(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 555 459**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.07.2012 E 12738039 (2)**

(97) Fecha y número de publicación de la concesión europea: **09.09.2015 EP 2732598**

(54) Título: **Método para mejorar la alta disponibilidad en una red de telecomunicaciones segura, y red de telecomunicaciones que comprende una pluralidad de nodos remotos**

(30) Prioridad:

15.07.2011 EP 11005796

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.01.2016

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

MAURER, JÜRGEN

(74) Agente/Representante:

LAZCANO GAINZA, Jesús

DESCRIPCIÓN

Método para mejorar la alta disponibilidad en una red de telecomunicaciones segura, y red de telecomunicaciones que comprende una pluralidad de nodos remotos

Antecedentes

La presente invención se refiere entre otras cosas a un método para mejorar la disponibilidad en una red de telecomunicaciones segura, la red de telecomunicaciones que comprende una pluralidad de nodos remotos, uno o una pluralidad de nodos de la red adicionales, y al menos un portal de enlace de seguridad, en donde cada uno de la pluralidad de nodos remotos se comunica al uno o la pluralidad de nodos de red adicionales, en donde en un primer modo de funcionamiento de la pluralidad de nodos remotos, durante el funcionamiento normal de el al menos un portal de enlace de seguridad, cada uno de la pluralidad de nodos remotos se comunica con él al menos un portal de enlace de seguridad por medio de un túnel de comunicación seguro. La presente invención se refiere además a una red de telecomunicaciones que comprende una pluralidad de nodos remotos, uno o una pluralidad de nodos de la red adicionales, y al menos un portal de enlace de seguridad, en donde la red de telecomunicaciones está dispuesta para mejorar la alta disponibilidad de la funcionalidad de comunicación segura entre el al menos un portal de enlace de seguridad y la una o la pluralidad de nodos de red adicionales.

La solicitud de patente de los Estados Unidos US2008/0034110 A1 describe un sistema para mejorar la disponibilidad en una red de telecomunicaciones por medio de un agente que selecciona una conexión o recursos a partir de una tabla de enrutamiento, en caso de conmutación por error.

Con la migración hacia el Protocolo de Internet (IP) a través de Ethernet sobre todo en la red de acceso, más y más nodos de red (o sitios de red), especialmente los nodos de red remotos, están protegidos por los túneles de comunicación seguros, como túneles IPsec (túneles del protocolo de seguridad de internet) , es decir, desde la estación base hasta algunos nodos centralizados o sitios, donde las portales de enlace de seguridad, por ejemplo, el Protocolo de Internet Portales de Seguridad (IPsecGWs), se encuentran. En redes más grandes varios cientos hasta unos pocos miles de estaciones base u otros nodos de la red pueden estar conectados a un par de IPSecGWs. Esto también significa que las fallas graves de los portales de enlace de seguridad (por ejemplo, insuficiencia IPsecGW) o problemas con el manejo certificado podría conducir a gran impacto para el servicio de radio.

Incluso cuando se proporciona redundancia de portales de enlace de seguridad, tales como la redundancia IPsecGW, así como proporcionar mecanismos de conmutación inteligentes o los mecanismos de conmutación de estado, hay un riesgo razonable de fallos graves de la agrupación de portales de enlace de seguridad, por ejemplo, agrupación redundante IPsec. E incluso un problema con respecto a la gestión de certificados podría conducir a la situación que todos los nodos de radio no estén ya autorizados a configurar túneles de comunicación seguros a la salida de seguridad, tales como túneles IPsec.

Como también el plano de gestión del nodo de radio estará protegido por el mecanismo de seguridad, especialmente IPsec. La pérdida de la funcionalidad del mecanismo de seguridad (por ejemplo, IPsec) significa no sólo la pérdida del servicio de radio, sino también la pérdida de acceso de gestión remota a los nodos de radio. Eso significa que los nodos de radio no se pueden cambiar de nuevo a la comunicación de no seguridad (por ejemplo, la comunicación no IPsec) por un operador sin visita al sitio.

Una vuelta automática del interruptor de los nodos de radio para la comunicación no-segura (por ejemplo, no IPsec) (i.e., en caso de que el túnel de comunicación segura, tal como el túnel IPsec, no se puede establecer) desde la perspectiva de la seguridad no es aceptable, ya que esto podría dar a un "hombre en el medio" la oportunidad de desactivar la medida de seguridad.

Resumen

Un objeto de la presente invención es proporcionar un método para mejorar la alta disponibilidad en una red de telecomunicaciones que normalmente utiliza túneles de comunicación seguros por medio de proporcionar un mecanismo simple y fácil y seguro a restaurar la comunicación una vez seguro túneles de comunicación o canales se rompen debido a un fallo grave de nodos de la red, sobre todo de los portales de enlace de seguridad.

La invención propone una solución cómo, en tales casos de insuficiencias severas, los nodos conectados normalmente por medio de un túnel de comunicación segura, especialmente nodos de radio (remotos) conectados, se pueden conmutar a un modo de comunicación no seguro de operación, especialmente la comunicación no IPsec, de una manera controlada por el operador. Esto permite al operador mantener el servicio de radio, incluso si la protección de IPSec se interrumpe temporalmente. Además, esto permite evitar la disminución persistente del nivel de seguridad en la comunicación entre nodos de la red de telecomunicaciones. Adicionalmente, una funcionalidad de autosanación se proporciona de tal manera que no es necesario un adicional fuera de los canales de comunicación de la banda (con respecto a la conectividad del protocolo de seguridad de internet entre los nodos remotos y los nodos de red adicionales).

El objeto de la presente invención se consigue mediante un método para mejorar la alta disponibilidad en una red de telecomunicaciones segura, de acuerdo con la reivindicación 1

De acuerdo con la presente invención, por lo tanto, es ventajosamente posible, que, en caso de un fallo grave de la agrupación de portales de enlace de seguridad, por ejemplo, un error de agrupación IPsec, un interruptor de apagado de la funcionalidad de la comunicación segura es posible, por ejemplo, desconectando la funcionalidad IPsec en el nodo remoto (por ejemplo, un nodo de radio o una estación base o un eNodoB) de un modo seguro y controlado por el operador. De acuerdo con la presente invención, el esfuerzo para esta funcionalidad de derivación de seguridad (o funcionalidad de derivación de emergencia IPsec) se puede reducir a un mínimo y, especialmente, no requiere ninguna visita al lugar en el sitio del nodo remoto o pluralidad de nodos remotos. Además, es posible con la presente invención que incluso una pluralidad de nodos remotos (o incluso todos los nodos remotos) afectados por el fallo del portal de enlace de seguridad, se pueda cambiar en un segundo modo de funcionamiento que corresponda a una funcionalidad de derivación de seguridad (o modo " derivación de emergencia IPsec") en muy poco tiempo.

De esta manera es ventajosamente posible, que el modo de funcionamiento en relación con la comunicación segura del nodo de red remoto no puede ser modificado, salvo con permiso del operador de la red. Especialmente, es posible de acuerdo con la presente invención que la contraseña de una vez se distribuya en sí, al el al menos un nodo remoto específico de la pluralidad de nodos remotos (antes de un fallo del primer modo de funcionamiento) de tal manera que es ventajosamente posible activar el segundo modo de funcionamiento

- en la iniciativa de el al menos un nodo remoto específico de la pluralidad de nodos remotos, pero

- bajo el control del nodo de gestión de red.

De acuerdo con la presente invención, el primer mensaje es, por ejemplo, un mensaje de descubrimiento de DHCP (i.e., solicita una dirección IP para ser utilizada por el al menos un nodo remoto específico de la pluralidad de nodos remotos), y el segundo mensaje es, por ejemplo: un mensaje de oferta de DHCP (i.e., la concesión de una dirección IP que se utiliza). De acuerdo con la presente invención, se prefiere que, en el primer modo de funcionamiento, un mensaje de oferta de DHCP (análogo al segundo mensaje) comprende, por ejemplo, sólo la dirección IP para ser utilizado por el al menos una vez nodo específico remoto de la pluralidad de nodos remotos, mientras que, en el segundo modo de funcionamiento, el segundo mensaje comprende especialmente datos opcionales, particularmente la contraseña de una sola vez, así como por lo general (de acuerdo con el estándar de DHCP) una dirección IP.

Además, se prefiere de acuerdo con la presente invención que la contraseña de una sola vez se almacena inicialmente en los nodos remotos (o una pluralidad de contraseñas de una sola vez se almacena inicialmente en los nodos remotos). Con el fin de lograr esto, una distribución de la contraseña de una sola vez o la pluralidad de contraseñas de una sola vez se realiza desde un nodo de la red central (por ejemplo, un nodo de sistema de gestión de red). Por lo tanto, se prefiere de acuerdo con la presente invención que esta distribución de la contraseña de una sola vez a él al menos un nodo remoto específico de la pluralidad de nodos remotos se realiza sólo durante el nodo remoto específico de la pluralidad de nodos remotos que se operan en el primer modo de funcionamiento y, preferiblemente, a través del túnel de comunicación segura.

De este modo, una mejora adicional del nivel de seguridad en la comunicación entre la pluralidad de nodos remotos, por una parte, y el portal de enlace de seguridad u otros nodos de la red de telecomunicaciones, por otro lado, es posible que la contraseña de una sola vez sea protegida por el establecimiento del canal de comunicación seguro entre la pluralidad de nodos remotos y el portal de enlace de seguridad o nodos de red adicionales de acuerdo con el primer modo de funcionamiento de la pluralidad de nodos de red remotos.

Aún más, se prefiere de acuerdo con la presente invención que en el caso de las siguientes condiciones se verifican de forma acumulativa, el primer mensaje se envía desde el al menos un nodo remoto específico de la pluralidad de nodos remotos:

- el túnel de comunicación segura no se puede establecer, y

- la interfaz física para la comunicación con él al menos un portal de enlace de seguridad está en funcionamiento, y

- el portal de enlace predeterminado es accesible por el al menos un nodo remoto específico de la pluralidad de nodos remotos.

Por ejemplo, la accesibilidad (por el al menos un nodo remoto específico) del portal de enlace predeterminado se detecta por medio de la detección de reenvío bidireccional (BFD).

De esta manera, es ventajosamente posible de acuerdo con la presente invención, que no sólo en caso de avería del portal de enlace de seguridad o agrupación de portales de enlace de seguridad (donde el portal de enlace de seguridad o una pluralidad de portales de enlace de seguridad pierden su funcionalidad), sino también en el caso de la

incapacidad de los componentes de la red para establecer un túnel de comunicación segura, es posible una conmutación en el segundo modo de funcionamiento de los nodos de red remotos.

De acuerdo con otra realización de la presente invención, se prefiere que el primer mensaje se envíe desde el al menos un nodo remoto específico de la pluralidad de nodos remotos sólo después de un primer intervalo de tiempo predeterminado después de establecer que las siguientes condiciones se verifican de forma acumulativa:

- el túnel de comunicación segura no se puede establecer, y

- la interfaz física para la comunicación con el portal de enlace de seguridad al menos uno está en funcionamiento, y

- el portal de enlace predeterminado es accesible por el al menos un nodo remoto específico de la pluralidad de nodos remotos.

Por ejemplo, la accesibilidad (por el al menos un nodo remoto específico) del portal de enlace predeterminada se detecta por medio de la detección de reenvío bidireccional (BFD).

De este modo, es ventajosamente posible reducir la carga de comunicación de un nodo de red proporcionada para manejar los primeros mensajes, tales como un servidor DHCP (Protocolo de configuración del huésped dinámico).

Además, se prefiere de acuerdo con la presente invención que después de enviar inicialmente el primer mensaje desde el al menos un nodo remoto específico de la pluralidad de nodos remotos sin recepción del segundo mensaje, el primer mensaje se repite a partir de el al menos un nodo remoto específico de la pluralidad de nodos remotos.

De acuerdo con esta realización adicional de la presente invención, es ventajosamente posible proporcionar una funcionalidad de autosanación en el caso de la comunicación interrumpida entre los nodos de la red de telecomunicaciones.

De acuerdo con una realización adicional de la presente invención, se prefiere que la repetición del primer mensaje se produce sólo después de un segundo intervalo de tiempo predeterminado después de que inicial o previamente de enviar el primer mensaje.

De este modo, es ventajosamente posible reducir la carga de comunicación de un nodo de red proporcionado para manejar los primeros mensajes, tales como un servidor DHCP (Protocolo de configuración del huésped dinámico).

Además, se prefiere de acuerdo con la presente invención que:

- el al menos un portal de enlace de seguridad es un portal de enlace IPsec (portal de enlace de seguridad del protocolo de internet) y el túnel de comunicación segura es un túnel IPsec, y/o que

- la pluralidad de nodos remotos son al menos en parte, los nodos que tienen una funcionalidad de la estación base en una red de red móvil terrestre pública (PLMN), especialmente una funcionalidad eNodeB.

La presente invención también se refiere a una red de telecomunicaciones que comprende una pluralidad de nodos remotos, uno o una pluralidad de nodos de la red adicionales, y al menos un portal de enlace de seguridad, y al menos un portal de enlace de seguridad, en donde la red de telecomunicaciones está dispuesta para mejorar la alta disponibilidad de la funcionalidad de la comunicación segura entre al menos un portal de enlace de seguridad y el uno o la pluralidad de nodos de red adicionales, en donde cada uno de la pluralidad de nodos remotos se proporciona para comunicar a el uno o la pluralidad de nodos de la red adicionales, en donde en un primer modo de funcionamiento de la pluralidad de nodos remotos, durante el funcionamiento normal de el al menos un portal de enlace de seguridad, la red de telecomunicaciones está dispuesta de tal manera que cada uno de la pluralidad de nodos remotos se comunica con él al menos un portal de enlace de seguridad por medio de un túnel de comunicación segura, en donde en un segundo modo de funcionamiento de la pluralidad de nodos remotos, durante el fallo del túnel de comunicación segura, la red de telecomunicaciones está dispuesta de tal manera que al menos un nodo remoto específico de la pluralidad de nodos remotos está conectado a el uno o la pluralidad de nodos de red adicionales evitando el portal de enlace de seguridad, en donde la red de telecomunicaciones está dispuesta de tal manera que el primer modo de funcionamiento se conmuta al segundo modo de funcionamiento por medio de un intercambio de al menos un primer mensaje y un segundo mensaje entre el al menos un nodo remoto específico de la pluralidad de nodos remotos y el uno o la pluralidad de nodos de la red adicionales utilizando el protocolo DHCP (Protocolo de configuración del huésped dinámico).

De esta manera es ventajosamente posible de acuerdo con la presente invención evitar, al menos en parte, las enormes consecuencias de una severa falla en los nodos de los portales de enlace de seguridad o agrupaciones de portales de enlace de seguridad.

De acuerdo con la presente invención, se prefiere - también con respecto a la red de telecomunicaciones - que el primer mensaje comprenda una petición del al menos un nodo remoto específico de la pluralidad de nodos remotos, y el

segundo mensaje comprenda una respuesta al primer mensaje por un nodo de gestión de red, el segundo mensaje que comprende una contraseña de una sola vez.

De esta manera es ventajosamente posible, que el modo de funcionamiento en relación con la comunicación segura del nodo de red remoto no pueda ser modificado, salvo con permiso del operador de la red. Especialmente, es posible de acuerdo con la presente invención que la contraseña de solo una vez ya sea distribuida a él al menos un nodo remoto específico de la pluralidad de nodos remotos (antes de un fallo del primer modo de funcionamiento) de tal manera que sea ventajosamente posible activar el segundo modo de funcionamiento

- en la iniciativa del al menos un nodo remoto específico de la pluralidad de nodos remotos, pero

- bajo el control del nodo de gestión de red.

Además, la presente invención se refiere a un programa que comprende un código de programa legible por ordenador que, cuando se ejecuta en un ordenador, hace que el ordenador pueda llevar a cabo un método de la invención de acuerdo con la presente invención.

La presente invención se refiere también a un producto de programa informático para mejorar la alta disponibilidad en una red de telecomunicaciones, el producto de programa de ordenador que comprende un programa informático almacenado en un medio de almacenamiento, el código de programa que comprende un programa de ordenador que, cuando se ejecuta en un ordenador, hace que el ordenador realice un método de la invención de acuerdo con la presente invención.

Estas y otras características, aspectos y ventajas de la presente invención serán evidentes a partir de la siguiente descripción detallada, tomada en conjunción con los dibujos adjuntos, que ilustran, a modo de ejemplo, los principios de la invención. La descripción se da en aras de ejemplo solamente, sin limitar el alcance de la invención. Las cifras de referencia citadas a continuación se refieren a los dibujos adjuntos.

En lo que sigue, se hace referencia al protocolo de seguridad de Internet (IPsec) y/o hasta el túnel de seguridad del protocolo de internet (túnel IPsec) como un ejemplo destacado de un protocolo o método de comunicación segura (y el túnel de comunicación segura) entre diferentes (y normalmente distantes) nodos de la red de telecomunicaciones. De acuerdo con la presente invención, en caso de que ningún túnel IPsec pueda ser establecido, un nodo remoto (especialmente un nodo radio tal como una estación base o eNodeB) deberán analizar sus condiciones de red actuales para identificar la causa de la falla. El interruptor en el segundo modo de funcionamiento del nodo de red remoto (i.e., la función de derivación de emergencia IPsec de acuerdo con la presente invención) no se limitará al caso de un portal de enlace IPsec inalcanzable, pero también se recurre para cubrir el caso donde la configuración del túnel sea rechazada (por ejemplo, si el portal de enlace IPsec no es aceptado debido a un error en el software aún con certificados válidos).

De acuerdo con la presente invención, se recurre al segundo modo de funcionamiento basado en las siguientes condiciones detectadas en el nodo remoto:

- túnel IPsec no se puede establecer (ya sea IPsecGW no alcanzable o configuración del túnel rechazada por el IPsecGW),

- interfaz física es hasta

- por defecto GW es alcanzable.

En tal situación, el nodo remoto (por ejemplo, una estación base) asumirá un fallo de la agrupación IPsec.

Tan pronto como se reconoce un fallo grave de la agrupación IPsec, el nodo remoto (especialmente una estación de base) tiene que verificar que el operador aprueba el cambio al segundo modo de funcionamiento del nodo remoto (i.e., la "derivación de emergencia IPsec"). Esto se hace mediante la solicitud de una contraseña de una sola vez desde la red del operador, es decir, desde un nodo de red adicional, por ejemplo, un nodo de sistema de gestión de red (o un nodo que proporciona la funcionalidad del sistema de gestión de red).

Para solicitar la contraseña de una vez, el nodo de red remoto (especialmente un nodo radio) envía el primer mensaje, especialmente una solicitud DHCP, a través de la configuración VLAN (red de área local virtual de configuración) utilizada durante el proceso SON PnP (Self Organizador Redes Plug and Play process). El planeado existente/operacional VLAN con su configuración IP se mantiene de acuerdo con la presente invención. La dirección IP temporal dictada por DHCP inmediatamente puede ser puesta en libertad, ya que se necesita sólo la información en el código de opción 43 (en caso de que el primer mensaje es un mensaje DHCP).

En caso de que la respuesta de DHCP contenga, en código de opción 43, una subopción predeterminada con sólo una cadena alfanumérica - por ejemplo, la subopción 80 sólo con una cadena alfanumérica - el nodo remoto (por ejemplo, el nodo radio) compara esa cadena con un operador de campo de parámetro configurable "contraseña de derivación IPsec

de emergencia". Si el valor en la subopción predeterminada del segundo mensaje (por ejemplo, la subopción 80) es igual al valor en este campo de parámetro (en el nodo remoto), los interruptores del nodo remoto (por ejemplo, el nodo radio) de la funcionalidad IPSec, es decir, los interruptores del primer modo de funcionamiento y los interruptores del segundo modo de funcionamiento.

En el modo de derivación de emergencia IPsec (i.e., en el segundo modo de funcionamiento de acuerdo con la presente invención), el nodo remoto (especialmente un nodo radio) utiliza el mismo ID de VLAN, dirección IP de la interfaz, direcciones IP de servicio (direcciones de bucle), GW por defecto (portal de enlace) y las reglas configuración del cortafuegos/ACL (Access Control List) (cortafuegos/ACL en frente del túnel IPsec para filtrar el tráfico que entra y que sale del túnel IPsec de acuerdo con la matriz de comunicación del nodo remoto (por ejemplo, nodo de radio)) como en el modo de IPsec (primer modo de funcionamiento de acuerdo con la presente invención). Eso significa que el nodo remoto (especialmente el nodo de radio) no necesita ningún dato de configuración adicional y puede desconectar la funcionalidad IPsec de forma autónoma pero sólo de una manera controlada (o permitido por la verificación de la contraseña de una sola vez) por el operador.

Una vez que el fallo de agrupación IPsec se resuelve y los todos nodos remotos (por ejemplo, nodos de radio) se han cambiado a IPSec (i.e., al primer modo de funcionamiento), es posible de acuerdo con la presente invención establecer una nueva contraseña de una vez en todos los nodos remotos conectados (por ejemplo, nodos de radio) por medio de un único comando.

Especialmente para - evitar situaciones de sobrecarga en el nodo manejando la multitud de primeros mensajes (enviados por la pluralidad de nodos remotos), especialmente un servidor DHCP, y - para controlar el conmutador sobre el proceso se prefiere de acuerdo con la presente invención el uso de un operador configurable (i.e., predeterminado) temporizador (o de intervalos de tiempo), es decir, un temporizador "retraso de derivación de emergencia IPsec" como un primer intervalo de tiempo predeterminado y un temporizador "reintento de derivación de emergencia IPsec" como un segundo intervalo de tiempo predeterminado.

Implementando el método de derivación de emergencia IPSec de acuerdo con la presente invención, todo el tráfico de un nodo remoto (por ejemplo, un nodo de radio) puede ser protegido con IPsec y el operador todavía tiene control de la red completa, incluso en caso de fallo del IPSec. Esto reduce en gran medida el riesgo de caídas de la red, incluso con una mayor seguridad de la red.

Breve descripción de los dibujos

La figura 1 ilustra esquemáticamente una red de telecomunicaciones de acuerdo con la presente invención.

La figura 2 ilustra esquemáticamente un diagrama de acuerdo con el método de la presente invención.

La figura 3 ilustra esquemáticamente una línea de tiempo que representa el método de la presente invención.

Descripción detallada

La presente invención se describirá con respecto a realizaciones particulares y con referencia a ciertos dibujos, pero la invención no se limita a los mismos sino solamente por las reivindicaciones. Los dibujos descritos son solamente esquemáticos y no limitativos. En los dibujos, el tamaño de algunos de los elementos puede estar exagerado y no dibujado a escala para fines ilustrativos.

Cuando un artículo indefinido o definido se utiliza para referirse a un sustantivo singular, por ejemplo, "a", "una", "el", esto incluye un plural de ese sustantivo a menos que se especifique otra cosa.

Además, los términos primero, segundo, tercero y similares en la descripción y en las reivindicaciones se utilizan para distinguir entre elementos similares y no necesariamente para describir un orden secuencial o cronológico. Se debe entender que los términos así usados son intercambiables bajo circunstancias apropiadas y que las realizaciones de la invención descritas en este documento son capaces de funcionar en otras secuencias que las descritas o ilustradas en este documento.

En la figura 1, se muestra esquemáticamente una red 10 de telecomunicaciones de acuerdo con la presente invención. La red 10 de telecomunicaciones comprende una pluralidad de nodos, llamados nodos 20 remotos. Un nodo específico o nodo remoto de esta pluralidad de nodos 20 de red o nodos 20 remotos es designada por el signo 21de referencia. Los nodos de red o nodos 20 remotos son especialmente llamados nodos de radio que tienen funcionalidad de la estación base, por ejemplo, Nodos NodoB o nodos eNodoB en una red móvil terrestre pública UTRAN y/o E- UTRAN.

La red 10 de telecomunicaciones, además, comprende también otros nodos 40 de red, por lo general parte de la red central de la red 10 de telecomunicaciones, tales como bases de datos de administración de redes y/o contenidos que proporcionan nodos o portales de enlace a otras partes de la red 10 de telecomunicaciones o para redes de telecomunicaciones de otros proveedores u operadores. A modo de ejemplo, plano de control y/o componentes de

plano de usuario XX (por ejemplo, una entidad de gestión de la movilidad (MME), una entidad SGW (Portal Servidor), un Portal de Medios (MGW) o un MSS (Servidor de centro de intercambiador móvil (MSC)), Nodo de Soporte de Servicio GPRS (SGSN), un nodo de soporte GPRS de portal de enlace GGSN), y los diferentes nodos de borde YY, ZZ de una red troncal (por ejemplo, componente IPMB o entidad de red (componente esqueleto móvil IP)) se muestran esquemáticamente en la figura 1.

Los nodos 20 remotos están conectados a los nodos 40 de red adicionales, por medio de una red 11 de agregación que es también parte de la red 10 de telecomunicaciones. Además, la red 10 de telecomunicaciones comprende al menos un portal de enlace 31 de seguridad. La comunicación entre los nodos 20 remotos y los nodos 40 de la otra red normalmente se realizan como una comunicación segura en el portal de enlace 31 de seguridad sirve para el manejo de contraseñas, claves de sesión y administra el uso de la infraestructura de clave pública. Los nodos 20 remotos se comunican con el portal de enlace 31 de seguridad por lo general por medio de un dispositivo enrutador 31' asignado al portal de enlace 31 de seguridad.

Para darse cuenta de la alta disponibilidad de la comunicación segura entre los nodos 20 remotos y los nodos 40 adicionales, un portal de enlace 32 de acceso más seguro (así como un dispositivo 32' enrutador adicional) se añade normalmente para permitir la redundancia para asegurar la comunicación segura. Juntos, el portal de enlace 31 de seguridad y el portal de enlace 32 de seguridad adicional (y los respectivos enrutadores 31', 32') también se conocen como el agrupamiento de seguridad. Los nodos 20 remotos se comunican con el portal de enlace 31 de seguridad y/o con el portal de enlace 32 de seguridad adicional de una manera segura, especialmente utilizando una variante del protocolo IPsec. Esto también se conoce con el término "primer modo operacional" de acuerdo con la presente invención.

En caso de que el portal de enlace de seguridad que se basa en un nodo 20 remoto (o en caso de que toda la agrupación de seguridad) falle, los nodos 20 remotos no pueden simplemente cambiar a una comunicación sin necesidad de utilizar el protocolo IPsec. Con el fin de mejorar el nivel de seguridad de la comunicación entre los nodos 20 remotos y los nodos 40 de red adicionales, la transición a una comunicación sin utilizar el protocolo de comunicación segura (especialmente el protocolo IPsec), que se conoce por el término "segundo modo de funcionamiento" de acuerdo con la presente invención, es controlado por la red central de la red 10 de telecomunicaciones, especialmente una funcionalidad de gestión de red.

La transición al segundo modo de funcionamiento de un nodo 21 remoto específico se ilustra esquemáticamente en la figura 2. En un primer paso 100, un fallo de la agrupación de seguridad o, al menos, el portal de enlace 31 de seguridad relevante es detectado por el nodo 20 remoto. Esto se desencadena a partir de un primer contador de tiempo que define un primer intervalo de tiempo predeterminado T1, en referencia a un retraso seguro de la comunicación de emergencia de derivación (o un retardo de derivación de emergencia IPsec). En un segundo paso 102, se decide si el primer intervalo de tiempo T1 ha expirado. Si no, el flujo se ramifica a un tercer paso 104, en caso afirmativo, el flujo se ramifica a una sexta paso 110. En el tercer paso 104, el restablecimiento de la comunicación segura con el portal de enlace 31 de seguridad o la agrupación de seguridad que se pretende. En un cuarto paso 106, se comprueba si el túnel de comunicación segura con el portal de enlace de seguridad fue (re) establecido con éxito o no. Si no, el flujo se ramifica al segundo paso 102; en caso afirmativo, el flujo se ramifica a un quinto paso 108 que significa que el modo remoto podría establecer con éxito el canal de comunicación seguro o un túnel con el portal de enlace de seguridad. En el sexto paso, un primer mensaje se envía desde el nodo 20 remoto a uno de los nodos 40 de red adicionales, por lo general a un DHCP (Protocolo de configuración del huésped dinámico) del servidor o nodo, solicitando una contraseña, especialmente una contraseña de una sola vez, lo que permite la transición al segundo modo de funcionamiento del nodo 21 remoto específico. En respuesta al primer mensaje, el nodo 40 adicional a la red dirigida por el primer mensaje (u otro nodo 40 de red adicional) envía un segundo mensaje al nodo 21 remoto específico, comprende especialmente un código 43 de opción DHCP y una subopción 80 con una cadena alfanumérica (como la contraseña de una sola vez). En un séptimo paso 112, se comprueba si la contraseña de una sola vez recibida por el nodo 21 remoto específico es correcta. En caso afirmativo, el flujo se ramifica a un undécimo paso 120. Si no, el flujo se ramifica a un octavo paso 114; Además, esto desencadena iniciar un segundo temporizador que define un segundo intervalo T2 de tiempo predeterminado, en referencia a un retraso seguro de comunicación de emergencia de reintento de derivación (derivación de emergencia o un retardo de reintento IPsec). En el octavo paso 114, un re-establecimiento del túnel seguro se intentó de nuevo (de forma análoga al tercer paso 104). En un noveno paso 116, se comprueba si el túnel de comunicación segura con el portal de enlace de seguridad fue con éxito (re) establecido o no. Si no, el flujo se ramifica a un décimo paso 118; en caso afirmativo, el flujo se ramifica al quinto paso 108, que significa que el modo remoto podría establecer con éxito el canal de comunicación seguro o un túnel con el portal de enlace de seguridad. En la décima paso 118, se comprueba si el segundo intervalo T2 de tiempo ha expirado. Si no es así, el flujo se ramifica al octavo paso 114; en caso afirmativo, el flujo se ramifica al sexto paso110.

En el undécimo paso 120, el nodo 21 remoto específico cambia al modo de comunicación de derivación segura, es decir, el segundo modo de funcionamiento de acuerdo con la presente invención. Esto permite en un duodécimo paso 122 para recuperar el nodo 21 remoto específico de tal manera que una comunicación con la red central (i.e., con uno o una pluralidad de los otros nodos 40) es posible sin una interacción manual en el sitio del nodo 21 remoto.

En la figura 3, el método de la invención se ilustra esquemáticamente de nuevo mediante una línea de tiempo. En el punto A, se interrumpe la comunicación segura (en el primer modo de funcionamiento del nodo 21 remoto específico). Durante el tiempo designado por el signo de referencia F, el nodo 21 remoto específico está fuera de servicio desde la perspectiva de la red central. La interrupción del túnel de comunicación segura inicia un temporizador en relación con el primer intervalo T1 de tiempo predeterminado. En el punto B, el primer mensaje (que comprende la solicitud al servidor DHCP) se emite desde el nodo 21 remoto específico. Además, en el punto B, se recibe una primera respuesta (por el nodo 21 remoto específico) desde el servidor DHCP. Esta primera respuesta normalmente no comprende la contraseña de una sola vez. Esto inicia el segundo intervalo T2 de tiempo predeterminado. En el punto C, el servidor DHCP se reconfigura por el operador de la red. Como resultado, respuestas adicionales (desde el servidor DHCP, provocado por el primer mensaje desde el nodo 21 remoto específico) hacen comprender la contraseña de una sola vez. En el punto D, el extremo del intervalo T2 predeterminado de segunda vez y un segundo intento del primer mensaje se puede enviar por el nodo 21 remoto específico al servidor DHCP. En la recepción, en el punto E. del segundo mensaje que comprende la contraseña (de una sola vez) (i.e., después operador activa la reconfiguración del servidor DHCP), el nodo remoto específico se conmuta al segundo modo de funcionamiento y es de nuevo visible y operativo desde la perspectiva de la red central, es decir, un autosanación se ha aplicado al enlace de comunicación entre los otros nodos 40 de la red y el nodo 21 remoto específico. Tal autosanación, por supuesto, que se aplicará a toda la pluralidad de controles de los nodos 20 remotos, siendo preferiblemente diferente el primero y segundo intervalo de tiempo con el fin de reducir la carga del pico al servidor DHCP.

Reivindicaciones

1. Método para mejorar la alta disponibilidad en una red (10) de telecomunicaciones segura, la red (10) de telecomunicaciones que comprende una pluralidad de nodos (20) remotos, uno o una pluralidad de otros nodos (40) de red, y al menos un portal de enlace (31) de seguridad, en donde cada uno de la pluralidad de nodos (20) remotos se comunica al uno o la pluralidad de nodos (40) de red adicionales,

en donde en un primer modo de funcionamiento de la pluralidad de nodos (20) remotos, durante el funcionamiento normal de al menos un portal de enlace (31) de seguridad, cada uno de la pluralidad de nodos (20) remotos se comunica con al menos un portal de enlace (31) de seguridad por medio de un túnel de comunicación segura,

en donde en un segundo modo de funcionamiento de la pluralidad de nodos (20) remotos, durante el fallo del túnel de comunicación segura, al menos un nodo (21) remoto específico de la pluralidad de nodos (20) remotos está conectado al uno o la pluralidad de nodos (40) de red adicionales evitando el portal de enlace (31) de seguridad,

en donde el primer modo de funcionamiento se conmuta al segundo modo de funcionamiento por medio de un intercambio de al menos un primer mensaje y un segundo mensaje entre el al menos un nodo (21) remoto específico de la pluralidad de nodos (20) remotos y el uno o la pluralidad de otros nodos (40) de la red, utilizando el protocolo DHCP (protocolo de configuración dinámico de huésped), en donde el primer mensaje comprende un requerimiento del al menos un nodo (21) remoto específico de la pluralidad de nodos (20) remotos, y el segundo mensaje comprende una respuesta al primer mensaje por un nodo de gestión de red, el segundo mensaje que comprende una contraseña de una sola vez.

2. Método de acuerdo con una de las reivindicaciones precedentes, en donde en caso de que las siguientes condiciones se verifiquen de forma acumulativa, el primer mensaje se envía desde el al menos un nodo (21) remoto específico de la pluralidad de nodos (20) remotos:

- el túnel de comunicación segura no se puede establecer, y

- la interfaz física para la comunicación con el al menos un portal de enlace (31) de seguridad está en funcionamiento, y

- el portal de enlace por defecto es accesible por el al menos un nodo (21) remoto específico de la pluralidad de nodos (20) remotos que está en funcionamiento.

3. Método de acuerdo con una de las reivindicaciones precedentes, en donde el primer mensaje se envía desde al menos un nodo (21) remoto específico de la pluralidad de nodos (20) remotos solamente después de un primer intervalo (T1) de tiempo predeterminado, después de establecer que las siguientes condiciones se verifican de forma acumulativa:

- el túnel de comunicación segura no se puede establecer, y

- la interfaz física para la comunicación con al menos un portal de enlace (31) de seguridad está en funcionamiento, y

- el portal de enlace por defecto es accesible por el al menos un nodo (21) remoto específico de la pluralidad de nodos (20) remotos.

4. Método de acuerdo con una de las reivindicaciones precedentes, en donde después de enviar inicialmente el primer mensaje desde el al menos un nodo (21) remoto específico de la pluralidad de nodos (20) remotos sin la recepción del segundo mensaje, se repite el primer mensaje desde el al menos un nodo (21) remoto específico de la pluralidad de los nodos (20) remotos.

5. Método de acuerdo con la reivindicación 5, en donde la repetición del primer mensaje se produce sólo después de un segundo intervalo (T2) de tiempo predeterminado, después de que inicial o previamente se ha enviado el primer mensaje.

6. Método de acuerdo con una de las reivindicaciones precedentes, en donde al menos el portal de enlace (31) de seguridad es un portal de enlace-IPsec (portal de enlace del protocolo de seguridad de internet) y en donde el túnel de comunicación segura es un túnel IPsec.

7. Método de acuerdo con una de las reivindicaciones precedentes, en donde la pluralidad de nodos (20) remotos son al menos parcialmente nodos que tienen una funcionalidad de estación base en una red de red móvil terrestre pública (PLMN), especialmente funcionalidad eNodoB.

8. La red (10) de telecomunicaciones que comprende una pluralidad de nodos (20) remotos, uno o una pluralidad de nodos (40) de red adicionales, y al menos un portal de enlace (31) de seguridad, en donde la red (10) de telecomunicaciones está dispuesto para mejorar la alta disponibilidad de la funcionalidad de la comunicación segura

entre el al menos un portal de enlace (31) de seguridad y la una o una pluralidad de nodos (40) de red adicionales, en donde cada uno de la pluralidad de nodos (20) remotos se proporciona para comunicar al uno o la pluralidad de nodos (40) de red adicionales,

en donde en un primer modo de funcionamiento de la pluralidad de nodos (20) remotos, durante el funcionamiento normal de el al menos un portal de enlace (31) de seguridad, la red (10) de telecomunicaciones está dispuesta de tal manera que cada uno de la pluralidad de nodos (20) remotos se comunica con al menos un portal de enlace (31) de seguridad por medio de un túnel de comunicación segura,

en donde en un segundo modo de funcionamiento de la pluralidad de nodos (20) remotos, durante el fallo del túnel de comunicación segura, la red (10) de telecomunicaciones está dispuesto de tal manera que al menos un nodo (21) remoto específico de la pluralidad de nodos (20) remotos está conectado al uno o la pluralidad de nodos (40) de red adicionales evitando el portal de enlace de seguridad (31),

en donde la red (10) de telecomunicaciones está dispuesta de tal manera que el primer modo de funcionamiento se conmuta al segundo modo de funcionamiento por medio de un intercambio de al menos un primer mensaje y un segundo mensaje entre el al menos un nodo (21) remoto específico de la pluralidad de nodos (20) remotos y el uno o la pluralidad de nodos (40) de red adicionales utilizando el protocolo DHCP (Protocolo de configuración dinámico de huésped), en donde el primer mensaje comprende uno de el al menos un nodo (21) remoto específico de la pluralidad de nodos (20) remotos, y el segundo mensaje comprende una respuesta al primer mensaje por un nodo de gestión de red, el segundo mensaje que comprende una contraseña de una sola vez.

9. Programa que comprende un código de programa legible por ordenador que, cuando se ejecuta en un ordenador, hace que el ordenador pueda llevar a cabo un método de acuerdo con una de las reivindicaciones 1 a 10.

10. Producto de programa de ordenador para mejorar la alta disponibilidad en una red (10) de telecomunicaciones, el producto de programa de ordenador que comprende un programa informático almacenado en un medio de almacenamiento, el código de programa que comprende un programa de ordenador que, cuando se ejecuta en un ordenador, hace que el ordenador pueda llevar a cabo un método de acuerdo con una de las reivindicaciones 1 a 10.

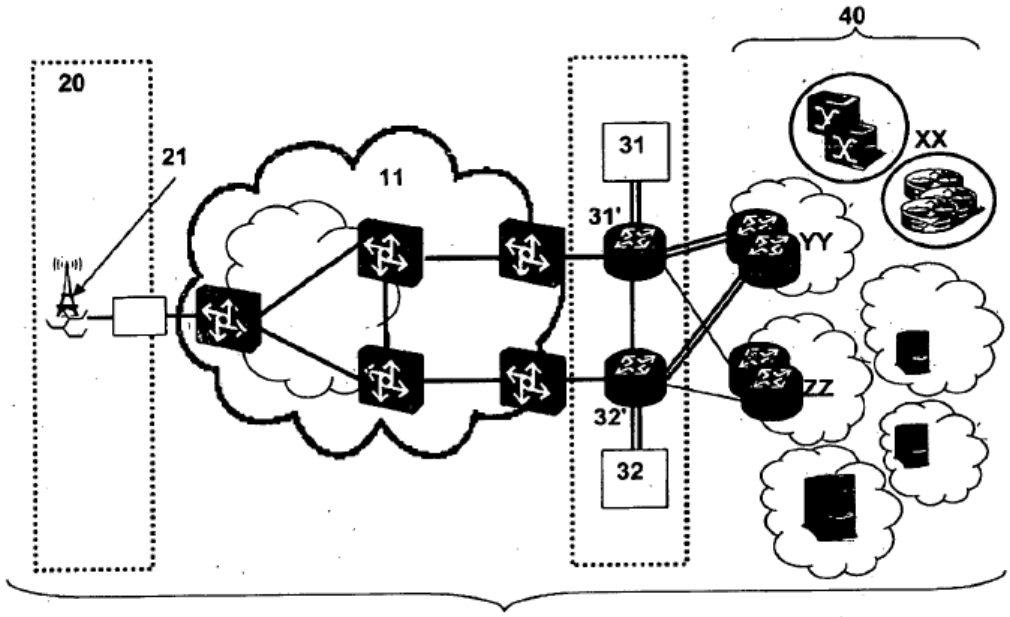
40
20
21
11
31
31'
XX
YY
ZZ
32'
32
10

Fig. 1

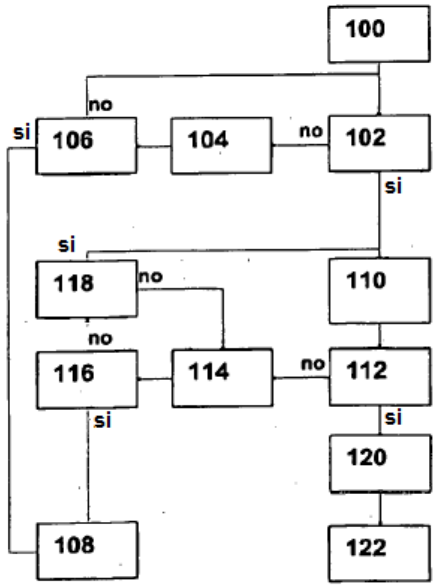
100
no
si
106
104
no
102
si
si
118
no
110
no
116
114
no
112
si
si
120
108
122

Fig. 2

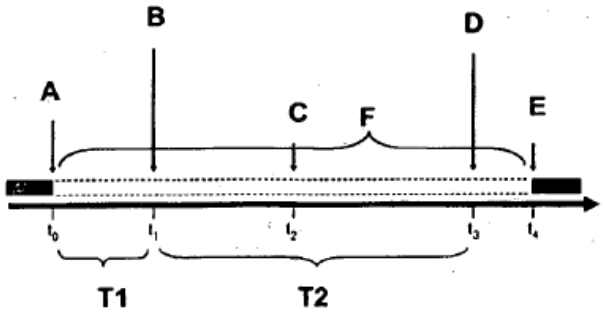

Fig. 3