



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.800

Enmienda 1
(10/96)

SERIE X: REDES DE DATOS Y COMUNICACIÓN
ENTRE SISTEMAS ABIERTOS

Seguridad

**Arquitectura de seguridad para la interconexión
de sistemas abiertos para aplicaciones del
CCITT**

**Enmienda 1: Servicios y mecanismos de
seguridad de capa 2 de las redes de área local**

Recomendación UIT-T X.800 – Enmienda 1

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES DE LA SERIE X DEL UIT-T

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

REDES PÚBLICAS DE DATOS	X.1–X.199
Servicios y facilidades	X.1–X.19
Interfaces	X.20–X.49
Transmisión, señalización y conmutación	X.50–X.89
Aspectos de redes	X.90–X.149
Mantenimiento	X.150–X.179
Disposiciones administrativas	X.180–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
Modelo y notación	X.200–X.209
Definiciones de los servicios	X.210–X.219
Especificaciones de los protocolos en modo conexión	X.220–X.229
Especificaciones de los protocolos en modo sin conexión	X.230–X.239
Formularios para declaraciones de conformidad de implementación de protocolo	X.240–X.259
Identificación de protocolos	X.260–X.269
Protocolos de seguridad	X.270–X.279
Objetos gestionados de capa	X.280–X.289
Pruebas de conformidad	X.290–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
Gestión de redes	X.600–X.629
Eficacia	X.630–X.649
Denominación, direccionamiento y registro	X.650–X.679
Notación de sintaxis abstracta uno	X.680–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión	X.730–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
Cometimiento, concurrencia y recuperación	X.850–X.859
Tratamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999

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

PREFACIO

El UIT-T (Sector de Normalización de las Telecomunicaciones) es un órgano permanente de la Unión Internacional de Telecomunicaciones (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 Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), 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 N.º 1 de la CMNT (Helsinki, 1 al 12 de marzo de 1993).

La Recomendación UIT-T X.800, Enmienda 1, ha sido preparada por la Comisión de Estudio 7 (1993-1996) del UIT-T y fue aprobada por el procedimiento de la Resolución N.º 1 de la CMNT el 5 de octubre de 1996.

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.

© UIT 1997

Es propiedad. Ninguna parte de esta publicación puede reproducirse o utilizarse, de ninguna forma o por ningún medio, sea éste electrónico o mecánico, de fotocopia o de microfilm, sin previa autorización escrita por parte de la UIT.

ÍNDICE

	<i>Página</i>
Anexo D – Servicios y mecanismos de seguridad de capa 2 de las redes de área local	1
D.0 <i>Introducción</i>	1
D.1 <i>Servicios de seguridad de las LAN</i>	1
D.2 <i>Mecanismos de seguridad de las LAN</i>	1
D.3 <i>Modificaciones del cuadro para tener en cuenta la seguridad de las LAN</i>	2

RESUMEN

La Recomendación X.800 da una visión general de los servicios de seguridad atribuidos a las siete capas del modelo de referencia de la interconexión de sistemas abiertos (OSI, *open systems interconnection*). La Enmienda 1, que se ha de publicar como Anexo D, amplía los servicios de seguridad de la capa de enlace de datos para tener en cuenta la seguridad de las redes de área local (LAN, *local area network*).

ARQUITECTURA DE SEGURIDAD PARA LA INTERCONEXIÓN DE SISTEMAS ABIERTOS PARA APLICACIONES DEL CCITT

Anexo D

Servicios y mecanismos de seguridad de capa 2 de las redes de área local

(Ginebra, 1996)

D.0 *Introducción*

Este anexo abarca los servicios y mecanismos de seguridad de capa 2 de las redes de área local (LAN, *local area network*).

La ilustración de la ubicación de los servicios de seguridad en el Cuadro 2 de la cláusula 7 hace pensar que sólo los servicios de confidencialidad deberían estar disponibles en la capa 2. Se reconoce, sin embargo, que en algunos entornos en los que existen redes de área local quizá se requieran servicios y mecanismos de seguridad de capa 2 adicionales. Por ejemplo, una organización puede no desarrollar la funcionalidad OSI plena o la incorporación de relevadores de capa 2 quizá requiera servicios de seguridad distintos de los de confidencialidad.

D.1 *Servicios de seguridad de las LAN*

La capa de enlace de datos puede proporcionar los siguientes servicios de seguridad de las LAN individualmente o combinados:

- a) autenticación de entidad par;
- b) autenticación del origen de los datos;
- c) servicio de control de acceso;
- d) confidencialidad en modo con conexión;
- e) confidencialidad en modo sin conexión;
- f) integridad en modo con conexión sin recuperación; y
- g) integridad en modo sin conexión.

D.2 *Mecanismos de seguridad de las LAN*

Los servicios de seguridad identificados se proporcionan como sigue:

- a) el servicio de autenticación de entidad par es proporcionado por una combinación apropiada de intercambios de autenticación o protegidos, mecanismos de intercambio derivados criptográficamente o protegidos, o por mecanismos protegidos de intercambio de contraseñas y firmas;
- b) el servicio de autenticación de origen de los datos puede proporcionarse por mecanismos de cifrado o de firma;
- c) el servicio de control de acceso se proporciona mediante el uso apropiado de mecanismos específicos de control de acceso;
- d) el servicio de confidencialidad en modo con conexión se proporciona mediante un mecanismo de cifrado;
- e) el servicio de confidencialidad en modo sin conexión se proporciona mediante un mecanismo de cifrado;
- f) el servicio de integridad en modo con conexión sin recuperación se proporciona utilizando un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado; y
- g) el servicio de integridad en modo sin conexión se proporciona utilizando un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado.

D.3 *Modificaciones del cuadro para tener en cuenta la seguridad de las LAN*

El Cuadro 2/X.800 no ha sido modificado, pero debería mostrar la leyenda S para la capa 2 (las LAN) para los siguientes servicios de seguridad:

- autenticación de la entidad par;
- autenticación del origen de los datos;
- servicio de control de acceso;
- integridad en modo con conexión sin recuperación; e
- integridad en modo sin conexión.

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	Transmisiones de señales radiofónicas, de televisión y de otras senales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Mantenimiento: 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 Z	Lenguajes de programación