Redes IP - Segurança e Mobilidade

FEUP/MRSC/RedesIP – 2001
MPR

Introdução

- Conceitos básicos
  - Criptografia
  - Segurança em redes IP
  - Túneis
  - VPNs
- IPSec
  - Associação de Segurança, Modos de funcionamento
  - AH, ESP, Processamento de tráfego, IKE
  - Aplicações tipo
- IP Móvel
  - Transferência de dados
  - Encapsulamento
  - IPv6

Conceitos Básicos: Criptografia

(De)Cifra

- Cifrar: mensagem aberta → mensagem cifrada
  - Função matemática + chave
- Decifrar: mensagem cifrada → mensagem aberta
  - Função matemática + chave
- Exemplo c/ DES
  - » Mensagem plana
    - *Encryption can make UNIX more secure*
  - » Chave
    - *nosmis*
  - » Mensagem cifrada
    - *M-itM-@g^B^?^B?^NM-XM-vZIM-U_h^X^$kM-^^sI^^M-f1M-^ZM-jM-gBM-6M->^@M-”^M-^JM-^JM-7M--M-^T*
    - Caracter de controlo precedido por ^. Bit mais sinificativo activo → M-

Métodos de Cifra

- Chave privada
  - » chave única para cifrar e decifrar → chave simétrica
    - DES_CBC (Data Encryption Standard, Chipher Block Chaining). Chave de 56 bits
    - IDEA (International Data Encryption Algorithm). Chave de 128 bits
    - 3DES – 3 chaves de 56 bits (1ª pode ser igual a 3ª)

- Chave pública
  - » 2 chaves: publica e privada → chave assimétrica
    - RSA (Rivest, Shamir, Adleman) – chaves longas

Resumo de Mensagem / Assinatura Digital

- Resumo de mensagem
  - » Pequeno valor (128 a 512 bit) obtido a partir de uma mensagem
  - » Função de Hash
  - » Algoritmos comuns
    - MD5 (Message Digest 5). 128 bit
    - SHA (Secure Hash Algorithm). 160 bit
- Assinatura digital
  - » Resumo de mensagem cifrado com chave privada (chave assimetrica)
    - Ex. MD5+RSA, SHA+RSA
  - » Resumo de mensagem cifrado com chave única (chave simétrica)

- Com assinatura digital consegue-se
  - » Integridade → sabe-se se mensagem foi modificada
  - » Autenticação → sabe-se quem assinou a mensagem (usando chave publica)

Conceitos Básicos: Segurança em Redes IP

Problemas de Segurança Frequentes

- Spoofing
- Session Hijacking
- Eaves dropping
- Man-in-the-Middle

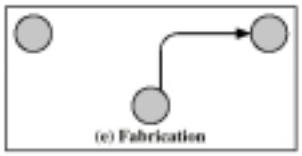
Spoofing

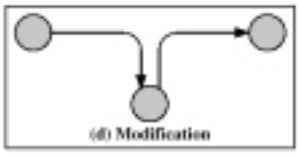
» Datagrama IP
- Cabeçalho → endereço origem, endereço destino, opções
- Dados → informação de níveis superiores

» Router
- Encaminha datagramas. Desconhece detalhes da arquitectura da rede

» Rota de um datagrama
- Não é controlada por origem nem destino
- Datagramas do mesmo fluxo podem seguir rotas diferentes. Qualquer rota é legítima

» Problema
- Cabeçalhos de datagrama IP → facilmente gerados/alterados em qualquer máquina
- Ex. Acesso a serviços configurados por endereços de rede. NFS





Roubo de Sessão. Monitoração de Tráfego

- Roubo de sessão (Session Hijacking)
  - Ex. Roubo de mail. Sobre ligação TCP/IP
  - Cliente estabelece ligação TCP/IP com servidor de mail. Autentica-se no servidor.
  - Usurpador entra, depois da autenticação e
    - Termina ligação com o servidor
    - Continua ligação com o cliente, recebendo o mail
  - IP: Identificação inicial -/→ segurança durante toda sessão

- Monitoração de tráfego (Eavesdropping)
  - LANs Ethernet → pacotes disponíveis em todos os nós da rede (Hubs e cabo)
  - Carta de rede
    - Modo normal → copia tramas que lhe forem endereçadas
    - Modo promíscuo → copia todas as tramas. Outros nós não sabem da sua existencia.
  - Acesso a toda a informação

Man-in-the-Middle

- Solução para problemas anteriores
  → utilização técnicas de cifra

- Cifragem
  - chaves de cifra (= bits de informação)
  - Algoritmos de cifragem → usados para cifrar /decifrar informação

- Problemas!
  - Troca de chaves não protegidas → intercepção → ataque *Man-in-the Middle*

  - Os comunicadores assumem que a comunicação é segura!!
  - Toda a comunicação pode ser espiada/ adulterada

Requisitos de Segurança em Redes

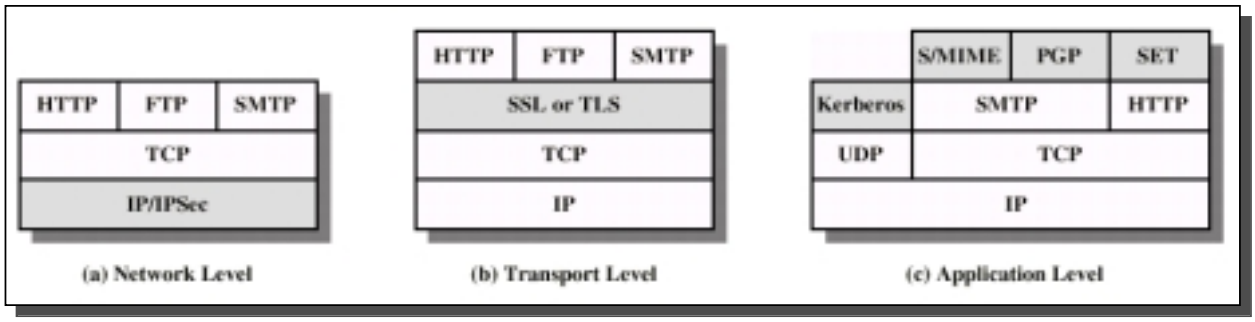
» Autenticação: O parceiro da comunicação deve ser o verdadeiro

» Confidencialidade: Os dados transmitidos não devem ser espiados

» Integridade: Os dados transmitidos não devem ser alterados

Segurança na Pilha TCP/IP

- Aplicação
  - » Kerberos → sistema de autenticação global. Baseado em bilhetes. Chave privada (DES)
  - » PGP (Pretty Good Privacy). Usado com mail para (de)cifrar mensagens. Assinaturas digitais
  - » S/MIME → Cifra de mensagens + assinaturas electónicas
  - » SSH → Secure Shell. Substituto seguro do rsh / rlogin
- Transporte
  - » TLS (Transport Layer Security). Nome antigo → SSL. Segurança de sessões HTTP
- Rede
  - » IPSec



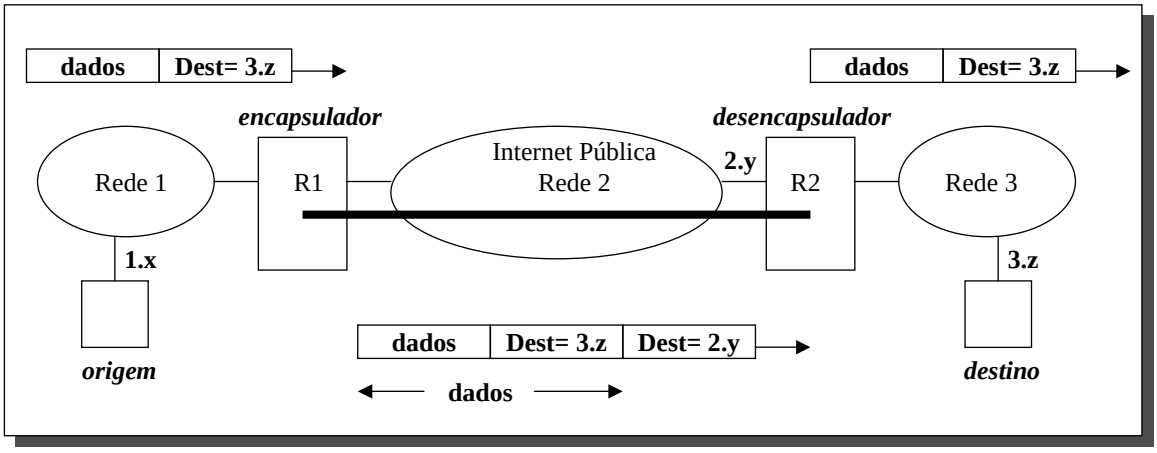
A Importância da Camada de Rede

- Comunicação TCP/IP modelizada em camadas. Cada camada
  - – Endereça um problema
  - – Oferece serviços ao nível superiror
  - » Camadas física/ligação lógica (por baixo do IP)
    - – Cablagem, cartas de rede, ligações
    - – Ex. Ethernet, ligações ponto a ponto
  - » Camada de rede (o IP)
    - – Usa serviços (envia/recebe dados) da camada ligação lógica
    - – Contém lógica de encaminhamento. Encaminha datagramas/pacotes de dados
  - » Camadas de aplicação (acima do IP)
    - – Ligações entre máquinas extremas (TCP/UDP)
    - – Aplicações, serviços de rede
- Camada de rede, em redes IP
  - – Homogénea, universal → todas as aplicações usam o IP
  - – Nas outras camadas podem ser usados protocolos alternativos
  - – IP seguro → rede segura

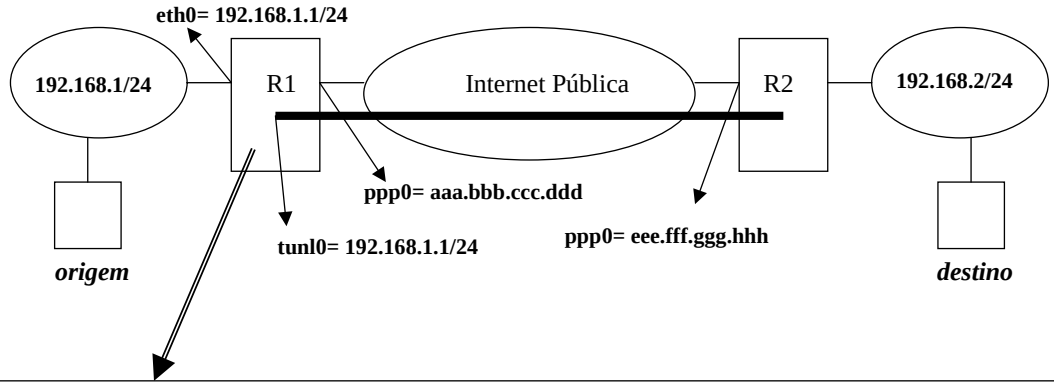
Conceitos Básicos: Túneis

Túnel

- » Ligação virtual ponto-a-ponto entre 2 nós
- » nós → separados por *n* redes /nós
- » Pacote encapsulado usando um protocolo do mesmo nível . Ex. IP em IP
- » Ganhos: privacidade, segurança → redes privadas virtuais



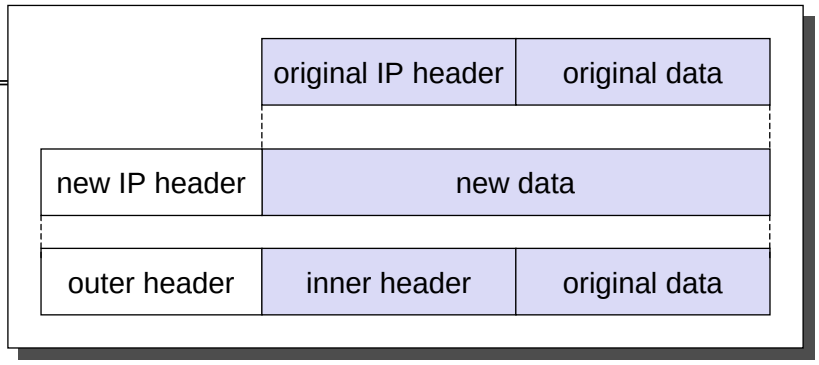
Túnel de Nível 3

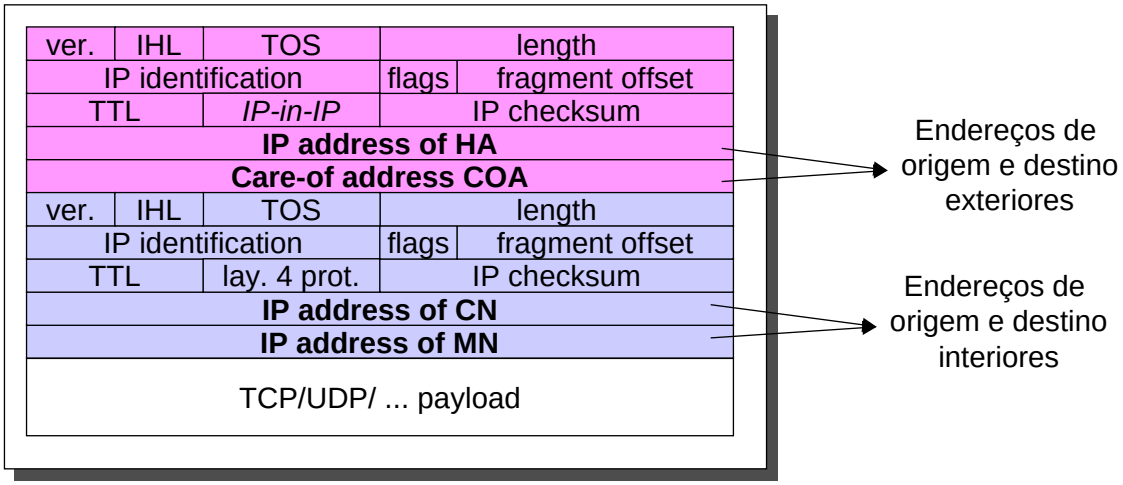



```
- ifconfig eth0 192.168.1.1 netmask 255.255.255.0 up
- route add -net 192.168.1.0 netmask 255.255.255.0 eth0
- route add default ppp0
- ifconfig tunl0 192.168.1.1 up
- route add -net 192.168.1.0 netmask 255.255.255.0 eth0
- route add -net 192.168.2.0 netmask 255.255.255.0 gw eee.fff.ggg.hhh tunl0
```


Túnel de Nível 3 – IP em IP

- RFC 2003





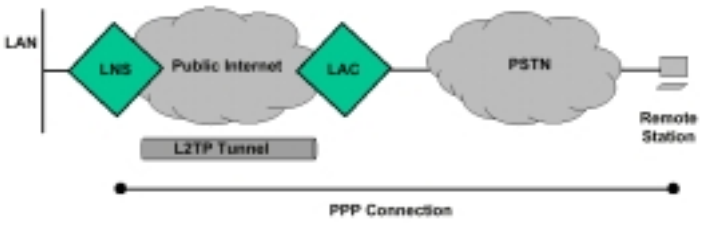
Túnel de Nível 3 – IP em IP, com Encapsulamento Mínimo

» Campos repetidos do cabeçalho enviados 1 vez
  Ex. IHL, version, TOS
» Aplicavel apenas a pacotes não fragmentados
» RFC 2004

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				

Túnel de Nível 2 – Layer 2 Tunnel Protocol (L2TP)

» Elementos
  – LAC, L2TP Access Concentrator
    ◆ No ISP
  – LNS, L2TP Network Server
    ◆ Na rede de destino



» Características
  – Ligação de nível 2, L2, (PSTN, ISDN, ADSL) entre estação remota e ISP
  – L2TP → continua L2 entre ISP e rede local
  – Tramas PPP trocadas entre estação remota e gateway rede local
  – Pode ser usado com IPSec
  – RFC 2661

Conceitos Básicos:
VPN – Virtual Private Nework

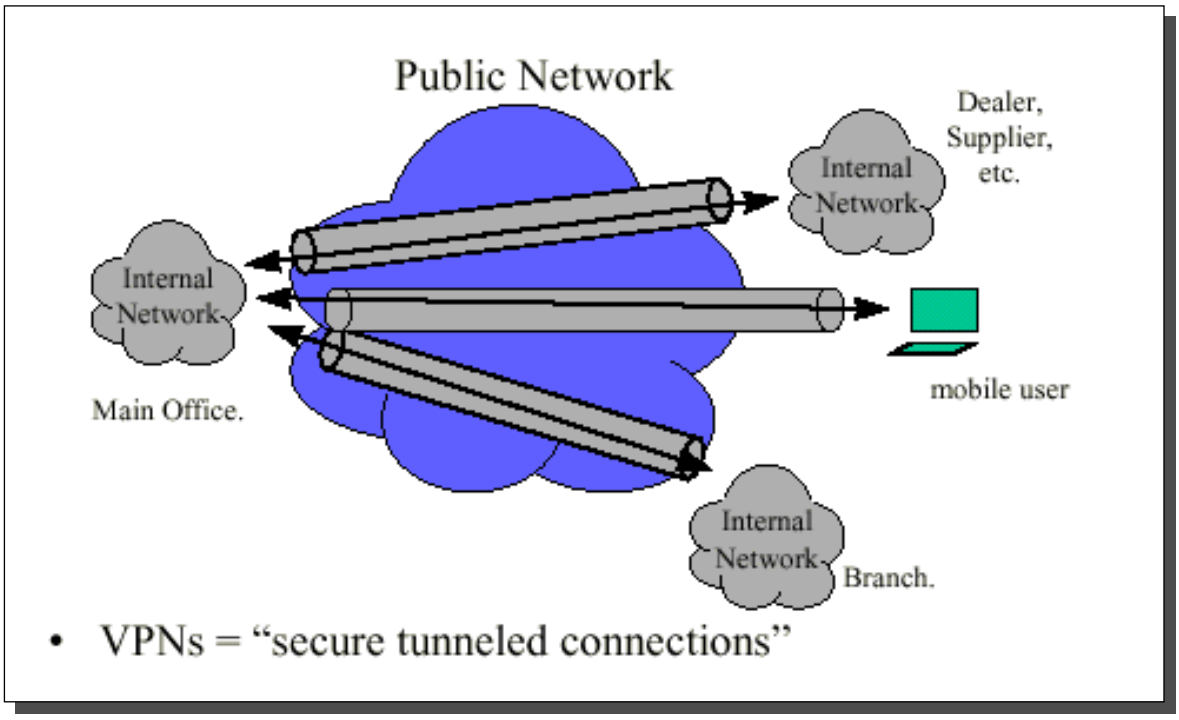
VPN – Virtual Private Network

- *Virtual*
  - » Esconde a estrutura real de rede ← rede estruturada em camadas
  - » Rede física
    - – pertence a outra entidade. Não é de confiança
- *Private*
  - » Originalmente → fechada
  - » Hoje → segura
    - – Ligações cifradas
    - – Origem dos dados autenticada
- *Network*
  - » Extensão de uma LAN
  - » Endereçamento uniforme

No Passado

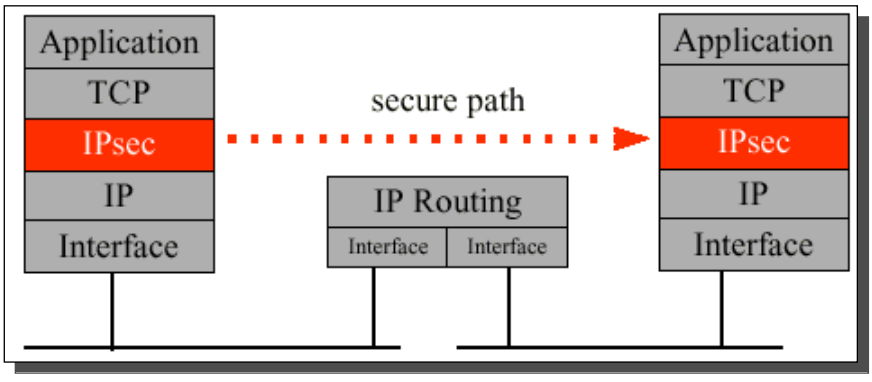
- Baseadas em linhas alugadas / circuitos dedicados
  Frame relay, ATM ou X.25
- Grupo fechado de utilizadores
- Problemas
  - » Caras. Difíceis de administrar e reconfigurar

Hoje - Solução Tipo



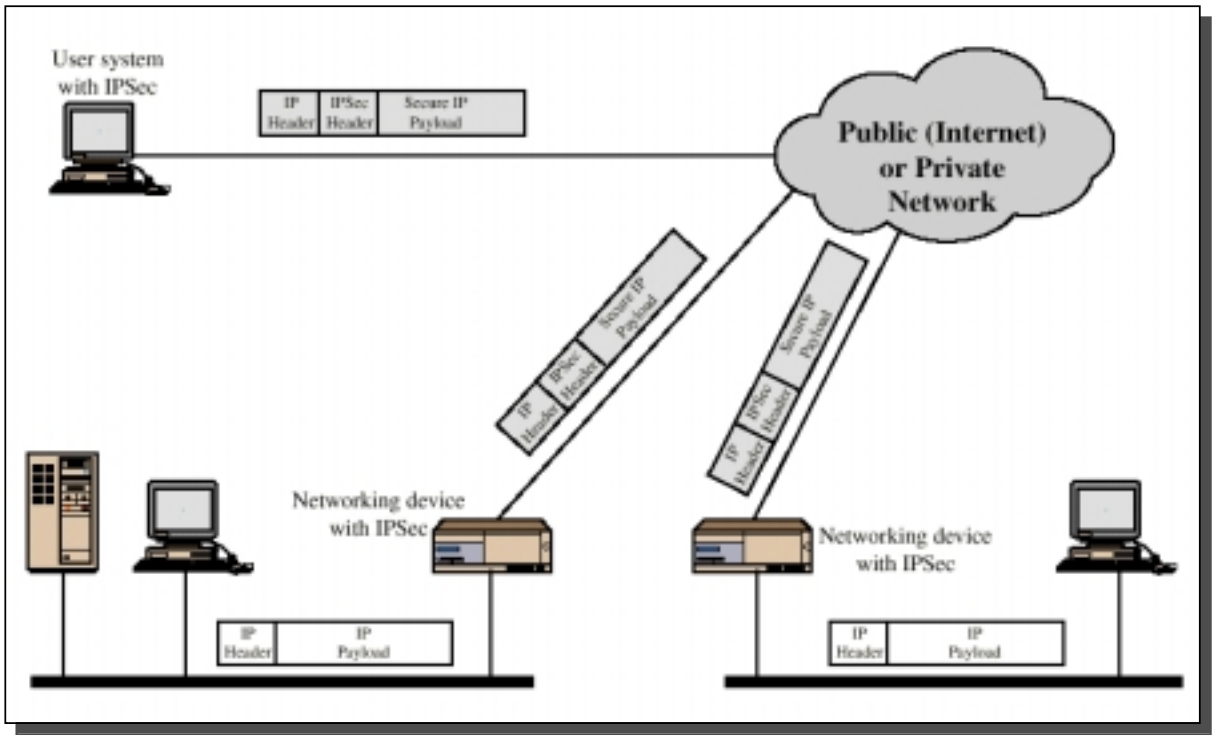
IPSec

IPSec



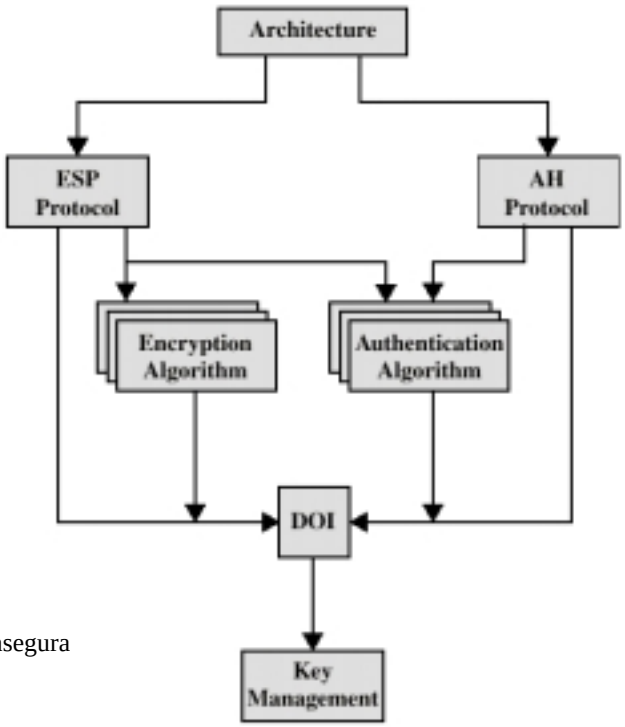
» Arquitectura segura para IP
- Aberta, normalizada
- Autenticação e integridade dos dados
- Protecção contra repetição de datagramas
- Algoritmos de cifra actuais
- Criação segura de chaves de segurança. Com duração limitada
- Integração de métodos adicionais de cifra / troca de chaves

Cenário de Utilização de IPSec

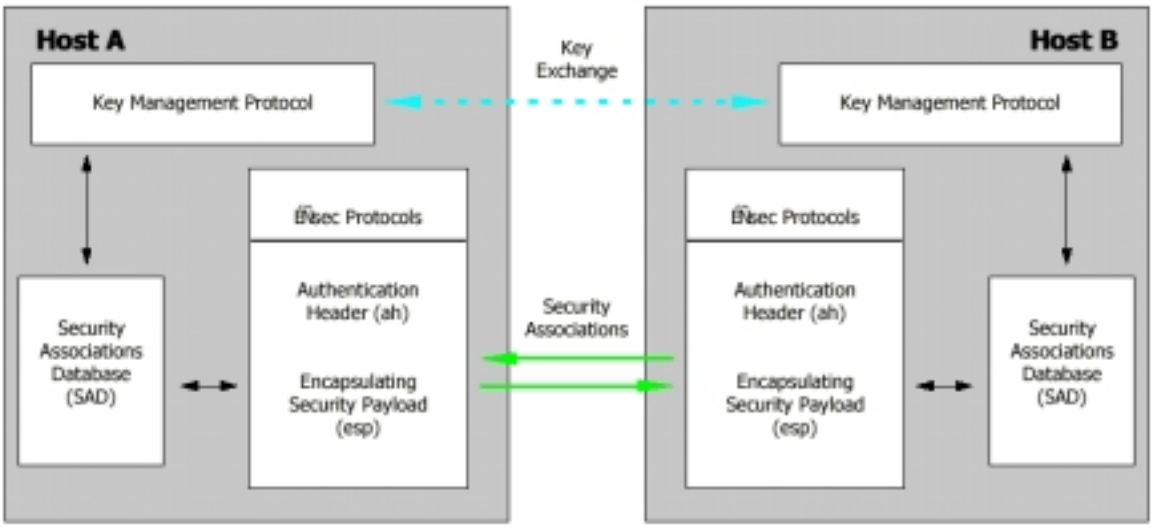


IPSec no IETF

- Grupo de trabalho do IETF →
  - » IP security (IPSec) protocol suite
  - » RFCs 2401, 2412, and 2451
- IPSec
  - » Compatível com IPv4
  - » Obrigatório com IPv6
  - » Transparente para utilizadores
  - » Escalável
- Quando usado,
  - » Protege comunicações, de todas as aplicações e todos os utilizadores
  - » Podem ser construídas VPN (Virtual Private Network) →
    - – Rede privada segura sobre rede pública insegura
    - – Estabelecida e terminada dinamicamente



Arquitectura



Associação de Segurança

- SA – Security Association
  - Ligação lógica unidireccional
  - Funcionamento (exclusivo) em modo túnel ou modo transporte
  - Suporta (apenas) 1 protocolo de segurança (ESP ou AH)

- Identificado por 3 valores
  - SPI, Security Parameter Index → 32 bit
  - Indereço IP de destino (só endereços unicast)
  - Protocolo de segurança → AH ou ESP

» 1 ligação bidireccional → estabelecimento de 2 SAs

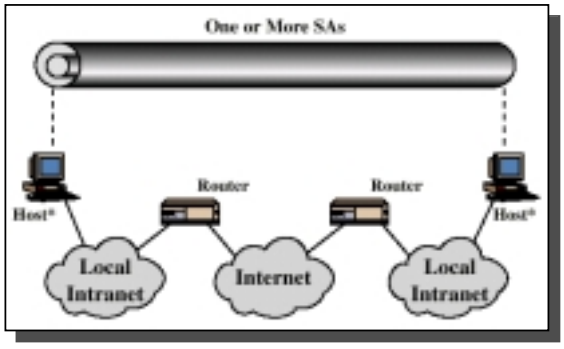
» Bidireccional c/ utilização de AH e ESP → estabelecimento de 4 SAs

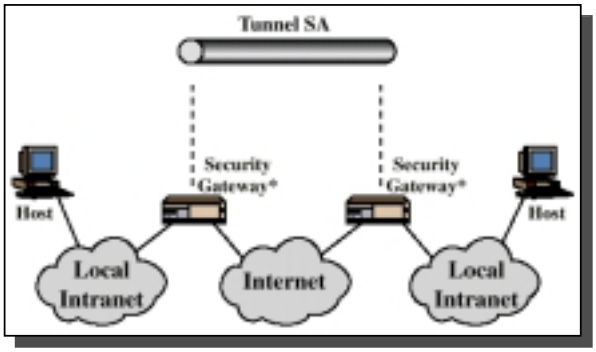
Modos de Funcionamento de uma SA - Transporte, Túnel

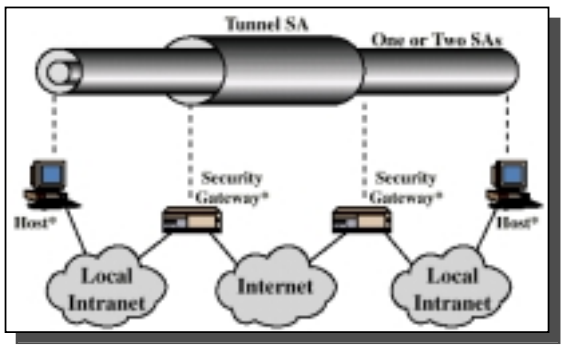
- Modo Transporte
  - » Cabeçalho do datagrama IP é mantido
  - » Usados endereços originais (globais)
  - » Alguns campos do cabeçalho não são autenticados
  - » Usado quando 2 máquinas querem comunicar directamente

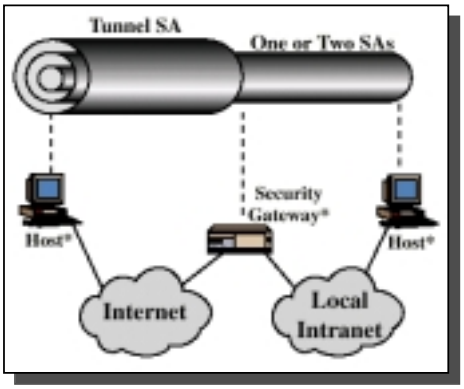
- Modo Túnel
  - » Datagrama original encapsulado dentro do novo pacote
  - » Protege completamente o datagrama original
  - » Datagrama original pode ter endereços internos (ilegais)
  - » Usado por gateways de segurança para implementar VPNs

Associações de Segurança

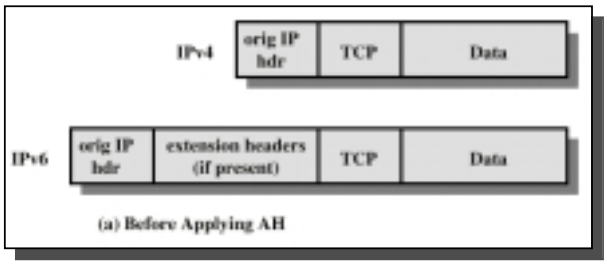


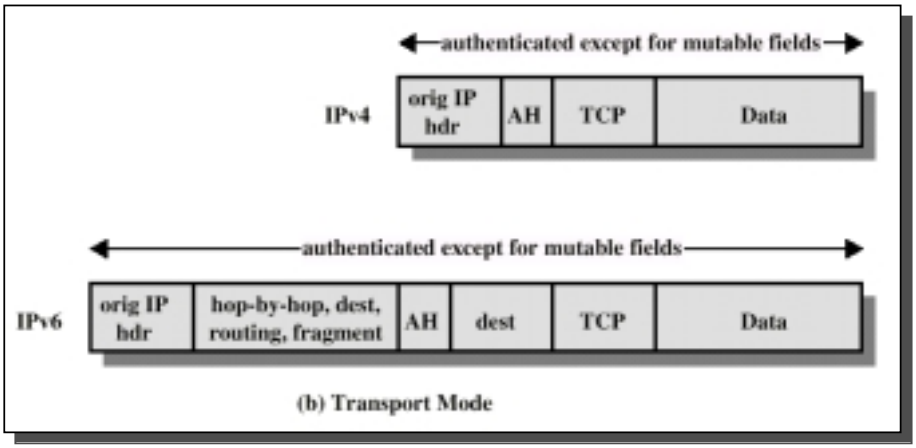




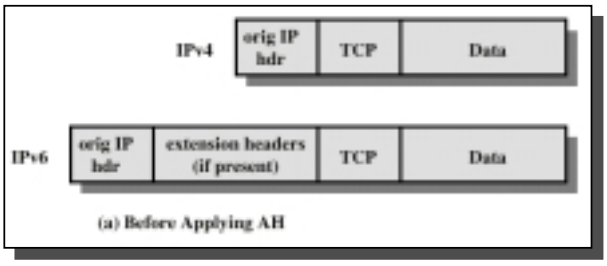


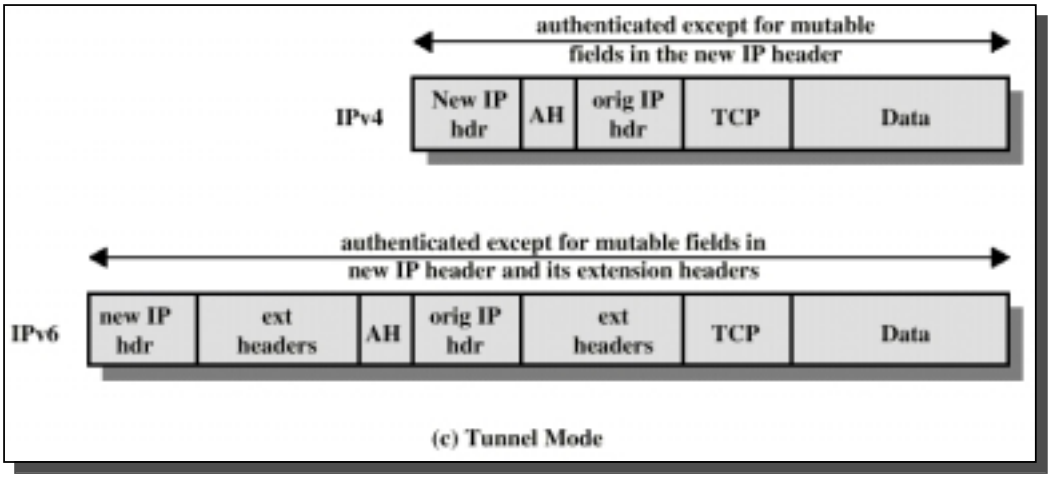
AH, Authentication Header – Modo Transporte



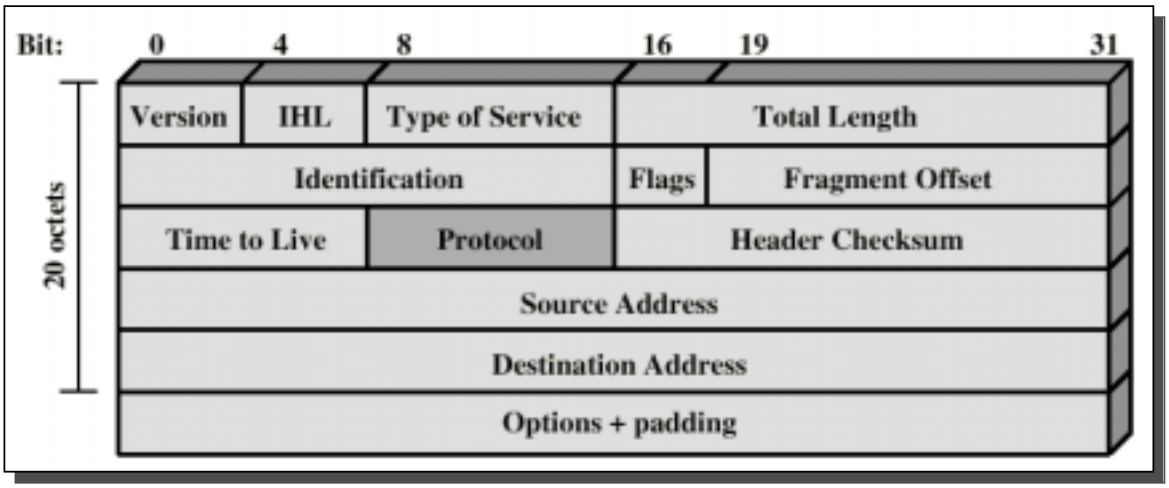


AH, Authentication Header – Modo de Túnel

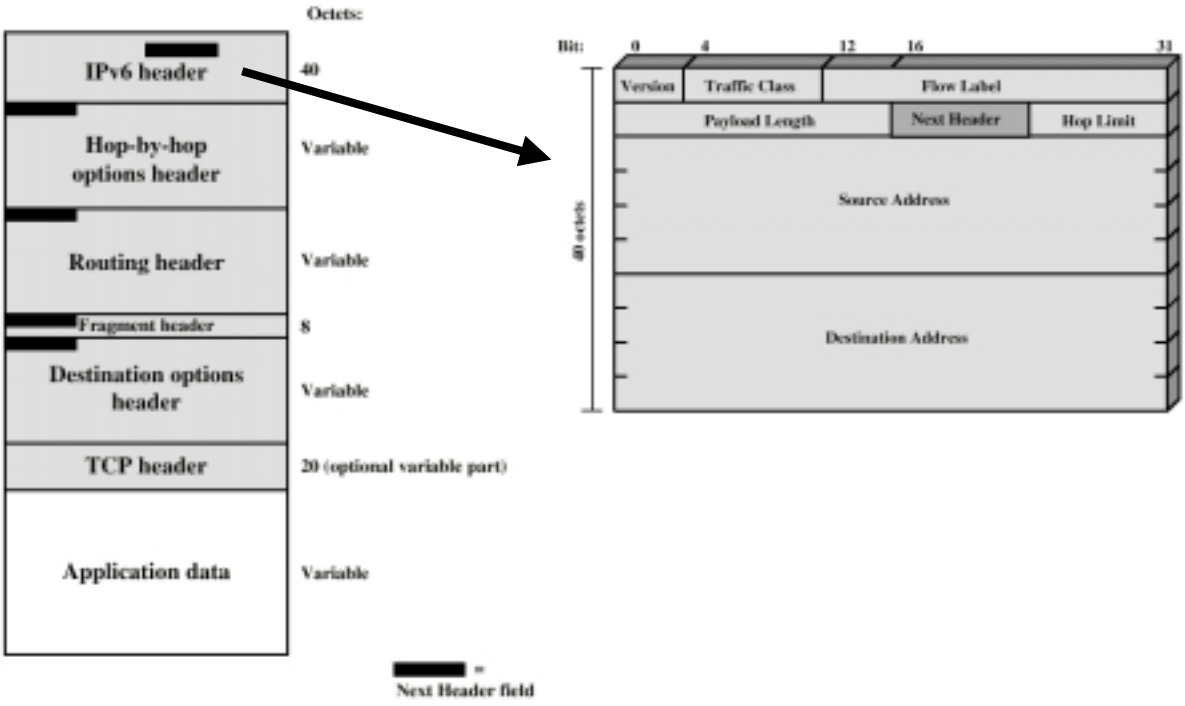




Cabeçalho IPv4

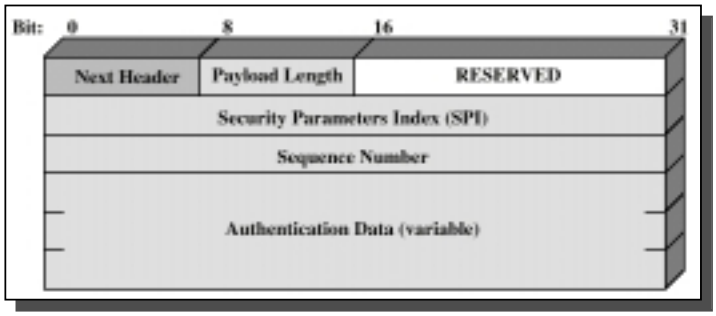


Pacote e Cabeçalho IPv6



Cabeçalho AH

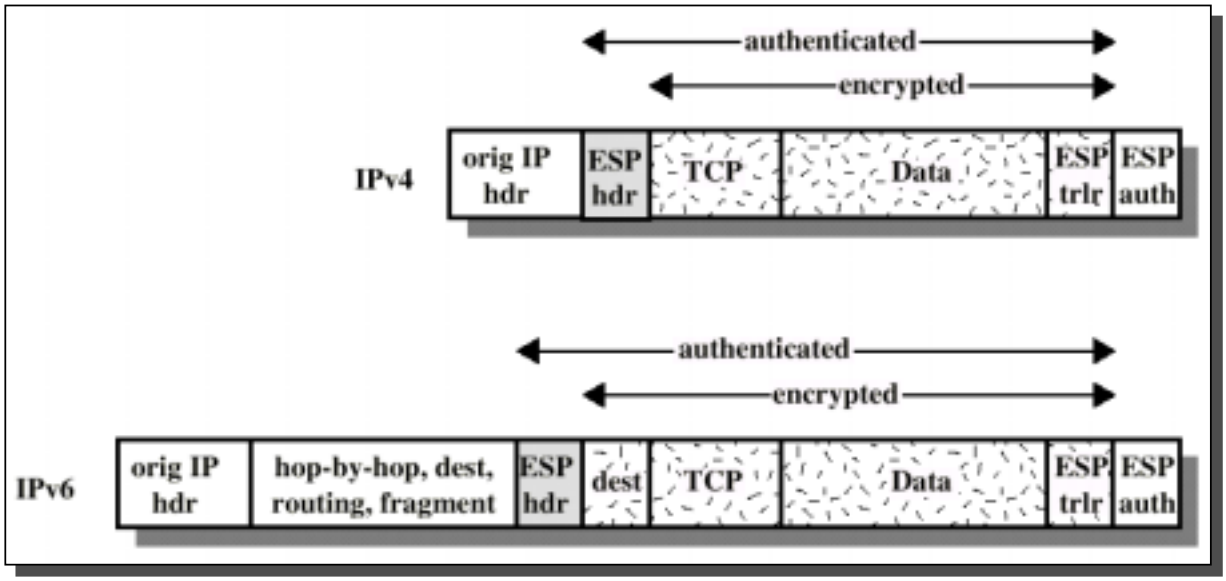
- Protocolo 51
- Campos
  - » Tipo do protocolo seguinte
    - Ex. TCP (6), ESP (50)
  - » Comprimento cabeçalho
    - Palavras 32 bits (-2)
  - » SPI
    - Identificador do grupo de segurança
  - » Número de sequência
  - » Assinatura digital
    - Cálculo do resumo do datagrama
      - Campos variaveis excluídos (ex. TTL)
      - Utilização de uma chave secreta *comum*
      - Algoritmos de hash MD5, SHA
      - RFC2403, RFC2404



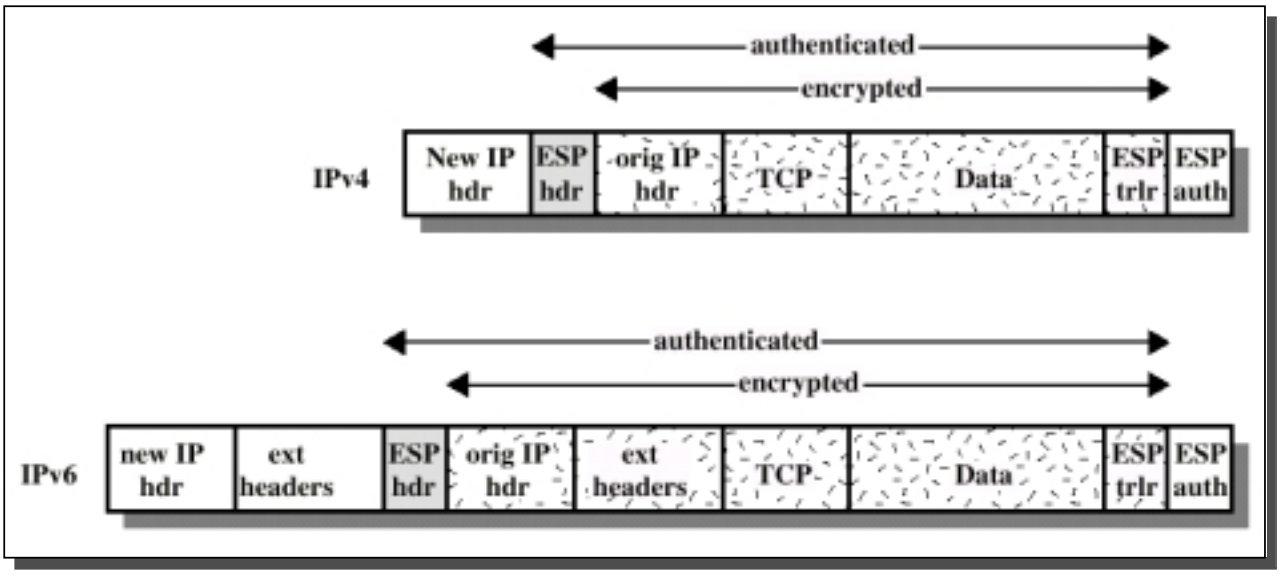
AH, Authentication Header

- Permite
  - » Autenticar o cabeçalho do datagrama
  - » Verificar a integridade dos dados
- Conteúdo do pacote não é cifrado
- Campos variáveis são excluídos do cálculo do resumo
  - » TOS, Flags, TTL, checksum, ...
- 24 octetos adicionados por datagrama

ESP, Encapsulating Security Payload – Modo Transporte

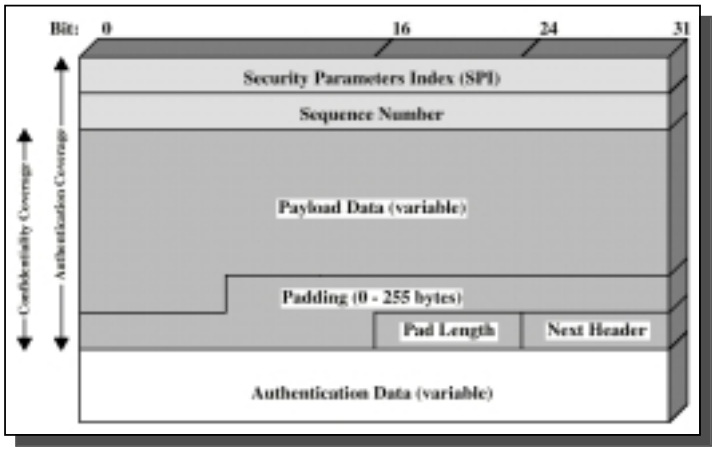


ESP, Encapsulating Security Payload – Modo Túnel



Cabeçalho ESP

- Protocolo 50
- Não cifrado
  - » SPI – Security Parameter Index
    - Grupo de segurança
  - » Número sequência
  - » Assinatura digital (opcional)
    - – Calculada sobre os outros campos do cabeçalho ESP
- Cifrado
  - » Dados
    - – (ex. Cabeçalho TCP + dados)
  - » *Padding*
    - – Para algoritmos de cifra de comprimentos pre determinados
  - » Comprimento do *padding*
    - – Tipo do protocolo seguinte



Encapsulating Security Payload (ESP)

- Cifra o conteúdo do pacote. Segredo (chave) partilhado
  - – Algoritmos de cifra: DES, IDEA, 3DES, etc

- Opcionalmente, permite (como o AH)
  - » Autenticar o cabeçalho do datagrama
  - » Verificar a integridade dos dados
  - » Técnicas de autenticação iguais às do AH

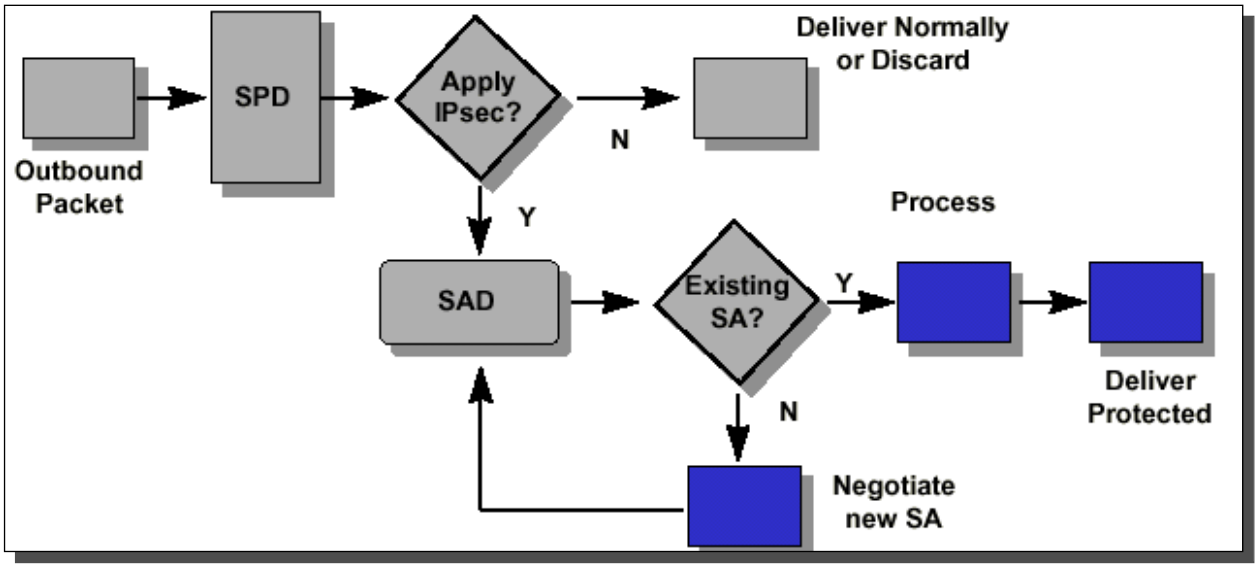
Bases de Dados de SAs

» 2 bases de dados por cada interface IPSec → SPD, SAD

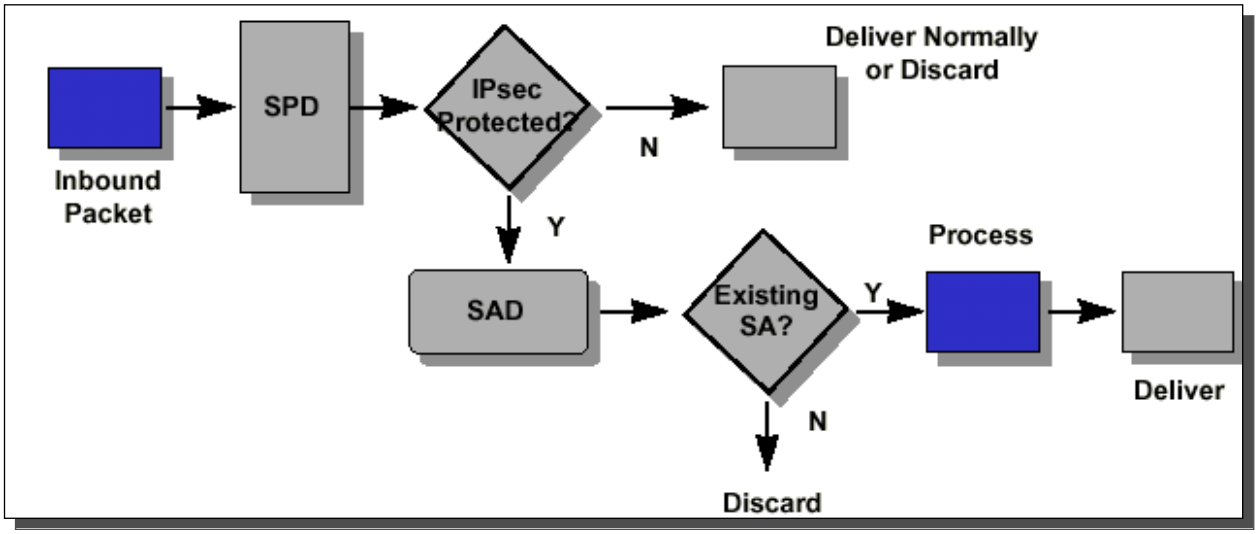
» SPD, Security Policy Database
- Lista ordenada de políticas de segurança. Selecção do tráfego IP a
  1) Eliminar; 2) Processar pelo IPSec; 3) Não processar por IPSec
- Políticas descritas com base em
  - Tipo de endereços: origem, destino
  - Tipo de tráfego: inbound (de entrada na interface), outbound (de saída)
- Políticas segurança ←→ Regras de filtragem (de pacotes) nas firewalls

» SAD, Security Associations Database
- Informação sobre as SAs estabelecidos
  - Protocolo, algoritmos

Processamento de Tráfego Outbound

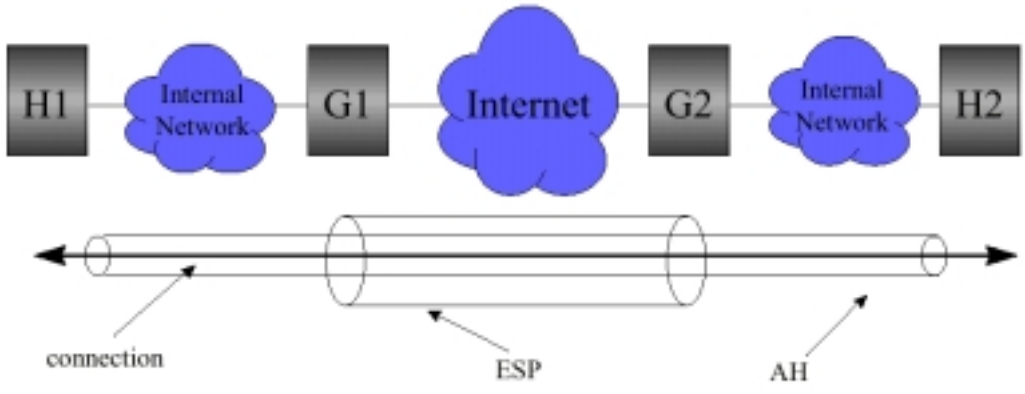


Processamento de Tráfego Inbound



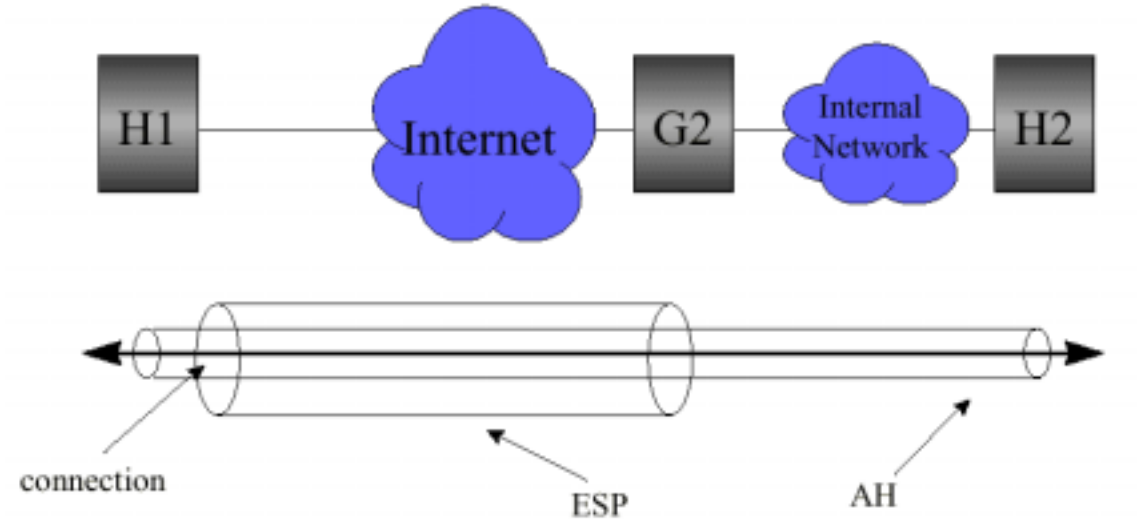
Aplicações Tipo do IPSec – VPN

- VPN c/ segurança extremo a extremo
- ESP protege (cifra) dados sobre a Internet pública
  - Pode ser usado em modo túnel
- AH assegura integridade dos dados extremo a extremo



Aplicações Tipo do IPSec – Guerreiro da Estrada

- Utilizador liga-se à empresa através da Internet pública
- ESP pode ser usado em modo túnel



Combinação de SAs

- Número of SAs cresce rapidamente
  - » Número de ligações
  - » 1 par de SAs para cada ligação
  - » Combinação de protocolos IPSec (AH, ESP, AH sobre ESP)
  - » Modos de funcionamento
  - » Gateway VPN → centenas de SAs

→ Gestão manual de SAs → complexa, impraticavel

→ Necessidade de mecanismos para

  - » Negociar, estabelecer e terminar SAs

Gestão de Chaves IPSec – Requisitos

- Independente dos métodos de cifra
- Independência dos protocolos de troca de chaves
- Autenticação das entidades gestoras de chaves
- Estabelecimento de SAs sobre meios de transporte não seguros
- Utilização eficiente de recursos
- Criação dinâmica de SAs, por
  - » Utilizador e sessão

IKE - Internet Key Exchange

- Protocolo usado para
  - » Estabelecer e terminar SAs
    - – Protocolos, algoritmos e chaves
  - » Autenticar as partes
  - » Gerir as chaves trocadas
- Sobre UDP, Porta 500. RFC 2409

Fases do IKE

» Fase 1 → partes estabelecem 1 canal seguro (SA IKE), em 3 passos
- Negociação de tipos de resumo e algoritmos de cifra a usar
- Troca de chaves públicas (método Diffie-Hellman)
  - Chaves de cifra comuns obtidas a partir de chaves públicas
  - Geração periódica e independente de chaves
- Verificação de identidade do parceiro

» Fase 2 → negociação de SAs genéricas, através do SA IKE

IKE Authentication Methods

Authentication method	How authentication is performed	Advantages	Disadvantages
Pre-shared keys	By creating hashes over exchanged information	• Simple	• Shared secret must be distributed out-of-band prior to IKE negotiations. • Can only use IP address as ID
Digital signatures (RSA or DSS)	By signing hashes created over exchanged information	• Can use IDs other than IP address • Partner certificates need not be available before	• Requires certificate operations (inline or out-of-band)
RSA public key encryption	By creating hashes over nonces encrypted with public keys	• Better security by adding public key operation to DH exchange • Allows ID protection with aggressive mode	• Public keys (certificates) must be available before IKE negotiations • Performance-intensive public key operations
Revised RSA public key encryption	Same as above	• Same as above • Fewer public key operations by using an intermediate secret	• Public keys (certificates) must be available before IKE negotiations

IP Móvel

Sumário

- Motivação
- Transferência de dados
- Encapsulamento
- IPv6

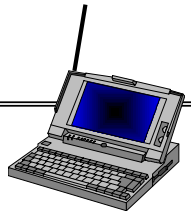
Motivação

- Encaminhamento 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)

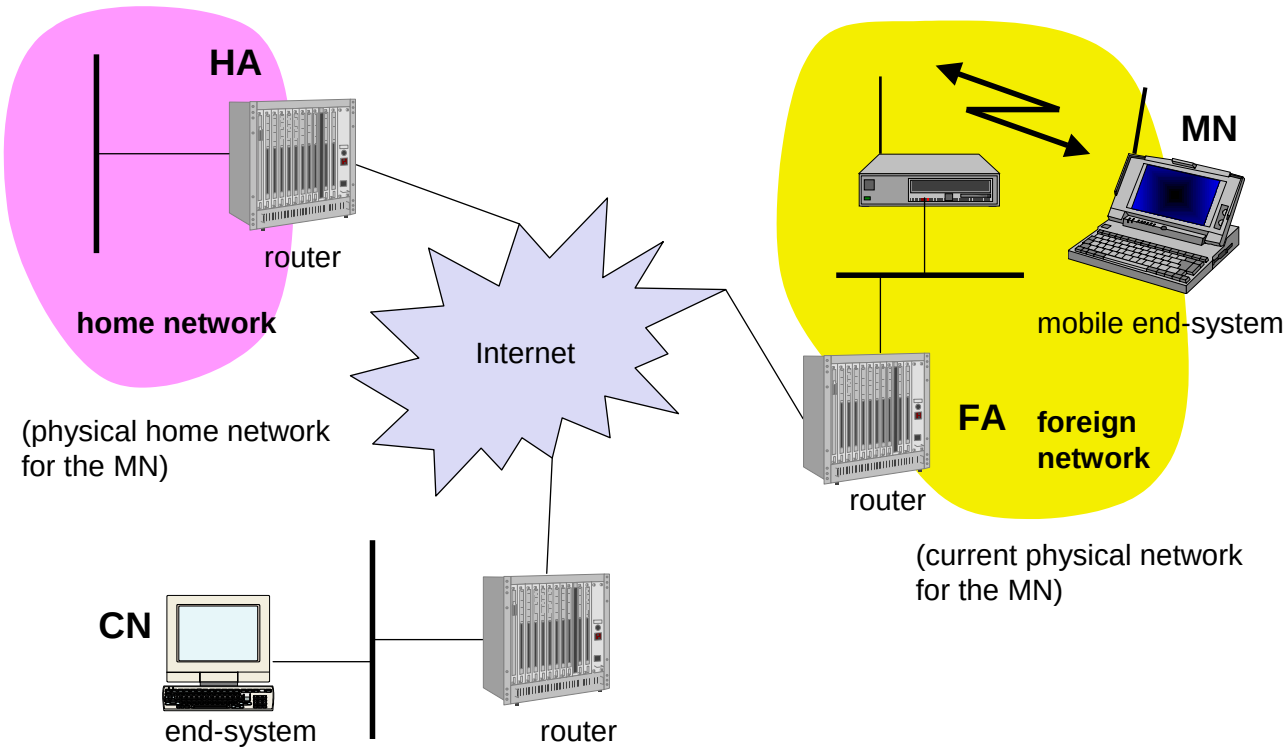
- Transparência
  - Estações móveis devem manter o seu endereço IP
  - Comunicação deve ser retomada depois de quebra da ligação (a mudança de rede)
  - Ponto de ligação à rede fixa pode ser alterado
- Compatibilidade
  - Deve suportar mesmos protocolos de nível 2 que IP
  - Não deve implicar alterações 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

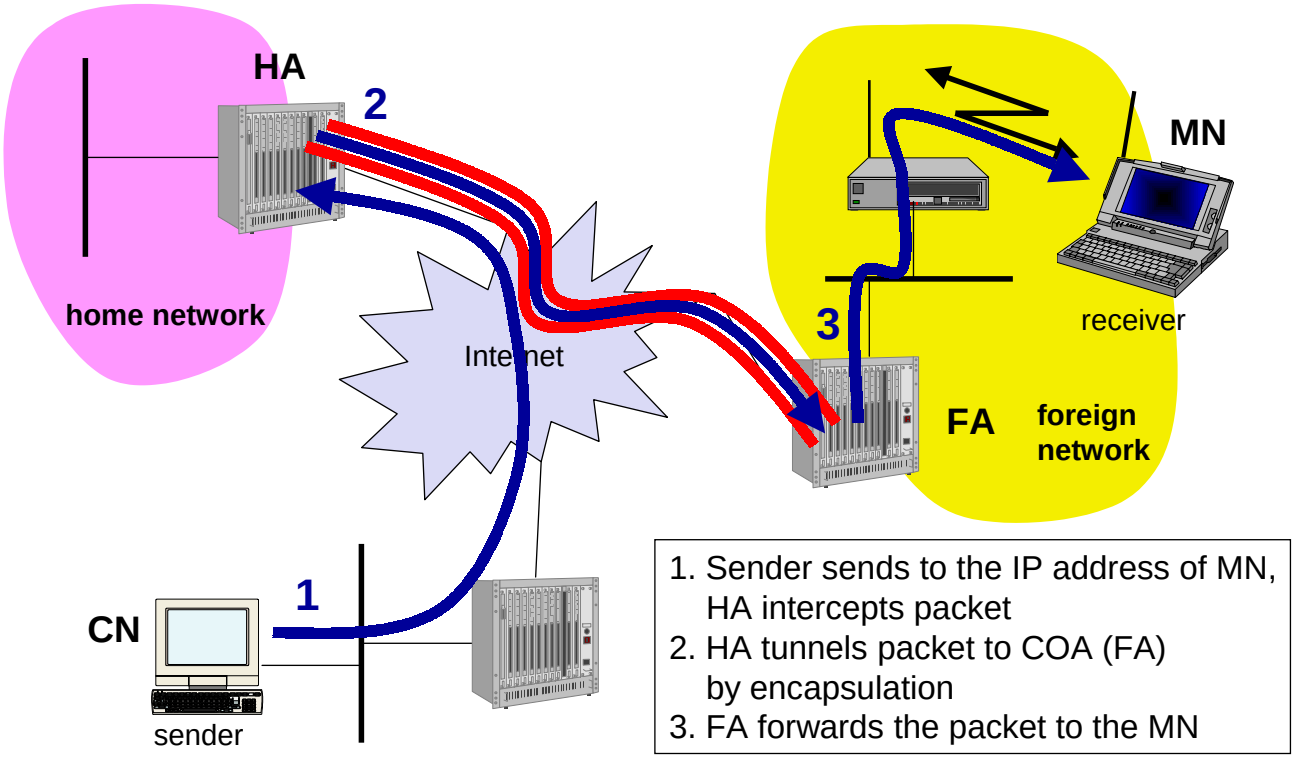


- MN, Mobile Node → estação móvel
  - Máquina móvel. Muda de ponto de ligação
  - Mantém endereço IP
- HA, Home Agent → Agente na rede origem
  - Sistema (router) na rede origem do MN
  - Regista localização do MN. Usa túnel para enviar datagramas IP para COA
- FA, Foreign Agent → Agente na rede visitada
  - 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

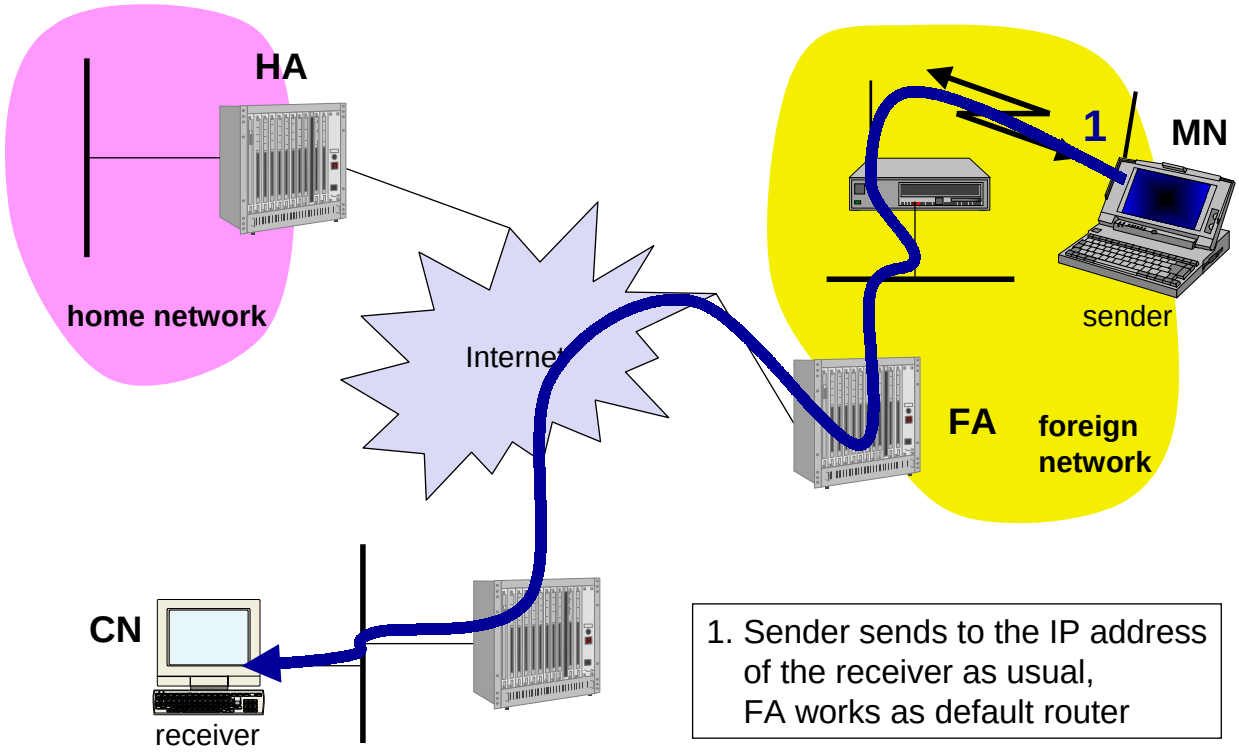


Transferência de Dados para o MN



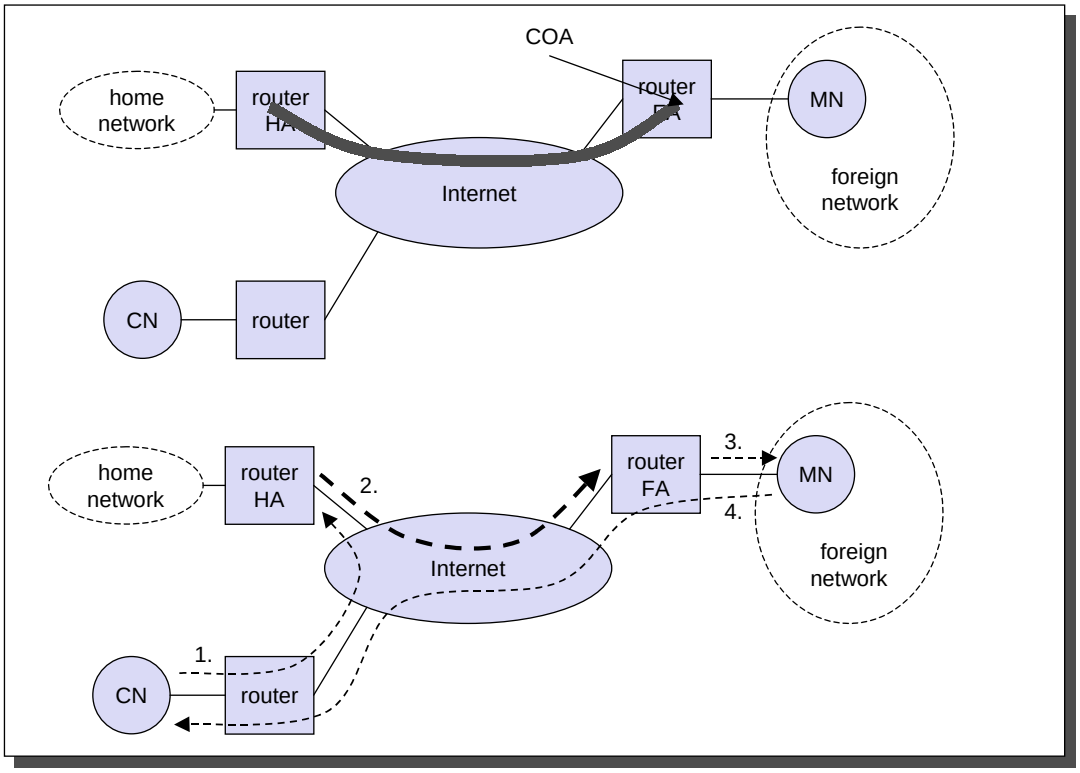
1. Sender sends to the IP address of MN, HA intercepts packet
2. HA tunnels packet to COA (FA) by encapsulation
3. FA forwards the packet to the MN

Transferência de Dados do MN



1. Sender sends to the IP address of the receiver as usual, FA works as default router

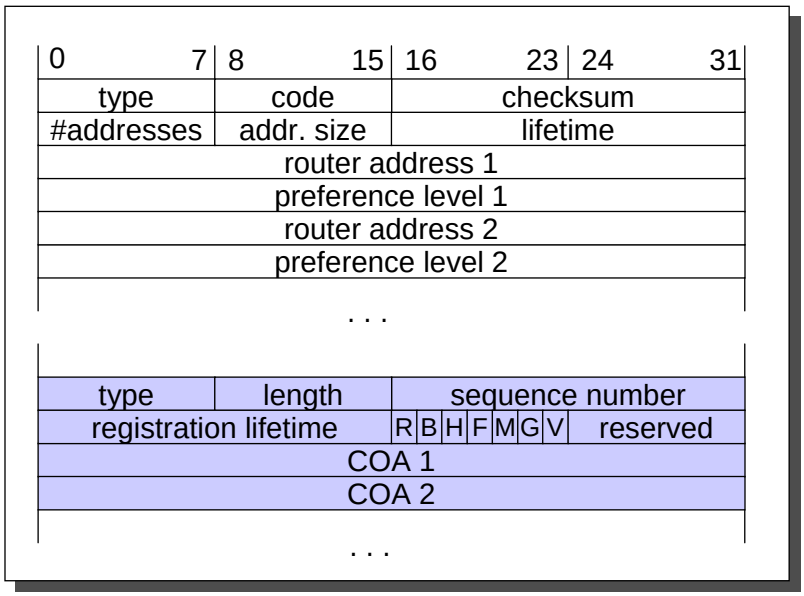
Fases da Mobilidade



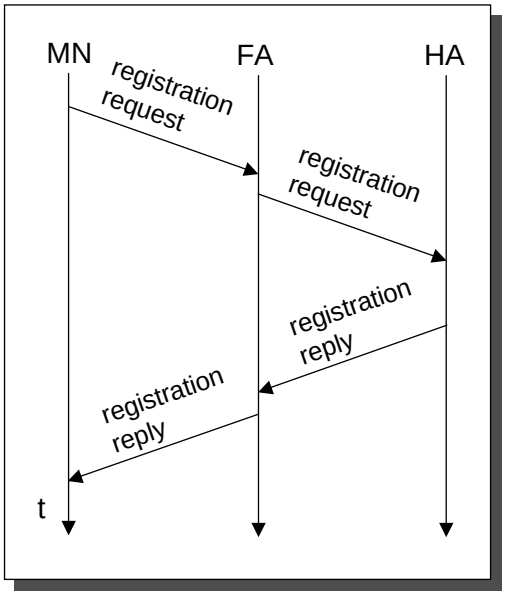
Comunicação com os Agentes

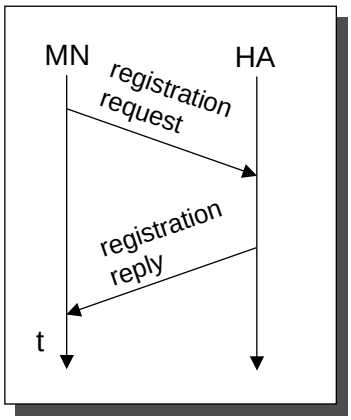
- MN determina rede de acolhimento
  - » HA, FA → geram regularmente mensagens de aviso para suas redes
    Adaptação de mensagens do ICMP Router Advertisment Protocol (RFC 1256)
  - » MN escuta mensagens; determina rede de acolhimento
    - – A sua, ou
    - – Uma rede visitada → conhecimento de COA
- 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

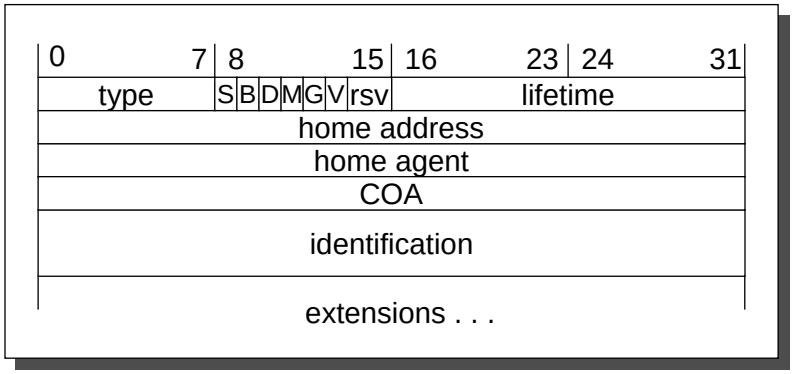


Registo do MN no Home Agent

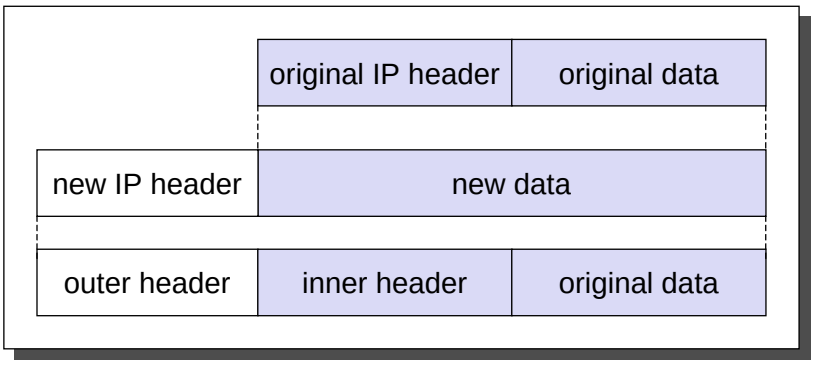




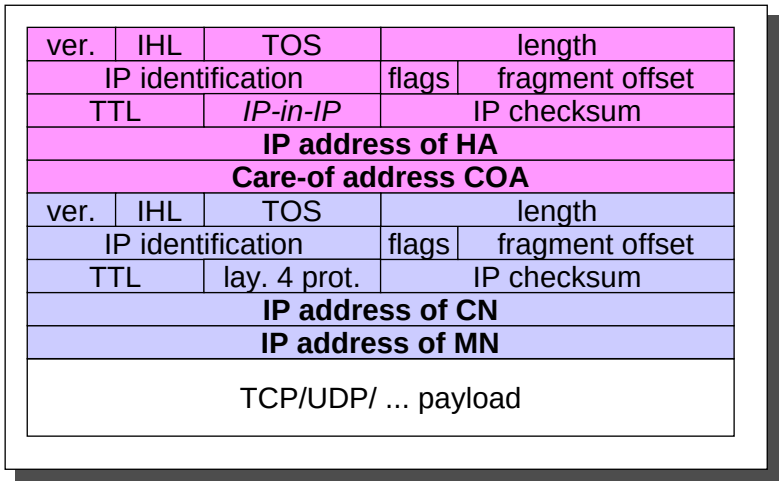
Mensagem de Pedido de Registo



Encapsulamento, Tuneis



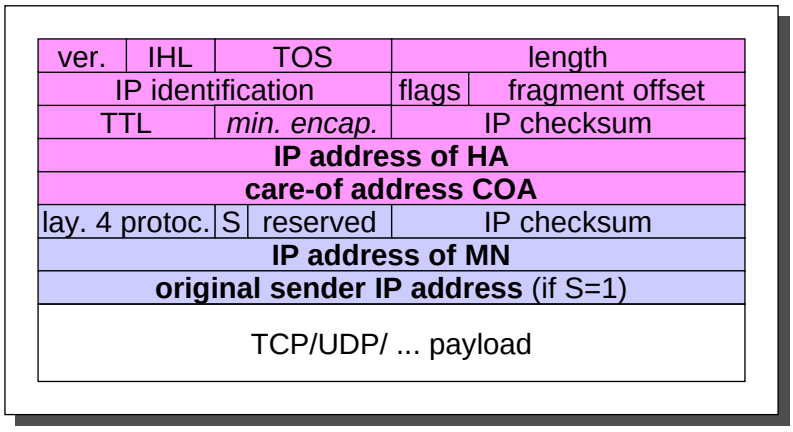
IP em IP (obrigatório)



Túnel entre HA e COA

Encapsulamento Mínimo (Opcional)

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



IP Móvel e IPv6

- IP desenvolvido para IPv4. IPv6 simplifica protocolos
  - » Segurança suportada nativamente IPv6
  - » COA pode ser atribuído por auto-configuração
  - » Qualquer router pode ser um FA ← routers enviam mensagens de aviso
  - » Suporte de “soft-handover”. Sem perda de pacotes
    - – Quando MN muda de rede visitada → avisa router antigo do seu novo COA
    - – Router antigo cria túnel para novo COA. Encaminha todos os pacotes recebidos