Departamento de Informática

Roteamento e Mobilidade para redes móveis infra-estruturadas (IP Móvel)

Departamento de Informática

Referências:

- J.D. Solomon, MobileIP: The Internet Unplugged
- D. Johnson and D. Maltz. "Protocols for Adaptive Wireless and Mobile Networking", IEEE Personal Communication, 3(1), February 1996
- B. Lancki, A. Dixit, V. Gupta, "Mobile-IP: Supporting Transparent Host Migration on the Internet," Linux Journal, June 1996

Roteamento IP

- Prefixos de rede são usados para encaminhamento hop-by-hop
- Sistema auto-configurável: Roteadores “aprendem” novas rotas (para IP.Source) através dos pacotes que chegam a eles (e armazenam o #hops para aquele destino)
- Periodicamente, roteadores trocam as entradas de suas tabelas de roteamento (mensagem: *Router Advertisements*)
- Assim, cada roteador pode identificar qual parece ser “melhor caminho” (menor número de hops) para cada destino
- Atualização das entradas não requer muitas mensagens
- Tabelas de roteamento possuem poucas entradas (roteadores não precisam ter todos os possíveis prefixos, em IPv4: ±4 milhões)

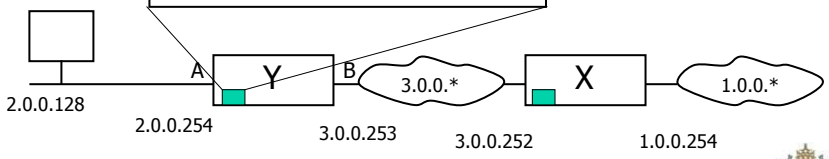
➔ Portanto, roteamento baseado em prefixos garante a escalabilidade do protocolo

Tabela de Roteamento

- Cada entrada consiste de
  [prefix, pref-length, nexthop, IntfaceID]
- Tipos de entrada:
  - Host-specific: entrega em 1 hop
  - Network specific: encaminhamento para outro roteador
  - Default

Tabela de Y

Target	Leng	nextHop	Interface	
2.0.0.128	32	direct	A	*Host-specific*
3.0.0.0	8	direct	B	*Network-prefix*
1.0.0.0	8	router X	B	*Network-prefix*
0.0.0.0	0	router X	B	*Default*

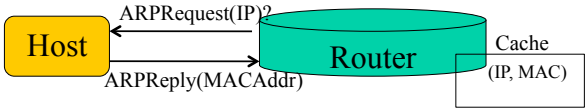


Address Resolution Protocol (ARP)

Objetivo: descobrir o endereço MAC de um host a partir do seu endereço IP

- Mensagens:
  - *ARPRequest(IP)* é um broadcast local (geralmente emitido por um Roteador)
  - O host com o IP procurado responde com *ARPReply (MAC-Addr)*

Requisitante guarda a associação (IPAddr, MACAddr) em um *ARPCache* durante um certo período



Obs:

- É possível que um ARPProxy responda em nome de um host (desconectado)
- Um novo host que é ligado à rede pode enviar um "ARPReply espontâneo"

Roteamento e Mobilidade: Problemas

- Os hosts na internet são **identificados** por um endereço IP
- E roteamento é feito usando este mesmo endereço IP, ou seja, **identidade do host coincide com sua localização** (em termos de rede/sub-rede)
- Mas hosts móveis se conectam à rede em diferentes pontos...

Duas Possibilidades:

1. Nó tem que mudar o seu endereço IP a cada vez que se conecta a um novo ponto de acesso
   - Requer que protocolos de camadas superiores tenham que tratar esta mudança (p.ex. TCP)
   - Endereço IP é usado como referência para diferentes tipos de associação/seção de segurança
2. Rotas específicas para cada host precisariam ser propagadas pela rede
   - O que tornaria as tabelas de roteamento enormes ➔ e não seria escalável

Roteamento IP e Mobilidade

Por que roteamento IP não funciona para hosts móveis?

- MH irá se conectar a diferentes sub-redes
- Roteamento IP é baseado no prefixo, que depende da localização do host

Por que o MH não troca de IP cada vez que se conecta à rede?

- Autenticação e protocolos de camadas superiores requerem que MH mantenha um endereço IP fixo

Conclusão:

➔ Mobilidade de hosts vai contra a principal regra do roteamento IP:

"Roteamento por prefixo, no qual pacotes IP são encaminhados na direção dos roteadores que anunciam a alcançabilidade para o prefixo de rede do endereço destino."

Exemplo

O que acontece se um nó móvel de IP com *prefixo1* se conecta a uma sub-rede de *prefixo2* ?

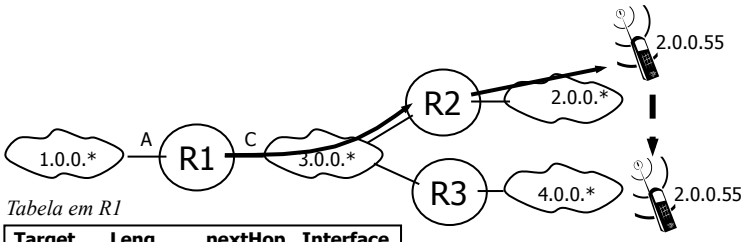


Tabela em R1

Target	Leng	nextHop	Interface
1.0.0.128	24	direct	A
3.0.0.0	24	direct	C
2.0.0.0	24	R2	C
4.0.0.0	24	R3	C

Departamento de Informática

Terminologia

- Nó correspondente (Corresponding Node - CN):: deseja mandar datagramas IP para um ...
- Nó móvel (Mobile Host -MH):: um host que muda o seu ponto de acesso (*point of attachment*), mas interage com os demais nós usando o seu endereço IP fixo
- Home Agent (HA):: um roteador na rede home (*home network*) do MH que re-encaminha datagramas (*tunel*) para o MH quando este está conectado em outra rede
- Foreign Agent (FA):: um roteador na rede visitada pelo MH (*visited network*) que provê os serviços de entrega de datagramas enquanto o MH está registrado

Departamento de Informática

Terminologia

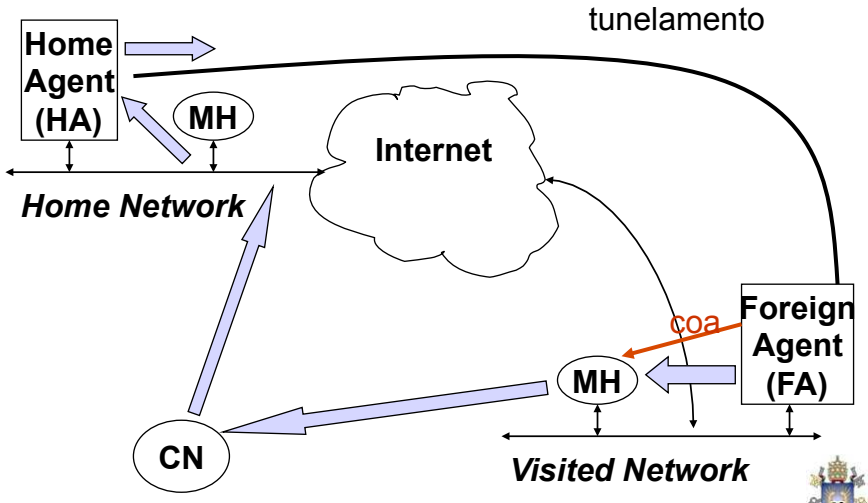
- Home address (ha):: endereço permanente do host em seu domínio origem
- Care-of-address (coa):: um novo endereço IP recebido pelo MH na rede visitada, que é usado para entregar datagramas ao MH. Pode ser
  - o endereço IP do FA
  - um endereço IP do próprio MH (co-located)

Portanto, cada MH tem 2 endereços:

- *ha*: IP fixo para identificação, e entrega quando estiver no home network
- *coa*: endereço IP no máximo a 1 hop do MH, para roteamento quando estiver em uma rede visitada

Funcionamento Básico

Request-Reply para um Mobile Host



CN= correspondent node

Visão Geral do Protocolo MIP

Principais componentes:

- Anúncio de Alcançabilidade (AgentAdvertisement):
  - Agentes de Mobilidade (HA e FA) devem anunciar os seus serviços
  - Um MH pode solicitar o serviço de um agente de mobilidade
- Registro (Binding):
  - Quando um MH está em uma rede visitada, deve registrar o seu coa junto ao seu HA
- Entrega de Datagramas (Tunelamento):
  - datagramas encaminhados do HA para o FA, para que este os entregue ao care-of-address
  - mecanismo deve contemplar todos os tipos de datagramas (incluindo broadcast/multicast)
  - para isto, cria-se um tunel entre HA e FA

Anúncio de Alcançabilidade (AA)

- Adaptou-se o protocolo ICMP (para descoberta de roteadores) para os agentes de mobilidade
- Roteadores difundem periodicamente (a cada *N* segundos) Anúncios de Alcançabilidade (*Agent Advertisements* - AA) para todas as subredes das quais fazem parte

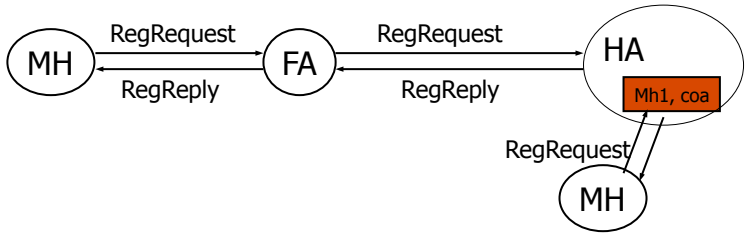
> AA é um pacote ICMP indicando:
> • Faixa de endereços coa disponíveis
> • Validade (lifetime)
> • Se o agente faz papel de HA ou FA (ou ambos)

- Um MH também pode enviar uma Solicitação de Anúncio, que fará com que roteadores próximos difundam AA
- MH obtém um coa:
  - diretamente do FA, por DHCP, ou fornecido pelo usuário

Binding (Registro)

- MH solicita ao FA que envie uma mensagem RegistrationRequest (RegRequest) anunciando o seu coa para o HA
  - FA pode negar, se coa apresentado não corresponde a um anunciado, ou então, se já está tratando muitos MHs
- O HA, ao receber de um MH o seu coa atual:
  - cria uma nova entrada (binding) em uma tabela que associa o home address com o coa do MH;
  - confirma a atualização do binding com uma mensagem RegReply
- Cada binding tem um tempo de validade, que precisa ser renovado periodicamente pelo MH
- Quando retorna para o home network, MH deve se deregistrar junto ao HA, que então remove o binding

Binding (cont.)



FA oferece o *serviço de redirecionamento*, que inclui o registro do coa no HA

MH gera RegRequest nas seguintes situações:

- Se detecta que está em nova rede
- Para renovar a validade do(s) seu(s) binding(s)
- Quando FA tiver sido re-inicializado

Binding (cont.)

Estrutura das mensagens Registration Request & Reply:

UDP header	Mobile IP header	Mobile Authentication Extension

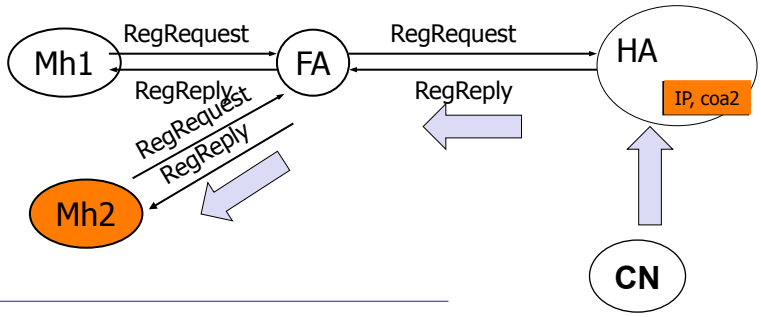
Campos/Bits do *Mobile IP header*:

- S: criar/remover um binding sem alterar os demais bindings
- B: envio tipo broadcast
- D: de-tunelamento no MH ou no FA
- M/G: Encapsulamento Minimal/ GRE
- home address do MH
- Endereço IP do HA
- Care-of-address
- ID do Request (precisa ser igual no Request e Reply)
- Lifetime: solicitação de quanto tempo o binding deve permanecer válido (no Request) e quanto tempo o HA irá manter o binding (no Reply)
- Code: se o registro teve sucesso (no Reply)

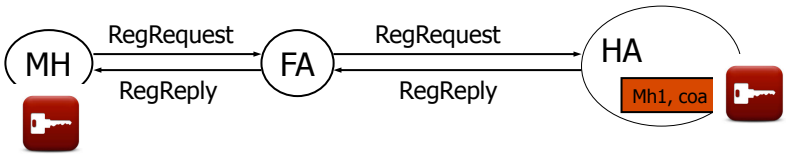
Authentication Extension é usada para a Assinatura Digital

Binding e Segurança

- Principal risco: um host de um intruso pode se fazer passar pelo FA e fazer que datagramas sejam direcionados para este host como se fosse o FA de um MH
- Para evitar *Ataques de redirecionamento* o HA e MH devem compartilhar uma chave secreta comum



Chave secreta compartilhada



- A chave secreta define uma "associação de segurança" entre os dois nós
- MH usa esta chave para se autenticar junto ao HA ao fazer o binding
- Chave não é usada para cifragem (criptografia) do RegRequest

- Por isto, cada RegRequest contém uma assinatura digital da mensagem,
- usa-se o Hashing "MD5"

Departamento de Informática

Visão Geral do Protocolo MIP

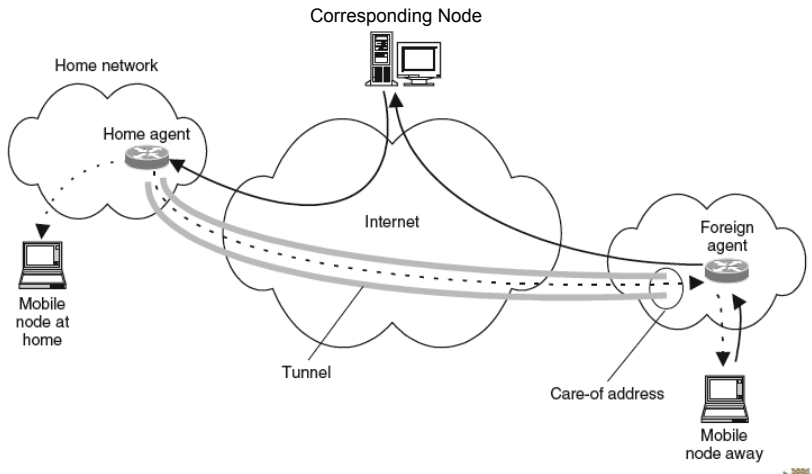
Principais componentes:

- ✓ Anúncio de Alcançabilidade (Advertisement):
  - Agentes de Mobilidade (HA e FA) devem anunciar os seus serviços
  - Um MH pode solicitar o serviço de um agente de mobilidade
- ✓ Registro (Binding):
  - Quando um MH está em uma rede visitada, deve registrar o seu coa junto ao seu HA
- Entrega de Datagramas (Tunelamento):
  - encaminhados do HA para o FA, para que este os entregue ao care-of-address (coa)
  - mecanismo deve contemplar todos os tipos de datagramas (incluindo broadcast/multicast)
  - cria-se um tunel, onde os datagramas originais são encaminhados para um host destino especifico, o FA ou MH

PUC RIO

Departamento de Informática

Tunelamento



PUC RIO

Tunelamento Básico

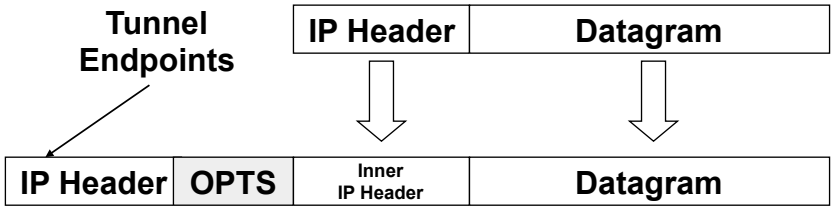
- HA intercepta datagramas para MH (como um ARP proxy)
- Encapsula o datagrama original como *payload* de um datagrama IP endereçado ao coa
- Ao receber um datagrama tunelado, o FA desempacota e entrega o datagrama original para o MACAddr do MH (consultando para isso o seu registro [ha, MAC-addr])
- Os endereços HA e o coa são chamados de Tunnel Endpoints.

Tunelamento

Existem várias alternativas para o tunelamento:

- Encapsulamento IP em IP
- Encapsulamento Minimal
- GRE: Generic Routing Encapsulation
- PPTP: Point to Point Tunnel Protocol [RFC2637]
- L2TP: Layer 2 Tunneling Protocol [RFC2661]

Tunelamento IP em IP



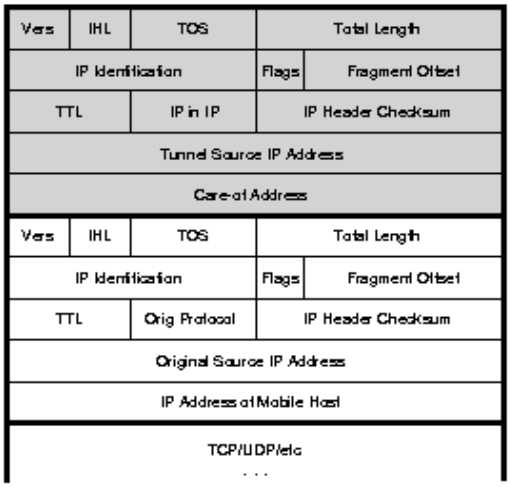
Encapsulamento IP em IP

Header IP-in-IP

Endpoints

Header encapsulado

Fonte & destino originais

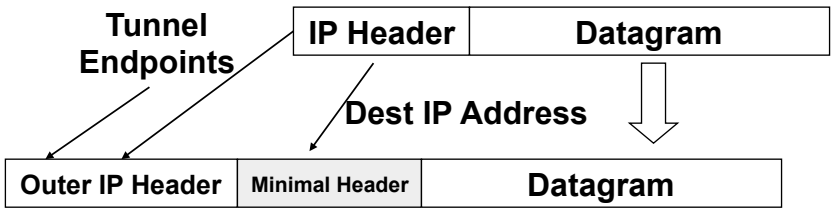


Encapsulamento IP em IP

- Header externo é do IPv4 e ocupa 20 bytes
- O end. fonte e destino no header interno não são modificados pelo encaspulador e (identificam os hosts fonte/destino originais)
- Outros headers externos podem ser adicionados (para fins de autenticação)
- alguns campos são simplesmente copiados do header interno para o externo (ex. vers, IHL, etc.)
- outros campos são re-calculados (p.ex. Checksum, length, etc.) de acordo com as características do novo datagrama.

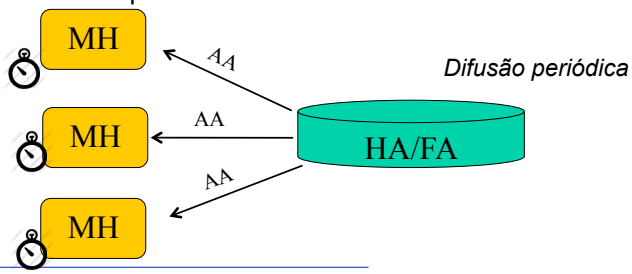
Encapsulamento Minimal

Motivação: evitar a duplicação de dados nos headers internos e externos



Como MH descobre que não está mais conectado ou que migrou?

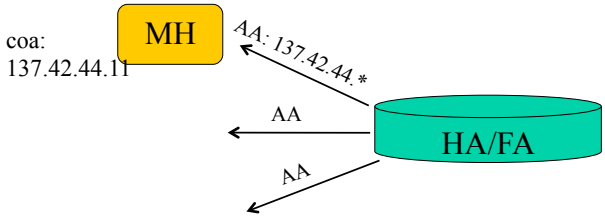
- Detecção de desconexão:
  - Cada *Agent Advertisement* (AA) contém campo validade=T
  - Agentes de Mobilidade (HA e FA) difundem um AA periodicamente
  - Se MH não recebeu AA no último período de tempo T, então MH sabe que está desconectado



Como MH sabe que não está mais conectado ou que migrou?

- Detecção de Migração:
  - MH compara o prefixo de rede do seu coa atual com o prefixo de rede do AA:
  - se for diferente, MH sabe que se conectou a uma nova rede

  Obs: podem existir vários FAs servindo uma sub-rede. Se prefixo permanecer igual, MH não precisa solicitar novo coa.



Departamento de Informática

Como MH sabe que migrou?

E como detectar migração entre dois AA consecutivos?

Alternativas:

1. Monitorar o progresso das conexões TCP (o deslocamento da janela deslizante)

   Se estiver sem progresso, isto provavelmente indica desconexão.

2. Em algumas tecnologias de rede é possível configurar a interface wireless para o "modo promíscuo", onde é possível monitorar todos os datagramas IP trafegando

   Se o prefixo de rede de um datagrama for diferente do prefixo do seu coa, o MH sabe que está em outra rede

Departamento de Informática

Papel fundamental do Address Resolution Protocol (ARP)

- Quando um MH está em uma rede visitada, o HA passa a ser o ARPProxy para receber mensagens destinadas ao MH
- Quando um MH deixa a rede home, HA usa *ARP gratuito* para atualizar todos os ARPCaches na sub-rede (redirecionando datagramas IP para sí)
- Quando um MH retorna para a rede home, este usa *ARP gratuito* para atrair datagramas para sí

Obs: Quando um MH está em uma rede visitada, não transmite qualquer ARPRequest ou ARPReply (pois o prefixo IP da rede visitada não coincide com o de seu ha)

Otimização de Rotas

Todo o tráfego para o MH é encaminhado para o HA e tunelado para o FA:

- desperdício de banda;
- maior latência
- assimetria de latência

Idéia: Permitir que os correspondentes possam encaminhar datagramas para o endereço (coa) do MH

Envolve novas mensagens:

- Binding Request
- Binding Update
- Binding Acknowledgement
- Binding Warning

Otimização de Rotas: idéia central

- Cada host (e não apenas o HA) possui um cache de bindings (ha, coa)
- Fazer com que o roteamento indireto (através do HA) tenha como efeito colateral a atualização do binding (Binding Update) (ha,coa) no nó correspondente (F)
- Isto cria caches distribuídos: ➔ tradicionalmente, existe preocupação em manter a consistência dos caches!

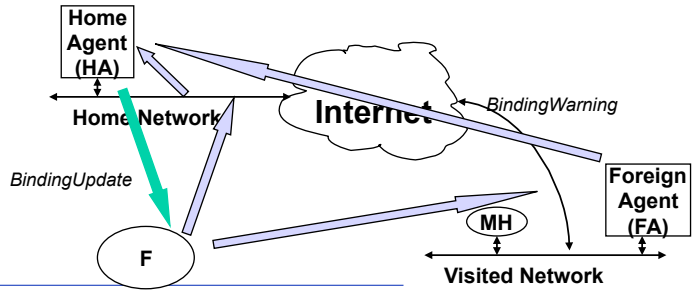
- Abordagem adotada no IP Móvel:
  - Tolerar caches inconsistentes!
  - Fazer atualizações somente por demanda
  - Criar um mecanismo para avisar o F quando um binding tornou-se obsoleto
  - HA será o único elemento autorizado a fazer as atualizações do endereço de MH no cache de F (assumindo que HA representa MH)

Binding Update (BU)

O HA envia um binding Update para atualizar o cache no nó correspondente F, :

- em resposta ao recebimento de um datagrama de (F) para o MH ausente (na rede visitada),
- em resposta a um Binding Request do F, ou
- um BindingWarning enviado por um FA (ao receber um datagrama de F),

É sempre um resultado de *uma ação iniciada pelo F*.



Binding Update

Requer uma associação de segurança entre HA e F

- F precisa ser capaz de autenticar o HA no BindingUpdate

Solução: Gerenciamento Assimétrico de Chaves

- HA assina BU com sua chave privada (criptografia assimétrica)
- F usa chave pública de HA para comprovar a autenticidade do BU (saberá que só HA poderia ter cifrado o BU)

Binding Updates não precisam ser confirmados!

Departamento de Informática

Binding Warning

Binding Warning (BW) é uma mensagem FA → HA:

- Em resposta a um datagrama tunelado para um MH que já não está mais presente, o FA envia ao HA um BindingWarning (para que este esteja ciente de que o coa está desatualizado)
- Este datagrama foi perdido ☹
- Espera-se que o MH logo atualize o seu coa no HA

- Binding Warning também não é confirmado, pois não afeta o roteamento IP

Departamento de Informática

Handover Suave

Objetivo:

- Minimizar a quantidade de datagramas IP perdidos devido à migração de nós móveis sem que o Binding tenha sido atualizado (i.e., endereços coa desatualizados)

Duas situações:

- HA acabou de tunelar um datagrama IP para um coa antigo (desatualizado)
- F tem uma entrada obsoleta do binding em seu Cache, e tunela o datagrama para o coa antigo

Handover Suave

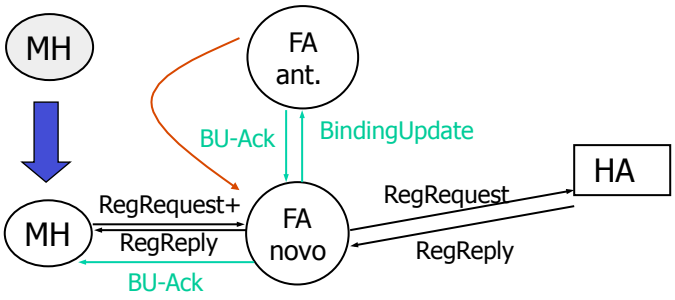
Idéia Central:

- Após migrar para uma nova rede, o RegRequest (solicitado por um MH ao novo FA) causa o envio de um BindingUpdate para o FA anterior
  - O FA anterior cria um redirecionamento (forwarding pointer) para o novo FA, ...
  - ... e pode liberar recursos previamente alocados para servir o MH

Obs:

- Handover Suave é uma solicitação especial de RegRequest ao FA atual,
- O FA pode ou não prover este serviço (i.e. estar implementado com esta funcionalidade).

Handover Suave

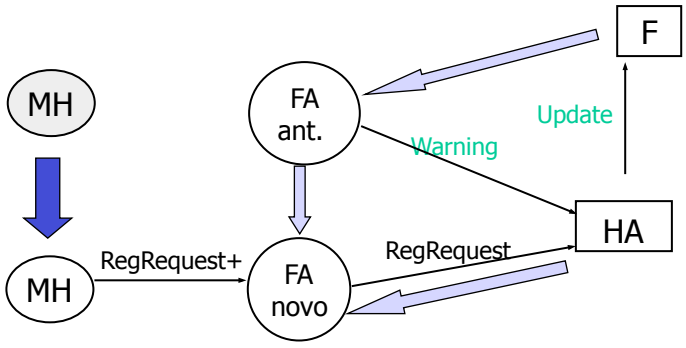


- Seja RegRequest+ uma solicitação com pedido de Handover Suave
- Os FAs capazes de prover Handover Suave anunciam isto através do AA
- Se MH não receber o BU-Ack, poderá pedir repetidas vezes.

Handover Suave & Segurança

- A autenticidade do BU precisa ser garantida, pois senão poderia haver redirecionamento malicioso de datagramas
- FA anterior precisa saber que MH de fato solicitou o BU ➔Faz-se necessária uma associação de segurança entre o MH e cada FA
- Cada vez que o MH se conecta a um novo FA, cria-se uma chave secreta temporária compartilhada entre o MH e FA (p.ex. baseada no MAC-Addr do MH, e BSS-ID/ESS-ID em 802.11)
- Usando esta chave, o FA anterior consegue autenticar o BU (de MH) sem que FA novo possa interferir

Handover Suave



Alternativas de Encaminhamento se F tem binding obsoleto:

- Se FA anterior tem ponteiro para FA novo, redireciona diretamente para FA novo
- Senão, apenas avisa HA de que MH não está mais alcançável
- F encaminha para HA, que encaminha para FA novo

Suporte à Mobilidade em IPv6

- IPv6 possui praticamente o mesmo roteamento daquele mostrado para Mobile IP, com suporte a Otimização de Rota, e Handover Suave, etc.

Suporte à Mobilidade em IPv6

Principais diferenças com relação ao MIPv4:

1. Não há mais necessidade de designar um roteador como FA; o próprio MH detecta a rede visitada através das facilidades de *Descoberta de vizinhos* e *Auto-configuração* do IPv6, e obtém o seu coa (da rede visitada)

Auto-configuração pode ser:

- Stateful: com DHCPv6
- Stateless: com apoio do ICMPv6 -> combinando prefixos divulgados pelos roteadores com o próprio endereço MAC (ou número randômico); na ausência de roteadores usa-se o FE80 para gerar "link-local address"

Departamento de Informática

Descoberta de Vizinhos

- Roteadores da rede (local) divulgam a sua presença através de envios periódicos de "Router Advertisements"
- Um host IPv6 pode solicitar roteadores através de "Router Solicitation"
- Múltiplos roteadores possíveis com alternativas para determinadas redes;

PUC RIO

Departamento de Informática

Suporte à Mobilidade em IPv6

Principais diferenças:

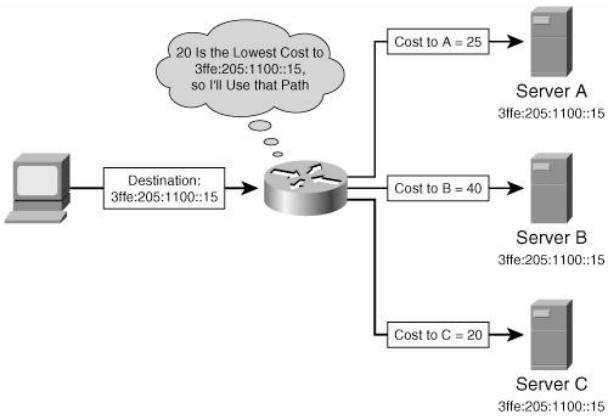
2. No lugar de encapsulamento de datagramas (tunelamento), usa-se apenas o header IPv6, que já inclui o home address do MH e o coa
   - A partir do header IPv6, o próprio MH reconhece que o pacote é para ele.

3. Podem haver vários roteadores Home Agents para o prefixo de rede "home" do MH,
   - Estes compartilham um endereço anycast

PUC RIO

Princípio do Anycast

Um endereço Anycast identifica múltiplas interfaces.
Pacotes endereçados a um endereço anycast são encaminhados para a interface mais próxima (menor número de hops)



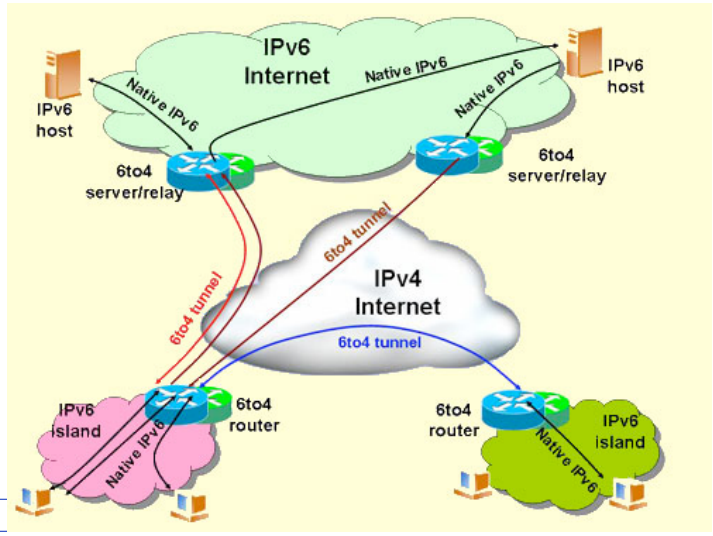
Suporte à Mobilidade em IPv6

Principais diferenças (cont):

- Sempre que adquire um novo coa, o MH atualiza o binding no(s) Home Agent(s) usando anycast,
- E em todos os nós correspondentes (F), com os quais esteja se comunicando (correspondent registration)
- Mantém uma lista de nós para os quais já enviou ou Binding Update.

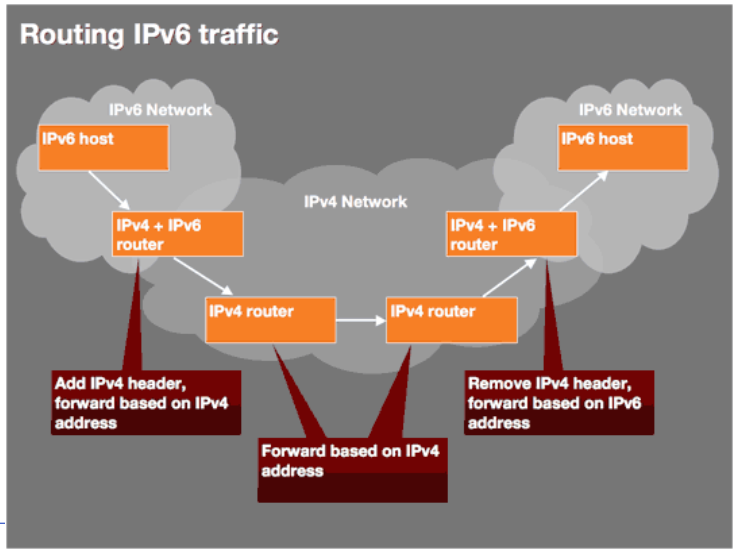
Departamento de Informática

Convergência de IPv6 e IPv4



Departamento de Informática

Roteamento híbrido IPv4-IPv6



Resumo

- Conhecimento da localização corrente é essencial para o encaminhamento de pacotes para o MH
- O Mobile IP (e o IPv6) disponibilizam duas soluções ligeiramente diferentes para *gerenciamento de localização/ mobilidade* que:
  - são independentes de tecnologia de rede (infra-estruturada)
  - São totalmente compatíveis com o protocolo IP
  - escondem a mobilidade para as camadas de protocolo superiores (transporte, sessão)

Referências

- C.Perkins, D. Johnson. Mobility Support in IPv6, MobiCom 1996.
- IETF, IP Version 6 Working Group (www.ietf.org/ html.charters/ipv6-charter.html)
- T. Kato, R. Takechi, H. Ono, A Study on Mobile IPv6 Based Mobility Management Architecture, Fujitsu Sci. Tech. Journal, 37(1), (http://magazine.fujitsu.com/us/ vol37-1/paper09.pdf)