A mobilidade na Internet através do protocolo HIP (Host Identity Protocol)

Wander Barbato
Especialista em Administração de Sistemas de Informação - UFLA
Professor da Faculdade Comunitária de Limeira
e-mail: wbarbato@ceset.unicamp.br

Resumo

A Internet tem se tornado cada vez mais importante na vida das pessoas, seja para trabalho, busca de informação, entretenimento ou negócios. Com a evolução dos dispositivos móveis, a necessidade de acesso à rede mundial está além do escritório ou do lar, ou seja, as pessoas gostariam de acessar a Internet através de seu notebook enquanto estão no caminho para o trabalho, para casa ou para a escola. Para resolver o problema da mobilidade na Internet já existe o padrão Mobile IP. Porém, o Mobile IP não resolve totalmente as questões da mobilidade e segurança na Internet e, por isso, outras propostas estão sendo estudadas. Este trabalho descreve as principais características do protocolo HIP (Host Identity Protocol), que propõe o gerenciamento da mobilidade de um usuário e suas aplicações de forma inovadora, através da separação das funções de identificação e localização. Com o HIP, será possível fornecer acesso permanente a uma rede, independentemente da localização física dos dispositivos.

Palavras-chave: Host Identity Protocol, Mobilidade na Internet, Multi-homing.

Abstract

The Internet has been each time more important for people's life, either for work, information searching, entertainment or business. With the evolution of mobile devices, the necessity of access to the world-wide net is beyond the office or home, or either, people would like to access the Internet through their notebooks while they are in the way to the work, house or school. For to solve the problem of Internet mobility already exists the Mobile IP. However, Mobile IP does not solve totally the questions of mobility and security in the Internet and, therefore, other proposals are being studied. This work describes the main features of HIP (Host Identity Protocol), that it considers the mobility management of an user and its applications of innovative form, through separation of identification and location functions. With the HIP, it will be possible to supply permanent access to the net independently of the physical location of the devices.

Key-words: Host Identity Protocol, Internet Mobility, Multi-homing.

Introdução

Assim como outras tecnologias do passado, tais como a transmissão de rádio e televisão e a telefonia, a Internet revolucionou a vida da maioria das pessoas. A diversidade de serviços oferecidos, a comodidade proporcionada e a velocidade com que novas aplicações são criadas impressionam, mas freqüentemente são necessárias mudanças ou extensões na arquitetura original de protocolos para que os serviços coexistam.

Por muitos anos, os computadores raramente eram realocados no espaço físico e suas interfaces de rede possuíam endereços fixos. Ainda hoje, na arquitetura de protocolos da Internet, o endereço IP de um host acumula duas funcionalidades distintas: localizador do equipamento na topologia da rede (utilizado pelo serviço de roteamento) e identificador do nó na Internet (utilizado pelas aplicações na camada de transporte). No entanto, alguns protocolos, tais como DHCP - Dynamic Host Control Protocol - e PPP - Point-to-Point Protocol, atribuem endereços IP dinamicamente para os computadores e, portanto, uma mesma interface de rede pode ter endereços IP diferentes no decorrer do tempo. Além disso, a escassez de endereços na Internet fez com que muitas empresas implementassem o serviço NAT (Network Address Translator) e utilizassem endereços privados em suas redes internas, quebrando o paradigma da identificação de um nó através do endereço IP nas conexões fim-a-fim (NIKANDER et al, 2003).

Atualmente muitos computadores possuem tamanho físico reduzido e são portáteis (notebooks e PDA's, por exemplo) e várias tecnologias de comunicação sem fio foram desenvolvidas, facilitando o uso da Internet móvel. Com isso, quando um computador conectado à Internet migra de uma rede para outra, possivelmente o seu endereço IP é alterado para adaptar-se à nova topologia.

Devido a esse deslocamento de nós móveis na Internet, alguns problemas devem ser levados em consideração, tais como a perda de identidade do host após a alteração do endereço IP e a conseqüente perda das conexões ativas, já que as aplicações utilizam o par <endereço IP,porta>[1] para identificar os processos comunicantes.

Uma solução existente, o Mobile IP, procura administrar a mobilidade na Internet através da criação de um endereço fixo para identificação do host (home address) e um endereço de visitante (care-of-address) para fins de alcançabilidade (YLITALO & NIKANDER, 2004). Os pacotes sempre são destinados para o endereço fixo na rede doméstica do host, mas agentes de encaminhamento são responsáveis por fazer o redirecionamento das mensagens para o endereço de visitante do host. Sempre que houver uma migração de rede, o endereço de visitante é alterado, mas o home address continua o mesmo. Assim, as conexões ativas são mantidas de forma transparente para o usuário e para as aplicações. A Figura 1 ilustra o funcionamento básico do Mobile IP.

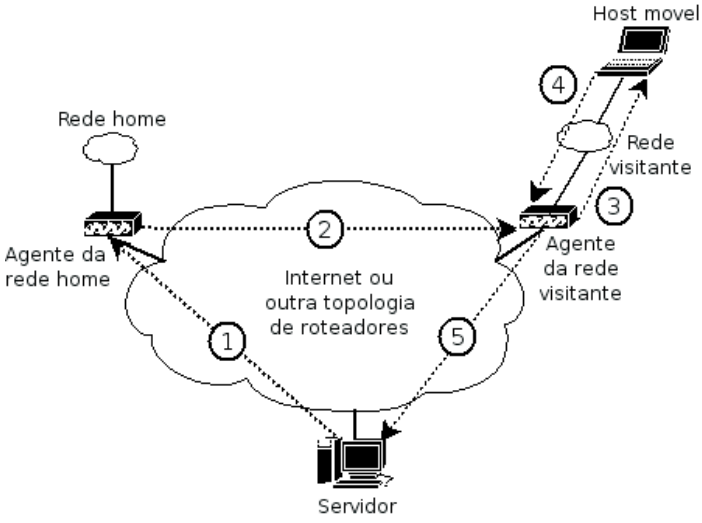

Figura 1 - Funcionamento básico do Mobile IP

No entanto, para Nikander et al (2003), o Mobile IP tem algumas deficiências e não leva em consideração questões de segurança, confiando integralmente no sistema de roteamento. Um host mal-intencionado pode passar-se por outro ou pode efetuar ataques de negação de serviço (DoS - Denial of Service) através do envio de mensagens falsas de atualização de endereço.

Na próxima seção será descrita uma outra proposta de gerenciamento da mobilidade através do protocolo HIP (Host Identity Protocol), que cria um novo espaço de nomes na Internet.

Host Identity Protocol (HIP)

A principal idéia do protocolo HIP é criar um novo espaço de nomes entre as camadas de rede e de transporte na arquitetura de protocolos da Internet. Conforme Moskowitz e Nikander (2006), essa nova camada, a camada de identidade do host, utiliza um identificador (HI - Host Identifier) que representa a identidade de um nó na Internet e possui uma ligação dinâmica com o endereço IP, o qual continua desempenhando a função de localizador do nó na topologia da rede e é utilizado pelo serviço de roteamento. A Figura 2 mostra as diferenças das ligações na arquitetura atual e na arquitetura proposta.

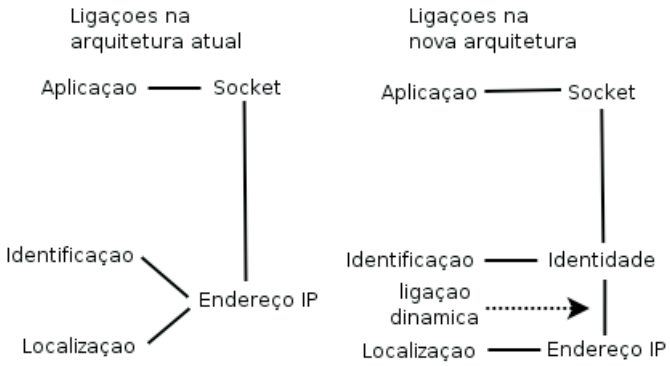

Figura 2 - Ligações na arquitetura atual e na arquitetura proposta pelo protocolo HIP

A separação da localização e da identificação do host faz com que as aplicações não estejam mais vinculadas ao endereço IP de uma interface, independentemente de sua localização topológica e dos resultados de sua movimentação, tornando o HIP uma boa solução para implementar a mobilidade na Internet de forma transparente.

O identificador (HI) é criado por um nó HIP-capaz a partir de um valor aleatório e tem significado global no sistema de nomes. O HI é uma chave pública de uma tupla de chaves pública-privada, na qual a chave pública é acessível para outros nós HIP-capazes e a chave privada representa a identidade do host proprietário (somente ele tem a sua posse). Opcionalmente, a camada de identidade do host pode criar uma HIT (Host Identity Tag). A HIT é um valor

codificado de 128 bits calculado por uma função de hashing sobre o HI. A HIT tem tamanho fixo, o que facilita sua utilização por outros protocolos, é auto-certificadora (autentica um host sem a necessidade de uma entidade externa) e possui uma única chave privada correspondente (MOSKOWITZ & NIKANDER, 2006).

Segundo Jokela et al (2004), é possível fazer uma analogia entre uma rede HIP-capaz e o mundo real. Com o HIP, os hosts podem se deslocar continuamente e ter diferentes endereços IP, pois o HI (chave pública) é que representa a sua identidade (chave privada). O endereço IP é apenas uma referência à localização do host em determinado momento. No mundo real, os indivíduos também podem visitar diferentes lugares, mas são reconhecidos através de seus identificadores (documentos, fotos e assinaturas, por exemplo) que dão autenticidade à sua única identidade. No entanto, ao contrário do mundo real, com o protocolo HIP um mesmo nó pode ter várias identidades. Isso pode ocorrer por razões de privacidade, já que é mais viável um host criar várias chaves privadas temporárias do que utilizar uma única chave privada permanente, para evitar o rastreamento de atividades que realizou ao longo do tempo.

Com o HIP, os sockets da camada de transporte utilizam o par <HI,porta> e mesmo quando o endereço IP é alterado as conexões ativas são mantidas. É claro que para que esse mecanismo funcione corretamente, deve haver um serviço de tradução da identidade de um nó para o respectivo endereço IP na camada de identidade do host. A Figura 3 ilustra a arquitetura proposta pelo protocolo HIP.

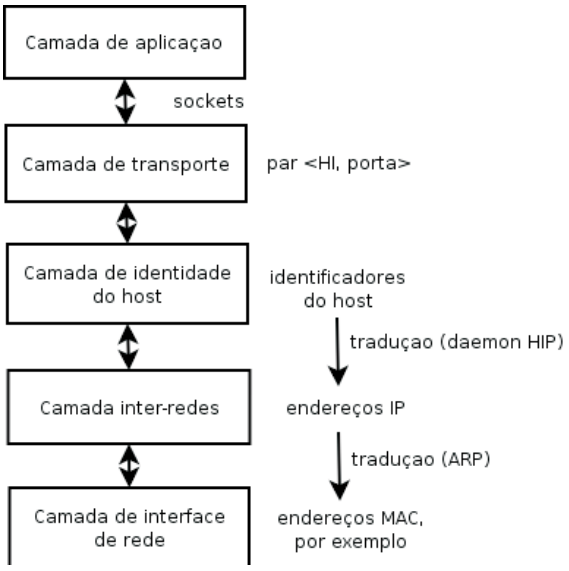

Figura 3 - A arquitetura da Internet proposta pelo protocolo HIP

Para que dois nós HIP-capazes se comuniquem, é estabelecida uma conexão segura.

Estabelecimento de conexões

Como o protocolo HIP independe de uma entidade certificadora externa e a Internet é uma rede pública que, originalmente, não provê segurança na transmissão de dados, um par de nós HIP-capazes primeiramente cria uma sessão segura através da autenticação mútua e troca de chaves compartilhadas. Para a criação dessa sessão há uma troca de mensagens em 4 estágios e o algoritmo Diffie-Helmman[2] é utilizado.

Conforme Ylitalo & Nikander (2004), primeiramente o nó iniciador envia ao outro host (respondedor) uma mensagem inicial contendo as HIT's dos dois hosts (exceto se o modo oportunístico for usado, pois não é necessário enviar a HIT do nó respondedor). O respondedor retorna uma segunda mensagem contendo um desafio computacional que deve ser resolvido para que a comunicação continue. O nó iniciador deve enviar uma terceira mensagem, contendo a resolução do desafio e a autenticação do respondedor. Se a mensagem não contiver o desafio computacional resolvido, ela é descartada; assim, os hosts tornam-se mais resistentes a ataques de negação de serviço (DoS). O respondedor ainda deve retornar uma quarta mensagem autenticando o host iniciador e, enfim, são estabelecidas duas associações de segurança IPSec[3], uma em cada direção do tráfego, e os dados da camada de transporte passam a ser encapsulados com o IPSec ESP (Encapsulated Security Payload) ou outro protocolo de segurança fim-a-fim. A escolha do protocolo IPSec é opcional, mas vale ressaltar que ele não exige extensões nos protocolos utilizados e é totalmente compatível com o HIP, funcionando como se estivesse em um domínio IPv6 [7]. A Figura 4 ilustra o procedimento descrito acima.

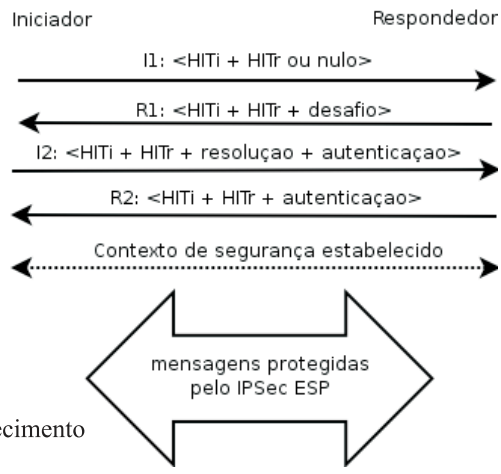

Figura 4 - Estabelecimento de uma sessão HIP

Agentes de encaminhamento

Um agente de encaminhamento permite que todos os pacotes enviados para um determinado endereço IP (virtual) sejam redirecionados para outro endereço IP (real). Essa funcionalidade é adequada quando um determinado host precisa se deslocar, mas não quer perder a conexão com a rede em que se encontra ou quando ele necessita estar presente (mesmo que virtualmente) em várias redes distintas.

A implementação de um agente de encaminhamento também ajuda a resolver o problema do duplo-salto que ocorre quando dois hosts com conexões ativas deslocam-se simultaneamente.

No entanto, antes de atender uma solicitação de redirecionamento de endereço IP, o agente de encaminhamento deve certificar se a assinatura (chave privada) do requisitante corresponde à chave pública. Mensagens não certificadas devem ser descartadas e, para garantir maior segurança no processo e proteger-se de ataques de negação de serviço (DoS) é recomendável que seja enviada ao host requisitante uma mensagem com um desafio computacional a ser resolvido.

Tipos de interfaces

Segundo Moskowitz & Nikander (2006), o protocolo HIP trata basicamente de três tipos de interfaces: interfaces reais, virtuais e multi-homing.

Uma interface real representa uma interface física com um único ponto de conexão na rede, tal como uma placa de rede Ethernet ou Wi-Fi.

Uma interface virtual é um agente de encaminhamento que representa um nó localizado em uma região topologicamente diferente de sua rede ou até mesmo em outra rede. A interface virtual redireciona todos os pacotes recebidos para a interface real com a qual está relacionada. Uma interface virtual pode ser um roteador de acesso (AR - Access Router), por exemplo.

Uma interface multi-homing possui um conjunto de interfaces reais, sejam elas na mesma rede ou em redes distintas. Uma interface multi-homing pode ser necessária por diversas razões, por exemplo: para balancear o tráfego de entrada, para ter conexões físicas de backup no caso de falhas, para representar o nó em redes diferentes, entre outras. Um host multi-homing deve informar a outros nós qual é a sua interface preferencial para o estabelecimento de conexões.

A Figura 5 apresenta os diferentes tipos de interfaces.

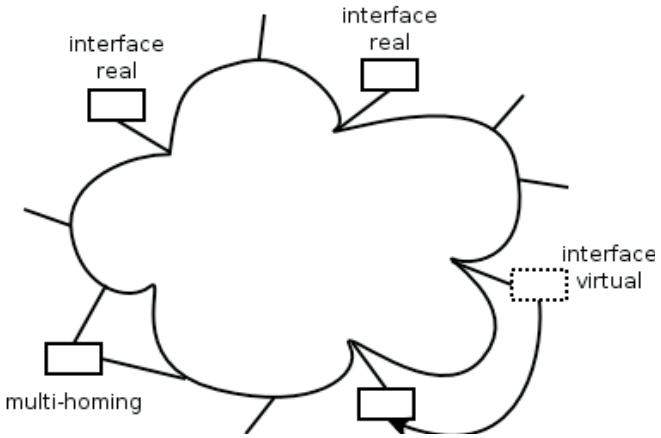

Figura 5 - Tipos de interfaces de rede: real, virtual e multi-homing

Atualizações de endereço

Quando um host desloca-se de uma rede para outra ou por alguma outra razão o seu endereço IP precisa ser alterado, ele necessita enviar uma mensagem de atualização de endereço para seus pares.

No caso mais simples, o host atualiza a ligação de sua identidade com o novo endereço IP e envia uma mensagem de reendereçamento de pacotes (REA) para os nós pares com que mantém conexões ativas (MOSKOWITZ & NIKANDER, 2006). Seus pares lhe enviam uma requisição de confirmação da atualização de endereço e, em seguida, o host responde com uma mensagem confirmando o novo endereço; em seguida, o contexto da comunicação volta a ser totalmente funcional. A Figura 6 exemplifica essa situação. No entanto, também é necessário que nos nós pares a camada de identidade do host resolva a nova identidade para encontrar o novo endereço IP.

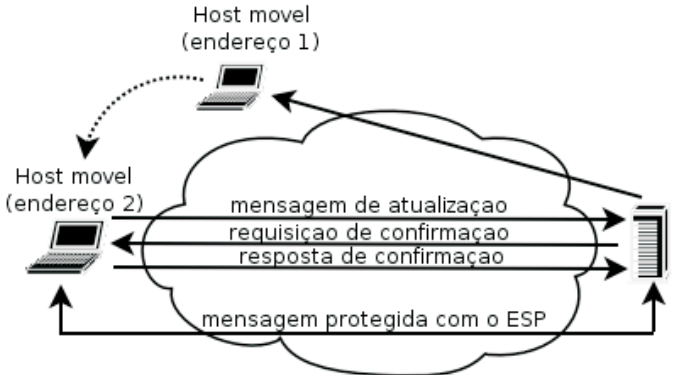

Figura 6 - Exemplo de atualização de endereço

Segundo Nikander et al (2003), em outra situação, o host pode decidir renovar suas associações de segurança IPSec e enviar parâmetros adicionais na mensagem de atualização de endereço. Os pares da comunicação trocam novamente suas chaves e, assim

como no caso anterior, requisitam a confirmação do endereço atualizado, aguardam uma mensagem de resposta e criam uma nova sessão.

Finalmente, uma mensagem de atualização de endereço com um parâmetro adicional também pode ser enviada por um host multi-homing que deseja especificar a seus pares uma nova interface preferencial para suas conexões de rede.

Mobilidade entre IPv4 e IPv6

Conforme descrito anteriormente, o protocolo HIP não utiliza o endereço IP como identificador do host nas conexões fim-a-fim, já que separa as camadas de rede e de transporte e permite o deslocamento de um nó móvel sem perder as conexões ativas. Portanto, o trânsito de hosts entre redes IPv4 e IPv6 é possível sem maiores complicações (YLITALO & NIKANDER, 2004).

No entanto, do ponto de vista da aplicação, há todo um contexto que deve ser adaptado. O identificador (HI) deve ser utilizado de forma compatível com as API's (Application Program Interfaces) das duas versões do protocolo IP, pois há aplicações que suportam apenas o IPv4, algumas suportam apenas o IPv6 e outras suportam ambas as versões. No IPv6, o identificador utilizado é a HIT (Host Identity Tag), que ocupa 128 bits e possui escopo global. Já no IPv4, o identificador utilizado é o LSI (Local Scope Identifier), que ocupa 32 bits e possui escopo local, mas garante a compatibilidade entre versões. Na prática, o HIP sempre utiliza um pseudo-cabeçalho no formato do IPv6 e algumas aplicações específicas do IPv6 podem funcionar em um domínio IPv4. A Figura 7 mostra o trânsito de uma aplicação de uma rede IPv4 para uma rede IPv6.

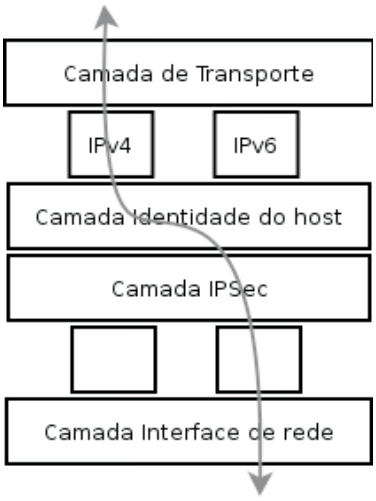

Figura 7 - Aplicação em trânsito de uma rede IPv4 para uma rede IPv6

Infraestrutura de registro e localização

Para que o protocolo HIP possa ser implementado, é necessária uma infraestrutura confiável que permita gerenciar o registro e a pesquisa de identificadores, disseminar as mudanças de estado e endereços IP das interfaces, promover o contato inicial de dois nós e configurar agentes de encaminhamento, entre outras funções.

Em redes menores, é possível que um host estabeleça conexões diretamente com o nó de destino mesmo sem conhecer o seu identificador (HIT). Nesse modo, chamado oportunístico, o host respondedor aceita mensagens iniciais sem a especificação de sua chave pública. Deve haver um mecanismo de sinalização fim-a-fim que informe as mudanças de endereços e o estado das interfaces. O principal problema da comunicação direta é a mobilidade simultânea de dois nós pares com conexões ativas.

Para a utilização do HIP em redes maiores, é fundamental que haja um serviço de descoberta dos nós HIP-capazes. Esse serviço poderia utilizar um diretório centralizado para registrar e localizar identificadores, como o DNS (Domain Name System), conforme ilustra a Figura 8.

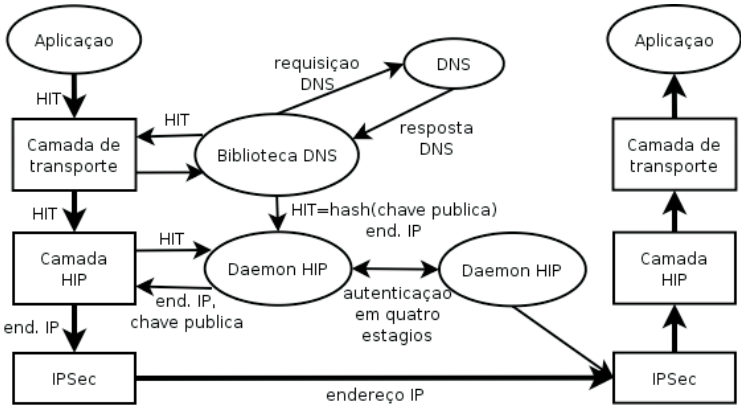

Figura 8 - Funcionamento do HIP com o servidor de DNS

A proposta existente em Nikander & Laganur (2006), cria extensões para que os servidores de DNS armazenem HI's ou HIT's adicionalmente aos endereços IP de um host. Assim, quando um servidor de DNS recebe uma requisição de resolução de nome, ele retorna uma resposta com o endereço IP e a HIT. Já quando o nome de um nó HIP-incapaz é pesquisado, o servidor de DNS retorna apenas o seu endereço IP, ou seja, o processo de migração e implementação do HIP pode ser gradual. No entanto, manter um servidor de DNS dinâmico não é uma tarefa simples, pois as mudanças nas ligações das identidades dos hosts são constantes e

a latência de atualização das ligações entre HIT's e endereços IP em todos os nós HIP-capazes é considerável. Portanto, um host em movimento permaneceria inalcançável por algum tempo.

A proposta mais interessante consiste em utilizar um servidor de rendezvous[4] (RVS) juntamente com o servidor de DNS (LAGANIER & EGGERT, 2006). O servidor de DNS registra as HIT's dos hosts e o IP do servidor de rendezvous responsável. O servidor de rendezvous é utilizado para fazer o contato inicial entre dois hosts e mantém atualizados os mapeamentos de HIT's em endereços IP dos hosts. Um nó HIP-capaz é alcançável através do endereço IP do servidor de rendezvous e é através dele que a troca inicial de mensagens é feita entre dois hosts. A Figura 9 ilustra o contato inicial de dois nós através de um servidor de rendezvous.

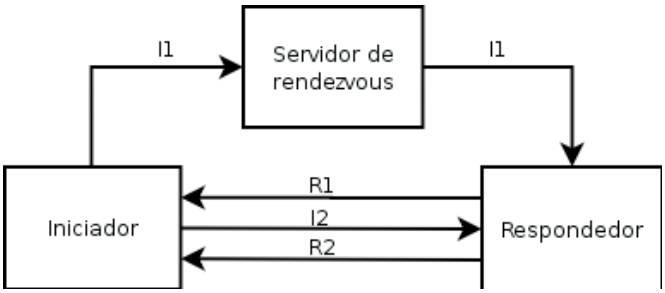

Figura 9 - Contato inicial de dois hosts com um RVS

No entanto, para garantir escalabilidade e tolerância a falhas, é interessante manter as informações de um host em mais de um servidor de rendezvous. Há estudos que sugerem a utilização de uma estrutura de servidores com tabelas hash distribuídas (DHT - Distributed Hash Tables) (GURTOV & JOSEPH, 2004).

Assim como no estabelecimento inicial de uma conexão entre nós HIP-capazes, o processo de atualização de HIT's de um host e a alteração do endereço IP de um servidor de rendezvous nos registros do servidor de DNS devem ser feitas em um contexto de comunicação seguro, caso contrário um nó mal-intencionado pode se registrar com informações falsas para ter acesso a pacotes destinados a outrem.

Conclusão

Como visto neste documento, o protocolo HIP pode ser uma boa solução para resolver as questões relacionadas à mobilidade de nós e aplicações na Internet.

O HIP cria um novo espaço de nomes na Internet e separa as funções de localização e identificação dos hosts, permitindo um melhor gerenciamento da mobilidade e multi-homing, a compatibilidade de aplicações IPv6 em redes IPv4 e vice-versa, adiciona aspectos de segurança e suporta diferentes esquemas de endereçamento (IPv4 e IPv6).

Novos estudos podem ser realizados visando alcançar a sinergia entre o protocolo HIP e sistemas baseados em diretórios centralizados, tais como o DNS (Domain Name System) e o LDAP (Lightway Directory Access Protocol), servidores de rendezvous e tabelas hash distribuídas (DHT - Distributed Hash Tables).

Referências Bibliográficas

GURTOV, A. & JOSEPH, A. *Friends or Rivals: Insights from Integrating HIP and i3*, Workshop on HIP and Related Architectures, Novembro de 2004.

JOKELA, P. et al. *Host Identity Protocol - Extended Abstract.* In Proc. of WWRF8bis, Fevereiro de 2004.

LAGANIER, J. & EGGERT, L. *Host Identity Protocol (HIP) Rendezvous Extension,* Internet draft, draft-ietf-hip-rvs-05, Junho de 2006.

MOSKOWITZ, R. & NIKANDER, P. *Host Identity Protocol (HIP) Architecture,* RFC 4423, Maio de 2006.

NIKANDER, P. & LAGANIER, J. *Host Identity Protocol (HIP) Domain Name System (DNS) Extensions,* Internet draft, draft-ietf-hip-dns-06, Fevereiro de 2006.

NIKANDER, P.; YLITALO, J. & WALL, J. *Integrating security, mobility, and multi-homing in a HIP way.* In Proc. of Network and Distributed Systems Security Symposium (NDSS), Fevereiro de 2003.

YLITALO, J. & NIKANDER, P. *A new Name Space for End-Points: Implementing secure Mobility and Multi-homing across the two versions of IP.* In Proc. of the Fifth European Wireless Conference, Mobile and Wireless Systems beyond 3G (EW2004), Fevereiro de 2004.

Notas

[1]Na camada de transporte, as aplicações especificam um protocolo e um identificador formado pelo endereço IP e por uma porta lógica de conexão para estabelecer a comunicação com um host.

[2]No algoritmo Diffie-Hellman, dois hosts obtêm a mesma chave compartilhada (chave de sessão) através de um cálculo matemático sem comprometer o segredo da chave.

[3]IPSec é um protocolo que encapsula o tráfego da camada de transporte para garantir a sua integridade e/ou cria túneis criptografados para garantir a segurança da comunicação.

[4]O servidor de rendezvous promove a localização dos nós HIP-capazes que nele se registraram, mantém as ligações entre HI's (ou HIT's) e endereços IP constantemente atualizadas e facilita o estabelecimento de conexões entre dois hosts.

Recebido em 22 de junho de 2007 e aprovado em 14 de agosto de 2007.