(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 357 751**

(51) Int. Cl.:
H04L 29/06 (2006.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07804610 .9**
(96) Fecha de presentación : **13.07.2007**
(97) Número de publicación de la solicitud: **2177007**
(97) Fecha de publicación de la solicitud: **21.04.2010**

(54) Título: **Sistema y procedimiento de protección contra la denegación de servicio en un sistema de telecomunicaciones.**

(45) Fecha de publicación de la mención BOPI:
29.04.2011

(45) Fecha de la publicación del folleto de la patente:
29.04.2011

(73) Titular/es: **Telefonaktiebolaget LM Ericsson (publ)**
164 83 Stockholm, SE

(72) Inventor/es: **Haddad, Wassim;**
Näslund, Mats y
Mehes, András

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

CAMPO TÉCNICO DE LA INVENCIÓN

La presente invención versa en general acerca de redes de comunicaciones y, en particular, acerca de redes de comunicaciones que emplean protección contra la denegación de servicio.

DESCRIPCIÓN DE LA TÉCNICA RELACIONADA

Un nodo móvil (NM) es un dispositivo que puede moverse y, por lo tanto, cambiar su punto de conexión a una red, lo que típicamente significa que puede cambiar su dirección (IP) de red con el tiempo. Un nodo de múltiples interfaces es un dispositivo que puede tener simultáneamente varios puntos de conexión a la red, teniendo por ello, simultáneamente, varias direcciones IP. En consecuencia, un nodo móvil de red de múltiples interfaces (NMM) es un nodo que puede tener simultáneamente muchas direcciones y cualquiera o todas estas direcciones pueden cambiar con el tiempo. Un atacante móvil de múltiples interfaces (AMM) es una entidad maliciosa que controla un NMM (o más). El AMM puede ser el usuario del NMM o alguien (o alguna otra entidad) que haya plantado un "virus" o alguna otra funcionalidad en el NMM y que, así, puede no estar "físicamente" conectado al NMM.

Es posible que un AMM use un NMM para lanzar un ataque de inundación de red contra cualquier red a la cual el AMM sea capaz de conectar el NMM. Esta conexión del NMM puede llevarse a cabo usando un protocolo móvil de tipo Protocolo de Internet versión 6 (MIPv6). El ataque por inundación procedente del NMM se hace posible moviéndose a un contexto en el cual el AMM está controlando simultáneamente diferentes interfaces conectadas a diferentes redes. En tal contexto de múltiples interfaces, el AMM es capaz de aprovechar los mensajes de señalización de movilidad para combinar cualesquiera dos o más interfaces y presentarlas al nodo o a los nodos correspondientes como si cada una fuera bien una red propia o una red ajena.

Para combatir a tal AMM, puede utilizarse un filtrado de entrada, que es común en redes como las redes de 3GPP. Sin embargo, aunque el filtrado de entrada puede proporcionar una capacidad de identificar a un atacante, el filtrado de entrada puede no impedir el ataque. Además, en un entorno distinto del 3GPP, el problema es mucho más grave, porque el sistema de telecomunicaciones tiene menos control, debido a que se trata de un entorno más abierto y "público". Por ejemplo, no todos los NM conectadas pueden ser debidamente autentificados si están fuera de un entorno 3GPP. Además, tal como se describirá, el filtrado de entrada puede no siempre ser efectivo.

La FIG. 1 es un diagrama simplificado de bloques que ilustra un procedimiento de ruteabilidad de retorno (RR) ejecutado en un ataque convencional por inundación procedente de un AMM que control un NMM 14 en un sistema 12 de telecomunicaciones. El sistema de telecomunicaciones incluye un nodo móvil 14 de red de múltiples interfaces (NMM). El NMM 14 incluye una primera interfaz I_1 y una segunda interfaz I_2. Las interfaces pueden estar asociadas con direcciones IP. El sistema de telecomunicaciones también incluye nodos correspondientes (NC) 18 y 20.

Para lanzar el ataque por inundación de red, el AMM debe conectar una de las interfaces del NMM (por ejemplo, la I_1) a su correspondiente red propia o ajena y la otra interfaz (I_2) a un nodo objeto de ataque (por ejemplo, el NC 18 o 20).

Para comenzar el ataque por inundación, el AMM utiliza la interfaz I_1 del NMM para establecer diferentes sesiones con diferentes NC. Después de establecer estas diferentes sesiones con diferentes NC, el AMM conmuta el NMM a un modo de optimización de ruta (RO) desencadenando un procedimiento de ruteabilidad de retorno (RR). El procedimiento de RR requiere una prueba de asequibilidad de la dirección inicial (HoA), que conlleva el intercambio de mensajes HoTI/HoT 30 y 32 con cada NC 18 y 20 y una prueba de asequibilidad de la dirección de custodia (CoA), intercambiando mensajes 34 y 36 con los NC. Con este fin, la prueba de asequibilidad de la HoA se lleva a cabo usando la dirección IPv6 del NMM configurada en la I_1, como la HoA. Además, la prueba de asequibilidad de la CoA se realiza usando la dirección IPv6 del NMM configurada en la I_2, como la CoA.

La FIG. 2 es un diagrama simplificado de bloques que ilustra un procedimiento de intercambio de actualizaciones de enlaces durante el ataque convencional por inundación lanzado por el NMM 14 en el sistema 12 de telecomunicaciones. Después de completar todos los procedimientos de RR, se obliga al NMM 14 a enviar un mensaje de actualización de enlace (BU) a cada NC 18 y 20 por la interfaz I_2 para solicitar la creación de un enlace entre las dos direcciones y el reencaminamiento de paquetes de datos hacia la red objeto de ataque. En el protocolo móvil optimizado IPv6 (OMIPv6), el primer intercambio de mensajes de BU y de acuse de recibo del enlace (BA) 40 y 42 permite que el NMM comparta con el NC un secreto de larga duración. Además, se envían mensajes 44 y 46 de datos entre los NC y el NMM.

La FIG. 3 es un diagrama simplificado de bloques que ilustra paquetes de datos que inundan la red objeto de ataque en el ataque convencional por inundación en el sistema 12 de telecomunicaciones. El ataque comienza cuando el AMM 10 desconecta la interfaz I_2, con lo que el NMM desaparece de la red

objeto de ataque. A la vez, se hace que el NMM 14 sega enviando mensajes 50 y 52 de acuse de recibo (ACK) a cada NC por la interfaz I_1 para inundar a la red objeto de ataque durante todo el tiempo que haga falta. El AMM puede volver a conectar la interfaz I_2 del NMM a la red objeto de ataque en cualquier momento, autoconfigurar una nueva dirección IP y usar la nueva dirección IP para enviar un nuevo mensaje de BU a los NC 18 y 20 antes de volver a desaparecer.

El ataque descrito en lo que antecede es inmune contra el filtrado de entrada, especialmente cuando cada interfaz está usando su propia dirección IP legítima y está enviando únicamente el mensaje apropiado de señalización. Fundamentalmente, la características principal del ataque es que el NMM 14 asociado con el AMM copa todo el fondo común de direcciones disponibles (es decir, HoA y CoA) configurado en las interfaces. En una extensión al ataque por inundación de la red, se utilizan varias interfaces como si cada una fuera una red propia diferente y se usan las interfaces para enviar mensajes ACK a los NC.

No existe ningún sistema ni procedimiento para combatir un ataque por inundación procedente de un NMM. En un entorno de 3GPP, puede suponerse que está implementado el filtrado de entrada. Sin embargo, el filtrado de entrada no puede impedir el ataque. En un entorno de 3GPP, es posible que se sea capaz de identificar y hacer un seguimiento del atacante después del ataque, debido al uso de una autentificación robusta. Sin embargo, en un entorno de 3GPP, el ataque por inundación no puede impedirse. El patrón de señalización aprovechado por el AMM es completamente legítimo y no puede detectarse que se esté usando para lanzar un ataque malicioso. En el caso de un sistema de telecomunicaciones que utilice un entorno distinto del 3GPP, es aún más susceptible al ataque de un AMM.

La técnica relacionada dentro de esta especialidad se da a conocer, por ejemplo, en AURA T. et. al: “Effects of mobility and multihoming on transport-protocol security”, que presenta los modelos de amenaza y los mecanismos de seguridad usados en el diseño de protocolos de capas de transporte, centrándose en el SCTP.

En consecuencia, existe la necesidad de un sistema y un procedimiento de protección de un sistema de telecomunicaciones contra los ataques por parte de AMM. La presente invención proporciona tal sistema y tal procedimiento.

RESUMEN DE LA INVENCIÓN

La presente invención es un sistema y un procedimiento de protección de un sistema de telecomunicaciones contra un ataque por inundación procedente de un nodo de red de múltiples interfaces, en particular un nodo móvil de red de múltiples interfaces (NMM). De forma alternativa, el atacante (AMM) puede ser el usuario del NMM o alguien (o alguna otra entidad) que haya plantado un “virus” o alguna otra funcionalidad en el NMM y pueda así no estar “físicamente” conectado al NMM. La presente invención proporciona tanto protección como disuasión contra un ataque detectado de denegación de servicio (DoS) por inundación.

En una realización, se supone que el AMM tiene el control de un único NMM y, así, los términos NMM/AMM pueden usarse de manera intercambiable, dado que las acciones del AMM son realizadas por el AMM que controla el NMM para llevar a cabo ciertas acciones de protocolo. Por supuesto, el caso en que el AMM controla varios NMM es más serio, pero los ataques distribuidos de denegación de servicio (DDoS) pueden gestionarse uno a uno (o en paralelo) aplicando el mismo procedimiento descrito en lo que sigue a cada NMM controlado.

Así, en un aspecto, la presente invención está dirigida a un sistema para proteger una red de telecomunicaciones contra un ataque por inundación procedente de un nodo de red de múltiples interfaces, proporcionando la red de telecomunicaciones comunicaciones a un nodo de red que actúa como nodo correspondiente (NC) para el nodo de red de múltiples interfaces. El sistema incluye un medio para determinar si el nodo de red de múltiples interfaces sigue estando asequible un tiempo predeterminado después de que el NC y el nodo de red de múltiples interfaces empiezan a intercambiar entre sí paquetes de datos; y un medio sensible a una determinación de que el nodo de red de múltiples interfaces ya no es asequible para limpiar del NC la información almacenada en memoria intermedia asociada con el nodo de red de múltiples interfaces. El nodo de red de múltiples interfaces puede ser un nodo móvil de red de múltiples interfaces (NMM) que tenga una pluralidad de direcciones IP. El medio para determinar si el nodo de red de múltiples interfaces sigue siendo asequible puede ser un encaminador de acceso (EA) asociado con el NC, que lleva a cabo la prueba de asequibilidad con el NMM. Si el nodo de red de múltiples interfaces ya no es asequible, el EA envía un mensaje al NC que da instrucciones al NC para que limpie la información almacenada en memoria intermedia asociada con el nodo de red de múltiples interfaces. Una vez se ha limpiado la memoria intermedia, se detiene, de hecho, la transmisión de datos hacia la red objeto de ataque.

En otro aspecto, la presente invención está dirigida a un procedimiento de protección de una red de telecomunicaciones contra un ataque por inundación procedente de un nodo de red de múltiples

interfaces, proporcionando la red de telecomunicaciones comunicaciones a un nodo de red que actúa como nodo correspondiente (NC) para el nodo de red de múltiples interfaces. El procedimiento incluye las etapas de transferir datos entre el NC y el nodo de red de múltiples interfaces; y determinar si el nodo de red de múltiples interfaces sigue siendo asequible. Si el nodo de red de múltiples interfaces sigue siendo asequible, el procedimiento continúa transfiriendo datos entre el NC y el nodo de red de múltiples interfaces. Si el nodo de red de múltiples interfaces ya no es asequible, el procedimiento limpia del NC la información almacenada en memoria intermedia asociada con el nodo de red de múltiples interfaces. El nodo de red de múltiples interfaces puede ser un nodo móvil de red de múltiples interfaces (NMM) que tenga una pluralidad de direcciones IP.

En otro aspecto adicional, la presente invención está dirigida a un nodo de protección de redes para proteger una red de telecomunicaciones contra un ataque por inundación procedente de un nodo de red de múltiples interfaces, proporcionando la red de telecomunicaciones comunicaciones a un nodo de red que actúa como nodo correspondiente (NC) para el nodo de red de múltiples interfaces. El nodo de protección incluye un medio para determinar si el nodo de red de múltiples interfaces sigue siendo asequible un tiempo predeterminado después de que el NC y el nodo de red de múltiples interfaces comiencen a transferir entre sí paquetes de datos; y un medio de comunicaciones, sensible a la determinación de que el nodo de red de múltiples interfaces ya no es asequible, para enviar un mensaje al NC que da instrucciones al NC para que limpie la información almacenada en memoria intermedia asociada con el nodo de red de múltiples interfaces. En una realización preferente, el nodo de protección de redes es un encaminador de acceso.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

En la siguiente sección, se describirá la invención con referencia a realizaciones ejemplares ilustradas en las figuras, en las que:

la FIG. 1 (técnica anterior) es un diagrama simplificado de bloques que ilustra un procedimiento de ruteabilidad de retorno (RR) ejecutado en un ataque convencional por inundación procedente de un NMM en un sistema de telecomunicaciones;

la FIG. 2 (técnica anterior) es un diagrama simplificado de bloques que ilustra un procedimiento de intercambio de actualizaciones de enlaces durante el ataque convencional por inundación procedente del NMM en el sistema de telecomunicaciones;

la FIG. 3 (técnica anterior) es un diagrama simplificado de bloques que ilustra paquetes de datos que inundan la red objeto de ataque en el ataque convencional por inundación procedente del NMM en el sistema de telecomunicaciones;

la FIG. 4 es un diagrama simplificado de bloques de componentes de un sistema de telecomunicaciones que emplea una protección contra DoS en una realización ejemplar de la presente invención;

la FIG. 5 es un diagrama de señalización que ilustra el flujo de mensajes en la defensa contra un ataque procedente del NMM en la realización ejemplar de la presente invención; y

las FIGURAS 6A-6B son porciones de un diagrama de flujo que ilustra las etapas de una realización ejemplar del procedimiento de la presente invención en la defensa contra un ataque procedente del NMM.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

La FIG. 4 es un diagrama simplificado de bloques de componentes de un sistema 100 de telecomunicaciones que emplea una protección contra DoS en una realización ejemplar de la presente invención. La presente invención proporciona protección contra los ataques de denegación de servicio (DoS) dentro de un sistema 100 de telecomunicaciones. El sistema incluye un NC 102, un NC 104 y un encaminador de acceso (EA) 106. Como en los escenarios convencionales, el NMM 108 intenta atacar, por medio de los NC, una red seleccionada.

La presente invención implica activamente a la red ajena en el mantenimiento del funcionamiento del modo MIPv6 de optimización de ruta (RO) entre los dos puntos extremos de la red. En una realización de la presente invención se utilizan tres provisiones para la defensa contra estos ataques. La primera provisión es delegar las pruebas de asequibilidad de la CoA del NMM en el encaminador de acceso (EA) del NMM. La segunda provisión es introducir un nuevo mensaje de señalización, que les dice a los NC, deteniendo con ello el ataque, que limpien la información almacenada en memoria intermedia dentro de los NC, que, si no, se usaría para mantener el flujo de datos con la red objeto de ataque. La tercera provisión es hacer consciente al AMM de que en la red están implementados los dos pasos anteriores. Esto proporciona disuasión contra los ataques de NMM haciéndolos conscientes de que hay implementadas contramedidas.

En la primera provisión, se llevan a cabo las pruebas 110 de asequibilidad de la CoA entre el NMM 108 y el EA 106, que sustituyen a los mensajes CoTI/CoT de la FIG. 1 con una prueba de asequibilidad de prefijos.

En la segunda provisión de la presente invención, el fin principal es aumentar la capacidad de la red ajena para protegerse contra la ataque por inundación descrito en las FIGURAS 1-3. Para facilitar este fin, la confianza entre el NMM y su EA, que se obtiene ejecutando el protocolo OptiSEND, es aprovechada para construir también una relación de confianza entre el EA y el o los NC y también está muy asociada con el NMM. Debería entenderse que el NMM puede ser el atacante. Así, el fin no es crear una confianza "transitiva" del NMM hacia el NC, sino más bien al revés. Así, si el NMM es, en efecto, el atacante, la principal confianza aprovechada es entre el EA 108 y los NC 102 y 104. Esta confianza puede estar asociada con un NMM particular 108.

La relación de confianza entre el NC y el EA permite que el EA 106 solicite de manera explícita y segura al NC que limpie de sus entradas 120 de enlaces almacenadas en memoria intermedia (BCE) cualquier CoA que se haya usado para lanzar un ataque por inundación contra la red. Con este fin, preferentemente, el EA envía al o a los NC un nuevo mensaje de señalización de movilidad denominado mensaje 112 de "solicitud de limpieza de enlaces" (BFR) que contiene la HoA del NMM. Si el EA 106 ha autentificado debidamente al NMM 108 y se tiene confianza en el EA, puede vincularse con el NMM un ataque descubierto y, en general, los NC pueden vincular un mensaje de limpieza con el NMM particular implicado en el ataque.

Tras la recepción de un mensaje 112 válido de BFR, los NC borran la entrada correspondiente al NMM de sus BCE 120 y cierran todas las sesiones en curso con el NMM 108. Además, preferentemente, cada NC responde al EA 106 enviando un mensaje 122 de acuse de recibo de la limpieza de enlaces (BFA). Preferentemente, el mensaje BFA es autentificado también con una clave usada por el EA.

La tercera provisión de la presente invención es hacer al NMM 108 controlado por un AMM plenamente consciente de las medidas de protección (es decir, las dos primeras provisiones) que se emplean en el sistema 10 de telecomunicaciones. Preferentemente, la advertencia al AMM en cuanto a las reglas de la red ajena se provee añadiendo una extensión al protocolo OptiSEND, que solicita explícitamente al NMM que comparta con el EA la clave calculada de su secreto compartido (Ks) de larga duración obtenido de la ejecución del protocolo OMIPv6. La extensión del protocolo OptiSEND puede incluir establecer un nuevo bit en el mensaje de anuncio de encaminamiento (RtAdv) enviado periódicamente por el EA. También puede utilizarse el protocolo SEND para alertar al AMM de que se están empleando medidas de protección en el sistema de telecomunicaciones.

La nueva clave compartida, denominada Kc, permite que el EA 106 y los NC autentifiquen los mensajes de las pruebas de asequibilidad de prefijos (es decir, implícitamente, la validez de la Kc de la prueba) y que autentifiquen los mensajes de BFR y BFA, tal como se ha expuesto más arriba.

La FIG. 5 es un diagrama de señalización para la defensa contra un ataque procedente de un AMM en la realización ejemplar de la presente invención. En 190, se transfieren datos entre el NC 102 y 104 y el NMM 108 del AMM. Durante el periodo de tiempo en que el NC está transfiriendo paquetes, en 200 se lleva a cabo una prueba 110 de asequibilidad entre el EA 106 y el NMM 108. En 202, el EA desencadena un procedimiento de detección de inasequibilidad. Debería hacerse notar que el NMM ha desconectado su interfaz antes de inundar la red, lo que desencadena la detección de inasequibilidad por parte del EA. El procedimiento de detección de inasequibilidad muestra el EA que el NMM es inasequible por el enlace. El EA 106 espera entonces un periodo de tiempo predefinido en 206. Tras el paso del periodo de tiempo predefinido, el EA envía un mensaje 112 de BFR a cada dirección de NC almacenada en su memoria intermedia en 208. Preferentemente, todos los mensajes de BFR se autentifican con la Kc. Durante el periodo de tiempo de espera, el EA puede almacenar los paquetes de datos recibidos en su memoria intermedia, dado que el NMM puede simplemente estar fuera de alcance por otros factores posibles (por ejemplo, ruido en el enlace y similares).

Tras la recepción del mensaje 208 de BFR, los NC 102 y/o 104 determinan en 210 si la CoA llevada en el mensaje ya está almacenada en la BCE 120 del NC. A continuación, el NC recupera la correspondiente Kc y valida la autentificación en 212. En 214, el NC limpia la entrada correspondiente a la CoA y cierra la sesión. Al final de esta etapa se detiene el ataque por inundación. Además, todos los NC han borrado las entradas del atacante de sus BCE. El NC puede proporcionar una directriz especificada para aceptar una nueva solicitud de conexión procedente de un nodo que tenga la misma HoA. Después de limpiar la entrada correspondiente del NMM, cada NC envía, preferentemente, un mensaje 122 de BFA al EA 106 en 216. El mensaje de BFA puede ser autentificado con la Kc.

Las FIGURAS 6A-6B son porciones de un diagrama de flujo que ilustra las etapas de una realización ejemplar del procedimiento de la presente invención en la defensa contra un ataque procedente de un NMM. En lo que sigue, se explicará el procedimiento con referencia a las FIGURAS 4, 5, 6A y 6B. el procedimiento comienza en la etapa 300, en la que se transmiten datos entre el NC 102 y 104 y el NMM 108 (y el AMM 110). A continuación, en la etapa 302, se realiza una prueba 110 de asequibilidad entre el

EA 106 y el NMM 108. El procedimiento pasa entonces a la etapa 304, en la que se determina que el NMM no es asequible (es decir, el EA no puede llevar a cabo la prueba 110 de asequibilidad de la CoA con el NMM). Si se determina que el NMM es asequible, el procedimiento vuelve a la etapa 300, en la que siguen transfiriéndose datos al NMM desde el NC.

Sin embargo, en la etapa 304, si se determina que el NMM no es asequible, el procedimiento pasa entonces a la etapa 306, en la que el EA desencadena un procedimiento de detección de inasequibilidad. Durante el ataque, el NMM ha desconectado su interfaz antes de inundar la red, lo que desencadena la detección de inasequibilidad por parte del EA. El procedimiento de detección de inasequibilidad muestra al EA que el NMM es inasequible por el enlace. Durante el periodo de tiempo de espera, el EA puede almacenar los paquetes de datos recibidos en su memoria intermedia, dado que el NMM puede simplemente estar fuera de alcance por otros factores posibles (por ejemplo, ruido en el enlace y similares). Acto seguido, en la etapa 308, el EA aguarda durante un periodo de tiempo predefinido. Al final del periodo de tiempo predefinido, el procedimiento pasa a la etapa 310, en la que vuelve a determinarse si el NMM es asequible. Si se determina que el NMM es asequible (es decir, por pruebas 110 de asequibilidad coronadas por el éxito), el procedimiento vuelve a la etapa 300, en la que siguen transfiriéndose datos. Sin embargo, en la etapa 310, si el NMM sigue siendo inasequible, el procedimiento pasa a la FIG. 6B, etapa 312, en la que el EA envía un mensaje 112 de BFR a cada dirección de NC almacenada en su memoria intermedia. Preferentemente, todos los mensajes de BFR se autentifican con la Kc.

A continuación, en la etapa 314, tras la recepción de un mensaje 122 de BFR, los NC 102 y/o 104 determinan si la CoA llevada en el mensaje ya está almacenada en la BCE 120 del NC. El procedimiento pasa entonces a la etapa 316, en la que el NC recupera la correspondiente Kc y valida la autentificación. A continuamente, en la etapa 318, el NC limpia la entrada correspondiente a la CoA y cierra la sesión. Al final de esta etapa se detiene el ataque por inundación. Además, todos los NC borran las entradas del atacante de sus BCE. El NC puede proporcionar una directriz especificada para aceptar una nueva solicitud de conexión procedente de un nodo que tenga la misma HoA. El procedimiento pasa a la etapa 320, en la que, después de limpiar la entrada correspondiente del NMM, cada NC envía, preferentemente, un mensaje 216 de BFA al EA 106. El mensaje de BFA puede ser autentificado con la Kc.

La presente invención proporciona protección y disuasión contra un ataque detectado de DoS. La presente invención puede utilizar una o la totalidad de las provisiones para combatir el ataque. Específicamente, el componente de disuasión de la presente invención puede ser implementado o no con la presente invención.

Por supuesto, la presente invención puede ser llevada a cabo de otras maneras específicas distintas a las expuestas en el presente documento sin apartarse de las características esenciales de la invención. Por lo tanto, las presentes realizaciones deben ser consideradas en todos los aspectos como ilustrativas y no restrictivas, y se entiende que todos los cambios que están dentro del significado y el abanico de equivalencias de las reivindicaciones adjuntas están abarcados por las mismas.

REIVINDICACIONES

1. Un procedimiento para un encaminador de acceso para proteger una red de telecomunicaciones contra un ataque por inundación procedente de un nodo de red de múltiples interfaces, proporcionando el encaminador de acceso comunicaciones entre el nodo de red de múltiples interfaces y un nodo de red que actúa como nodo correspondiente NC para el nodo de red de múltiples interfaces, comprendiendo el procedimiento las etapas de:

transferir (300) datos entre el nodo de red de múltiples interfaces y el NC;

determinar (302) si el nodo de red de múltiples interfaces sigue siendo asequible;

si el nodo de red de múltiples interfaces sigue siendo asequible, continuar transfiriendo datos entre el NC y el nodo de red de múltiples interfaces; y

después de determinar que el nodo de red de múltiples interfaces ya no es asequible, dar al NC instrucciones para que limpie la información almacenada en memoria intermedia asociada con el nodo de red de múltiples interfaces.

2. El procedimiento de protección de un sistema de telecomunicaciones según la reivindicación 1 en el que el nodo de red de múltiples interfaces es un nodo móvil NMM de red de múltiples interfaces y en el que paso de determinar si el nodo de red de múltiples interfaces sigue siendo asequible incluye llevar a cabo un procedimiento de detección de asequibilidad de direcciones IP vecinas entre el encaminador de acceso y el NMM.

3. El procedimiento de protección de un sistema de telecomunicaciones según la reivindicación 1 en el que la etapa de dar instrucciones al NC para que limpie la información almacenada en memoria intermedia incluye dar instrucciones al NC para que limpie las entradas de enlaces de la memoria intermedia del NC.

4. El procedimiento de protección de un sistema de telecomunicaciones según la reivindicación 2 que comprende además alertar al NMM acerca de la protección contra la denegación de servicio dentro del sistema de telecomunicaciones y en el que la etapa de alertar al NMM acerca de la protección contra la denegación de servicio incluye añadir una extensión a un mensaje de protocolo OptiSEND o a un mensaje de protocolo SEND para alertar al NMM.

5. Un encaminador (106) de acceso para proteger una red de telecomunicaciones contra un ataque por inundación procedente de un nodo (108) de red de múltiples interfaces, proporcionando el encaminador de acceso comunicaciones entre el nodo de red de múltiples interfaces y un nodo de red que actúa como nodo correspondiente NC para el nodo de red de múltiples interfaces, comprendiendo la disposición:

un medio para transferir datos entre el nodo de red de múltiples interfaces y el NC;

un medio para determinar si el nodo de red de múltiples interfaces sigue siendo asequible un tiempo predeterminado después de que comience la transferencia de datos; y

un medio para dar al NC instrucciones para que limpie la información almacenada en memoria intermedia asociada con el nodo de red de múltiples interfaces, en respuesta a una determinación de que el nodo de red de múltiples interfaces ya no es asequible.

6. El encaminador de acceso para proteger una red de telecomunicaciones según la reivindicación 5 en el que el nodo de red de múltiples interfaces es un nodo móvil NMM de red de múltiples interfaces que tiene una pluralidad de direcciones IP.

7. El encaminador de acceso para proteger una red de telecomunicaciones según la reivindicación 5 en el que, tras determinar que el nodo de red de múltiples interfaces ya no es asequible, el encaminador de acceso está adaptado para enviar un mensaje al NC dando instrucciones al NC para que limpie la información almacenada en memoria intermedia asociada con el nodo de red de múltiples interfaces.

8. El encaminador de acceso para proteger una red de telecomunicaciones según la reivindicación 7 en el que el encaminador de acceso está adaptado para determinar si el nodo de red de múltiples interfaces sigue estando asequible llevando a cabo un procedimiento de detección de asequibilidad de direcciones IP vecinas entre el encaminador de acceso y el nodo de red de múltiples interfaces.

9. El encaminador de acceso para proteger una red de telecomunicaciones según la reivindicación 7 en el que el mensaje para limpiar la información almacenada en memoria intermedia es una solicitud de limpieza de enlaces para limpiar el NC de cualquier dirección asociada con el NMM.

10. El encaminador de acceso para proteger una red de telecomunicaciones según la reivindicación 5 que además comprende un medio para informar al NMM acerca de la protección contra la denegación de servicio dentro del sistema de telecomunicaciones.

11. Un nodo de protección para proteger una red de telecomunicaciones contra un ataque por inundación procedente de un nodo de red de múltiples interfaces, proporcionando el nodo de protección comunicaciones entre el nodo de red de múltiples interfaces y un nodo de red que actúa como nodo correspondiente NC para el nodo de red de múltiples interfaces, comprendiendo el nodo de protección:

un medio para transferir datos entre el nodo de red de múltiples interfaces y el NC;

un medio para determinar si el nodo de red de múltiples interfaces sigue siendo asequible un tiempo predeterminado después de que comience la transferencia de datos; y

un medio de comunicaciones, en respuesta a la determinación de que el nodo de red de múltiples interfaces ya no es asequible, para enviar un mensaje al NC que le da instrucciones para que limpie la información almacenada en memoria intermedia asociada con el nodo de red de múltiples interfaces.

12. El nodo de protección de red según la reivindicación 11 en el que el nodo de red de múltiples interfaces es un nodo móvil NMM de red de múltiples interfaces que tiene una pluralidad de direcciones IP y en el que el ataque está controlado por un atacante móvil AMM de red y de múltiples interfaces que es el usuario del NMM o una entidad que ha plantado funcionalidad en el NMM o tiene el control de otra manera del NMM.

13. El nodo de protección de red según la reivindicación 11 en el que el medio de comunicaciones incluye un medio para enviar una solicitud de limpieza de enlaces para dar instrucciones al NC para que limpie cualquier dirección asociada con el NMM, y un medio para informar al NMM acerca de la protección contra la denegación de servicio dentro de la red de comunicaciones que incluye un medio para añadir una extensión a un mensaje de protocolo OptiSEND o a un mensaje de protocolo SEND para alertar al NMM.

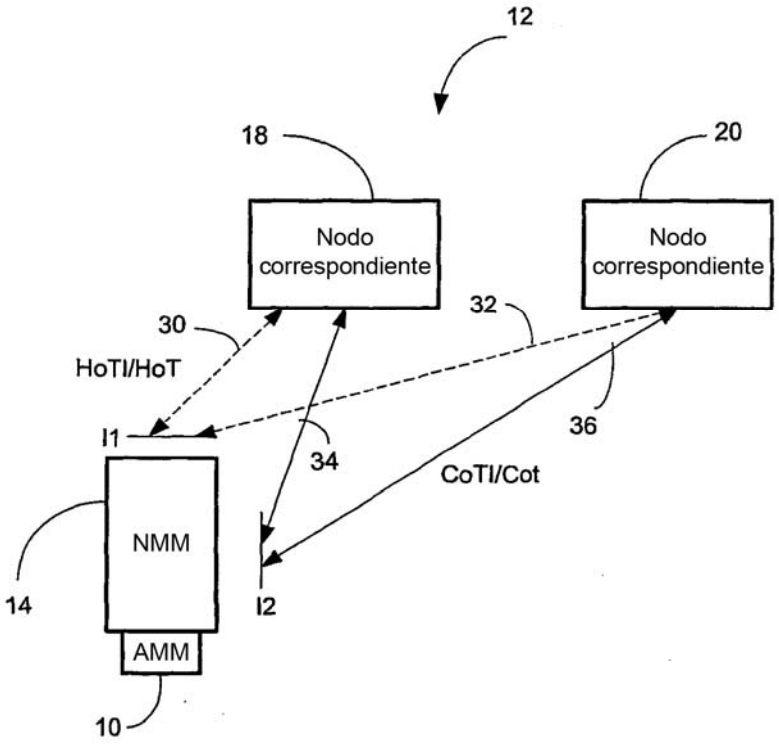


FIG. 1
(Técnica anterior)

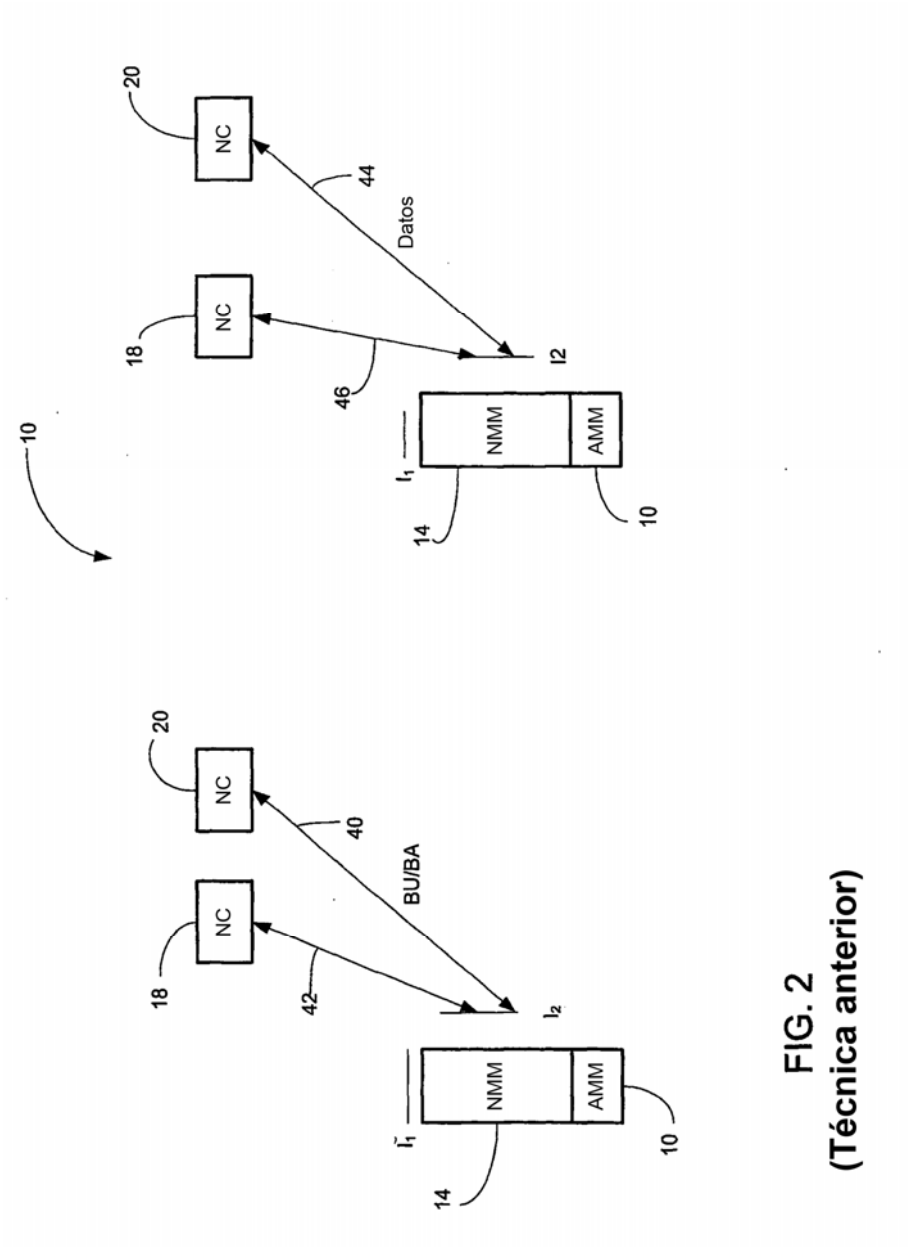


FIG. 2
(Técnica anterior)

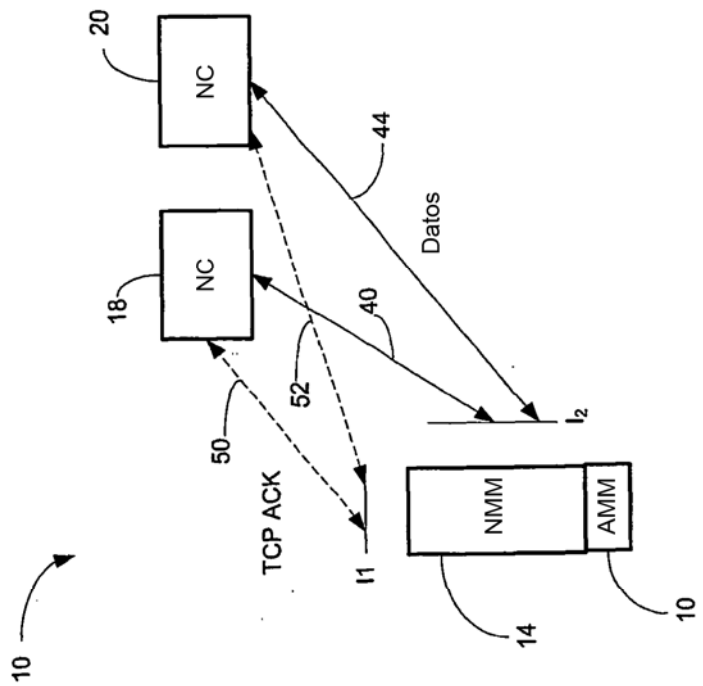


FIG. 3
(Técnica anterior)

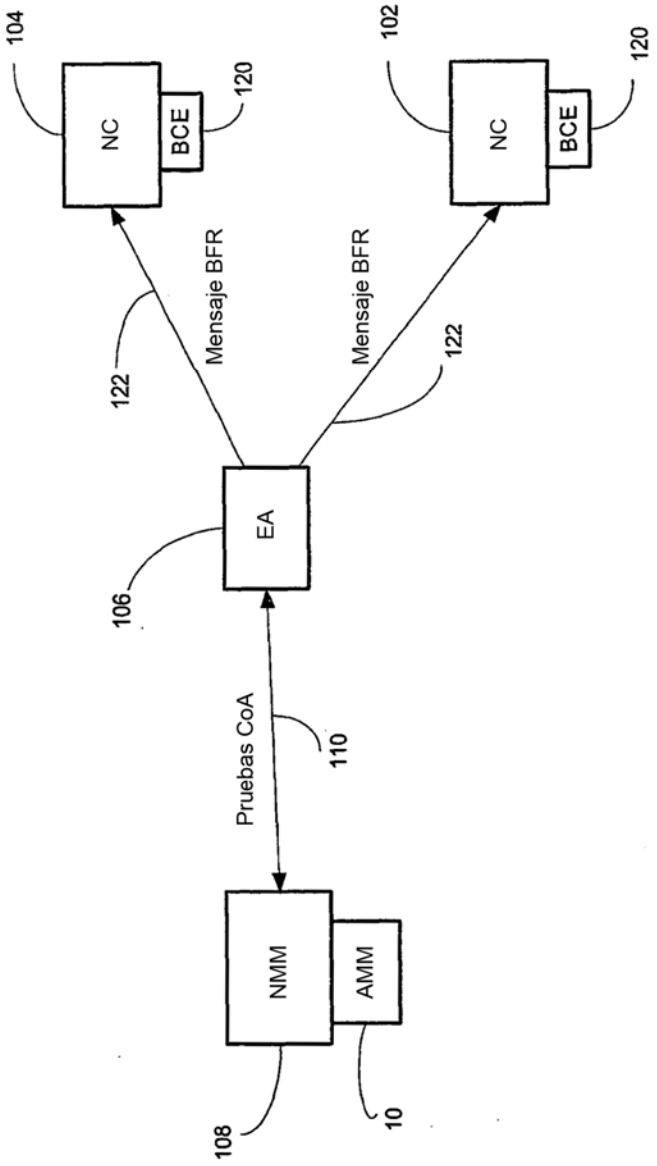

104
NC
BCE
120
102
NC
BCE
120
Mensaje BFR
122
Mensaje BFR
122
EA
106
Pruebas CoA
110
NMM
AMM
108
10

FIG. 4

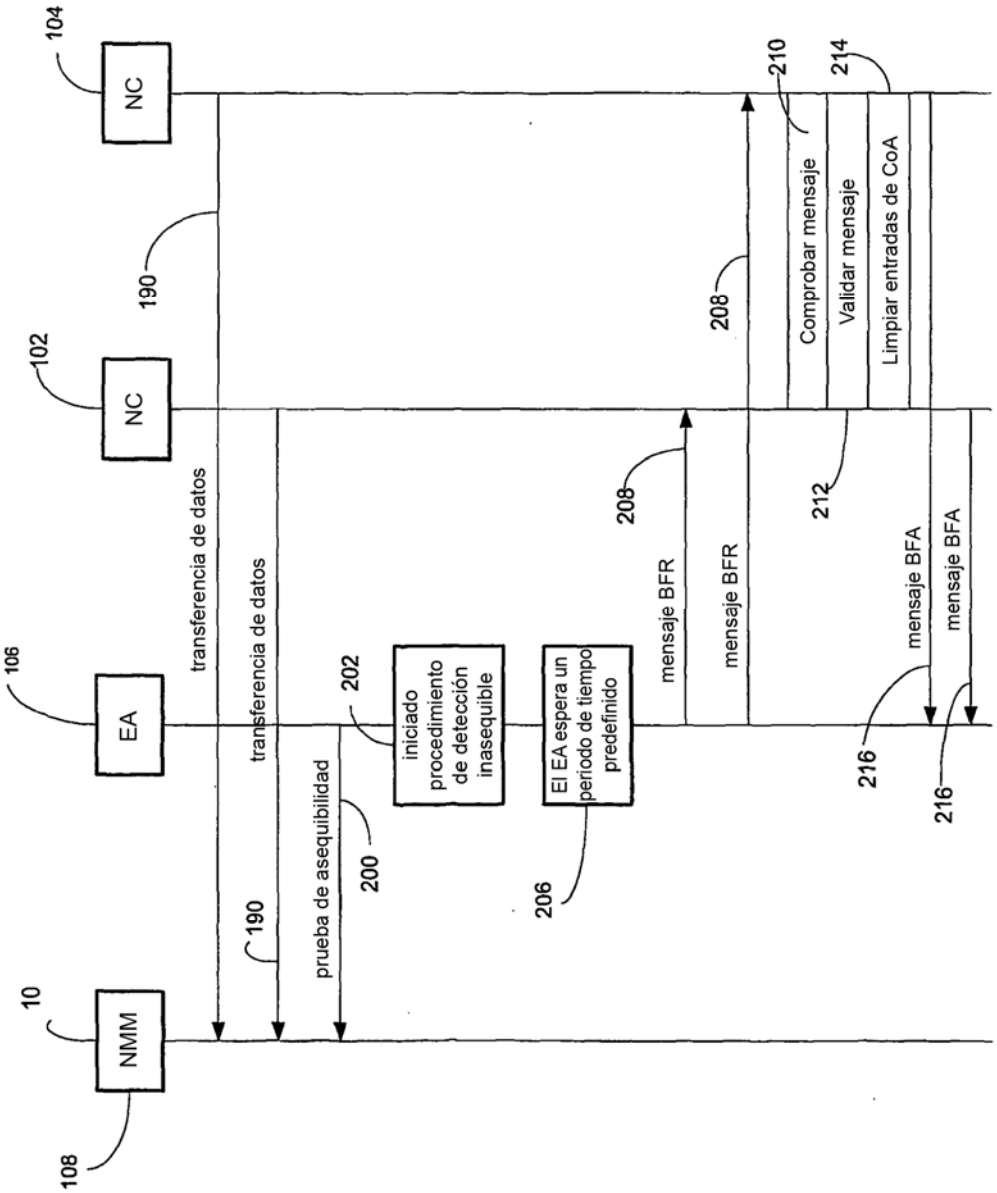

NMM
EA
NC
NC
10
106
104
102
108
transferencia de datos
transferencia de datos
prueba de asequibilidad
iniciado procedimiento de detección inasequible
El EA espera un período de tiempo predefinido
mensaje BFR
mensaje BFR
Comprobar mensaje
Validar mensaje
Limpiar entradas de CoA
mensaje BFA
mensaje BFA
190
190
200
202
206
208
208
210
212
214
216
216

FIG. 5

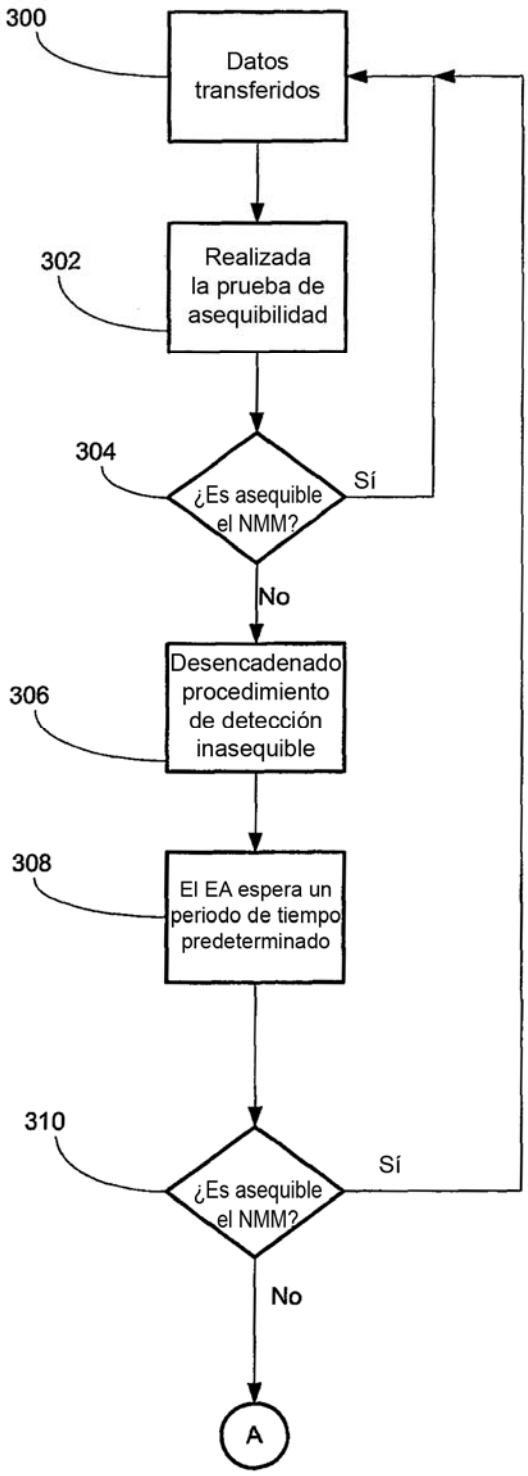
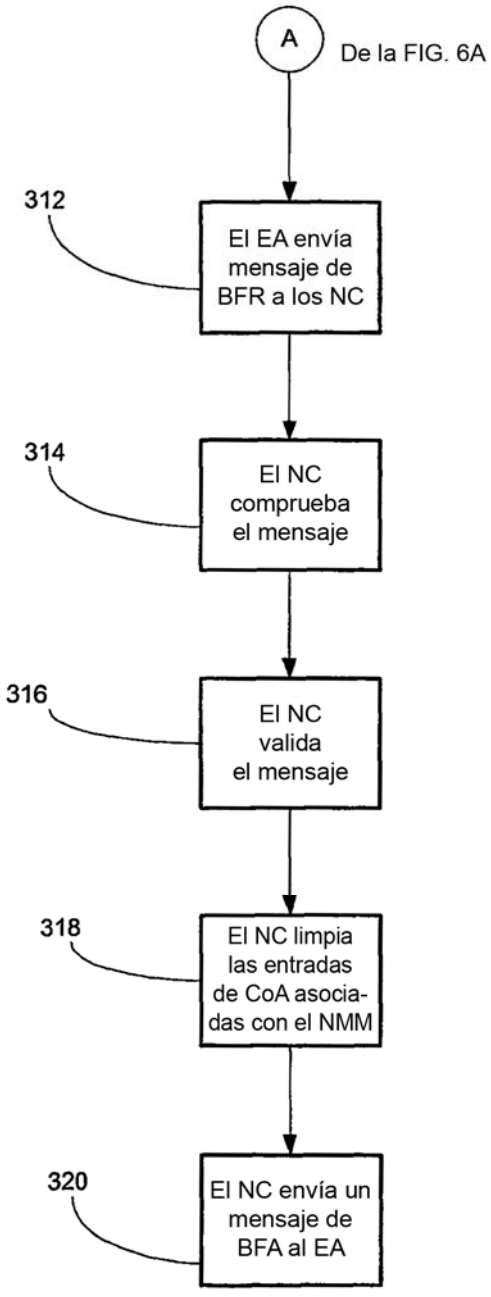

300
Datos transferidos
302
Realizada la prueba de asequibilidad
304
¿Es asequible el NMM?
Sí
No
306
Desencadenado procedimiento de detección inasequible
308
El EA espera un periodo de tiempo predeterminado
310
¿Es asequible el NMM?
Sí
No
A

FIG. 6A

FIG. 6B


A
De la FIG. 6A
312
El EA envía mensaje de BFR a los NC
314
El NC comprueba el mensaje
316
El NC valida el mensaje
318
El NC limpia las entradas de CoA asociadas con el NMM
320
El NC envía un mensaje de BFA al EA