(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 667 530**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/00 (2006.01)
H04L 29/06 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.02.2006 PCT/CN2006/000248**

(87) Fecha y número de publicación internacional: **24.08.2006 WO06086931**

(96) Fecha de presentación y número de la solicitud europea: **21.02.2006 E 06705669 (7)**

(97) Fecha y número de publicación de la concesión europea: **04.04.2018 EP 1858195**

(54) Título: **Método de control de acceso entre iguales basado en puertos**

(30) Prioridad:

21.02.2005 CN 200510041713

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.05.2018

(73) Titular/es:

CHINA IWNCOMM CO., LTD (100.0%)
A201, Qinfeng Ge Xi'an Software Park No. 68 Keji 2nd Road Xi'an High-Tech Industry Dev. Zone
Xi'an
Shaanxi 710075, CN

(72) Inventor/es:

LAI, XIAOLONG;
CAO, JUN;
ZHANG, BIANLING;
HUANG, ZHENHAI y
GUO, HONG

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Método de control de acceso entre iguales basado en puertos

Campo de la invención

La presente invención se refiere a una técnica de red, en particular a un método de control de acceso de iguales basado en puerto.

Antecedentes

El control de acceso a red implica en general tres sistemas: usuario, punto de acceso y servidor de fondo que controla de forma central tanto el usuario como el punto de acceso. IEEE 802.1x se denomina protocolo de control de acceso a red basado en puerto. En las redes de cable de la técnica anterior, además del tradicional método de control de acceso a navegador web y protocolo punto a punto por Ethernet, los métodos de acceso emergentes se basan en la técnica de IEEE 802.1x. La técnica de IEEE 802.1x tiene ventajas como la separación de control y servicio, alta flexibilidad, fuerte adaptabilidad, y ha tenido amplio uso en varias redes. La técnica de IEEE 802.1x ha sido adoptada por varias redes inalámbricas, tal como LAN inalámbrica (IEEE 802.11, MAN inalámbrica (IEEE 802.16e), etc.

La autenticación es la clave del control de acceso a red, cuya finalidad es establecer confianza, que es la base de la provisión del servicio de red, entre el usuario y el punto de acceso. Se necesita un mecanismo de seguridad para habilitar la autenticación mutua entre la red y el usuario ya se use acceso a red de cable o acceso a red inalámbrica.

IEEE 802.1X es un método que implementa la autenticación en la capa de enlace, y es una técnica basada en puerto. Un puerto de sistema proporciona un método por el que el sistema es habilitado para acceder a los servicios de otros sistemas y proporcionar servicios a otros sistemas.

IEEE 802.1X define tres tipos de entidades:

Autenticador: la entidad de control de puerto de un sistema autentica y autoriza al solicitante antes de que se permita el acceso a los servicios proporcionados por el sistema. El sistema se denomina un sistema de autenticador; su entidad de control de puerto se denomina un autenticador.

Solicitante: un sistema que pide acceso a los servicios proporcionados por un sistema de autenticador se denomina un sistema solicitante, cuya entidad de control de puerto se denomina solicitante.

Servidor de autenticación: un servidor de autenticación es la entidad que representa al autenticador para identificar la cualificación del solicitante, determina si el sistema solicitante puede ser autorizado para que acceda a los servicios proporcionados por el autenticador. Como se expone en IEEE 802.1X-2004, cláusula 6.3, el servidor de autenticación realiza la función de autenticación necesaria para comprobar las credenciales del solicitante en nombre del autenticador e indica si el solicitante está autorizado para acceder al servicio del autenticador.

Un sistema de autenticador tiene dos puntos de acceso al medio de transmisión. Un punto de acceso se denomina puerto controlado, que tiene dos estados: autenticado y no autenticado, y permite el paso de paquetes solamente cuando está en el estado autenticado; el otro punto de acceso se llama puerto no controlado, que permite el paso de paquetes independientemente de su estado.

La relación entre las entidades funcionales de IEEE 802.1X se representa en la figura 1.

IEEE 802.1X proporciona solamente una estructura para autenticación, que se usa en combinación con el protocolo de autenticación extensible para proporcionar autenticación y negociación de clave en la práctica. IEEE 802.1X tiene una estructura asimétrica, la funcionalidad difiere en gran medida en el solicitante y el autenticador. No hay función de autenticación en el autenticador. Por lo tanto, la autenticación se realiza entre el solicitante y el servidor de autenticación. Aunque el servidor de autenticación y el autenticador pueden implementarse en un solo sistema, la ventaja de IEEE 802.1X, es decir, el control central por el autenticador, se reduciría en gran medida. Actualmente es práctica común que el servidor de autenticación y el autenticador se implementen en sistemas separados. En IEEE 802.1X-2004, cláusula 6.3, nota 3, se expone que, aunque es posible la posición conjunta del servidor de autenticación con un autenticador, la implementación más común de este mecanismo implicará probablemente el uso de un servidor de autenticación que sea externo a los sistemas que contienen los autenticadores.

Durante la autenticación, el servidor de autenticación pasa directamente el resultado de la autenticación al autenticador. Si también se requiere negociación de clave, deberá realizarse entre el servidor de autenticación y el solicitante, y luego la clave negociada es enviada por el servidor de autenticación al solicitante, el solicitante y el

autenticador realizan autenticación y negociación de clave en base a clave compartida dinámica. Por lo tanto, las desventajas de IEEE 802.1X son las siguientes:

1. La estructura de IEEE 802.1X es asimétrica, la funcionalidad difiere en gran medida en el solicitante y el autenticador. El autenticador no tiene función de autenticación, que se realiza entre el solicitante y el servidor de autenticación. Aunque el servidor de autenticación y el autenticador pueden implementarse en un solo sistema, la ventaja de IEEE 802.1X, es decir, el control central por el autenticador, se reduciría en gran medida.

2. Pobre extensibilidad. Hay un canal de seguridad predefinido entre cada autenticador y el servidor de autenticación. Los recursos requeridos del sistema del servidor de autenticación aumentan y la gestión es más compleja con el número creciente de canales de seguridad, de modo que no es adecuado configurar un lote de canales de seguridad, la escalabilidad de red es limitada.

3. Proceso complicado de negociación de clave. La clave se usa para protección de datos entre el solicitante y el autenticador, pero es necesario que la negociación se realice en primer lugar entre el solicitante y el servidor de autenticación antes de que pueda realizarse entre el solicitante y el autenticador.

4. Se introducen nuevos puntos de ataque de modo que la seguridad disminuye. El servidor de autenticación pasa al autenticador la clave primaria negociada por el solicitante y el servidor de autenticación. Pasando la clave por la red se introducen nuevos puntos de ataque a la seguridad.

5. El autenticador no tiene identidad independiente. Con respecto al solicitante, la identidad de los autenticadores gestionada por el mismo servidor de autenticación no es distinguible. Hay que añadir entidades funcionales adicionales en entornos de aplicación cuando hay que distinguir los autenticadores, lo que introduce complejidad adicional.

Contenido de la invención

El objeto de la invención es superar los defectos existentes en la técnica anterior, proporcionar un método de control de acceso de iguales cambiando la estructura asimétrica de la técnica anterior. El método de la invención puede satisfacer los requisitos de gestión central, así como resolver los problemas técnicos del método de control de acceso a red de la técnica anterior, incluyendo un proceso complicado, pobre seguridad, pobre escalabilidad, de modo que proporciona una garantía esencial para la seguridad del acceso a red.

La solución técnica de la invención es un método de control de acceso de iguales basado en puerto, que incluye:

1) Iniciar entidades de control de autenticación, donde cada uno de dos sistemas incluye una entidad de control de autenticación, donde la respectiva entidad de control de autenticación de cada sistema es iniciada en primer lugar cuando los dos sistemas han de comunicar; cada dicha entidad de control de autenticación tiene una identidad única para autenticación, e incluye un subsistema de autenticación y dos puntos de acceso o puertos que conectan el subsistema de autenticación y el medio de transmisión; dichos dos puntos de acceso o puertos incluyen un puerto controlado y un puerto no controlado; cada dicho subsistema de autenticación incluye la función de implementación de autenticación y control de puerto, dicho subsistema de autenticación está conectado al puerto no controlado, el cambio del estado del puerto controlado es controlado por el subsistema de autenticación;

2) Dos entidades de control de autenticación se autentican una a otra, donde las dos entidades de control de autenticación comunican a través de los puertos no controlados, y sus subsistemas de autenticación se autentican uno a otro, los subsistemas de autenticación realizan la función de autenticación por sí mismos, o conjuntamente con una entidad servidora de autenticación que proporciona la información necesaria para autenticación a los subsistemas de autenticación;

3) Establecimiento del estado del puerto controlado, donde, si la autenticación es exitosa, el subsistema de autenticación pone el estado del puerto controlado como autenticado; de otro modo, el subsistema pone el estado del puerto controlado como no autenticado, el puerto controlado todavía permanece abierto.

El método anterior puede incluir además:

Habilitar la entidad servidora de autenticación: el usuario y el punto de acceso habilitan en primer lugar la entidad de control de autenticación y la entidad servidora de autenticación, mientras han de comunicar; dicha entidad servidora de autenticación guarda la información de gestión de seguridad relacionada con la entidad de control de autenticación; dicha entidad servidora de autenticación está conectada al subsistema de autenticación de dicha entidad de control de autenticación, la entidad servidora de autenticación comunica la información de gestión de seguridad con el subsistema de autenticación de la entidad de control de autenticación, para proporcionar la información necesaria para autenticación; dicho subsistema de autenticación completa el proceso de autenticación con o sin la asistencia de la entidad servidora de autenticación, o completa la negociación de clave por sí mismo.

La entidad servidora de autenticación anterior guarda la información de atributos de la entidad de control de autenticación, y transmite tal información de atributos a la entidad de control de autenticación.

El método anterior puede incluir además:

Dos subsistemas de autenticación que negocian la clave: dicho subsistema de autenticación incluye la función de negociación de clave, la negociación de clave puede ser realizada durante o después del proceso de autenticación mientras dichas dos entidades de control de autenticación se autentica una a otra; si la negociación de clave se ha de hacer independientemente después de terminar la autenticación, la harían las dos entidades de control de autenticación propiamente dichas.

Si la negociación de clave anterior se completa simultáneamente con la autenticación durante el proceso de autenticación, el subsistema de autenticación puede completar el proceso de negociación de clave con la asistencia de la entidad servidora de autenticación, o completar la negociación de clave por sí mismo.

La entidad servidora de autenticación anterior guarda la información de atributos de la entidad de control de autenticación, y transmite tal información de atributos a la entidad de control de autenticación.

El método anterior puede incluir además:

Poner el estado del puerto controlado: después de que la autenticación y el proceso de negociación de clave finalizan satisfactoriamente, el subsistema de autenticación pone el estado del puerto controlado como autenticado, el estado del puerto controlado cambia de abierto a cerrado, permitiendo el paso de paquetes; si la autenticación y el proceso de negociación de clave no son exitosos, el subsistema de autenticación pone el estado del puerto controlado como no autenticado, el puerto controlado todavía permanece abierto.

La entidad de control de autenticación anterior y la entidad servidora de autenticación pueden implementarse en un solo sistema o en sistemas separados; dicho solo sistema puede incluir una o varias entidades de control de autenticación.

Las ventajas de la invención son las siguientes:

1. Control de iguales. El método de la presente invención tiene dos sistemas (generalmente uno es el usuario y el otro es el punto de acceso) que incluyen una entidad de control de autenticación, de modo que los dos sistemas pueden autenticar directamente, es decir, iguales, para proporcionar un soporte más potente de la función de autenticación.

2. Las entidades de control de autenticación son distinguibles. La entidad de control de autenticación tiene identidad independiente, y no está simplemente bajo el control del servidor de autenticación. La identidad independiente de la entidad de control de autenticación permite no depender de la entidad servidora de autenticación esencialmente, y así la entidad de control de autenticación propiamente dicha puede distinguirse.

3. Buena extensibilidad. No hay ningún canal de seguridad predefinido existente entre la entidad de control de autenticación y la entidad servidora de autenticación, y así se facilita el control central por la entidad servidora de autenticación para las entidades de control de autenticación y se puede lograr buena extensibilidad.

4. Buena seguridad. La entidad de control de autenticación puede negociar directamente la clave con otras entidades de control de autenticación, y así recupera el carácter directo de la negociación de clave, simplifica la implementación de red, y mejora la seguridad.

5. Proceso simple de negociación de clave. La entidad de control de autenticación puede negociar directamente la clave con otras entidades de control de autenticación, reduciendo así la complejidad y mejorando la eficiencia de la negociación de clave.

6. Sistema relativamente completo. La entidad servidora de autenticación es el gestor de seguridad de la entidad de control de autenticación, e incluye la función de gestión de clave de la técnica de autenticación. Las entidades de la invención forman conjuntamente un sistema seguro completo, y completan independientemente las funciones de autenticación y negociación de clave.

7. Alta flexibilidad. Las entidades servidoras de autenticación pueden proporcionar un lote de funciones adicionales para lograr alta flexibilidad.

8. Implementación flexible. No hay que implementar las entidades funcionales definidas por la invención en diferentes sistemas de red, un sistema de red puede implementar una o varias entidades funcionales. Como se representa en la figura 3, la entidad de control de autenticación y la entidad servidora de autenticación pueden

implementarse en el mismo sistema de red. Mientras tanto, no es preciso que una entidad servidora de autenticación corresponda a una entidad de control de autenticación, mientras que una entidad servidora de autenticación puede corresponder y gestionar un número de entidades de control de autenticación. Como se representa en la figura 4, la entidad de control de autenticación 1 comunica con la entidad servidora de autenticación a través del puerto no controlado de la entidad de control de autenticación 2.

Descripción de los dibujos

La figura 1 es el diagrama para la relación de conexión entre las entidades funcionales de IEEE 802.1X.

La figura 2 es el diagrama para la relación de conexión entre las entidades funcionales de la invención.

La figura 3 es el diagrama esquemático de una realización en la que la entidad servidora de autenticación y la entidad de control de autenticación se implementan en un solo sistema.

La figura 4 es el diagrama esquemático de una realización en el que una entidad servidora de autenticación corresponde a un número de entidades de control de autenticación.

Realizaciones

La invención incluye las dos entidades siguientes:

1) Entidad de control de autenticación:

La entidad de control de autenticación incluye dos puertos conectados al medio de transmisión. Un puerto se denomina el puerto controlado, que tiene dos estados: el estado autenticado y el estado no autenticado. Permite el paso de paquetes solamente si está en el estado autenticado. El otro puerto se llama puerto no controlado, que siempre permite el paso de paquetes independientemente de su estado. El puerto controlado y el puerto no controlado de la entidad de control de autenticación reciben simultáneamente los paquetes del medio de transmisión subyacente.

La entidad de control de autenticación incluye un subsistema de autenticación, que implementa las funciones de seguridad, incluyendo funciones de seguridad tales como autenticación, negociación de clave, así como funciones de control de puerto. El subsistema de autenticación está conectado al puerto no controlado, el cambio de estado del puerto controlado es controlado por el subsistema de autenticación.

La entidad de control de autenticación tiene una identidad única para autenticación, y así puede implementar la función de autenticación independientemente.

2) Entidad servidora de autenticación:

La entidad servidora de autenticación guarda la información de gestión de seguridad relacionada con la entidad de control de autenticación, y conecta con el subsistema de autenticación de la entidad de control de autenticación. Mientras la entidad de control de autenticación y otras entidades de control de autenticación están autenticando, la entidad servidora de autenticación comunica la información de gestión de seguridad con el subsistema de autenticación de la entidad de control de autenticación para proporcionar la información necesaria para autenticación, pero la entidad servidora de autenticación no completa la autenticación que presenta a la entidad de control de autenticación. La entidad servidora de autenticación también guarda la información de atributos de la entidad de control de autenticación, y transmite la información de atributos a la entidad de control de autenticación según los requisitos de aplicación.

La relación entre la entidad de control de autenticación y la entidad servidora de autenticación se ilustra en la figura 2.

Un proceso del método de control de acceso de iguales de la invención incluye:

1) Iniciar la entidad de control de autenticación: el usuario y el punto de acceso deben iniciar en primer lugar la entidad de control de autenticación cuando han de comunicar.

2) Dos entidades de control de autenticación se autentican una a otra: dos entidades de control de autenticación comunican a través del puerto no controlado, sus subsistemas de autenticación se autentican uno a otro. El subsistema de autenticación puede completar el proceso de autenticación por sí mismo, sin la asistencia de la entidad servidora de autenticación.

3) Dos entidades de control de autenticación negocian la clave: si dos entidades de control de autenticación tienen que negociar la clave, la negociación de clave puede completarse simultáneamente con la autenticación en el proceso de autenticación, o puede realizarse independientemente después de finalizar el proceso de autenticación. Si la negociación de clave se ha de realizar independientemente después de finalizar la autenticación, la negociación de clave la completarían independientemente las dos entidades de control de autenticación, sin necesidad de implicar a la entidad servidora de autenticación.

4) Poner el estado del puerto controlado: si la autenticación y la negociación de clave son exitosas, el subsistema de autenticación pone el estado del puerto controlado como autenticado, el estado del puerto controlado pasa de abierto a cerrado, permitiendo el paso de paquetes; o en otro caso, el subsistema de autenticación pone el estado del puerto controlado como no autenticado, el puerto controlado todavía permanece abierto.

Otro proceso del método de control de acceso de iguales de la invención incluye:

1) Iniciar la entidad de control de autenticación y la entidad servidora de autenticación: tanto el usuario como el punto de acceso deben iniciar en primer lugar la entidad de control de autenticación y la entidad servidora de autenticación antes de que hayan de comunicar.

2) Dos entidades de control de autenticación se autentican una a otra: dos entidades de control de autenticación comunican a través del puerto no controlado, sus subsistemas de autenticación se autentican uno a otro. El subsistema de autenticación puede completar el proceso de autenticación con la asistencia de la entidad servidora de autenticación, o completar el proceso de autenticación por sí mismo.

3) Dos entidades de control de autenticación negocian la clave: si dos entidades de control de autenticación tienen que negociar la clave, la negociación de clave puede completarse simultáneamente con la autenticación en el proceso de autenticación, o puede realizarse independientemente después del proceso de autenticación. Si la negociación de clave se ha de realizar independientemente después de finalizar la autenticación, la negociación de clave la completarían independientemente las dos entidades de control de autenticación, sin necesidad de implicar a la entidad servidora de autenticación.

4) Establecimiento del estado del puerto controlado: si la autenticación y la negociación de clave son exitosas, el subsistema de autenticación pone el estado del puerto controlado como autenticado, el estado del puerto controlado pasa de abierto a cerrado, permitiendo el paso de paquetes; de otro modo, el subsistema de autenticación pone el estado del puerto controlado como no autenticado, el puerto controlado todavía permanece abierto.

La relación entre la entidad de control de autenticación y la entidad servidora de autenticación se representa en la figura 2.

El principio de la invención es el siguiente:

Teniendo tanto el usuario como el punto de acceso como un sistema e incluyendo ambos una entidad de control de autenticación, el usuario y el punto de acceso pueden autenticar directamente, es decir, control de acceso de iguales, proporcionando un soporte más potente para la función de autenticación. La entidad de control de autenticación tiene identidad independiente, y no está simplemente bajo el control de la entidad servidora de autenticación. La identidad independiente de la entidad de control de autenticación permite no depender esencialmente de la entidad servidora de autenticación, y así la entidad de control de autenticación propiamente dicha es distinguible. La entidad de control de autenticación puede negociar directamente la clave con otras entidades de control de autenticación, y así recupera el carácter directo de la negociación de clave. La entidad servidora de autenticación es el gestor de seguridad de la entidad de control de autenticación, e incluye la función de gestión de clave de la técnica de autenticación. Las entidades de la invención forman conjuntamente un sistema seguro completo, y completan independientemente las funciones de autenticación y negociación de clave.

En la práctica, tanto el usuario como el punto de acceso logran autenticación a través de la entidad de control de autenticación en el control de acceso a red.

El glosario técnico usado en la invención es el siguiente:

IEEE 802.1X: Protocolo de control de acceso a red basado en puerto

PPPoE: Protocolo punto a punto por Ethernet

IEEE 802.11: LAN inalámbrica

IEEE 802.16e: MAN inalámbrica

Autenticador

Solicitante

Servidor de autenticación

EAP - Protocolo de autenticación extensible

REIVINDICACIONES

1. Un método de control de acceso de iguales basado en puerto **se caracteriza porque** dicho método incluye:

1) Iniciar entidades de control de autenticación, donde cada uno de dos sistemas incluye una entidad de control de autenticación, donde la respectiva entidad de control de autenticación de cada sistema es iniciada en primer lugar cuando los dos sistemas han de comunicar; cada entidad de control de autenticación tiene una identidad única para autenticación, e incluye un subsistema de autenticación, así como dos puertos incluyendo un puerto controlado y otro no controlado que conectan el subsistema de autenticación y un medio de transmisión; cada dicho subsistema de autenticación incluye la función de implementación de autenticación y control de puerto, dicho subsistema de autenticación está conectado al puerto no controlado, el cambio de estado del puerto controlado es controlado por el subsistema de autenticación;

2) Dos entidades de control de autenticación se autentican una a otra, donde las dos entidades de control de autenticación comunican a través de los puertos no controlados, y sus subsistemas de autenticación se autentican uno a otro, los subsistemas de autenticación realizan la función de autenticación por sí mismos, o conjuntamente con una entidad servidora de autenticación que proporciona información necesaria para la autenticación a los subsistemas de autenticación;

3) Establecer el estado del puerto controlado, donde, si la autenticación es exitosa, el subsistema de autenticación pone el estado del puerto controlado como autenticado; de otro modo, el subsistema pone el estado del puerto controlado como no autenticado, el puerto controlado todavía permanece abierto.

2. El método de control de acceso de iguales basado en puerto según la reivindicación 1 **se caracteriza porque** dicho método incluye dos entidades de control de autenticación que negocian la clave, donde dicho subsistema de autenticación incluye la función de negociación de clave, cuando dichas dos entidades de control de autenticación se autentican una a otra, la negociación de clave puede ser completada durante o después del proceso de autenticación; si la negociación de clave se ha de realizar independientemente después de finalizar la autenticación, la negociación de clave la completarían independientemente las dos entidades de control de autenticación.

3. El método de control de acceso de iguales basado en puerto según la reivindicación 2 **se caracteriza porque**, mientras se completa dicha negociación de clave simultáneamente con la autenticación en el proceso de autenticación, el subsistema de autenticación puede completar el proceso de negociación de clave con o sin la asistencia de la entidad servidora de autenticación, o completar el proceso de autenticación por sí mismo.

4. El método de control de acceso de iguales basado en puerto según la reivindicación 1 **se caracteriza porque** dicha entidad servidora de autenticación guarda la información de atributos de la entidad de control de autenticación, y transfiere dicha información de atributos a la entidad de control de autenticación.

5. El método de control de acceso de iguales basado en puerto según la reivindicación 1 **se caracteriza porque** dicho paso de poner el estado del puerto controlado es como sigue: cuando la autenticación es exitosa, el subsistema de autenticación pone el estado del puerto controlado como autenticado, mientras que el estado del puerto controlado se cambia de abierto a cerrado con el fin de permitir el paso de paquetes de datos; de otro modo, dicho subsistema de autenticación pone el puerto controlado como no autenticado, entonces el puerto controlado permanece abierto.

6. El método de control de acceso de iguales basado en puerto según la reivindicación 2 **se caracteriza porque** dicho paso de establecimiento del estado del puerto controlado es como sigue: dicha entidad servidora de autenticación guarda la información de atributos de la entidad de control de autenticación, y transfiere dicha información de atributos a la entidad de control de autenticación.

7. El método de control de acceso de iguales basado en puerto según la reivindicación 2 **se caracteriza porque** dicho método incluye establecer el estado del puerto controlado, donde, si la autenticación y la negociación de clave son exitosas, el subsistema de autenticación pone el estado del puerto controlado como autenticado, el estado del puerto controlado pasa de abierto a cerrado, permitiendo el paso de paquetes; o, en otro caso, el subsistema de autenticación pone el estado del puerto controlado como no autenticado, el puerto controlado todavía permanece abierto.

8. El método de control de acceso de iguales basado en puerto según la reivindicación 1 **se caracteriza porque**: dicha entidad de control de autenticación y la entidad servidora de autenticación pueden implementarse en un único sistema o en sistemas separados; dicho único sistema puede incluir una o varias entidades de control de autenticación.

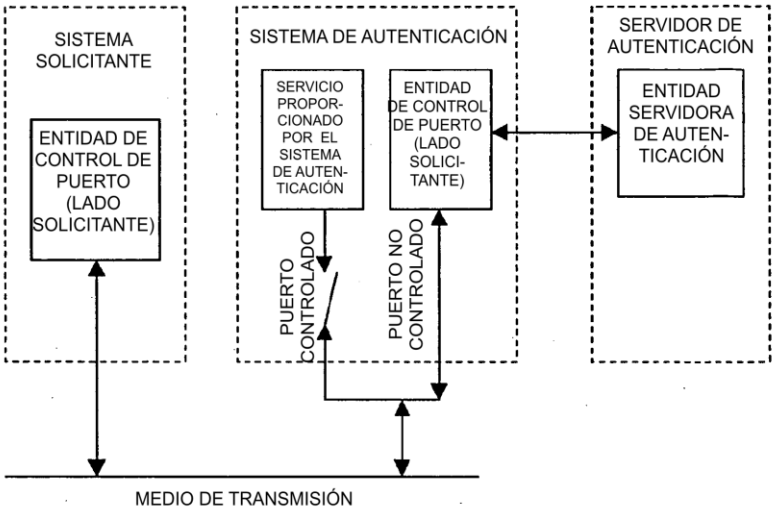
SISTEMA SOLICITANTE
ENTIDAD DE CONTROL DE PUERTO (LADO SOLICITANTE)
SISTEMA DE AUTENTICACIÓN
SERVICIO PROPOR-CIONADO POR EL SISTEMA DE AUTEN-TICACIÓN
ENTIDAD DE CONTROL DE PUERTO (LADO SOLICI-TANTE)
PUERTO CONTROLADO
PUERTO NO CONTROLADO
SERVIDOR DE AUTENTICACIÓN
ENTIDAD SERVIDORA DE AUTEN-TICACIÓN
MEDIO DE TRANSMISIÓN

Fig.1

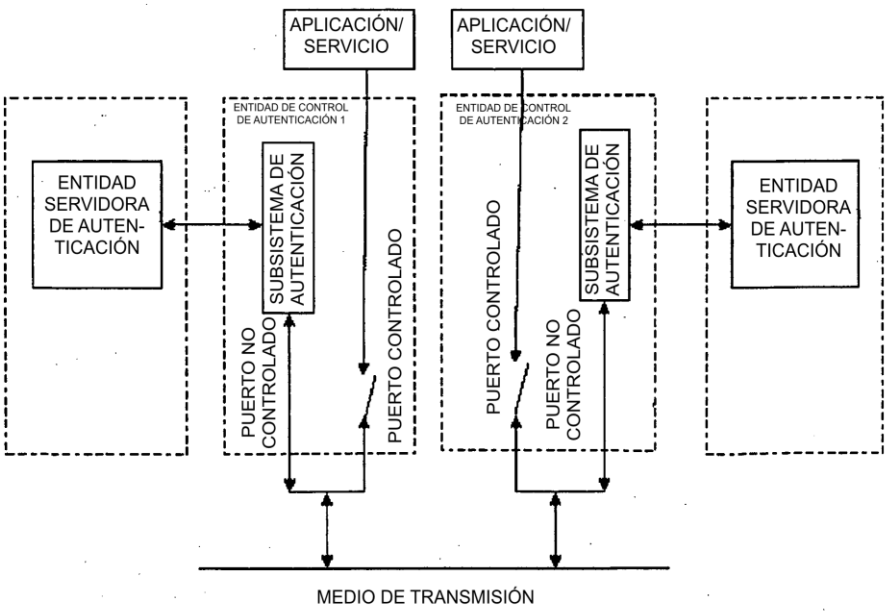
APLICACIÓN/ SERVICIO
APLICACIÓN/ SERVICIO
ENTIDAD DE CONTROL DE AUTENTICACIÓN 1
ENTIDAD DE CONTROL DE AUTENTICACIÓN 2
ENTIDAD SERVIDORA DE AUTEN-TICACIÓN
SUBSISTEMA DE AUTENTICACIÓN
PUERTO NO CONTROLADO
PUERTO CONTROLADO
PUERTO CONTROLADO
SUBSISTEMA DE AUTENTICACIÓN
PUERTO NO CONTROLADO
ENTIDAD SERVIDORA DE AUTEN-TICACIÓN
MEDIO DE TRANSMISIÓN

Fig.2

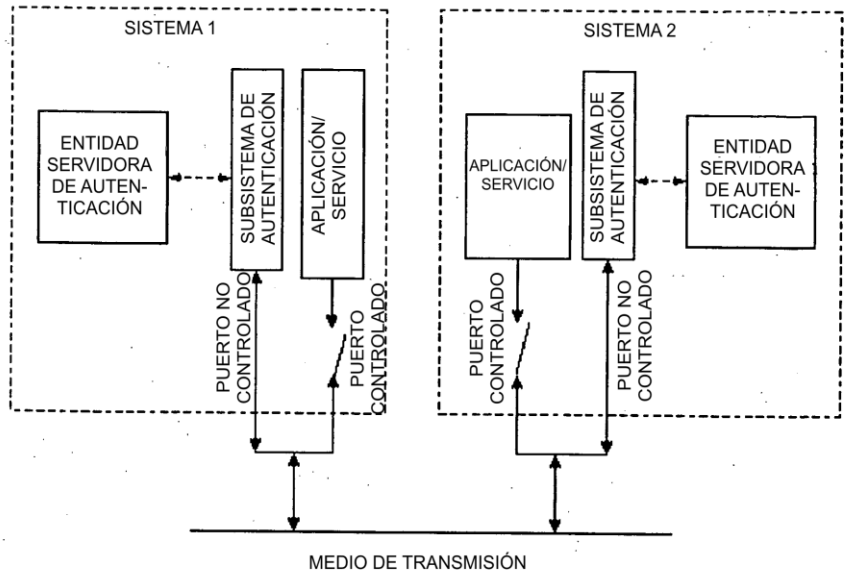
SISTEMA 1
ENTIDAD SERVIDORA DE AUTEN-TICACIÓN
SUBSISTEMA DE AUTENTICACIÓN
APLICACIÓN/ SERVICIO
PUERTO NO CONTROLADO
PUERTO CONTROLADO
SISTEMA 2
APLICACIÓN/ SERVICIO
SUBSISTEMA DE AUTENTICACIÓN
ENTIDAD SERVIDORA DE AUTEN-TICACIÓN
PUERTO CONTROLADO
PUERTO NO CONTROLADO
MEDIO DE TRANSMISIÓN

Fig.3

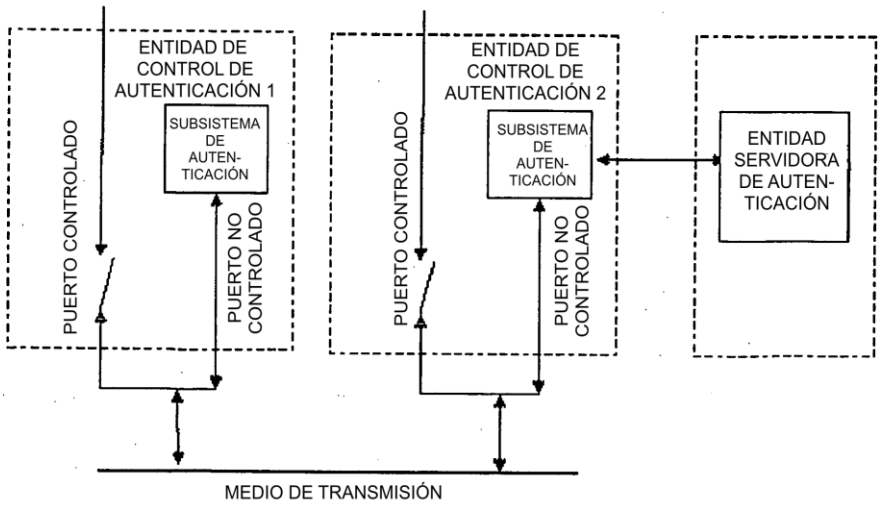
ENTIDAD DE CONTROL DE AUTENTICACIÓN 1
SUBSISTEMA DE AUTEN-TICACIÓN
PUERTO CONTROLADO
PUERTO NO CONTROLADO
ENTIDAD DE CONTROL DE AUTENTICACIÓN 2
SUBSISTEMA DE AUTEN-TICACIÓN
PUERTO CONTROLADO
PUERTO NO CONTROLADO
ENTIDAD SERVIDORA DE AUTEN-TICACIÓN
MEDIO DE TRANSMISIÓN

Fig.4