos con clase ampliada no cumplirán los criterios. Si el gestor exige que se seleccionen objetos

pertenecientes tanto a las clases ampliadas como a las clases compatibles, el filtro deberá incluir OR{equal{objectClass, x}, nonullIntersection {{x}, allomorphs}}.

I.4.5 Delimitación solamente

El gestor pide que se realicen operaciones proporcionando un objeto base y un nivel de alcance.

Caso 1: El objeto base es la clase implementada por el agente:

– El agente no soporta el alomorfismo y responde indicando la clase real de los objetos seleccionados (con independencia de si ha implementado la definición ampliada que comprende o ha implementado solamente una definición). El gestor puede recibir respuestas para objetos con valores no reconocidos del campo de clase (porque no reconoce el nuevo esquema). El gestor puede proporcionar interoperabilidad limitada en base al nombre y a otras características que sí reconoce.

– El agente soporta el alomorfismo y ha implementado las definiciones ampliadas dentro del alcance seleccionado. Efectúa la operación de acuerdo con las clases reales de los objetos que se hallan dentro de ese alcance. La respuesta utiliza la clase real de la clase de objetos gestionados porque es posible que el agente no sepa cuál o cuáles valores del atributo alomorfos puede reconocer el gestor y cuáles son los detalles pertinentes de esa clase (atributos, resultado de la acción, etc. como se indica más arriba). Incluso si soporta el alomorfismo, resulta más sencillo responder en este caso utilizando la clase real y las propiedades correspondientes a esa clase. El gestor puede proporcionar interoperabilidad si comprende ambas versiones de las definiciones, o bien interoperabilidad limitada (sólo reconoce una versión). (Si el gestor soporta el alomorfismo, quizá convenga, para la operación OBTENCIÓN delimitada, pedir que se devuelva el valor del atributo alomorfos.)

Caso 2: El objeto base es de una clase distinta de la que figura en la petición pero el nombre es reconocido (la clase es una definición más reciente que la que figura en la petición o una definición más antigua):

– El agente no soporta el alomorfismo e implementa una definición más antigua. Puede rechazar la petición porque la clase no es reconocida o puede utilizar el nombre y responder con objetos que se hallen dentro del alcance. Si el gestor recibe una indicación de "no existe esa clase de objeto" o "conflicto de ejemplar de clase", puede reenviarla con la clase apropiada para el objeto base. Tal cosa sólo es posible si el gestor proporciona interoperabilidad y sabe cuál es la versión que soporta el agente. Quizá el agente identifique el objeto base a partir del nombre (con independencia de la clase), seleccione los objetos que se hallen dentro del alcance y responda al gestor utilizando la clase real. Si el gestor proporciona interoperabilidad, deberá hacer caso omiso de la información que no reconozca.

– El agente soporta el alomorfismo y determina si la clase de objeto base es un alomorfo. Si tal cosa es cierta, efectúa las operaciones en los objetos seleccionados (utilizando la clase real) y responde utilizando la clase real (el gestor proporciona interoperabilidad).

En los dos casos anteriores, si no se identifica el objeto base se devuelve una indicación de error.

Caso 3: Aunque poco probable, es posible que el agente proporcione interoperabilidad si conoce las versiones soportados por el gestor o los gestores. En este caso, la respuesta puede ser personalizada al conocimiento específico del gestor.

I.4.6 Delimitación y filtrado

Cuando en la petición figuran tanto el alcance como el filtro, se ha de considerar cualquiera de los tres casos analizados arriba. Se aplica el análisis efectuado en I.4.4, "Filtrado en un único objeto", en cada uno de los casos que dé lugar a la selección de objetos aplicando delimitación. No se requiere ningún comportamiento adicional.

I.4.7 Denominación

Como se ha indicado más arriba, la Rec. UIT-T X.720 | ISO/CEI 10165-1 define el alomorfismo como una propiedad del objeto gestionado. En principio, no hace falta que dos clases (la compatible y la ampliada) estén relacionadas por herencia para manifestar un comportamiento alomórfico. Aunque no se especifique en la Rec. UIT-T X.720 | ISO/CEI 10165-1, es necesario que la estructura de denominación sea la misma en esas dos clases. Incluso si el parámetro clase de objetos gestionados se refiere a una clase alomórfica, para que el agente reconozca el objeto gestionado es necesario que el campo de objeto gestionado utilice la misma estructura para la clase real y la clase alomórfica. Igual estructura significa que la secuencia de elaboración de nombres locales y distinguidos es la misma [la clase superior y los atributos de nombre distinguido relativo (RDN) son los mismos para las clases ampliada y alomórfica]. Esta condición se cumple en la mayoría de los casos cuando las dos clases están relacionadas por herencia [la vinculación de nombres puede incluir la frase AND SUBCLASSES (y subclases)].

En el ejemplo del paquete de circuitos multipuerto, las reglas de estructuración para la denominación son las mismas que los del paquete de circuitos aunque el primero no pueda derivarse como una subclase (debido a la ampliación de los valores permitidos). Así pues, desde el punto de vista de la denominación, cabe considerar que una ejemplificación de paquete de circuitos multipuerto es alomórfica a la clase de objeto paquete de circuitos.

I.5 Ejemplos de utilización del alomorfismo

Esta cláusula contiene ejemplos de los escenarios en los que los sistemas gestor y gestionado implementan las diferentes versiones de un modelo de información. Puesto que no es posible una adaptación inmediata de todos los sistemas a la misma versión, la utilización del alomorfismo constituirá una medida importante para el soporte de la interoperabilidad entre sistemas.

En las figuras se supone que el sistema de agente y el sistema de gestor proceden de múltiples suministradores. Por ello, los números de versión y la relación con la versión implementada del modelo de información no están correlacionados entre los suministradores.

La figura I.2 describe un escenario sencillo. El esquema del modelo de información de gestión (SMK, *schema for management information model*) corresponde exactamente a las mismas definiciones (ambas se hallan en la misma versión desde la perspectiva de la interfaz). Se utiliza numeración diferente para indicar la posibilidad de que, cuando los sistemas los proporcionen fabricantes diferentes, se utilicen opciones de numeración de versión diferentes.

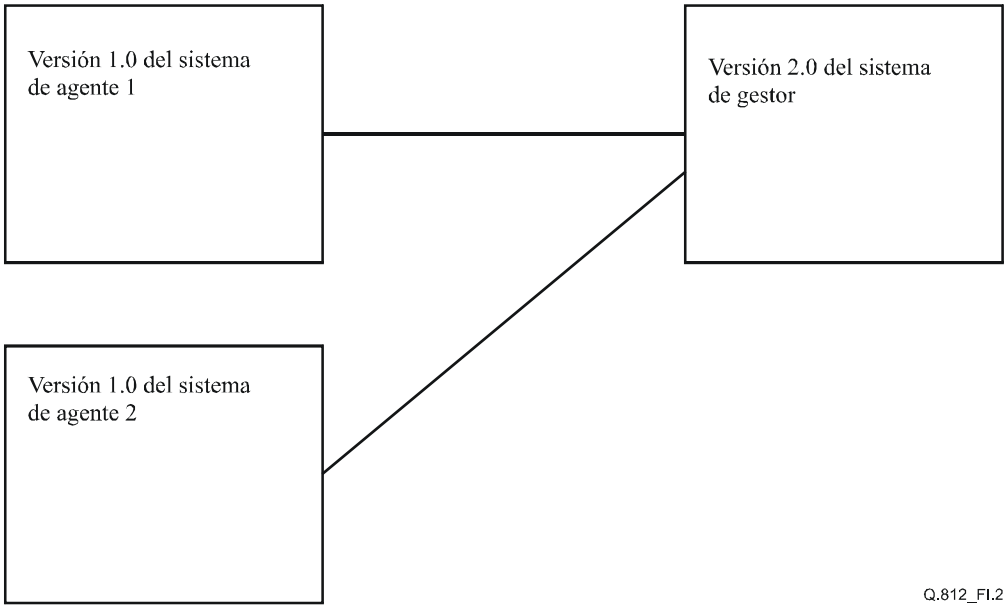

Figura I.2/Q.812 – Escenario 1

En este caso, la interoperabilidad no exige el soporte o no del alomorfismo. No se prevé que el sistema de agente o el sistema de gestor envíen o reciban información de gestión diferente de la definida por el esquema.

La figura I.3 describe un escenario en el que el esquema del modelo de información de gestión (SMK) que implementa al gestor tiene más capacidad que la versión 1.0 del sistema de agente. El sistema de gestión gestiona más de un sistema de agente (diferentes suministradores). La versión 1.5 del sistema de agente 2 y la versión 3.0 del sistema de gestor implementan las mismas características (el SMK es el mismo desde la perspectiva de la interfaz). El sistema de agente 2 también fue gestionado por el sistema de gestor 2, que no se mejoró para incluir las nuevas características.

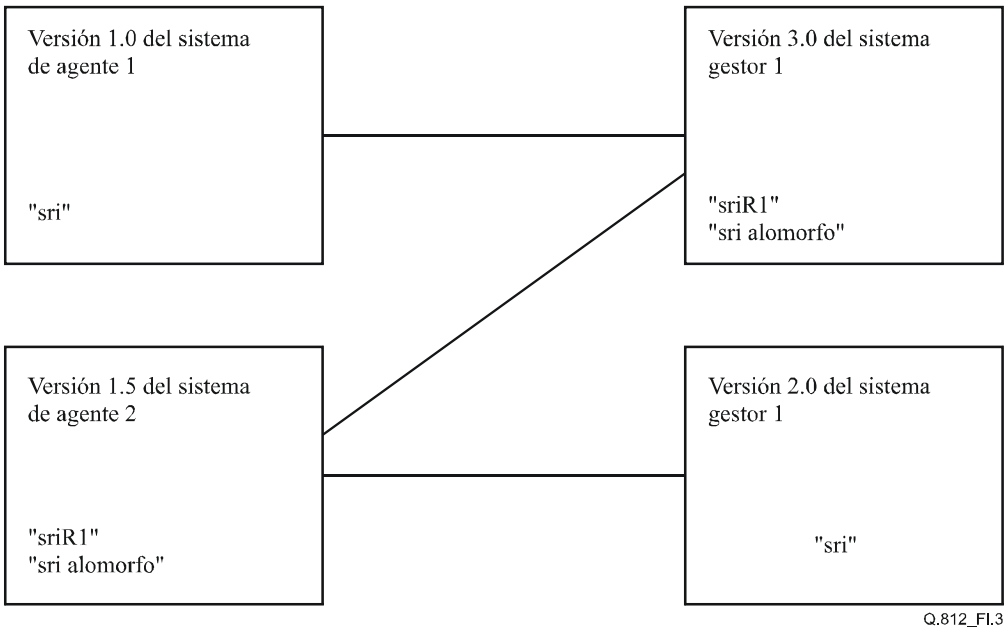

Figura I.3/Q.812 – Escenario 2

Caso 1: Interoperabilidad proporcionada por el gestor: Para simplificar, supóngase una clase de objeto gestionado único "sri" y una clase ampliada "sriR1". Las soluciones de interoperabilidad se pueden explicar utilizando este caso sencillo sin pérdida de la generalidad (aunque un sistema puede optar por soportar el alomorfismo para algunas clases y no para otras). Se supone que el sistema gestor de la versión 3 puede gestionar ampliaciones no ofrecidas por el sistema de agente 1 sino por el sistema de agente 2.

Caso 2: El soporte o no del alomorfismo por el sistema de agente 1 no es pertinente. El sistema de agente 2 soporta el alomorfismo y ha implementado la clase "sriR1". El atributo alomorfo contiene el valor "sri". Las interacciones entre el sistema gestor 1 y los dos agentes son las mismas que en el caso 1. El gestor 2 no comprende las capacidades adicionales de "sriR1" y para las notificaciones del sistema de agente 2 (utilizando la clase ampliada sriR1), el comportamiento puede que no sea el mismo que en el caso 1. En el caso de notificaciones definidas solamente para sriR1, el gestor 2 no sabrá cómo procesarlas y deberá por tanto ignorarlas en lo que se refiere a la actividad de gestión. Puesto que el sistema de agente 2 soporta el alomorfismo, cuando el gestor pida una operación utilizando la clase "sri", efectuará la operación de acuerdo con las especificaciones correspondientes a la clase "sriR1" real. El agente puede informar al gestor de que la clase real es la "sriR1" incluyéndola en la respuesta (algo que no se requiere si la petición se dirigió a una ejemplificación específica). En base a la operación pedida, la información proporcionada concordará con la de la clase real. El gestor 2 deberá ser capaz de ignorar información no reconocida sin interrumpir la asociación. Esto significa que el gestor tiene que proporcionar un cierto nivel mínimo de interoperabilidad.

Apéndice II

Cuadro II.1/Q.812 – Capa de transporte

Norma base (Rec. UIT-T X.224 | ISO/CEI 8073)				ISP
Ident.	**Característica**	**Subcláusula**	**Estado**	**Estado**
NAC2	Clase 2	6.5.4 h	NC2: ninguno 0,1,2	NC2: por lo menos 0
NAC4	Clase 4	6.5.4 h	NC4: ninguno 0,1,2,3,4	NC4: por lo menos 0
NEF2	Clase 2	6.5.4 k	I2R2, T2F14:O	I2R2, T2F14:oo
NEF5	Clase 3	6.5.4 k	I3R2, T3F14:O	I0R2, T0F14:oo I2R2, T2F14:oo
NEF6	Clase 4	6.5.4 k	I4R2, T4F14:OO	I2R2, T2F14:oo I4R2, T4F14:oo
RC4	¿Con qué clases se puede responder si CR sólo propone clase 4?	6.5.4 h Cuadro 3	I4R2 o I2R2:4 ó 2	I2R2:2, I4R2:4
RC4a	¿Con qué clases se puede responder si CR propone clase 4 como clase preferida y está presente el parámetro de clase preferida?	6.5.4 h Cuadro 3	I4R2:4, I2R2:2, I0R2:0 En función del código de la clase alternativa	I4R2:4, I2R2:2, I0R2:0 En función del código de la clase alternativa
S2	Soporte de la función NCMS	Anexo B	O	oi
S3	Soporte de la clase 4 sobre CLNS		O	oi

Cuadro II.1/Q.812 – Capa de transporte

Norma base (Rec. UIT-T X.224 | ISO/CEI 8073)				ISP
Ident.	**Característica**	**Subcláusula**	**Estado**	**Estado**
TED6	Clase 2	6.5.4 r	I2R2, T2F15:O	I2R2, T2F15:oo
TED8	Clase 4	6.5.4 r	I4R2, T4F15:O	I0R2, T0F15:ox
NUC1	¿Se propone en CR la "no utilización de suma de verificación"?	6.5.4 m	I4R1:mo	I4R1:mo
NUC2		6.5.4 m	I4R2:O	I4R2:mo

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	**Conmutación y señalización**
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2005