(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 603 836**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.07.2004 PCT/IB2004/051130**

(87) Fecha y número de publicación internacional: **20.01.2005 WO05006706**

(96) Fecha de presentación y número de la solicitud europea: **06.07.2004 E 04744498 (9)**

(97) Fecha y número de publicación de la concesión europea: **31.08.2016 EP 1645100**

(54) Título: **Método de creación y de administración de una red local**

(30) Prioridad:

14.07.2003 CH 123303

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.03.2017

(73) Titular/es:

NAGRAVISION SA (100.0%)
22, ROUTE DE GENÈVE
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

MOREILLON, GUY

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método de creación y de administración de una red local

[0001] La presente invención se refiere al dominio de la creación y la administración de una red local, en particular una red local conectada a un punto de acceso en un flujo de datos con acceso condicional.

[0002] La gestión del acceso a datos sometidos a condiciones es ampliamente conocida y practicada desde hace mucho tiempo particularmente en el dominio de la televisión de pago.

[0003] El usuario dispone de un descodificador a cargo de descifrar el flujo cifrado gracias a claves ligadas a su abono o sus derechos.
Estas claves son habitualmente almacenadas en un módulo de seguridad preferiblemente desmontable para hacer evolucionar las funciones ofertadas así como la seguridad.

[0004] La mayoría de los descodificadores, una vez descifrado el flujo de datos, convierten estos datos en forma analógica para ser explotados por un órgano de visualización como una pantalla de televisión.

[0005] La llegada de las pantallas digitales ha alterado en cierto modo este esquema.
En efecto, la salida del descodificador hacia la pantalla siendo de tipo digital, esta salida puede ser utilizada de manera fraudulenta para efectuar copias ilícitas.

[0006] Por esta razón, antes de que las pantallas digitales, y más generalmente todos los aparatos que explotan estos datos en forma digital tales como los registradores digitales, se utilicen de forma masiva, se han propuesto soluciones con el fin de evitar la diseminación de datos con acceso condicional.

[0007] Por lo tanto se ha propuesto una protección completa de principio a fin del contenido y, por lo tanto, conservar en forma cifrada este contenido hasta el órgano de restitución (televisor, por ejemplo).

[0008] La fuente, tal como un descodificador o un lector de DVD, tratará el contenido cifrado y autorizará su acceso siempre y cuando las condiciones se cumplan (según el abono del usuario, por ejemplo).
El contenido, antes de ser enviado a la red local del usuario, se recifra según una clave propia para esta red con el fin de que sólo pueda ser accesible en esta red.
Todo uso fuera de esta red es imposible porque la clave es única por red doméstica.

[0009] La noción de red doméstica, aunque se define con respecto a un usuario, puede resultar confusa porque un vecino puede conectarse fácilmente a la misma red y disponer de la misma clave de red.
Por esta razón, la solución más sencilla es limitar el número de participantes en una red local.

[0010] Para que una tal red local protegida pueda ser utilizada, es necesario que cada dispositivo disponga de un módulo de seguridad que contendrá los secretos propios de esta red.
Estos módulos son en general en forma de una tarjeta inteligente desmontable o de módulos de seguridad directamente instalados en el aparato.

[0011] Según una primera solución conocida, esta noción de limitación ha sido realizada por la transmisión del carácter progenitor de la adhesión a la red.
Para la instalación de una red local, un primer módulo contiene o es capaz de generar la clave que servirá de punto común a esta red.
Una vez que este primer módulo ha generado la primera clave, se convierte en módulo progenitor y puede funcionar de manera solitaria.
En el momento de la aparición de otro módulo en este misma red, este carácter progenitor se transmite a este segundo módulo, permitiendo a este último pertenecer a la misma red.
El primer módulo pierde la facultad de progenitor y esta facultad se transfiere al segundo módulo.
Por supuesto, otros parámetros tales como el número de futuros módulos que participan en esta red es igualmente disminuido y almacenado en el nuevo módulo progenitor.

[0012] Esta capacidad progenitora que se desplaza responde a criterios de seguridad porque un módulo sólo puede introducir un único otro módulo en la misma red.
Sin embargo esta solución supone problemas porque la cadena se puede interrumpir por desconocimiento del principio si un usuario se separa de uno de sus elementos que justamente se había convertido en el módulo progenitor.
Además, si el aparato en el cual se encuentra este módulo fuera dañado, el usuario lo lleva de nuevo al punto de venta y

un intercambio con otro aparato provoca la interrupción de la posibilidad de extender esta red.

[0013] El documento WO01/67705 describe un sistema de transferencia protegida y de manipulación de datos en la red internet que comprende un módulo de transferencia y de encriptación de datos en una unidad de usuario, y un módulo de manipulación de datos en una unidad servidor.
La transferencia de datos se efectúa por un desplazamiento de los datos de una ventana mostrada en la pantalla asociada a la unidad de usuario de o hacia una ventana asociada a la unidad servidor.
Cada ventana está asociada a una contraseña de tal manera que el desplazamiento de los datos de una ventana a la otra comporta la encriptación o la re-encriptación de una contraseña asociada a la otra.
El sistema utiliza una encriptación con claves simétricas acoplada al protocolo de transferencia de ficheros y permite una transferencia protegida de ficheros de datos de gran tamaño iguales o superiores a 100 megaoctetos.
Esta transferencia de datos de la unidad servidor hacia la unidad de usuario o viceversa puede efectuarse un número ilimitado de veces independientemente de la red y del emplazamiento de las unidades sobre la red.

[0014] El documento EP 0 666 694 describe la transmisión de contenidos con acceso condicional y la difusión en una red regional.
El dispositivo en cabecera de red (headend) recibe el contenido, lo desencripta y lo reencripta para transmitirlo a los terminales conectados a esta red regional.
El dispositivo en cabecera de red puede igualmente encargarse del control de acceso y de la facturación.
El formato de reencriptación es diferente del formato de codificación original con el fin de minimizar los riesgos de ataques contra el contenido encriptado.

[0015] El objetivo de la presente invención es proponer un método de creación y de administración de una red local que permita paliar los inconvenientes descritos anteriormente.

[0016] Este objetivo se alcanza por un método de creación y de administración de una red local, esta red que comprende al menos un dispositivo de difusión y de recifrado de un flujo de datos cifrados y un dispositivo de restitución de todos o parte de dichos datos cifrados, estos dispositivos que incluyen módulos de seguridad, este método que comprende las etapas siguientes iniciales:

- conexión de un módulo de seguridad llamado maestro en un dispositivo de difusión y de recifrado o en un dispositivo de restitución conectado a la red local,
- establecimiento de una clave de red por dicho módulo de seguridad maestro,
- transmisión protegida de esta clave de red a uno o varios módulos de seguridad llamados de usuario,

y, en el momento de la recepción de un flujo de datos cifrados por un punto de acceso de la red,:

- recepción, por un dicho dispositivo de difusión y de recifrado, del flujo de datos cifrados;
- verificación, por el módulo de seguridad ligado a dicho dispositivo de difusión y de recifrado, de la existencia de derecho de acceso a dicho flujo de datos cifrados;
- en caso de existencia de los derechos, descifrado de los datos cifrados gracias a las informaciones proporcionadas por el módulo de seguridad asociado a este dispositivo de difusión y de recifrado;
- recifrado de los datos por dicho dispositivo de difusión y de recifrado por una clave local,
- transmisión de los datos recifrados por dicha clave local al dispositivo de restitución,
- descifrado por dicho dispositivo de restitución a través del módulo de seguridad de usuario que está asociado a él que dispone de medios para recuperar la clave local.

[0017] Un dispositivo de restitución es un dispositivo en el cual es imperativo que los datos estén descifrados para su uso, de manera sonora, visual u otra, tales como datos bursátiles o juegos.
El ejemplo más característico es un televisor.

[0018] Todas las otras etapas de desplazamiento de los datos se hacen sobre datos cifrados.

[0019] Una clave de sesión es una clave que se genera aleatoriamente y que es a continuación cifrada con la clave de red.
Los datos cifrados se acompañan por esta clave de sesión cifrada por la clave de red.
Así, el conocimiento de la clave de red permite obtener la clave de sesión y acceder a los datos.

[0020] Se puede naturalmente considerar utilizar directamente la clave de red y no transmitir más que los datos recifrados.
Para la continuación de la descripción, la clave local cubre las dos nociones, a saber la clave de sesión o la clave de red.

[0021] Para el cifrado de los datos existen dos principios.

El primero hace referencia al cifrado por la clave local del conjunto de los datos.
El módulo de seguridad llamado módulo convertidor dispone de los medios, si los derechos existen, para descifrar los datos y recifrarlos con la clave local.
Según la cantidad y el tamaño de los datos, las capacidades requeridas para esta operación pueden ser muy importantes.

[0022] Un segundo principio se basa en un fichero de claves, conocido con la denominación "palabras de control".
Los datos propiamente dichos no se modifican y permanecen cifrados por el conjunto de las claves, sólo el fichero de claves es descifrado por el módulo convertidor y recifrado por la clave local.

[0023] Debe destacarse que el conjunto de las claves se puede reducir a una clave por evento y tratada como se ha descrito anteriormente, es decir, que el mensaje que comprende esta clave es descifrado por el módulo convertidor y recifrado por la clave local.

[0024] Un dispositivo de difusión y de recifrado es, por ejemplo, un descodificador conectado a una red que proporciona datos con acceso condicional o un lector de datos cifrados como un lector DVD.

[0025] Este dispositivo verifica si el derecho existe para descifrar los datos antes de difundirlos en la red local.
Si este derecho existe, después de la etapa de descifrado, éstos son recifrados gracias a la clave local.

[0026] Al final, estos datos sólo podrán ser explotados en esta red.

[0027] Estos datos así recifrados pueden almacenarse en un disco duro o ser grabados en un DVD.
El interés de la red local reside en el hecho de que estos datos son inexplotables fuera de esta red local.
En el momento de la explotación de estos datos, el dispositivo de almacenamiento difundirá los datos en la red, estos datos comprendiendo una parte útil cifrada (audio y video, por ejemplo) y una parte de gestión que comprende la clave de sesión cifrada por la clave de red.

[0028] El módulo de seguridad maestro estará a cargo de iniciar cada módulo de seguridad de usuario que quiera formar parte de esta red.
Así, para el usuario parece claro que este primer módulo tiene una función particular y que es importante no perderlo.

[0029] Este módulo maestro contiene igualmente un contador que define el número máximo de módulos que se pueden inicializar y un certificado que prueba la pertenencia de este módulo al sistema de redes locales.

[0030] El problema de separarse de un aparato en el cual se encuentra el módulo maestro es, por lo tanto, resuelto.
Por razones prácticas, el módulo maestro tendrá una distinción visual respecto a los otros módulos.

[0031] El establecimiento de una clave de red se puede efectuar de dos maneras.
La primera es generar aleatoriamente esta clave en el momento de la primera inicialización de la red local.

[0032] La segunda consiste en utilizar una clave cargada durante un procedimiento de personalización del módulo maestro.
Las claves son, por lo tanto, conocidas por anticipado por la autoridad emisora.

[0033] El módulo maestro tiene como primera misión iniciar una red.
El módulo de usuario es un miembro pasivo de esta red y recibirá la clave de red establecida por el módulo maestro.
En la práctica, es posible integrar un módulo de usuario en el módulo físico que contiene el módulo maestro.
Esto permite actuar en una red con un solo módulo, la inicialización consistiendo en transferir la clave de red de la parte maestra a la parte usuario de un mismo módulo físico.

[0034] La invención se comprenderá mejor gracias a la descripción detallada siguiente y que se refiere al dibujo anexo que se da a modo de ejemplo en ningún caso limitativo, y que describe la configuración de una red local.

[0035] En la figura 1, la red local se identifica por LNT.
Ésta conecta los diferentes elementos conectados en una casa, por ejemplo.

[0036] Existen dos tipos de dispositivos, a saber los dispositivos de restituciones tal como un televisor DV1 y un ordenador DV2.
Los otros dispositivos son los dispositivos de difusión y de descifrado como un descodificador MD1 o un-lector de discos MD2.

[0037] El flujo de datos cifrados STE entra en el descodificador MD1 para ser tratado.
Este descodificador dispone de un módulo de seguridad CC1 que comprende los derechos ligados al contenido de los datos cifrados.
El módulo CC1 verifica los derechos para permitir el acceso a estos datos cifrados y, en el caso de transmisión de datos cifrados por palabras de control CW, descifra estas palabras de control y las recifra por la clave local.

[0038] Según el modo de funcionamiento, la clave local es una clave de sesión generada por el módulo convertidor MD1 y cifrada por la clave de red.
Esta etapa de cifrado de la clave local es efectuada no en el módulo convertidor MD1, sino en un módulo de usuario TC que sólo dispone de la clave de red.

[0039] Durante una etapa de inicialización, el módulo convertidor genera una clave de sesión aleatoria.
En colaboración con el descodificador, transmite una solicitud con el fin de determinar la presencia de una red local.
Un dispositivo de restitución reaccionará, por ejemplo el televisor DV1, y transmitirá la clave pública de su módulo de usuario TC1.

[0040] Esta clave servirá para cifrar la clave de sesión por el módulo convertidor MD1 y transmitir este conjunto cifrado al módulo de usuario del televisor.

[0041] El módulo de usuario TC1, gracias a su clave privada, descifrará este mensaje y extraerá la clave de sesión.
A continuación cifrará esta clave de sesión por la clave de red y transmitirá este nuevo mensaje al módulo convertidor.

[0042] Cuando el módulo convertidor recibe un mensaje que comprende una palabra de control proveniente del flujo de datos STE con acceso condicional, verifica los derechos contenidos en este mensaje y, si los derechos están presentes, descifra la contraseña de control y la recifra por la clave de sesión.
El nuevo mensaje contendrá la contraseña de control recifrada por la clave de sesión y la clave de sesión cifrada por la clave de red.

[0043] El funcionamiento de un dispositivo como un lector de DVD es sustancialmente similar.
Este dispositivo comprende igualmente un módulo convertidor CC2 que dispone de los medios para acceder a los datos cifrados contenidos en el disco.

[0044] Para nuestro ejemplo, se considerará que los datos son cifrados por una clave propia para este contenido según un algoritmo y/o una clave contenida en el módulo convertidor.

[0045] Este módulo convertidor CC2 verifica si el titular del módulo dispone del derecho para descifrar y difundir el disco CDE en una red local.
Si el derecho existe, puede haber dos posibilidades:

- el módulo convertidor CC2 descifra el contenido del disco y recifra por la clave de red, los datos recifrados y la clave de red siendo transmitida al dispositivo de restitución,
- el módulo convertidor se contenta con cifrar la clave del disco por la clave de red y transmitir los datos iniciales y la clave de disco cifrado por la clave de red. Este método implica que la clave de disco sea propia para cada contenido; en el caso inverso, el acceso a un contenido abre la posibilidad de acceder a todos los contenidos.

[0046] Según uno de los aspectos de la invención, el módulo maestro MC se encuentra en el televisor DV1.
Este módulo maestro ha permitido la generación de una red local y dispone de la clave de red NK.
En una forma de realización, este módulo comprende igualmente las funcionalidades de un módulo de usuario y puede, por lo tanto, descifrar los datos cifrados transmitidos por un dispositivo como el descodificador MD1.

[0047] En el momento de la conexión de un segundo módulo de usuario TC2 virgen conectado aquí en un ordenador DV2, una comunicación se establece entre el módulo maestro MC y este módulo virgen.
Después de la autentificación mutua, el módulo maestro transmite la clave de red NK al módulo de usuario TC2 que tiene, de ahí en adelante, la posibilidad de recibir y de descifrar los datos para esta red local.
De aquí en adelante, ya no necesita la presencia de la clave maestra MC para acceder a los datos cifrados por la clave local porque dispone de la clave de red NK.

[0048] El principio básico para calificar una red local es el número de módulos de usuario posibles.
Esta función está dedicada al módulo maestro que disminuye su contador siempre que un módulo de usuario recibe la clave de red.

[0049] Si se desea diferenciar claramente la función de creación de red y la función de acceso a los datos cifrados, es posible incluir en el módulo maestro MC sólo la función de gestor de red.
Después de haber inicializado el módulo de usuario TC2, se retira el módulo maestro MC para introducir un módulo de usuario TC1 previamente configurado.

[0050] La invención se extiende igualmente a un método de verificación de la conformidad de URL de red local.
Durante la negociación entre un módulo terminal TC y un módulo convertidor CC, el módulo terminal transmite informaciones propias al módulo maestro MC en la base de la formación de esta red.
Puede tratarse de un identificador, de una firma o de un certificado (X509, por ejemplo).

[0051] Por el hecho de que solos los módulos maestros MC pueden generar una red local, únicamente interesa este tipo de módulo cuyo número es bastante inferior al número de módulos de usuario en servicio.

[0052] El módulo convertidor CC almacenará esta información que nosotros llamaremos identificador de red local.

[0053] En el caso de un descodificador de televisión, de pago, es llevado a conectarse a un centro de gestión para actualizaciones, por razones de estadística o para la facturación del consumo local.

[0054] En esta ocasión, el módulo convertidor CC transmite, con los datos usuales, el identificador de red local conectado a este descodificador.

[0055] El centro de gestión dispone de una lista de identificadores de redes locales no autorizados a recibir datos descifrados por un módulo convertidor y comunica a dicho módulo esta información.

[0056] El módulo convertidor puede de ahí en adelante aceptar o rechazar funcionar con tal red.

[0057] Se debe señalar que un módulo convertidor puede ser llevado a interactuar con varias redes locales, si por ejemplo, un tercero conectara su módulo terminal en el televisor DV1.
En esta configuración, el módulo convertidor puede conservar en su memoria varios identificadores de red.

[0058] En una forma de realización, los datos cifrados, en particular los mensajes que contienen la o las claves de descifrado, pueden contener condiciones para que una tal verificación sea obligatoria y previa a todo recifrado para una red local dada.

[0059] El descodificador, por lo tanto, ejecutará una operación de verificación con el fin de validar el identificador de la red local que está conectada a él.
Si durante la negociación de la clave local otro identificador de red es anunciado, no permitirá el descifrado de las palabras de control hacia la red local.

[0060] Así, es posible introducir condiciones en los datos cifrados o las claves que los acompañan para definir un nivel de seguridad

[0061] Se debe señalar que la forma de aplicación de la invención se presta particularmente bien a dispositivos de restitución que disponen de módulo de seguridad directamente instalado sobre el circuito impreso.
Este módulo, en forma de un circuito electrónico (eventualmente soldado), comprenderá todas las funcionalidades de un módulo de seguridad de usuario.
Solo el módulo maestro será desmontable y estará conectado únicamente con el fin de iniciar la red y por lo tanto de cargar la clave de red en este circuito electrónico.
Si este dispositivo debe unirse a otra red, basta autorizar el borrado de la pertenencia a la red precedente y autorizar la unión a la nueva red.

[0062] Para una reutilización de los datos que habrían sido almacenados y cifrados por la clave de red, siempre queda el módulo maestro que desempeña entonces la función de módulo de usuario con su propia clave de red.

REIVINDICACIONES

1. Método de creación y de administración de una red local, esta red que comprende al menos un dispositivo de difusión y de recifrado de un flujo de datos cifrados y un dispositivo de restitución de todos o parte de dichos datos cifrados, estos dispositivos comprendiendo módulos de seguridad, este método comprendiendo las etapas siguientes iniciales:

- conexión de un módulo de seguridad llamado maestro en un dispositivo de difusión y de recifrado o en un dispositivo de restitución conectado a la red local,
- establecimiento de una clave de red por dicho módulo de seguridad maestro.
- transmisión protegida de esta clave de red a uno o varios módulos de seguridad llamados usuario,

y durante la recepción de un flujo de datos cifrados por un punto de acceso de la red:

- recepción por un dicho dispositivo de difusión y de recifrado del flujo de datos cifrados;
- verificación por el módulo de seguridad ligado a dicho dispositivo de difusión y de recifrado de la existencia de derecho de acceso a dicho flujo de datos cifrados;
- en caso de existencia de los derechos, descifrado de los datos cifrados gracias a las informaciones proporcionadas por el módulo de seguridad asociado a este dispositivo de difusión y de recifrado;
- recifrado de los datos por dicho dispositivo de difusión y de recifrado por una clave local,
- transmisión de los datos recifrados por dicha clave local al dispositivo de restitución,
- descifrado por dicho dispositivo de restitución a través del módulo de seguridad de usuario que está asociado a él que dispone medios para recuperar la clave local.

2. Método de creación y de administración de una red local según la reivindicación 1, **caracterizado por el hecho de que** dichos datos tienen una parte útil cifrada por una parte y una parte de gestión a cargo del control del descifrado de esta parte útil cifrada por otra parte; y por el hecho de que las etapas de descifrado y de recifrado de los datos se aplican a la parte útil.

3. Método de creación y de administración de una red local según la reivindicación 1, **caracterizado por el hecho de que** dichos datos tienen una parte útil cifrada por una parte y una parte de gestión a cargo del control del descifrado de esta parte útil cifrada por otra parte, y por el hecho de que las etapas de descifrado y de recifrado de los datos se aplican a la parte de gestión.

4. Método de creación y de administración de una red local según la reivindicación 1, **caracterizado por el hecho de que** la clave local es una clave de sesión generada aleatoriamente y cifrada por la clave de red.

5. Método de creación y de administración de una red local según la reivindicación 1, **caracterizado por el hecho de que** la clave local es la clave de red.

6. Método de creación y de administración de una red local según la reivindicación 1, **caracterizado por el hecho de que** el establecimiento de la clave de red se obtiene por generación pseudoaleatoria de una clave durante la inicialización de la red local.

7. Método de creación y de administración de una red local según la reivindicación 1, **caracterizado por el hecho de que** el establecimiento de la clave de red se efectúa durante una etapa de inicialización del módulo maestro.

8. Método de creación y de administración de una red local según la reivindicación 1, **caracterizado por el hecho de que** el módulo maestro se localiza en un módulo de seguridad desmontable.

9. Método de creación y de administración de una red local según la reivindicación 7, **caracterizado por el hecho de que** este módulo de seguridad desmontable comprende un módulo de usuario que forma parte de la red administrada por el módulo maestro.

10. Método de creación y de administración de una red local según la reivindicación 1, **caracterizado por el hecho de que** los módulos de seguridad de usuario son en forma de un circuito electrónico instalado durante la fabricación del dispositivo de restitución.

11. Método de creación y de administración de una red local según la reivindicación 1, **caracterizado por el hecho de que** el módulo de seguridad de usuario es en forma de un módulo de seguridad desmontable.

12. Método de creación y de administración de una red local según la reivindicación 1, **caracterizado por el hecho de que** el dispositivo de difusión y de recifrado comprende un módulo de seguridad llamado módulo convertidor, este módulo que recibe y conserva un identificador del módulo maestro que ha creado la red para la cual el módulo convertidor recifra los datos.

13. Método de creación y de administración de una red local según la reivindicación 10, **caracterizado por el hecho de que** este identificador del módulo maestro se transmite a un centro de gestión durante una fase de conexión con dicho centro de gestión.

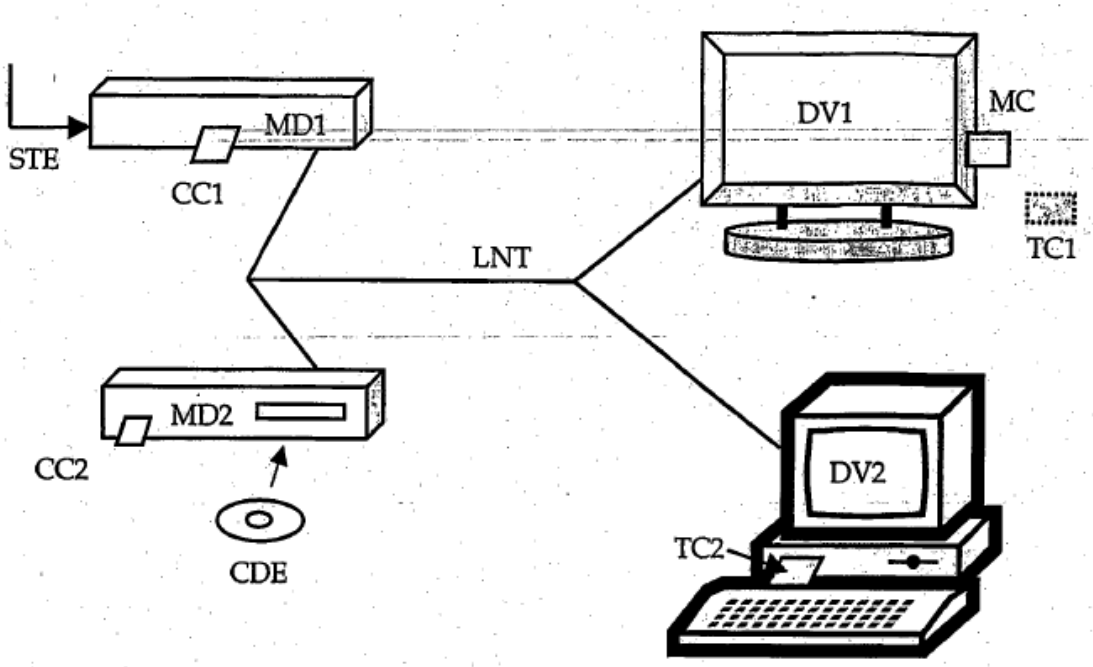

Fig. 1