

Instituto de Matemática e Estatística
Universidade de São Paulo

Mobilidade sobre IPv6

Dairton Luiz Bassi Filho dairton@ime.usp.br

Novembro / 2004

<i>Introdução.....</i>	<i>3</i>
<i>IPv6.....</i>	<i>4</i>
<i>Mobile IPv6.....</i>	<i>5</i>
<i>Binding.....</i>	<i>6</i>
<i>Estruturas de dados.....</i>	<i>6</i>
<i>Mensagens.....</i>	<i>7</i>
<i>Comunicação</i>	<i>8</i>
<i>Autoconfiguração.....</i>	<i>9</i>
<i>Otimização de caminhos.....</i>	<i>10</i>
<i>Segurança.....</i>	<i>10</i>
<i>Protocolo Hierárquico.....</i>	<i>11</i>
<i>Crescimento da rede.....</i>	<i>16</i>
<i>Comparação de performance.....</i>	<i>16</i>
<i>Conclusões a respeito do modelo hierárquico.....</i>	<i>17</i>
<i>Mecanismo de handoff no cliente.....</i>	<i>17</i>
<i>Handoff rápido para aplicações multimídia e de tempo real.....</i>	<i>19</i>
<i>Referências.....</i>	<i>21</i>

IPv6

Antes de explorar os mecanismos de comunicação do IPv6 Móvel convém apresentar o novo formato do cabeçalho dos pacotes, assim como algumas mudanças intrínsecas ao seu processamento.

Além da quantidade de endereços quase inimaginável e de endereços unicast e multicast, um novo tipo foi criado, o anycast que referencia um grupo de hosts mas entrega o pacote a apenas um, o mais próximo da origem conforme o protocolo de roteamento.

Considerando o crescimento da internet, uma das grandes preocupações dos projetistas do novo protocolo foi assegurar velocidade, por isto algumas características do processamento dos pacotes nos roteadores foram adaptadas a fim de manter viável a realidade onde a transferência de som, vídeo e o uso de aplicações de tempo real são cada vez mais comuns. A primeira grande mudança foi fixar o tamanho do cabeçalho, agora ele tem sempre 40 bytes. Esta medida torna mais veloz o processamento, pois é possível saber de antemão o que cada bit representa sem precisar ler o todos os que o precedem. Para fixar o tamanho alguns campos do IPv4 foram eliminados, outros acrescentados e alguns apenas sofreram mudanças no seu significado.

Dentre as inovações um novo conceito foi criado, o *fluxo*. Um fluxo é uma seqüência de pacotes para os quais é necessário um tratamento especial, como para serviços que requerem alta prioridade tais como serviços de tempo real, transmissão de vídeo ou uma conexão entre dispositivos móveis onde qualidade durante a transmissão deve ser assegurada. Dados que pertençam a aplicações tradicionais como requisições http ou transferência de arquivos não precisam participar de um fluxo.

Version	Priority	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

Cabeçalho IPv6

Versão: (4 bits) este campo identifica a versão do protocolo usado para criar o pacote.
Priority (Classe de tráfego): (8 bits) é equivalente ao campo *Tipo de Serviço* do IPv4, que classifica o tipo do pacote.
Rótulo de fluxo: (20 bits) serve para identificar um fluxo.
Comprimento da carga: (16 bits) este é o número de bytes de dados contidos no pacote após o cabeçalho.
Próximo cabeçalho: (8 bits) informa o protocolo que deve tratar o conteúdo do pacote.
Limite de saltos: (8 bits) é o número máximo de roteadores que o pacote deve passar, a cada roteador este campo é decrementado, quando chega em zero o pacote é descartado.
Endereço de origem: (128 bits) origem do pacote.
Endereço de destino: (128 bits) destino do pacote.

O cabeçalho IPv6 é bastante simples e enxuto em relação ao IPv4, qualquer informação adicional é transmitida encapsulada no pacote e informada através do campo *próximo cabeçalho*.

O tradicional campo checksum não existe mais, o que motiva tal mudança é o processamento rápido dos pacotes. No IPv4 este cálculo era feito a cada roteador. O que justifica essa mudança é a redundância, a camada de enlace já realiza um checksum, assim como os protocolos de transporte, UDP e TCP, também implementam mecanismos que asseguram uma transferência confiável dos dados, portanto, torna-se dispensável abrir mão desta checagem em vista do processamento poupado e do grau de confiabilidade oferecido pelas outras camadas.

Outras ausências são dos campos de opções que não fazem parte do cabeçalho padrão, graças a isto é possível que o cabeçalho tenha tamanho fixo. Entretanto, as opções ainda existem, mas estão encapsuladas no pacote e são referenciadas pelo campo *próximo cabeçalho*.

Mobile IPv6

Dentro do IP, o Mobile IPv6 é o protocolo que dá suporte à comunicação de dispositivos móveis. Com IPv6 não há mais problemas com a quantidade de endereços, assim cada unidade móvel pode possuir dois ou mais endereços, um estático, o home address, e um ou mais variáveis, os care-of address que são obtidos e usados quando a unidade móvel está fora de sua área de origem.

O caso trivial acontece quando a unidade móvel está na sua região de origem. A unidade móvel recebe diretamente os pacotes destinados a ela. Quando o dispositivo se moveu para uma região que não é sua origem ele necessita de um novo endereço. Este endereço será o

seu care-of address, que é um endereço da rede onde ele está, e será através dele que os agentes irão se comunicar com a unidade móvel.

Assim que a unidade móvel adquire o care-of address o home agente é informado para armazená-lo. A partir de então os pacotes endereçados ao home address serão interceptados e redirecionados através da rede fixa, via tunneling, para o care-of address da unidade móvel.

Este funcionamento é transparente para as camadas acima do IP, seja TCP, UDP ou outras aplicações, tudo se passa como se o dispositivo estivesse recebendo os pacotes no seu home address.

Binding

Quando a unidade móvel está fora de sua rede ela adquire um endereço da rede local, e informa a todos que conhecem o home address a respeito do seu novo endereço, o care-of address, para que os dois sejam associados. A associação entre os endereços é chamada de Binding e significa que os dois endereços referenciam a mesma unidade móvel.

Para realizar o Binding, a unidade móvel envia ao home agent uma mensagem do tipo Binding Update informando o seu care-of address. O home agent responde com um Binding Acknowledgment, e a partir deste momento o home agent redirecionará pela rede fixa os pacotes enviados ao home address ao care-of-address. O binding também é realizado em todos os hosts que se comunicam com a unidade móvel, a única diferença é que estes não enviam o Binding Acknowledgment. Caso o Binding update, por algum motivo, não chegue ao host comunicante, este enviará os pacotes endereçados com ao home address, o home agent irá redirecioná-los e enviará o binding ao host comunicante.

Estruturas de dados

Para viabilizar os mecanismos de binding e descoberta de agentes nós e agentes mantém algumas informações armazenadas em estruturas de dados bastante simples mas indispensáveis ao funcionamento do protocolo.

Binding cache, cada entrada desta lista possui o home address e o care-of-address de uma unidade móvel. As entradas permanecem no Binding cache até que expire seu tempo de vida ou chegue um pedido de cancelamento do binding, que ocorre quando a unidade móvel volta para sua rede de origem ou muda de rede estrangeira.

Todo host no IPv6 possui o Binding cache, toda vez que ele vai enviar um pacote o binding cache é consultado, se o endereço de destino é encontrado em alguma entrada o host endereça o pacote diretamente para o care-of address.

Binding Update List, também está presente em todos os nós IPv6, armazena a lista dos nós que receberam um binding update e que deverão ser avisados quando a unidade móvel deixar de usar um care-of address. Esta lista contém o endereço do home agent e dos hosts que a unidade móvel mantém ou manteve algum tipo de comunicação e que o binding ainda não teve seu tempo de vida expirado.

Home Agent List, esta lista existe em todos os routers que operam como home agents, ela contém informações a respeito de todos os home agents presentes em uma rede e é transmitida periodicamente entre os agentes.

Prefix List, lista dos prefixos de rede que a unidade conhece.

Essas estruturas permitem que todo nó móvel seja capaz de gerenciar seus bindings e manter-se informado a respeito dos bindings dos hosts com quem ele estabelece alguma comunicação.

Mensagens

Para gerenciar o tráfego na rede o protocolo ICMP foi melhorado e o ICMPv6 não é mais compatível com a versão atual. Ele é responsável por dois tipos de mensagens, de erro e de controle. Cada mensagem possui um campo tipo que contém um código de identificação da mensagem. As mensagens de erro possuem código reservado entre 1 e 127, as mensagens de controle de rede possuem código de 128 a 256. Atualmente a maior parte dos valores está livre para um uso futuro.

As mensagens de erro são apenas 4 e são enviadas quando houve algum problema na transmissão do pacote e o host destino não conseguiu recebe-lo. As mensagens de informação com valores entre 133 e 137 são usadas para procedimentos de autoconfiguração. As mensagens de número 128 e 129 são equivalentes a função *ping*. As mensagens de 130 a 132 são usadas para procedimentos de membros de grupos multicast.

Campo tipo	Mensagem
1	<i>Destination Unreachable</i>
2	<i>Packet Too Big</i>
3	<i>Time Exceeded</i>
4	<i>Parameter Problem</i>

128	<i>Echo Request</i>
129	<i>Echo Reply</i>
130	<i>Group Membership Query</i>
131	<i>Group Membership Report</i>
132	<i>Group MemberShip Termination</i>
133	<i>Router Solicitation</i>
134	<i>Router Advertisement</i>
135	<i>Neighbor Solicitation</i>
136	<i>Neighbot Advertisement</i>
137	<i>Redirect</i>

Comunicação

Para uma unidade móvel é extremamente importante saber quando o seu roteador padrão, se tornou inacessível, assim ela pode rapidamente percorrer sua Router list a procura de outro roteador ao seu alcance, e, se necessário, percorrer a Prefix list para conseguir outro care-of address.

O método para saber se um roteador está alcançável é o Neighbor Unreachability Detection, entretanto muitas vezes é possível perceber a presença do roteador sem enviar mensagens perguntando explicitamente que ele está sob alcance. Esta característica é muito importante para dispositivos móveis, pois a comunicação consome muito mais energia que o processamento e evita-la aumenta o tempo de vida da bateria. A unidade móvel pode inspecionar os pacotes recebidos para saber se eles passaram pelo roteador procurado. Ou verificar o progresso da comunicação das camadas superiores.

Quando uma unidade móvel envia um binding update, pode acontecer dele ou do Binding Acknowledgement não chegar ao seu destino, neste caso, após um segundo sem receber resposta, é enviado outro binding update, caso este também não seja respondido o reenvio acontece após dois segundos, a cada reenvio o tempo de espera pela resposta é dobrado até obter uma resposta ou o período de time-out atingir o seu valor máximo, que geralmente é 256 segundos.

Se um nó comunicante recebe uma mensagem ICMP - Host Unreachable ou Network Unreachable após enviar pacotes ao care-of address de uma unidade móvel, a entrada da binding list que corresponde a esta unidade móvel será deletada e os pacotes são reenviados ao home address até que chegue um binding update com o novo care-of address.

Autoconfiguração

Uma das novidades que o IPv6 provê é o recurso da autoconfiguração, através do qual os endereços dos roteadores são descobertos dinamicamente. Existem dois tipos de autoconfiguração, stateless e statefull, que utiliza o serviço DHCPv6.

Durante o processo de inicialização do IPv6, além do endereço, o host automaticamente se adiciona no grupo multicast *all nodes*, isto é feito configurando suas interfaces para receber todos os pacotes enviados para o endereço de multicast FF02::1. Envia uma mensagem ICMP “Router Solicitation” para o endereço de multicast *all routers*, FF02::2, em resposta os roteadores enviam mensagens do tipo “Router Advertisement”. Com estas respostas a unidade móvel não só conhece os roteadores da daquela rede como também preenche a Home Agent List.

Caso prefira a unidade móvel pode apenas aguardar que o recebimento de mensagens “Router Advertisements” que são enviadas periodicamente pelos roteadores para o endereço multicast *all hosts* a fim de manter atualizada a Router List. A partir do endereço do roteador a unidade móvel também cria uma entrada na Prefix List com o prefixo da rede que ela está conectada.

Quando um nó se conecta a uma rede, automaticamente lhe é atribuído um endereço IP, esta é a “stateless autoconfiguration”. Para dispositivos móveis este processo acontece quando a unidade móvel muda de rede e adquire o care-of address.

Opcionalmente para permitir maior controle sobre redes grandes, os roteadores podem não permitir a autoconfiguração stateless, neste caso, a autoconfiguração é stateful que consiste em conseguir um IP a partir de um servidor de nomes. Este processo é menos simples porém mais seguro que através de mensagens e é fornecido pelo DHCPv6.

Inicialmente o nó móvel não conhece o endereço IP do seu home agent, para descobri-lo é utilizado um mecanismo chamado Dynamic Home Agent Discovery. O processo consiste em enviar um Binding Update para um endereço anycast de home agents, que irá alcançar um dos roteadores que operam como home agent. O roteador que recebeu devolverá a lista dos roteadores que operam naquela região da rede. A unidade móvel segue enviando Binding Updates para os próximos roteadores da lista até que um deles registre o seu home address.

Otimização de caminhos

Uma questão bastante significativa é a ausência do agente estrangeiro, necessário no IPv4. Esta mudança promove ganho de performance, diminui o volume de tráfego na rede e diminui o delay de comunicação. A comunicação com uma unidade móvel em uma rede estrangeira acontece com auxílio apenas do home agent.

Quando uma unidade móvel fora de sua rede comunica-se com outro host, seja ele fixo ou móvel, este host envia os pacotes para o home address da unidade móvel, estes pacotes são capturados pelo home agent que os encapsula e endereça ao care-of address. A unidade móvel desencapsula os pacotes e descobre o endereço do nó que o enviou, enviando os pacotes diretamente para ele sem passar pelo home agent. Para evitar uma comunicação com Rota Triangular a unidade móvel envia um Binding update ao host comunicante para que ele possa enviar os pacotes diretamente ao care-of address. Esta otimização torna ainda mais salientes as vantagens proporcionadas pela eliminação do agente estrangeiro.

Durante este tipo de comunicação é importante perceber que quando o home agent intercepta um pacote para o home address, ele não pode inserir um cabeçalho ou alterar o destino do pacote, pois estaria modificando o conteúdo e causaria uma falha na autenticação feita pela unidade móvel. Por isso o home agent cria um novo pacote para transportar os dados interceptados.

Segurança

A especificação de segurança define que todo nó IPv6 deve ser capaz de realizar a autenticação dos dados recebidos através do IPsec, isto garante estabelecer uma comunicação segura com um host comunicante. Os mecanismos de segurança são dois: a autenticação de cabeçalho (Authentication Header) ou autenticação IP, e a segurança do encapsulamento IP (Encrypted Security Payload). A autenticação de cabeçalho assegura ao destinatário que os dados IP são realmente do remetente indicado no endereço de origem, e que o conteúdo foi entregue sem modificações. A autenticação utiliza o algoritmo MD5 (Message Digest 5). A segurança do encapsulamento assegura a confidencialidade dos dados através do algoritmo de criptografia DES (Data Encryption Standard) baseado em chaves de 56 bits acordadas previamente entre o transmissor e o receptor.

Os algoritmos de autenticação e criptografia utilizam o conceito de associação de segurança entre o transmissor e o receptor. Neste modelo o transmissor e o receptor devem concordar com uma chave secreta e com alguns parâmetros relacionados à segurança, conhecidos apenas pelos membros da associação.

Algumas das vulnerabilidades do IPv4 são consequência do uso do protocolo ARP, no IPv6 estes problemas estão superados pois em substituição ao ARP foi criado o mecanismo Neighbor Discovery eliminando as fraquezas do ARP.

No IPv4 há vários pontos onde a segurança não funciona como o desejado. Um deles é com a “ingress filtering” em muitos roteadores e firewalls que implementam um algoritmo de segurança que verifica se o endereço de origem dos pacotes pertence à rede de onde eles estão vindo. Caso não seja o pacote é descartado em resposta a uma possível tentativa de fraude. Este tipo de comportamento pode comprometer a comunicação entre dois nós quando um deles está fora de sua rede, pois o endereço de origem do pacote será o home address, que não pertence à rede de origem. No IPv6 uma simples medida resolve os com a “ingress filtering”, a unidade móvel endereça os pacotes com o care-of address no campo de origem do pacote.

Uma possível maneira de ataque sobre o IPv6 seria enviando pacotes com binding Update a fim de redirecionar dados do seu destino correto. Para evitar este tipo de fraude sempre que um Binding Update é enviado, é adicionado ao pacote um cabeçalho de autenticação garantindo a autenticidade do pedido.

Alguns problemas decorrentes do uso do NAT (Network Address Translation) não ocorrem mais na nova versão do IP pois o NAT é usado para suavizar o limitado número de endereços. No IPv6 a grande quantidade de endereços dispensa o uso de NAT e acaba com qualquer problema que ele possa gerar.

Protocolo Hierárquico

Considerando o constante crescimento da internet e do número de dispositivos móveis conectados simultaneamente, é muito importante que a próxima versão do protocolo de internet seja escalável. No entanto, o modelo apresentado pelo Mobile IPv6 não provê escalabilidade nas dimensões necessárias. Quando usado em um contexto com um número excessivo de unidades móveis, a tendência é a perda da qualidade de serviço e aumento do delay na entrega dos pacotes. Este comportamento ocorre porque, o Móvil IPv6 trata da mesma forma movimentações locais e globais.

Movimentações locais são aquelas que acontecem dentro de um site, movimentações globais são entre sites. Um site tem uma dimensão arbitrária e pode ser, por exemplo, a rede de uma empresa ou universidade e ser constituído por uma ou várias LANs.

O grande problema em tratar mobilidade local e global da mesma forma é o excesso de tráfego gerado na internet. Periodicamente as unidades móveis enviam a cada host que se correspondem um binding update informando ou apenas confirmando o seu ponto de

conexão. Com este comportamento, quando o número de unidades móveis crescer, a quantidade de bindings crescerá proporcionalmente e poderá causar sobrecarga na internet.

Conforme o estudo feito por [3], analisando os padrões de mobilidade de diversos profissionais, independente de possuírem algum dispositivo móvel, 69% das movimentações são locais. Este dado mostra que um modelo hierárquico que considera as movimentações locais e globais de forma diferente pode ser mais adequado à internet. Ele trás, sobretudo, duas vantagens cruciais: handoffs mais simples e rápidos, pois são realizados apenas localmente, reduzindo a perda de pacotes durante a transmissão e redução da carga de dados enviada pela internet, pois movimentos locais podem ser sinalizados sem que as mensagens precisem passar pela internet.

A idéia de hierarquia é baseada no conceito de Redes de Mobilidade. Uma rede de mobilidade de um site é uma LAN que define um espaço de endereçamento para unidades móveis. Cada rede de mobilidade deve possuir Servidores de Mobilidade, que funcionam como roteadores e armazenam os bindings das unidades móveis que estiverem usando a rede.

As movimentações de uma unidade móvel podem ser locais ou globais, intra-site e inter-site, e cada uma pode ser tratada de forma a minimiza a comunicação e o tráfego na internet.

Nas movimentações inter-site a unidade móvel recebe dois care-of address, o Private Care-of Address (PCoA), que é um endereço associado à rede local e equivale ao care-of address tradicional, e o Virtual Care-of Address (VCoA) que está associado à Rede de Mobilidade.

Ao movimentar-se inter-sites, uma unidade móvel re-configura seus endereços, PCoA e VCoA, e envia três tipos binding update. Um, enviado ao servidor de mobilidade, que realiza o binding entre o VCoA e o PCoA. Outro, enviado para cada unidade de fora do site com que a unidade móvel está se comunicando, que especifica o binding entre VCoA e o Home Address, aqui está incluído o binding para o home agent. E o terceiro que determina o binding entre Home Address e PCoA, enviado para as unidades de dentro do site com que a unidade móvel está se comunicando.

Para movimentações intra-site, a unidade móvel troca apenas o PCoA, e para informar o restante da rede são necessários apenas dois tipos de binding update. Um para o servidor de mobilidade determinando o binding entre PCoA e VCoA e um binding para cada unidade comunicante de dentro do site, informando o PCoA.

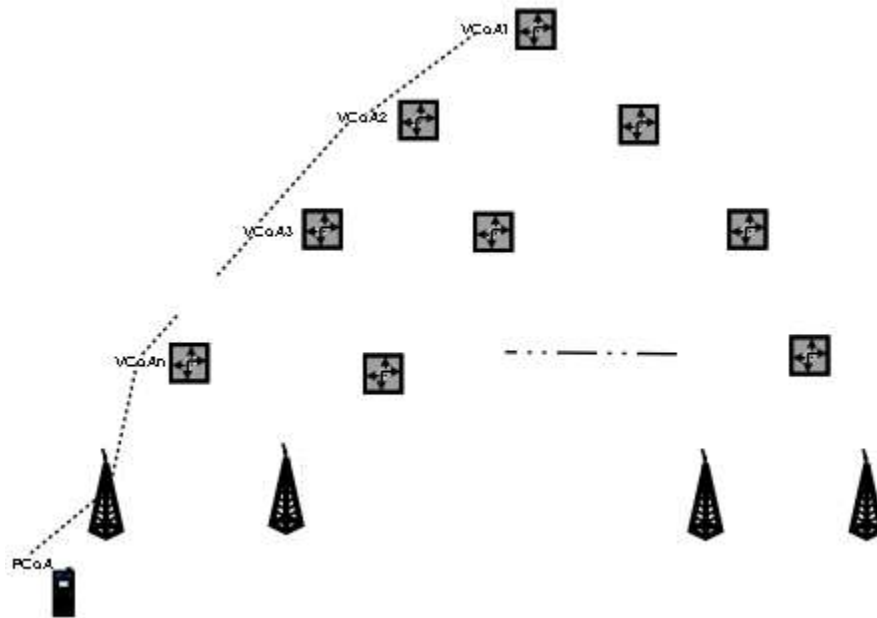
Como resultado, unidades locais enviam pacotes para a unidade móvel endereçando ao PCoA que são entregues diretamente. As unidades externas enviam pacotes endereçados

ao VCoA que são roteados para o servidor de mobilidade e encaminhados via tunneling ao PCoA.

Este modelo pode ser estendido para criar uma hierarquia de vários níveis de forma que cada site possa conter sub-sites e cada sub-site outros sub-sites. Conjunto de redes pode ser visto como uma árvore de redes de mobilidade, com uma rede de mobilidade para cada site e sub-site.

É importante perceber que para uma árvore de redes de mobilidade, qualquer unidade móvel que esteja dentro dela estará associada a um conjunto de no máximo h redes que determinam um caminho da raiz a uma folha na árvore de redes de mobilidade, onde h é a altura da árvore. Assim, a unidade móvel possuirá um VCoA em cada uma das redes deste caminho. Dentro deste caminho chamaremos de RM_1 a Rede de Mobilidade da raiz, RM_s cada uma das redes do caminho e RM_h a rede da folha.

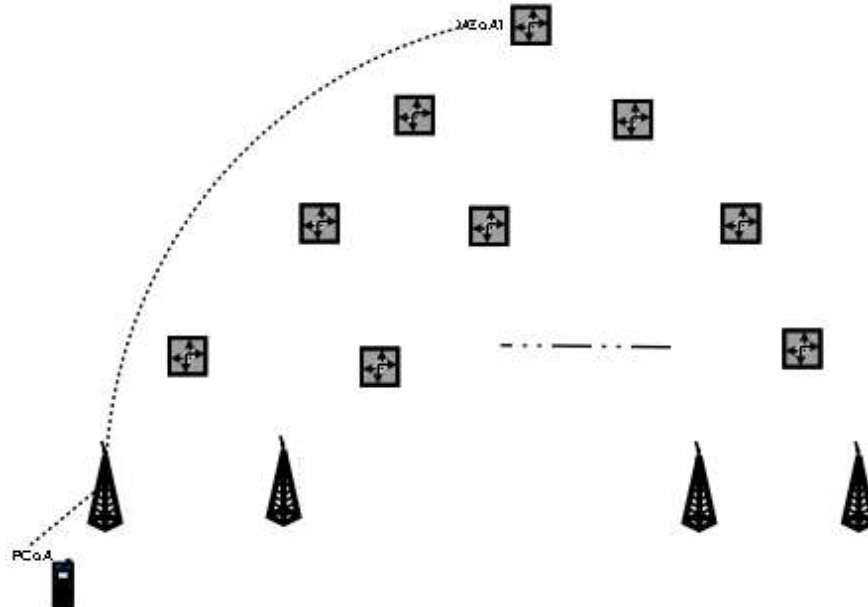
O modelo hierárquico explora a larga quantidade de endereços oferecida pelo IPv6, vinculando vários endereços a cada unidade móvel. Além do PCoA, vários VCoAs podem ser registrados, um para cada nível da hierarquia. Durante a movimentação, o registro dos endereços pode ser inter-site ou apenas intra-site.



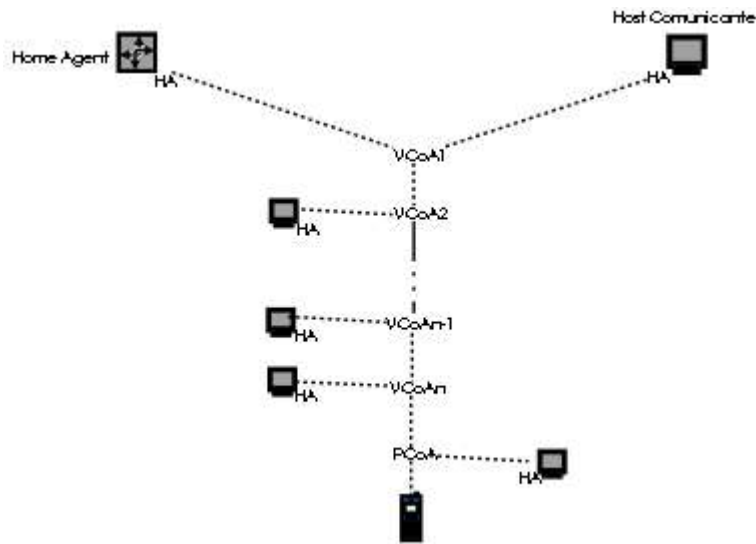
Quando a unidade móvel se movimenta localmente ela deve trocar de PCoA tomando um endereço da rede onde está. Considerando o movimento local em uma rede de mobilidade que possui sub-redes, a mudança no ponto de conexão acarreta mudança no caminho da

raiz às folhas na árvore de RM. Isso obriga a unidade móvel a adquirir um VCoA para cada rede de mobilidade que ela passa a participar. Em seguida, dentre as novas redes, da mais alta para a mais baixa na hierarquia, os VCoAs devem ser registrados. Sendo RM_s a rede mais alta, devem ser realizados Binding Update em RM_{i-1} entre $VCoA_{i-1}$ e $VCoA_i$, para i de s a h . Por fim, deve ser registrado um binding entre $VCoA_h$ e o novo PCoA na RM_h e outro entre o home address e PCoA em cada unidade comunicante de dentro do site.

Por questões de otimização em casos onde a unidade móvel não realiza muita movimentação, algumas RMs podem ser puladas, o PCoA pode ser registrado diretamente com o $VCoA_1$. Esta medida reduz a carga na rede local pois os pacotes são encaminhados diretamente sem passar por todos os níveis da hierarquia.



Quando ocorre uma movimentação global a unidade móvel sairá de uma árvore de RMs para outra e isto significa que todos os endereços associados ela serão trocados, exceto, é claro, o home address. A unidade móvel assume um novo PCoA e um novo VCoA para cada RM da nova hierarquia. Registra $VCoA_{i-1}$ com $VCoA_i$ através de binding update em RM_{i-1} , para i de 2 até h' , onde h' é um valor independente de h pois é a altura de outra árvore de redes. Registra o home address com o PCoA em cada unidade comunicante dentro do site. Registra o home address com o $VCoA_1$ para cada unidade comunicante fora do site e com o home agent.



Desta maneira, pacotes enviados ao home address são interceptados pelo home agent, encapsulados e encaminhados ao PCoA. As unidades que estão em outros ramos da árvore podem comunicar-se através do primeiro VCoA em comum, enquanto que as unidades comunicantes de dentro do site enviam pacotes endereçados diretamente para o PCoA.

Quando o nó comunicante está fora do site e envia pacotes à unidade móvel ele os endereça ao VCoA₁. Os pacotes são entregues à RM₁, onde são interceptados pelo servidor de mobilidade e encapsulados ao VCoA₂. O servidor da RM₂ os intercepta e apenas muda o endereço de destino do encapsulamento para VCoA₃. E assim segue até que o último nível de RMs redireciona-os para o PCoA.

Perceba que a simples mudança no endereço de destino pode ser feita a partir do segundo nível da RMs pois o primeiro nível não pode alterar os dados do pacote original, se isto fosse feito a unidade móvel invalidaria o pacote acusando falta de integridade dos dados.

Quando a unidade móvel deseja enviar um pacote ela coloca no endereço de origem o PCoA e adiciona como informação adicional o home address, independente de quem irá recebe-lo. Assim o nó receptor através de sua tabela de bindings pode enviar diretamente para o home address caso o PCoA não esteja mais disponível.

Desta maneira a maioria do trafego gerado por uma unidade móvel permanece na rede local, uma vez que a quantidade de bindings enviados para fora do site é menor. Exceto nos casos em que a unidade móvel troca completamente de RM, a mudança deixa de ser transparente para os nós comunicantes e eles são informados da mudança.

Crescimento da rede

Em uma estrutura hierárquica de gerenciamento de pacotes, de fato há um alívio na quantidade de dados que transitam pela internet, entretanto outro ponto pode tornar-se indesejável. O gargalo passa a ser no processamento dos servidores de mobilidade que podem perder performance quando o site cresce e aumenta muito o número de unidades móveis, o servidor possuiria um número demasiado de entradas em sua tabela de bindings tornando-o mais lento.

Antes de caracterizar uma solução para o problema da lentidão nos servidores convém observar mais uma característica das redes de mobilidade.

Durante a retransmissão dos pacotes, os servidores de mobilidade trabalham sem acrescentar nenhuma informação que torne possível ao destinatário identificá-lo. Esta característica torna possível que um servidor seja, dinamicamente, duplicado ou substituído de forma transparente para os nós comunicantes. Da mesma maneira um novo servidor pode ser acoplado a uma RM sem que seus usuários percebam. Isto permite que em casos de sobrecarga, um servidor específico seja duplicado para dividir o processamento ou que mais servidores sejam adicionados à rede para compartilhar o armazenamento dos bindings e o encaminhamento dos pacotes.

Comparação de performance

Uma comparação entre o modelo hierárquico e o Mobile IPv6 sobre três fatores importantes: a performance de roteamento, a performance de transmissão e a escalabilidade em cada modelo. O primeiro avalia a latência introduzida por cada modelo. O segundo analisa o quão rápido são executadas as transmissões de dados, e, o terceiro verifica o comportamento quando a rede e o número de unidades móveis cresce.

O roteamento dos pacotes acaba sendo bastante tendo um custo bastante próximo. O Mobile IPv6 faz o roteamento ótimo dos pacotes, usando sempre o caminho mais curto para entregar os pacotes, exceto na primeira comunicação como outro host, desta vez os pacotes passam pelo home agent. Enquanto isso o modelo hierárquico acrescenta uma indireção devido à implantação dos servidores de mobilidade, porém isto evita que pacotes tenham que entrar na internet.

A escalabilidade provê a principal diferença entre os dois modelos. Serão considerados três cenários, movimentação dentro do site, movimentação dentro de um site estrangeiro e movimentação entre sites.

No primeiro cenário um simples detalhe faz toda a diferença, no modelo hierárquico a unidade móvel envia um aviso ao DNS sobre seu VCoA, assim não é preciso enviar pacotes pela internet. No Mobile IPv6 a unidade móvel envia binding updates para cada um de seus nós comunicantes.

Para o terceiro caso não há diferença entre os protocolos pois são iguais no que diz respeito aos dados transmitidos pela internet.

No cenário de movimento em uma rede estrangeira é onde está a diferença mais significativa pois quanto maior a frequência de mudança da unidade maior é a diferença de desempenho em favor o modelo hierárquico pois a mudança é tratada como uma mudança local sendo transparente para os hosts de fora da rede.

Conclusões a respeito do modelo hierárquico

A respeito do tratamento da movimentação pudemos perceber um ganho significativo no durante o deslocamento local. O uso de várias camadas na hierarquia trás um overhead na comunicação local mas é compensado pela redução na comunicação através da internet, culminando ainda em uma menor perda de pacotes.

A estrutura de Redes de Mobilidade acrescenta um nível de indireção no roteamento, mas proporciona um mecanismo dinâmico de integração dos servidores e se torna transparente aos nós comunicantes. Além disso desloca o gargalo da sobrecarga da internet para a sobrecarga dos servidores de mobilidade que podem ser expandidos mais facilmente.

Mecanismo de handoff no cliente

Apesar do IPv6 fornecer suporte à mobilidade ainda há pontos que podem ser refinados para tornar a comunicação wireless tão sólida e transparente quanto uma rede fixa. Esta seção explora mecanismos que provêem a transição entre redes de forma menos traumática à unidade móvel.

A navegação através de redes estrangeiras não é totalmente transparente, muitas interrupções ocorrem durante a passagem de uma rede para outra. Muitas vezes a unidade móvel perde contato com a rede por onde está e para continuar é preciso conectar-se a outra rede. O objetivo é evitar, ou minimizar, a “quebra” na comunicação permitindo que o host móvel decida quando trocar seu ponto de conexão.

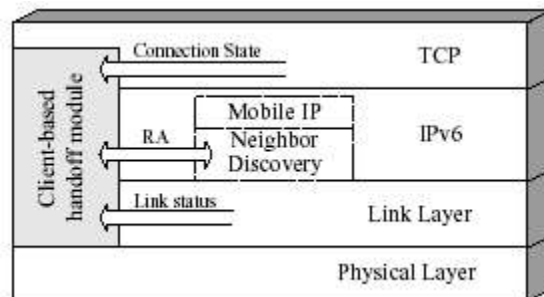
Uma das características previstas no FMIPv6 (Fast Mobile Internet Protocol versão 6) proposto pela IETF é a detecção de movimentos e a minimização da latência no handoff.

Quando o handoff é eminente a unidade móvel continua o trafego pela conexão e inicia o processo de registro em outro roteador. Entretanto, um ponto em aberto neste mecanismo é identificar quando iniciar o processo de handoff.

Uma possível abordagem para disparar um processo de handoff é adicionando algoritmos a entidades da rede, como roteadores e agentes, de forma que percebam o status das unidades móveis enviando avisos para a troca de rede. Esta técnica possui alta complexidade pois requer mudança em componentes da rede.

Uma segunda maneira de tratar este problema é adicionando inteligência no lado do cliente. Assim cada unidade móvel pode decidir quando o handoff é apropriado. Nesta abordagem é criado um Módulo de Handoff (MoH) que gerencia as trocas de rede.

Para identificar os roteadores e realizar o handoff com eficácia o MoH interage com três camadas da rede. A camada de enlace, consultando o status do link. A camada do IPv6 obtendo as informações sobre os Router Advertisements (RA) através do Neighbor Discovery. E com a camada de TCP por onde o status da conexão é acompanhado.



Posição do Módulo de Handoff em relação às camadas de rede

A unidade móvel inicia o processo de handoff sempre que recebe um RA, para evitar handoffs indesejados o MoH filtra os anúncios dos roteadores para evitar conexões com sinal mais fraco e força o handoff sempre que necessário.

Para determinar qual o melhor ponto de conexão é adicionado à unidade móvel um *RA cache*, que possibilitará estabelecer prioridades para escolher o melhor roteador. Os critérios de seleção de RA são divididos em dois grupos conforme sua importância, os de maior importância são:

- a qualidade do sinal
- o tempo desde a última atualização no RA cachê

Os critérios de menor importância são:

- o número de hops até o roteador

- se o roteador é ou não acessível no link local.

O MoH usa o status da camada de enlace para monitorar a conectividade do link. Isso ajuda a aumentar a velocidade da detecção da desconexão de um link.

Para iniciar um handoff existem dois cenários onde seguramente este processo faz sentido.

Quando o atual ponto de conexão apresenta algum erro ou torna-se inacessível. Neste caso para evitar a perda de muitos dados transmitidos ou que deveriam ser recebidos a unidade móvel deve fazer um Hard Handoff. O handoff é iniciado pelo handler do MoH que monitora o status do link assim que a desconexão é detectada usando a próxima entrada da RA cache.

O segundo caso ocorre quando o handler da camada de enlace detecta problemas com o link, nesta situação um Soft Handoff é iniciado, caso o MoH verifica o status da conexão TCP, se não existir uma conexão TCP o handoff é automaticamente iniciado, se existir alguma conexão, ela pode ser preservada, diminuindo o valor limite de qualidade de sinal. Se a qualidade do sinal continuar a cair e atingir o novo limite o processo de handoff é iniciado, conforme os critérios de prioridade.

O hard handoff oferece um risco potencial de perda de alguns pacotes enquanto o soft handoff, teoricamente, não perde nenhum pacote.

Se em qualquer dos cenários não houver nenhum RA na RA cache, o IPv6 Neighbor Unreachability Detection é invocado para encontrar um novo ponto e conexão.

Handoff rápido para aplicações multimídia e de tempo real

A especificação do IPv6 dá suporte a aplicações multimídia e de tempo real através dos campos *flow* e *classe de tráfego* do cabeçalho IP. Esta adaptação estimula ainda mais o crescimento deste tipo de aplicação. Na internet os dados dessas aplicações requerem um tratamento adequado para preservar a qualidade do serviço este tratamento é oferecido tratando os dados como um fluxo.

Para atender as requisições de qualidade de serviço alguns protocolos foram desenvolvidos, mas em geral são adequados para redes fixas e nunca tem o mesmo desempenho com dispositivos móveis.

O RSVP (Resource reSerVation Protocol) é usado em aplicações de tempo real reservando recursos no caminho entre um host e outro. Quando um dos hosts é móvel e muda seu ponto de conexão, o caminho deve ser re-configurado. A unidade móvel só pode fazer isso

depois de determinar seu novo care-of address e enviar um binding update ao host comunicante. O tempo gasto com o processo de handoff somado ao estabelecimento de uma nova seção do RSVP é considerável e prejudica a qualidade do serviço.

Para otimizar o processo de handoff o RSVP precisa ser adaptado para tornar possível que uma nova seção RSVP seja criada antes de encerrar a atual. Isto requer estabelecer um túnel entre o roteador antigo (RA), que a unidade móvel está, e o novo roteador (NR), para onde ela irá. Através deste túnel pacotes poderão ser recebidos e envidados pela unidade móvel até que ela finalmente estabeleça e mude seu ponto de conexão para receber diretamente os pacotes. A principal vantagem desta abordagem é que a comunicação continua enquanto a unidade móvel configura seu novo care-of address.

Esta técnica tornasse viável com IPv6 devido à capacidade da unidade móvel manter um endereço fixo, o home address, e adquirir outros care-of addresses simultaneamente, assim, a unidade móvel pode receber dados por uma interface enquanto configura outra.

Neste protocolo, para realizar um handoff de forma suave a unidade móvel notifica o RA com o endereço IP de NR. O RA estabelece com NR um túnel IP bidirecional por onde podem ser encaminhados pacotes para a unidade móvel. Porém este túnel não serve para a recepção dos dados pelo RSVP porque a nova seção RSVP ainda não possui um estado configurado.

Quando a unidade móvel adquire seu novo care-of address ela envia um binding update para o host correspondente sem deixar de usar o caminho antigo passará a enviar mensagens RSVP para o NR configurando o estado da seção RSVP e estabelecendo os termos da qualidade de serviço no caminho até NR.

Quando as mensagens percorrem o caminho até NR, passam por roteadores que ainda não acordaram com as requisições de qualidade de serviço, até que estes se acomodem às necessidades do serviço um tempo é perdido que prejudica e torna esta comunicação inaceitável. A solução é criar um segundo túnel, do RA para a unidade móvel, este é um túnel RSVP que garante a qualidade de serviço de um ponto ao outro. Assim, os dados são enviados passando pelo caminho antigo e pelo RA antes de chegarem na unidade móvel. Quando a nova rota fica pronta a unidade móvel envia um binding update definitivo para o host comunicante informando que a comunicação RSVP pode ser feita pelo novo caminho.

Referências

- [1] D. Johnson and C. Perkins. Mobility Support in IPv6.
IETF Internet Draft, drc~ietf-mobileip-ipv6-O9.txt, October 1999.
- [2] Claude Castelluccia.
HMIPv6: A Hierarchical Mobile Ipv6 Proposal.
Mobile Computing and Communications Review, Volume 4, Number 1, 2000
- [3] G Kirby. Locating the User.
Communicatoin Internatoinal, 1995
- [4] Patanapongpibul, Leo and Mapp, Glenford. A Client-based Handoff Mechanism for Ipv6 Wireless Networks, 2002
- [5] Plasto, Daniel. Fast RSVP Handovers in Mobile IPv6
First Australian Undergraduate Students' Computing Conference, 2003
- [6] Sousa, Tiago Monteiro, Edmundo e Boavida, Fernando.
Estudo do IPv6 Móvel em Linux, 2003
- [7] Huitema, Chistian
IPv6 The new Internet Protocol – second edition, 1997
- [8] Comer, Douglas
Internetworking with TCP/IP – third edition
- [9] Kurose, James e Ross, Keith
Redes de computadores e a Internet – primeira edição, 2003
- [10] RFC 3775 <http://www.ietf.org/rfc/rfc3775.txt>