IP Móvel, v4

FEUP
MPR

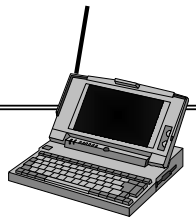
Motivação

- Encaminhamento tradicional de datagramas IP
  - Baseado em endereço IP de destino, prefixo de rede
  - Endereço de rede IP ←→ Rede física
  - Mudança de rede ➔ mudança de endereço IP
- Possíveis soluções para a mobilidade
  - » Alteração das rotas para as máquinas móveis?
    - ➔ mudança de tabelas de encaminhamento dos routers
    - ➔ solução não compatível (não escalável) com
      - Mudanças frequentes de posição
      - Número elevado de terminais móveis
    - ➔ problemas de segurança
  - » Mudança do endereço IP da máquina móvel?
    - ➔ Endereços dependentes da localização
    - ➔ Localização do terminal difícil ← Actualização de DNS é demorada
    - ➔ Quebra de ligações TCP. Problemas de segurança

Requisitos do IP Móvel (RFC 2002)

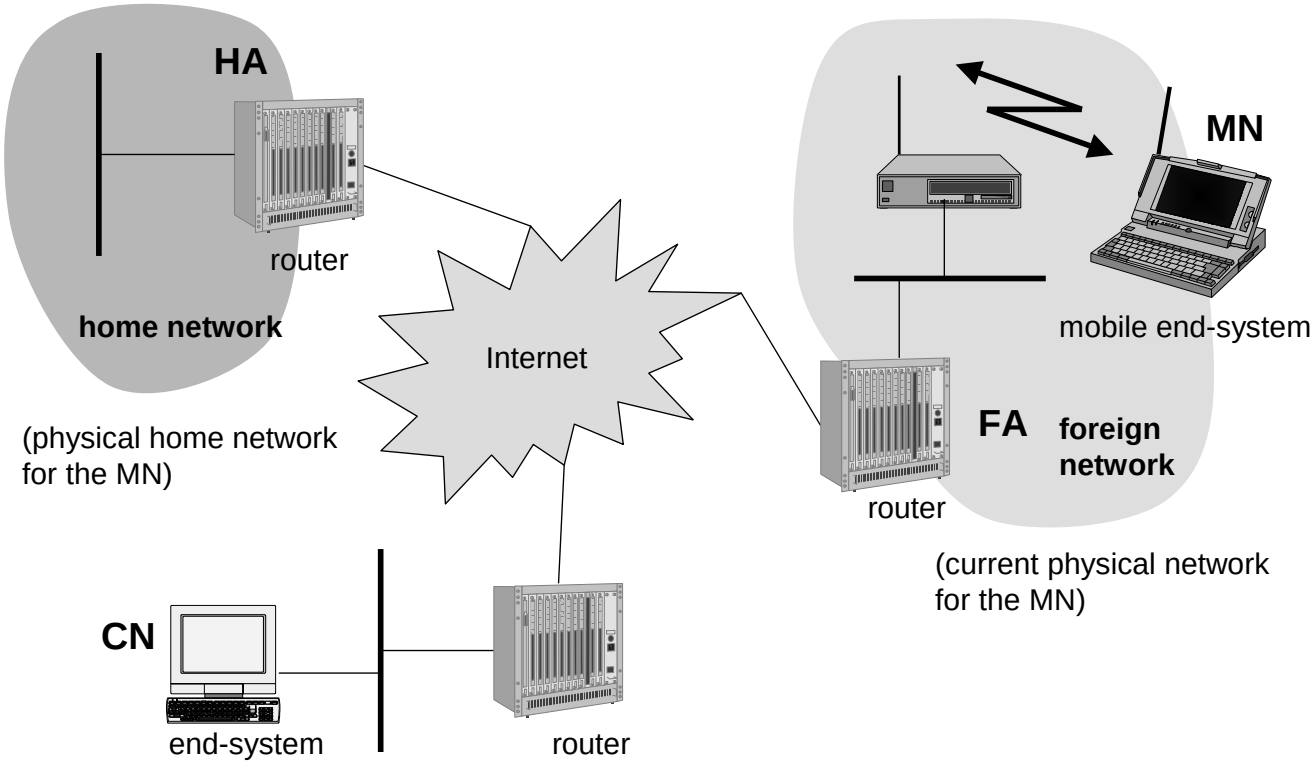
- Transparência
  - Estações móveis devem manter o seu endereço IP
  - Comunicação deve ser retomada depois de quebra da ligação (a mudança de rede)
  - Ponto de ligação à rede fixa pode ser alterado
- Compatibilidade
  - Deve suportar mesmos protocolos de nível 2 que IP
  - Não deve implicar alterações dos routers/máquinas existentes
  - Máquinas móveis devem comunicar c/ máquinas fixas
- Segurança
  - Mensagens de sinalização devem ser autenticadas
- Eficiência, escalabilidade
  - Sistema de sinalização leve
  - Sistema escalável à Internet global

Terminologia

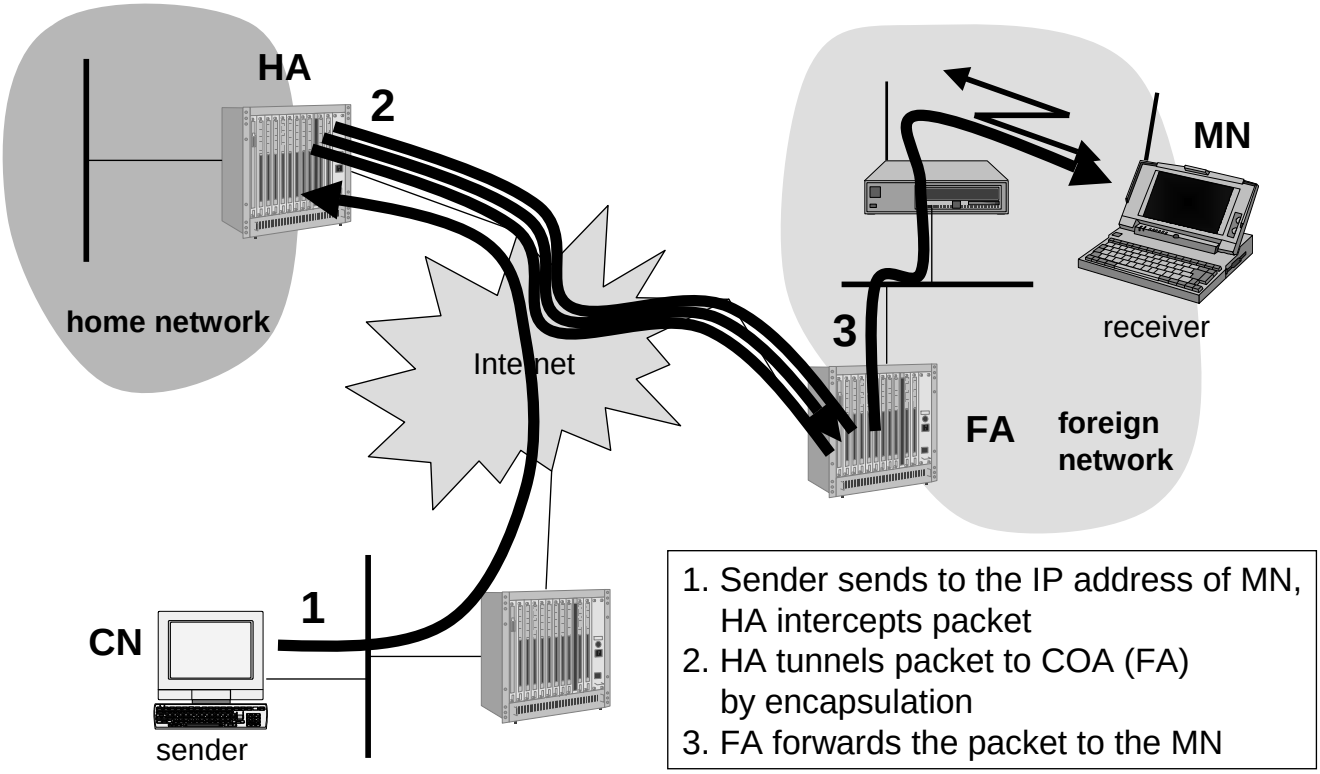


- MN, Mobile Node → estação móvel
  - Máquina móvel. Muda de ponto de ligação
  - Mantém endereço IP
- HA, Home Agent → Agente na rede origem
  - Sistema (router) na rede origem do MN
  - Regista localização do MN. Usa túnel para enviar datagramas IP para COA
- FA, Foreign Agent → Agente na rede visitada
  - Sistema (router) na rede visitada pelo MN
  - Entrega datagramas recebidos pelo túnel ao MN
- COA, Care-of Address
  - Endereço IP da extremidade do túnel na rede visitada
  - Localiza MN
  - Pode ser atribuído por DHCP
- CN, Correspondent Node
  - Máquina que comunica com o MN

Exemplo

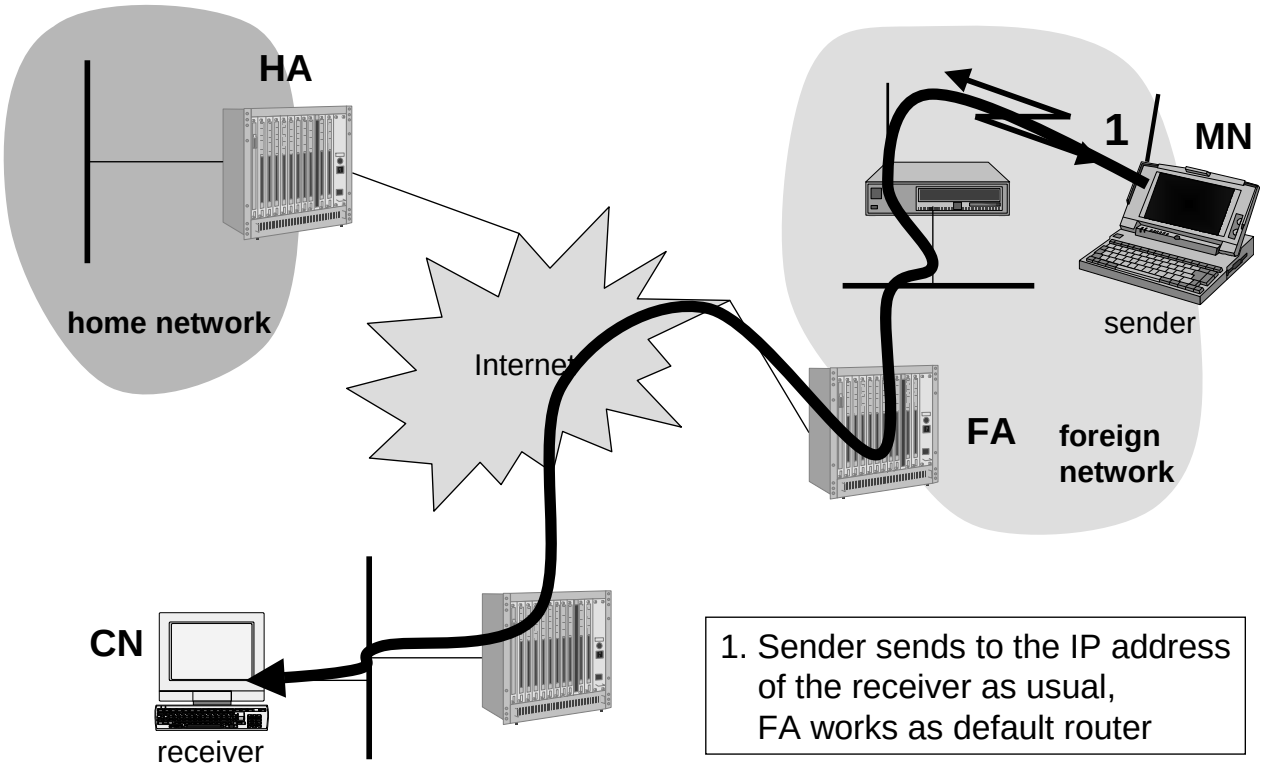


Transferência de Dados para o MN

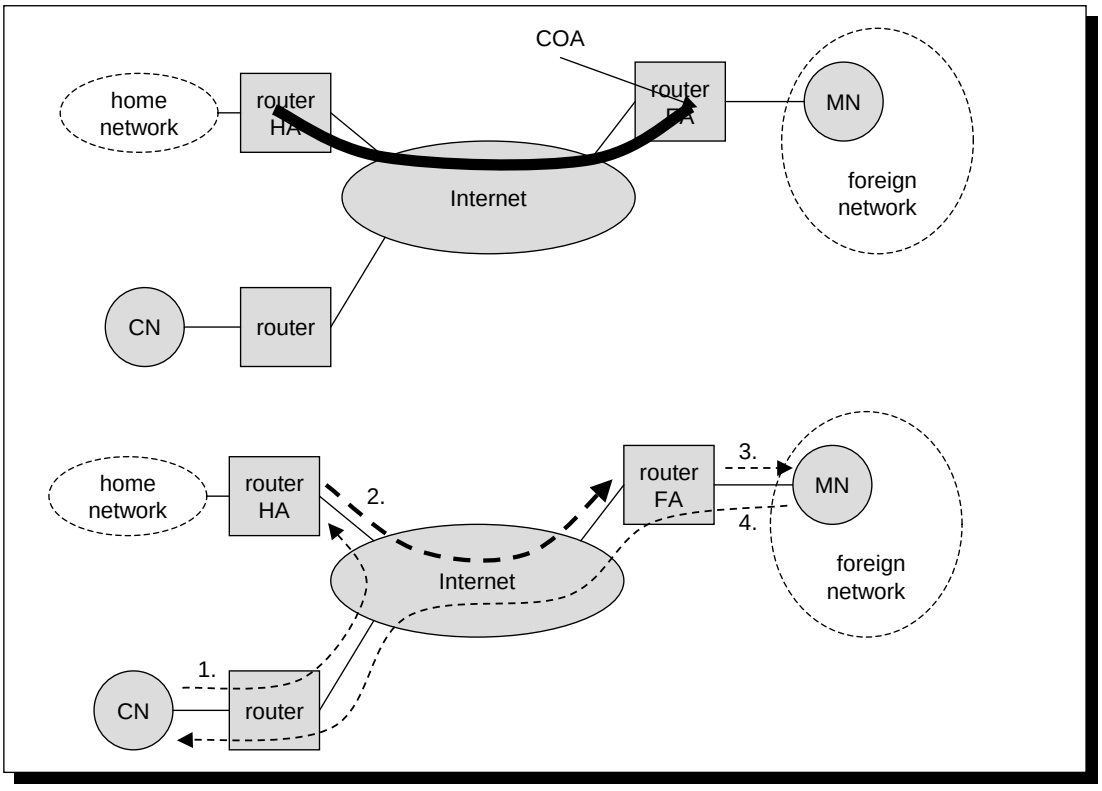


1. Sender sends to the IP address of MN, HA intercepts packet
2. HA tunnels packet to COA (FA) by encapsulation
3. FA forwards the packet to the MN

Transferência de Dados do MN



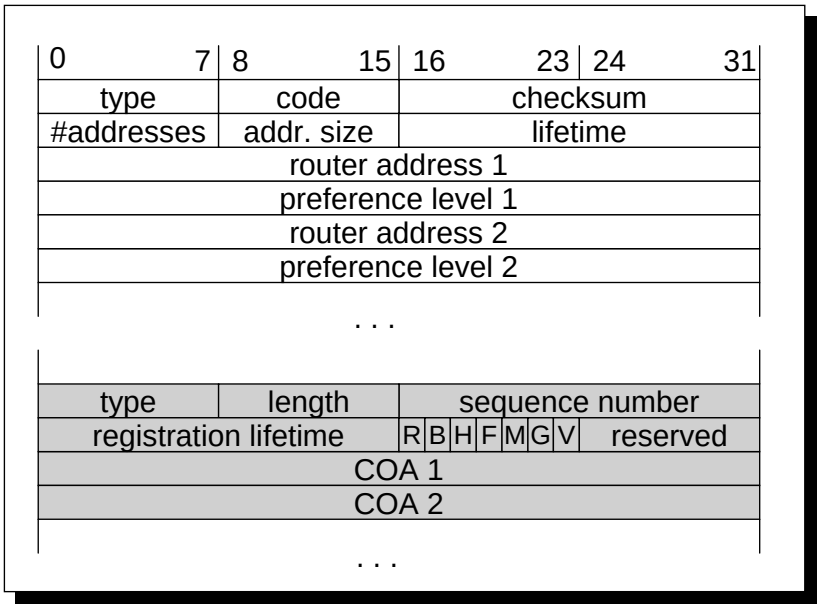
Fases da Mobilidade



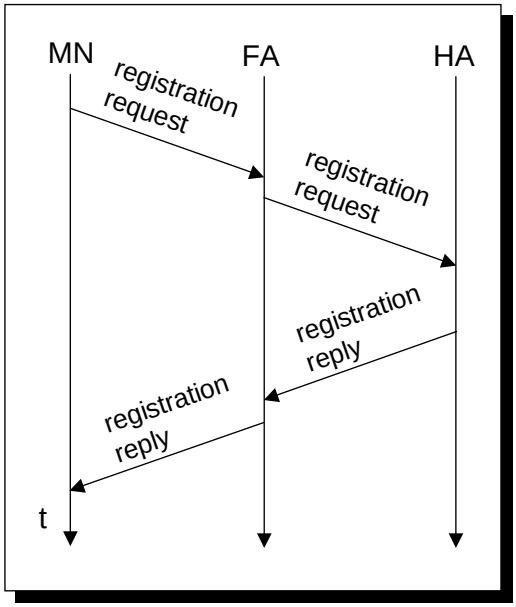
Comunicação com os Agentes

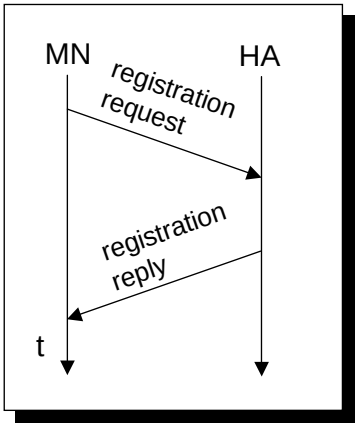
- MN determina rede de acolhimento
  - » HA, FA → geram regularmente mensagens de aviso para suas redes
    Adaptação de mensagens do ICMP Router Advertisment Protocol (RFC 1256)
  - » MN escuta mensagens; determina rede de acolhimento
    - – A sua, ou
    - – Uma rede visitada → conhecimento de COA
- MN regista-se, por tempo limitado
  - » MN envia COA para HA (via FA)
  - » HA confirma recepção
  - » Autenticação obrigatória → Associação de segurança entre MN e HA
- Na rede origem
  - » HA assume endereço IP do MN
  - » Routers (na rede origem) actualizam entradas
  - » Pacotes com destino MN são enviados para HA
  - » Processo independente de alterações de COA/FA

Agentes – Mensagens de Aviso

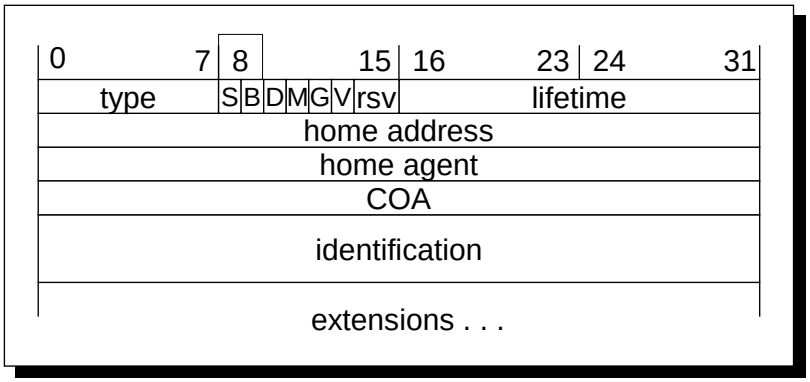


Registo do MN no Home Agent

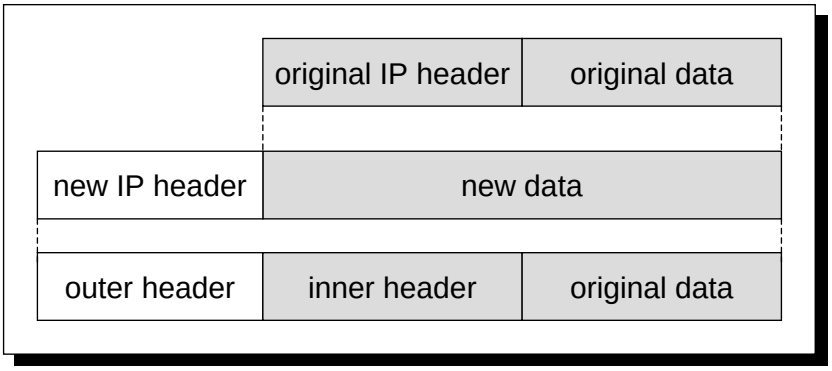




Mensagem de Pedido de Registo



Encapsulamento, Tuneis



IP em IP (obrigatório)

ver.	IHL	TOS	length
IP identification		flags	fragment offset
TTL	*IP-in-IP*	IP checksum	
IP address of HA			
Care-of address COA			
ver.	IHL	TOS	length
IP identification		flags	fragment offset
TTL	lay. 4 prot.	IP checksum	
IP address of CN			
IP address of MN			
TCP/UDP/ ... payload			

Túnel entre HA e COA

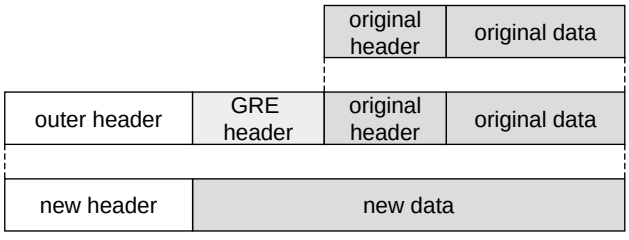
Encapsulamento Mínimo (Opcional)

- Campos repetidos não são enviados
  - TTL, IHL, version, TOS
- Aplicavel apenas a pacotes não fragmentados

ver.	IHL	TOS	length
IP identification		flags	fragment offset
TTL	*min. encap.*	IP checksum	
IP address of HA			
care-of address COA			
lay. 4 protoc.	S	reserved	IP checksum
IP address of MN			
original sender IP address (if S=1)			
TCP/UDP/ ... payload			

GRE - Generic Routing Encapsulation

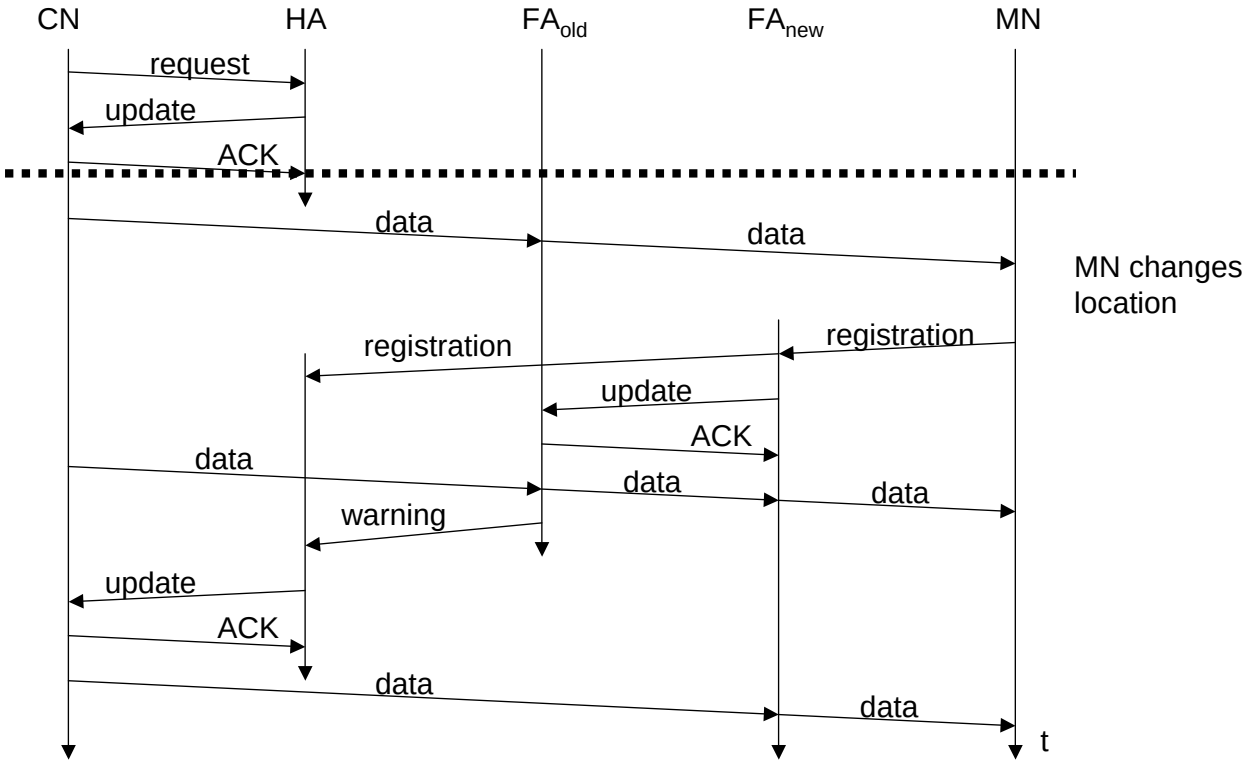
ver.	IHL	TOS	length
IP identification		flags	fragment offset
TTL	*GRE*	IP checksum	
IP address of HA			
Care-of address COA			
C R K S s rec.	rsv.	ver.	protocol
checksum (optional)		offset (optional)	
key (optional)			
sequence number (optional)			
routing (optional)			
ver.	IHL	TOS	length
IP identification		flags	fragment offset
TTL	lay. 4 prot.	IP checksum	
IP address of CN			
IP address of MN			
TCP/UDP/ ... payload			



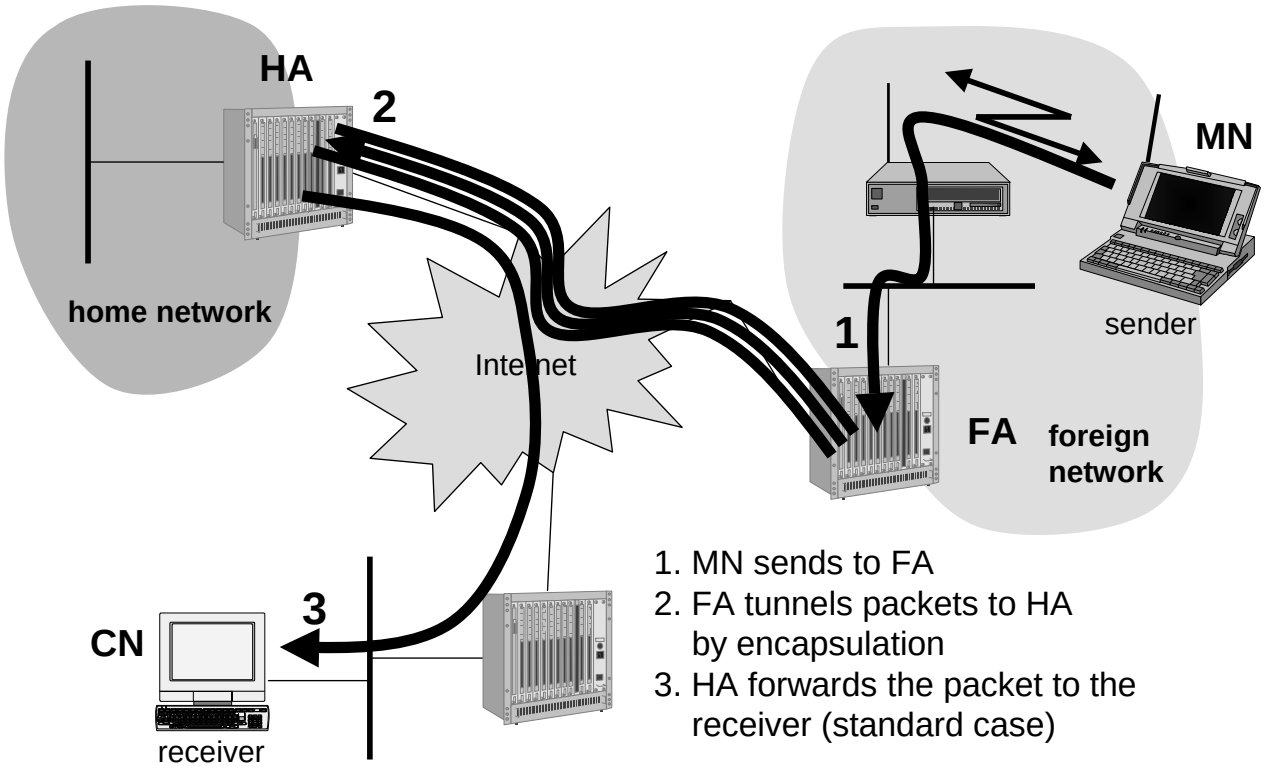
Encaminhamento de Pacotes – Optimização

- Rotas triangulares
  - » CN envia pacotes para MN via Ha ➔ Atraso grande, carga na rede
- Soluções alternativas
  - » CN aprende localização do MN → Túnel directo → CN ➔MN
  - » HA informa CN da localização do MN → Problemas de segurança
- Mudança de FA
  - » Pacotes em trânsito podem ser perdidos
  - » Para evitar perdas
    - – FA-novo informa FA-antigo
    - – FA-antigo encaminha últimos pacotes para FA-novo
    - – FA-antigo termina reserva de recursos para MN

Mudança de FA



Túnel em Sentido Inverso (RFC 2344)



Túnel em Sentido Inverso

- Firewall pode só aceitar endereços topológicamente correctos
  - » Pacote do MN encapsulado pelo FA → topológicamente correcto
  - » Problemas de multicast, TTL → resolvidos
- Túnel em sentido inverso não resolve
  - » Problemas de segurança → túnel pode ser usado para entrar na rede
  - » Optimização das rotas → duplo encaminhamento triangular

Problemas do IP Móvel

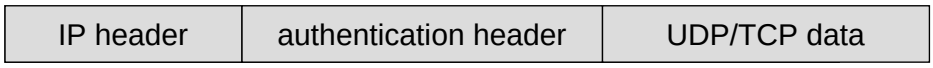
- Segurança
  - » Autenticação do FA → problemática. FA pertence a outra organização
  - » Não existem (ainda) protocolos normalizados de gestão/distribuição de chaves
- Firewalls
  - » IP móvel convive mal com Firewalls
  - » Necessárias configurações especiais
- QoS
  - » Túneis dificultam fornecimento de QoS a fluxos de pacotes específicos
- Tópicos em investigação → Segurança, Firewalls, QoS

Segurança no IP Móvel – Requisitos (RFC 1825)

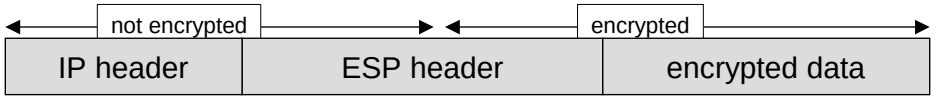
- Integridade
  - » Alterações nos dados entre emissor e receptor devem ser detectáveis por emissor
- Autenticação
  - » Endereço do emissor deve ser verdadeiro
  - » Toda a informação recebida é enviada pelo emissor
- Confidencialidade
  - » Apenas receptor (e emissor) conhecem os dados
- Não repudiação
  - » Emissor não pode negar o envio de dados
- Análise de tráfego
  - » Não deve ser possível criar perfis de tráfego ou utilizador
- Protecção contra repetição
  - » Receptores devem poder detectar mensagens repetidas.

Arquitectura de Segurança IP

- Para estabelecer uma associação de segurança, 2 ou mais parceiros
  - » negoceiam mecanismos de segurança
  - » escolhem mesmos parâmetros
- Dois cabeçalhos para segurar pacotes IP
  - » Authentication-Header (AH)
    - – Garante a integridade e autenticidade dos pacotes IP
    - – Com cifragem assimétrica → não repudiação

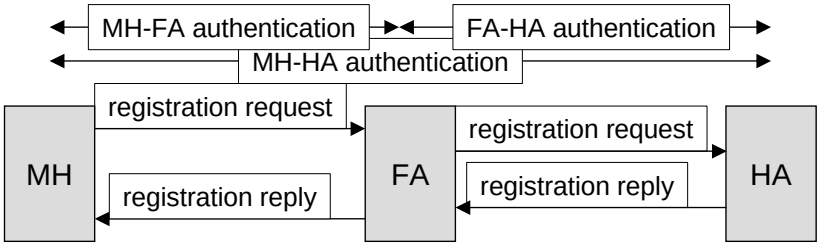


  - » Encapsulation Security Payload (ESP)
    - – confidencialidade dos dados (dados cifrados)



Arquitectura de Segurança – IP Móvel

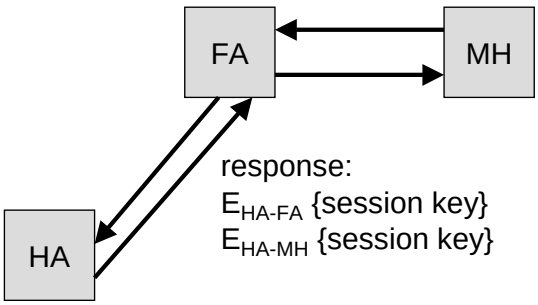
- Associações de Segurança (Móveis) para registos
  - » Parâmetros para o MH, HA e FA
- Extensões à arquitectura de segurança IP
  - » Autenticação acrescida no registo



  - » Prevenção contra repetição de registos
    - – timestamps: timestamps de 32 bits + random number de 32 bits
    - – nonces: número aleatório de 32 bits (MH) + número aleatório de 32 bits (HA)

Distribuição de Chaves

- HA distribui as Chaves de Sessão



- FA tem associação de segurança com o HA
- MN faz registo (binding) no HA
- HA responde com nova Chave de Sessão para FA e MN