GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

Redes de Computadores 2
EEL 879

Parte VI
IPv6

Luís Henrique M. K. Costa
luish@gta.ufrj.br

Universidade Federal do Rio de Janeiro -PEE/COPPE
P.O. Box 68504 - CEP 21945-970 - Rio de Janeiro - RJ
Brasil - http://www.gta.ufrj.br

Porque do IPv6?

- **Esgotamento dos endereços IPv4**
  - IPv4: apenas 4,3 bilhões de endereços
- **Cabeçalho simplificado**
  - Processamento mais eficiente nos roteadores
- **Melhor suporte a opções**
- **Segurança**

Requisitos do IPv6 (RFC 1752)

- Serviço de datagrama não confiável (~IPv4)
- Suporte unicast e multicast
- Endereçamento adequado para além de um futuro imediato
- Compatibilidade com o IPv4 (não renumerar redes)
- Suporte para autenticação e criptografia
- Não fazer suposições sobre a topologia física
- Não fazer nada que afete o desempenho dos roteadores
- Protocolo extensível e capaz de evoluir
- Suporte para estações móveis, redes e interconexão de redes
- Permitir interconexões de redes privadas em cima da infra da Internet

Esgotamento dos Endereços IPv4

- **Fatores de pressão**
  - Número de redes
  - Dispositivos móveis
  - Internet das coisas
- **Fatores de alívio**
  - CIDR, melhor gerenciamento de endereços Classe A
  - *Network Address Translation* (NAT)
- **Outro aspecto: tamanho das tabelas**
  - IPv6 em si, não reduz
  - Alocação mais cuidadosa >> maior agregação

GTA/UFRJ

IPv4 x IPv6: Endereços

- **IPv4 (1981)**
  - Tamanho: 32 bits
  - Notação: 192.168.27.134
    (4 decimais separados por .)
  - Baseado em classes
- **IPv6 (1999)**
  - Tamanho: 128 bits
  - Notação: 3FFE:F200:234:AB00:123:4567:8901:FEFE
    (8 grupos de 4 hexadecimais, separados por :)
  - Sem classes

GTA/UFRJ

Quantidade de Endereços

- **IPv4**
  - 2^{32} endereços = 4.294.967.296 (~4,2 bilhões)
- **IPv6**
  - 2^{128} endereços = 3.40282×10^{38}
  - = 340.282.366.920.938.463.463.374.607.431.768.211.456

GTA/UFRJ

Tipos de Comunicação no IPv6

- IPv4
  - Unicast
  - Multicast
  - Broadcast
- IPv6
  - Unicast
  - Multicast
  - Anycast

GTA/UFRJ

Tamanho da Unidade de Transmissão

- MTU – Maximum Transfer Unit
  - Máxima quantidade de dados transportados em um quadro da camada 2
  - Exemplos
    - Ethernet (IEEE 802.3): MTU = 1500 Bytes (tamanho da carga útil)
- No IPv6, há uma MTU mínima que deve ser suportada pela camada 2
  - 1280 Bytes

GTA/UFRJ

Tempo de Vida do Endereço IPv6

- Endereços IPv6 não são “dados, mas emprestados”
- Tempo de vida associado a cada endereço
  - Quando termina, o endereço torna-se inválido e pode ser reutilizado por outra interface
  - Tempo de vida padrão: 30 dias
  - Endereços local-ao-enlace possuem tempo de vida ilimitado
- Permite a renumeração dos endereços
  - Desejável que se faça de forma suave, para não quebrar conexões em andamento

GTA/UFRJ

Tempo de Vida do Endereço IPv6

- Mecanismo de obsolescência
  - Vários endereços IPv6 podem ser associados a uma interface...
  - Escolha do endereço a utilizar: baseada no **estado** do endereço
- **Estados** do endereço com respeito ao tempo de vida
  - Preferível
    - Endereço pode ser utilizado sem restrições
  - Depreciado
    - Não deve ser usado como endereço fonte para novas comunicações
    - Mas pode ser endereço fonte em comunicações em andamento
  - Inválido
- Na atribuição de um endereço, são definidos o tempo de vida (validade) e o tempo de duração preferencial

Endereços IPv6: Representação

2033:0000:0123:00FD:000A:0000:0000:0C67

⬇

Retirada de zeros no início de palavras

⬇

2033:0:123:FD:A:0:0:C67

⬇

Retirada de blocos “todos-zeros” (compressão)

⬇

2033:0:123:FD:A::C67

- Compressão pela omissão de zeros
  - Uma única vez: seria impossível saber quantas palavras em zero, senão

Estrutura do Endereço IPv6

8145:010C:0000:0000:	1100:1A06:8800:0001
parte de rede	parte de estação

- Parte de Rede
  - **64 bits MSB**
  - **Configurável (sub-campos)**
- Parte de Estação
  - **64 bits LSB**
  - **Fixa**
  - Calculada pela própria estação

Estrutura do Endereço IPv6

8 MSB do endereço IPv6:
Format Prefix (FP)

- Definem o tipo de endereço

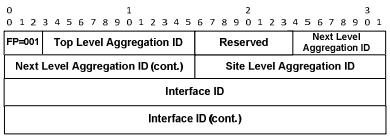
Bits FP	Uso	Número de endereços	Faixa
0000 0000	Reservados	2^{120}	0000::/8
0000 0001	Não atribuídos	2^{120}	0100::/8
0000 001	NSAPs	2^{121}	0200::/7
0000 01	Não atribuídos	2^{122}	0400::/6
0000 1	Não atribuídos	2^{123}	0800::/5
0001	Não atribuídos	2^{124}	1000::/4
001	Endereços Unicast Globais	2^{125}	2000::/3
01	Não atribuídos	2^{126}	4000::/2
10	Não atribuídos	2^{126}	8000::/2
110	Não atribuídos	2^{125}	C000::/3
1110	Não atribuídos	2^{124}	E0000::/4
1111 0	Não atribuídos	2^{123}	F0000::/5
1111 10	Não atribuídos	2^{122}	F800::/6
1111 110	Não atribuídos	2^{121}	FC00::/7
1111 1110 0	Não atribuídos	2^{119}	FE00::/9
1111 1110 10	Endereços unicast locais ao enlace	2^{118}	FE80::/10
1111 1110 11	Endereços unicast locais ao site	2^{118}	FEC0::/10
1111 1111	Endereços multicast	2^{120}	FF00::/8

Tipos de Endereços IPv6

- Unicast Global
- Unicast Local ao Enlace
- Unicast Local ao Site
- Multicast
- NSAP (Network Service Access Point) (ISO)
  - (em desuso)
- IPX (Novell)
  - (em desuso)

GTA/UFRJ

Endereço IPv6 Unicast Global



- Top Level Aggregation ID (13 bits)
- Reserved (8bits)
- Next Level Aggregation ID (24 bits)
- Site Level Aggregation ID (16 bits)
- Interface ID (64 LSB)

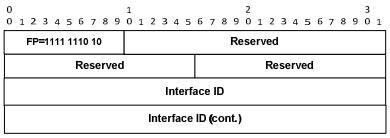
GTA/UFRJ

Endereço IPv6 Unicast Global (cont.)

- Topologia Pública
  - Top Level Aggregation ID (13 bits)
    - Identificadores para grandes operadores de rede, tipicamente, provedores da DFZ (*default-free zone*)
  - Reserved (8bits)
    - Reserva, permite aumentar o número de TLAs ou de NLAs
  - Next Level Aggregation ID (24 bits)
    - Identificador do site (ou domínio)
- Topologia do Site
  - Site Level Aggregation ID (16 bits)
    - Endereço de sub-rede
    - Permite a hierarquização do site
  - Interface ID (64 bits)
    - Endereço da Interface

GTA/UFRJ

Endereço IPv6 Unicast Local ao Enlace



- Não-roteável
  - Comunicação entre máquinas no mesmo enlace apenas
- Faixa
  - FE80::/10
- Equivalente IPv4
  - 169.254.0.0/16

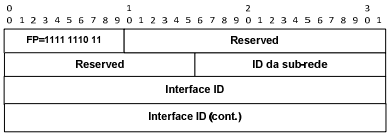
GTA/UFRJ

Endereço IPv6 Unicast Local ao Enlace (cont.)

- Utilização do endereço *local-ao-enlace*
  - Protocolo de configuração de endereço global (subst. do ARP)
  - Protocolo de descoberta de vizinhos (*neighbor discovery*)
  - Protocolo de descoberta de roteadores (*router discovery*)
- Devem ser únicos no enlace
  - Garantia: Protocolo de detecção de endereço duplicado
- Podem repetir em enlace ou redes diferentes
- Normalmente não são usados em aplicações clássicas
  - Alcance limitado ao enlace

GTA/UFRJ

Endereço IPv6 Unicast Local ao Site



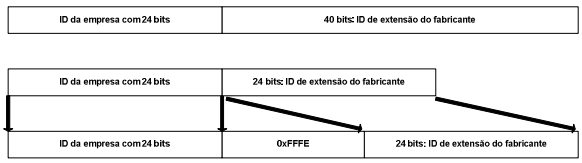
- Escopo
  - Rede de um site, roteadores de borda devem filtrá-los
- Faixa
  - FEC0::/10
- Equivalente IPv4
  - 10.0.0.0/8

Endereço IPv6 Unicast Local ao Site (cont.)

- Utilização
  - Rede de um site que ainda não está conectado à Internet
- Dificuldades de utilização
  - Definição exata de um site
  - Plano de endereçamento SLA ID é o mesmo para os endereços globais?
  - Como definir se um parceiro está no mesmo site
  - Que endereço o servidor DNS deve informar
- Vantagem
  - Não há a necessidade de renumeração quando se troca o provedor de acesso à Internet

Endereços IPv6 Unicast: Interface ID

- Endereços MAC
  - 48 bits (IEEE 802) ou 64 bits (IEEE EUI-64)
- Interface ID no IPv6: 64 bits



Endereços Unicast IPv6 Especiais

- Endereço indeterminado
  - 0:0:0:0:0:0:0:0 (ou ::)
    - Utilizado unicamente durante inicialização da máquina
- Endereço de loopback
  - 0:0:0:0: 0:0:0:1 (ou ::1)

GTA/UFRJ

Endereços Unicast IPv6 Especiais

- Endereços "IPv4-mapped IPv6"
  - 80 '0's + FF + endereço IPv4 (32 bits)
  - Exemplos
    - ::FFFF:129.144.52.38 (forma IPv6-IPv4 decimal)
    - ::FFFF:8190:3426 (forma IPv6-comprimida)
- Utilização
  - Dupla pilha:
    - Máquina IPv6 pode conversar com máquinas IPv6 ou IPv4
    - Na transmissão:
      - Se endereço de destino IPv4 mapeado em IPv6, pacote emitido na pilha IPv4
    - Na recepção:
      - Um pacote IPv4 recebido na pilha IPv4 é apresentado à aplicação na forma de um pacote IPv6 com endereço de destino IPv4 mapeado em IPv6

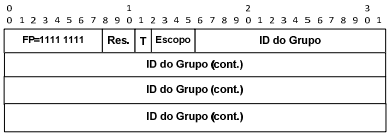
GTA/UFRJ

Endereços Unicast IPv6 Especiais

- Endereços "Compatíveis IPv4"
  - 96 '0's + endereço IPv4 (32 bits)
  - Exemplos
    - ::129.144.52.38 (forma IPv6-IPv4 decimal)
    - ::8190:3426 (forma IPv6-comprimida)
- Utilização
  - Túnel IPv6/IPv4 automático
    - Pacote transmitido a ::a.b.c.d é encapsulado em um pacote IPv4
    - No destino, o pacote IPv6 é desencapsulado e entregue à aplicação
  - Uso generalizado é desaconselhável
    - Gestão de uma rede IPv4 com endereços acrescidos de 96 '0's…
    - Melhor opção: tunelamento na Entrada/Saída do Site

GTA/UFRJ

Endereço IPv6 Multicast



- Flags: Reserved (3 bits) + T (1 bit)
  - T = 0: endereço permanente
  - T = 1: endereço temporário
- Escopo (4 bits)
  - Alcance do tráfego
- ID do Grupo (112 bits)

Endereço IPv6 Multicast

- Faixa
  - FF00::/8
- Exemplos
  - FF02::1
    - "All-nodes": equivalente ao broadcast IPv4
  - FF02::2
    - "All-routers": equivalente ao broadcast IPv4

Endereço IPv6 Multicast: Escopo

- Interface-local
- Link-local
- Subnet-local
- Site-local
- Admin-local
- Organization-local
- Global

- Substitui a limitação do escopo através do campo TTL no IPv4

Endereço IPv6 Multicast: Escopo

- Exemplos
  - FF02::101 : todos os servidores NTP (*Network Time Protocol*) no mesmo enlace que o emissor
  - FF05::101 : todos os servidores NTP no mesmo site que o emissor
  - FF0E::101 : todos os servidores NTP na Internet

GTA/UFRJ

Endereços Multicast Especiais IPv6

- **All-nodes multicast groups**
  - Interface-local all-nodes group (FF01::1)
  - Link-local all-nodes group (FF02::1)
- **All-routers multicast groups**
  - Interface-local all-routers group (FF01::2)
  - Link-local all-routers group (FF02::2)
  - Site-local all-routers group (FF05::2)
- **Solicited-node multicast group**

GTA/UFRJ

Endereços Multicast Nó-Solicitado

- Formação
  - Prefixo FF02::1:FF00/104 + 24 LSB do endereço unicast ou anycast do nó
- Utilização
  - A máquina constrói endereços multicast nó solicitado a partir de seus endereços unicast e/ou anycast
  - Outra máquina que conheça o endereço IPv6 da máquina, mas não seu endereço MAC, pode utilizar o endereço nó solicitado para se comunicar (~ARP do IPv4)
- Utilidade
  - Protocolo de detecção de endereços duplicados e de descoberta de vizinhos
  - Mais eficiente que 255.255.255.255 no IPv4

GTA/UFRJ

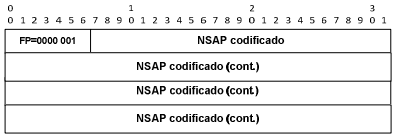
Exemplo de Formação do Endereço Multicast Nó-Solicitado

Endereço alvo (notação comprimida):
`fe80::3ab:ff:fe54:5a9f`
Endereço alvo (últimos 24 bits)
`fe80:0000:0000:0000:03ab:00ff:fe`**`54:5a9f`**

Prefixo Solicited-node Multicast Address (notação comprimida)
`ff02::1:ff00:0/104`
Prefixo Solicited-node Multicast Address (primeiros 104 bits)
`ff02:0000:0000:0000:0000:0001:ff``00:0000/104`

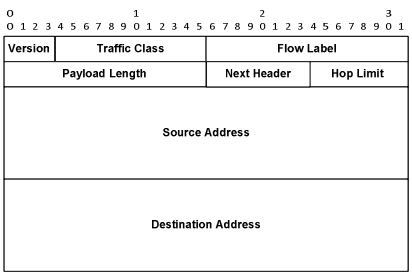
Resultado:
`ff02:0000:0000:0000:0000:0001:ff54:5a9f`
Resultado (notação comprimida):
`ff02::1:ff54:5a9f`

Endereço IPv6 NSAP



- Network Service Access Point (NSAP)
  - Formato de endereço generalizado, definido pela ISO

IPv6 - O Cabeçalho



- Todos os campos são fixos

Cabeçalho IPv4 x IPv6

- Campos **eliminados** em relação ao IPv4
  - IHL (4bits)
    - Cabeçalho IPv6 tem tamanho fixo
  - Identification, Flags e Fragment Offset (16, 8 e 8 bits)
    - No IPv6, o roteador não faz fragmentação
  - Header Checksum (4bits)
    - O IPv6 não faz controle de erros, deixado para outras camadas
- Campos **acrescidos** em relação ao IPv4
  - Flow Label (16 bits)
    - Identificação de fluxo

Cabeçalho IPv4 x IPv6

- Campos **modificados** em relação ao IPv4
  - ToS >> Traffic Class
  - Total Length >> Payload Length
    - Tamanho da carga útil, sem o cabeçalho do IPv6 (40 bytes)
  - TTL >> Hop Limit
  - Protocol >> Next Header
    - Indica o tipo de protocolo transportado, ***ou***
    - Campo opcional (substitui as Opções do IP)

Campos do Cabeçalho IP

- Versão (4bits)
  - Versão atual = 6
- Traffic Class (8 bits)
  - Differentiated Services, como no IPv4 (RFC 2474)

Campos do Cabeçalho IP

- Flow Label (16 bits)
  - Número único escolhido pela fonte
  - Utilidade
    - Qualidade de Serviço (QoS): uso pelo RSVP (*ReSource reserVation Protocol*)
    - Tratamento específico do fluxo: escolha de uma rota
- Identificação de fluxo no IPv4
  - Fluxo geralmente identificado por uma tupla
    - (@-orig; @-dest; #porta orig; #porta dest; protocolo)
- No IPv6: maior eficiência
  - Um campo específico
  - Se utilizada confidencialidade, até o número de porta de pode estar escondido

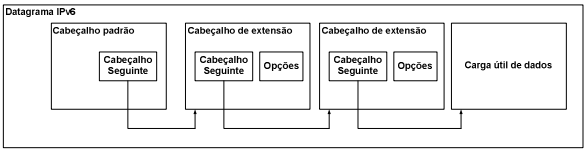
Campos do Cabeçalho IP

- Payload Length (16 bits)
  - Tamanho da carga útil, sem considerar o tamanho do cabeçalho
  - Se houver cabeçalhos de extensão, são contados no Payload Length
  - Para pacotes de tamanho maior que 65.535 bytes
    - Payload Length = 0
    - Opção "jumbograma" é utilizada
- Next Header (8 bits)
  - Protocolo de nível superior (ICMP, UDP, TCP, ...)
  - **Ou** identificação do próximo cabeçalho de extensão

Campos do Cabeçalho IP

- Hop Limit (8 bits)
  - Número de saltos
    - Deixa de significar tempo em segundos, como inicialmente proposto no IPv4
- Source Address e Destination Adress (128 bits cada)
  - Endereços IP de Origem e de Destino do pacote

Cabeçalhos de Extensão



- Tratamento de opções no IPv6
  - Apenas as extensões "hop-by-hop" são tratadas por todos os roteadores
  - Todas as outras são tratadas apenas no destino em questão
  - Maior eficiência que no IPv4, onde pacotes com opções sempre seguem pelo *slow-path* dos roteadores

Cabeçalho de Extensão: Considerações

- Comprimento: múltiplo de 8 bytes
- Início: campo Next Header (1 byte)
  - ("Cabeçalho Seguinte")
- Se extensão de tamanho variável
  - Próximo byte: comprimento da extensão, em palavras de 8 bytes, sem contar a primeira palavra
    - (Uma extensão de 16 bytes possui comprimento "1"

Cabeçalho de Extensão: Considerações

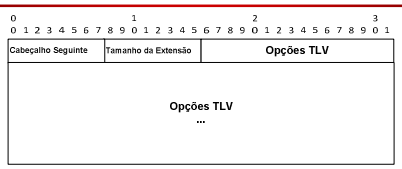
- Ordem recomendada (RFC 2460)
  - Salto-a-salto (sempre deve ser a primeira extensão)
  - Destino (será também tratada pelos roteadores impostos pelo roteamento pela fonte)
  - Roteamento pela fonte
  - Fragmentação
  - Autenticação
  - Destino (será tratada apenas pelo equipamento destino final)

Valores de "Cabeçalho Seguinte"

Valor	Extensão
0	Opções salto-a-salto
43	Roteamento pela fonte
44	Fragmentação
50	Encapsulamento seguro de payload
51	Autenticação
59	Fim de cabeçalho sem payload
60	Opções de destino

Valor	Protocolo
6	TCP
17	UDP
41	IPv6
58	ICMPv6

Opções no Cabeçalho de Extensão



- Cabeçalho seguinte: indica o próximo cabeçalho de extensão
- Tamanho da extensão: inteiro em unidades de 8 bytes
- Opções TLV
  - Extensão salto-a-salto (Tipo 0)
    - Opções que são aplicadas a cada salto do caminho
  - Extensão de destino (Tipo 60)
    - Opções que são aplicadas apenas no destino, ou no próximo salto, no caso de roteamento pela origem

Opções Salto-a-salto: Considerações

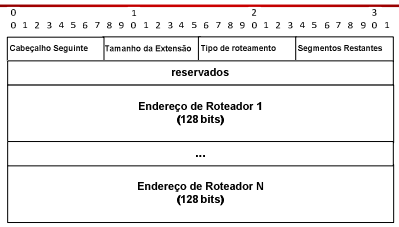
- São Opções TLV
- Codificação do Tipo da Opção
  - 2 MSB: tratamento de uma opção desconhecida pelo roteador
    - 00: o roteador ignora a opção
    - 01: o roteador descarta o pacote
    - 10: o roteador descarta o pacote e retorna uma mensagem ICMPv6 de "inalcançabilidade"
    - 11: o roteador descarta o pacote e retorna uma mensagem ICMPv6 de "inalcançabilidade" se o destino não for multicast
  - Próximo bit
    - =1: o roteador pode modificar o conteúdo do campo de opções
    - =0: o roteador não pode modificar o conteúdo do campo de opções

Tipos de Opções Salto-a-salto

- Pad1 (tipo 0): introduz um byte de enchimento
- PadN (tipo 1): introduz dois ou mais bytes de enchimento (de acordo com campo tamanho da extensão)
- Jumbograma (tipo 194 ou 0xC2):
  - Permite pacotes maiores que 65535 bytes
  - Usada geralmente em conexões da alta velocidade entre duas máquinas
  - Neste caso, o tamanho da carga útil no cabeçalho principal vale zero
  - Obs: inicia com "11": o roteador informa à fonte se não suportar o jumbograma
- Router Alert (tipo 5)
  - Solicitação ao roteador de examinar o pacote
  - Normalmente, a tarefa do roteador é encaminhar o pacote o mais rápido possível
  - Utilização
    - Protocolo de reserva de recursos RSVP
    - Protocolo de gerenciamento de grupo MLD

GTA/UFRJ

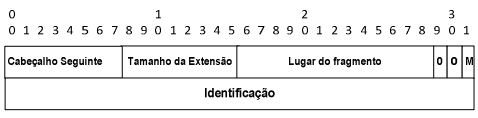
Extensão de Roteamento pela Fonte



- Cabeçalho de Extensão tipo 43
  - Tipo = 0: roteamento pela fonte, semelhante ao *loose source routing* do IPv4
    - (A utilização do *strict source routing* tornou-se rara)
  - Conteúdo
    - Número de segmentos (saltos) restantes até o destino
    - Lista dos próximos roteadores até o destino

GTA/UFRJ

Extensão de Fragmentação



- Fragmentação: ineficiente no IPv4
  - Mecanismos de descoberta de MTU servem para evitá-la
  - Porém, algumas aplicações supõem que a rede realiza a fragmentação, eliminá-la no IPv6 significaria reescrever as aplicações
- IPv6: fragmentação realizada no emissor
- Cabeçalho de Extensão tipo 44
  - Algoritmo semelhante ao IPv4
  - Conteúdo:
    - Lugar do fragmento (13 bits) – posição em número de palavras de 8 bytes
    - Bit M – "More fragments", como no IPv4

GTA/UFRJ

Cabeçalhos de Extensão de Segurança

- Authentication Header (AH)
  - Autenticação da Fonte
- Encapsulation Security Payload (ESP)
  - Criptografia dos Dados

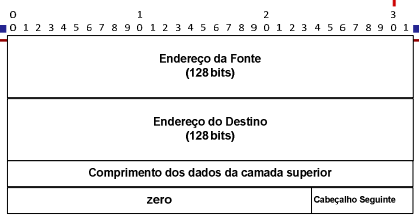
GTA/UFRJ

Checksum no Nível de Transporte

- IPv4: checksum protege o cabeçalho IP
  - IPv6: checksum eliminado do cabeçalho
- IPv6
  - Todos os protocolos acima do IPv6 devem considerar no checksum os dados do cabeçalho IPv6
    - TCP: modificação do cálculo, que era obrigatório
    - UDP: modificação do cálculo e torná-lo obrigatório
  - Criação de um pseudo-cabeçalho, que não é transmitido
  - Checksum: mesmo cálculo do IPv4
    - Soma em complemento a 1 das palavras de 16 bits

GTA/UFRJ

Checksum no Nível de Transporte



- Campos do pseudo-cabeçalho
  - Endereço da Fonte (128 bits) e Endereço do Destino (128 bits)
  - Comprimento dos dados da camada superior (32 bits)
    - Ex. Cabeçalho TCP + Dados
    - Comporta o valor do comprimento da opção jumbograma, se utilizada
  - Campo Cabeçalho Seguinte
    - Não contém necessariamente o mesmo valor do campo do pacote que será transmitido, e já que extensões não são consideradas no cálculo do checksum

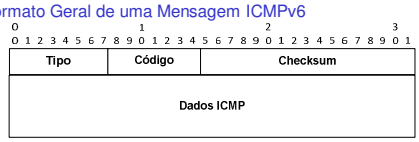
GTA/UFRJ

ICMPv6

- *Internet Control Message Protocol* (ICMP)
- Funções semelhantes ao ICMP do IPv4
  - Detecção de erros
    - Ex.: destino inalcançável, tempo expirado
  - Teste e diagnóstico
    - Ex.: ping
  - Configuração automática de equipamentos
    - Ex.: redirecionamento ICMP, descoberta de roteador
- Novas funções
  - Gerenciamento de grupos multicast
    - Integra o MLD (*Multicast Listener Discovery*) (IGMP no IPv4)
  - Função do ARP no IPv4

ICMPv6

- Formato Geral de uma Mensagem ICMPv6



- Campo Tipo (8 bits)
  - Tipos < 127: mensagens de erro
  - Outros: mensagens de informação
    - Ex. Mensagens do protocolo de descoberta de vizinhos
- Campo Código (8 bits)
  - Causa da mensagem ICMP
- Campo Checksum (16 bits)
  - Calculado com o pseudo-cabeçalho IPv6

ICMPv6

- Conteúdo do Campo Dados ICMP
  - Nas mensagens de erro
    - Contém **(parte da)** Carga útil do datagrama que gerou o erro
    - Comprimento da mensagem ICMPv6 é limitado a 1280 bytes para evitar ter que realizar a descoberta de MTU
      - (como consequência, o conteúdo do pacote pode ser truncado)
  - Nas outras mensagens
    - Campos dependentes do protocolo

Tipos de Mensagens ICMPv6: Gerenciamento de Erros

Tipo	Código	Significado
1		Destino inalcançável:
	0	- não há rota para o destino
	1	- comunicação com o destino impedida administrativamente
	2	- destino fora do alcance do endereço fonte
	3	- endereço inacessível
	4	- número de porta inacessível
2		Pacote grande demais
3		Tempo expirado:
	0	- atingido limite do número de saltos
	1	- tempo de remontagem expirado
4		Erro de parâmetro:
	0	- algum campo de cabeçalho incorreto
	1	- campo de próximo cabeçalho (next header) desconhecido
	2	- opção não reconhecida

Tipos de Mensagens ICMPv6: Informação e Multicast

- Informação

Tipo	Código	Significado
128		Echo Request
129		Echo Response

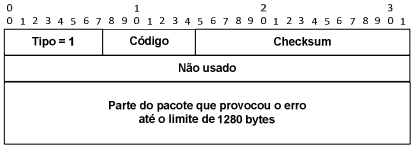
- Gerenciamento de grupos multicast (MLD)

Tipo	Código	Significado
130		Demanda de grupos multicast (Query)
131		Relatório de grupos multicast (Report)
132		Fim de interesse no grupo

Tipos de Mensagens ICMPv6: Descoberta de Vizinhos

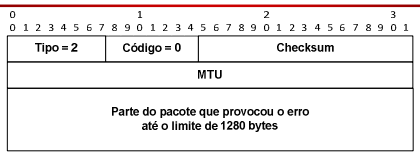
Tipo	Código	Significado
133		Solicitação de roteador
134		Anúncio de roteador
135		Solicitação de vizinho
136		Anúncio de vizinho
137		Redirecionamento (*redirect*)

ICMPv6: Destino Inalcançável



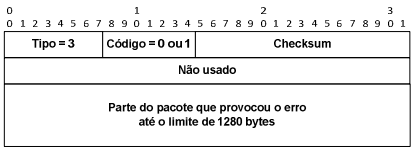
- Mensagem Tipo 1 emitida quando
  - o roteador não possui rota para o destino (Código 0)
  - a mensagem foi filtrada por um firewall (Código 1)
  - endereço inacessível, p. ex. a tentativa de rotear um endereço de tipo local ao enlace (*link-local*) (Código 3)
  - não há aplicação associada à porta de destino (Código 4)

ICMPv6: Pacote Grande Demais



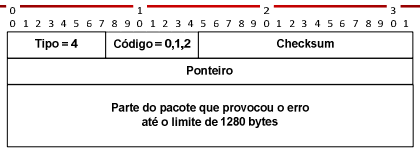
- Mensagem emitida quando o pacote é maior que a MTU do próximo enlace
  - utilizada no procedimento de descoberta de MTU
- Campo MTU: unidade de transferência máxima que o roteador pode aceitar
  - Este campo não existia no IPv4, facilita a descoberta de MTU
- Campo Dados
  - Parte do pacote que provocou o erro, limitando a msg. ICMPv6 a 1280 B

ICMPv6: Tempo Estourado



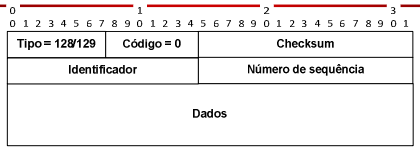
- A mensagem indica que o datagrama foi descartado pelo roteador
  - porque o campo número de saltos (*hop limit*) chegou a zero (Código = 0)
  - ou porque um fragmento se perdeu e o tempo máximo de remontagem foi ultrapassado (Código = 1)
- Mensagem utilizada pelo programa ***traceroute***, como no IPv4

ICMPv6: Erro de Parâmetro



- A mensagem indica erro no cabeçalho ou nos cabeçalhos de extensão do datagrama
- Causa do erro (campo Código)
  - erro de sintaxe no cabeçalho (Código 0)
  - número de próximo cabeçalho (next header) desconhecido (Código 1)
  - uma opção do cabeçalho de extensão desconhecida (e os 2 primeiros bits da opção definem o envio de uma mensagem ICMPv6) (Código 2)
- Ponteiro
  - Indica o byte do datagrama onde ocorreu o erro

ICMPv6: Echo Request e Response



- Utilizadas no programa ping, funcionamento semelhante ao do IPv4
- Campo Identificador
  - Serve para distinguir diversas instâncias do ping sobre a mesma máquina
- Campo Número de Sequência
  - associa uma resposta a um pedido
  - permite medir o tempo de ida e volta e detectar perdas
- Campo Dados
  - permite estatísticas com diferentes tamanhos de datagrama

Gestão de Grupos Multicast

- MLDv1
  - Operação idêntica ao IGMPv2 do IPv4
- MLDv2
  - Operação idêntica ao IGMPv3 do IPv4

ICMPv6: Configuração Automática e Controle

- Protocolo de Descoberta de Vizinhos (ND - *Neighbor Discovery*)
  - Permite a uma estação se comunicar com outros equipamentos na mesma rede física
  - Utiliza 5 tipos de mensagem ICMPv6
  - Campo número de saltos deve ser 255
    - As mensagens não devem ser roteadas: se o valor recebido < 255, datagrama rejeitado
- Funções do *Neighbor Discovery*
  - Resolução de endereços: substitui o ARP do IPv4
  - Detecção de inalcançabilidade de vizinhos
  - Configuração
  - Redirecionamento

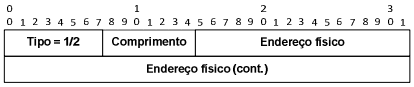
ND: Funções de Configuração

- **Descoberta de Roteadores**
  - Permite aos equipamentos descobrir os roteadores no enlace físico
- **Descoberta de prefixos**
  - Permite conhecer o(s) prefixo(s) utilizados na rede
  - Prefixos podem ser utilizados para construir o(s) endereço(s) dos equipamentos (auto-configuração)
- **Detecção de endereços duplicados**
  - Há riscos de erros, dada a configuração automática
- **Descoberta de parâmetros**
  - Permite conhecer parâmetros do enlace físico, ex.:
    - Tamanho da MTU
    - Número máximo de saltos (valor inicial recomendado do Hop Limit)
    - Se a configuração automática com estado (DHCP) está disponível

Dados das Mensagens de Descoberta de Vizinhos

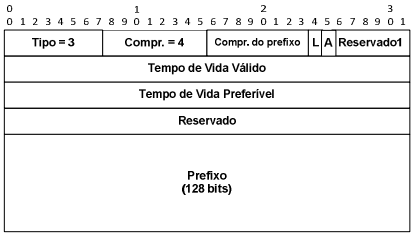
- Maior parte das mensagens da Descoberta de Vizinhos utiliza opções comuns
  - Endereço físico da fonte
  - Endereço físico do alvo
  - Informação de prefixo
  - Cabeçalho redirecionado
  - MTU
- Formato
  - Tipo
  - Comprimento (em palavras de 64 bits)
  - Dados

Dados das Mensagens ND: Endereço Físico da Fonte/do Alvo



- Campo Comprimento
  - Tamanho da opção em palavras de 64 bits
    - Ex. Endereço MAC de 48 bits (6 bytes) – Comprimento = 1
    - Há desperdício de espaço, mas força-se alinhamento em 64 bits
- Tipo 1: endereço físico da fonte
- Tipo 2: endereço físico do alvo

Dados das Mensagens ND: Informação de Prefixo



- Campo Comprimento do Prefixo
  - Número de bits significativos do prefixo anunciado

Dados das Mensagens ND: Informação de Prefixo

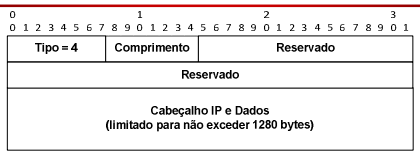
- Bit L = 1
  - Indica que todos os equipamentos que compartilham o prefixo estão no mesmo enlace físico
    - (O IPv6 permite que eles não estejam; neste caso os datagramas devem ser enviados por padrão ao roteador)
- Bit A = 1
  - Indica que o prefixo anunciado pode ser utilizado para construir o endereço do equipamento (auto-configuração)
- Campo Duração de Validade
  - Tempo durante o qual o prefixo é válido
- Campo Duração Preferível
  - Tempo durante o qual um endereço construído a partir deste prefixo estará *preferível*

Dados das Mensagens ND: Informação de Prefixo

- Obs.
  - Para os dois campos de Duração, o valor `0xffffffff` representa "duração infinita"
- Campo Reservado2
  - Permite o alinhamento em palavras de 64 bits
- Campo Prefixo
  - O prefixo anunciado
  - Tamanho fixo de 128 bits para manter o alinhamento

GTA/UFRJ

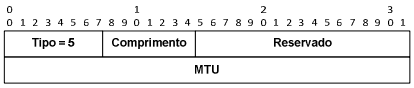
Dados das Mensagens ND: Cabeçalho Redirecionado



- Opção utilizada na Mensagem de Redirecionamento
  - Campo Cabeçalho IP e Dados
    - Parte do Pacote que provocou a mensagem de redirecionamento (limitada de forma à mensagem < 1280 bytes)
  - Campos Reservado
    - Alinhamento em palavras de 64 bits

GTA/UFRJ

Dados das Mensagens ND: MTU



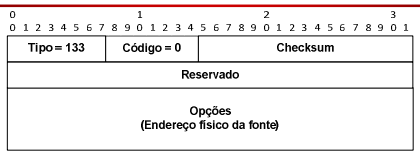
- Campo MTU
  - Tamanho máximo dos dados que podem ser transmitidos sobre o enlace físico
- Campo Reservado
  - Alinhamento em palavras de 64 bits
- Comprimento = 1

GTA/UFRJ

Funções do Protocolo de Descoberta de Vizinhos (ND)

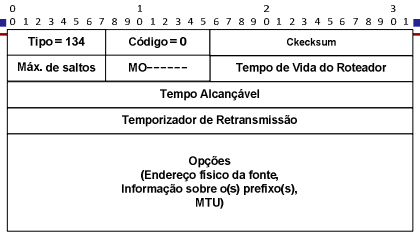
- Descoberta de Roteadores
  - Mensagens *Router Sollicitation* e *Router Announcement*
- Descoberta de Vizinhos
  - Mensagens *Neighbor Sollicitation* e *Neighbor Announcement*
- Redirecionamento

Mensagem de Solicitação de Roteador



- Emitida por um equipamento durante inicialização
  - Obtenção rápida de informações sobre o roteador
- Enviada a `ff02::2` (multicast "todos os roteadores no enlace")
- Campo Opções contém o endereço físico do equipamento fonte

Mensagem de Anúncio de Roteador



- Enviada pelo roteador, periodicamente, ou em resposta a uma mensagem de solicitação de roteador
  - Endereço fonte: endereço link-local do roteador
  - Endereço destino: do equipamento que solicitou, ou `ff02::01`
- Campo Máx. de Saltos (*Current Hop Limit*)
  - Valor padrão sugerido para o campo Hop Limit dos datagramas enviados na rede

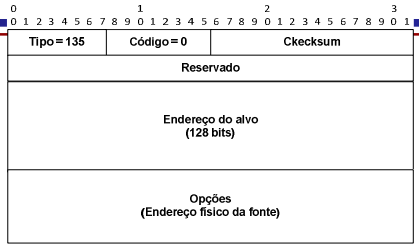
Mensagem de Anúncio de Roteador

- Bit M (“Managed address configuration”)=1: o endereço do equipamento deve ser obtido através do protocolo de configuração DHCP
- Bit O (“Other configuration”) = 1: o protocolo de configuração DHCP fornece outras informações além do endereço (ex. DNS)
- Bit H (“Home agent”)=1: o roteador pode ser utilizado como home agent por um nó móvel
- Tempo de vida do roteador
  - Tempo (em segundos) durante o qual o roteador serve como roteador default
  - Máximo: 18h12m, mas não é limite estrito, já que a mensagem é periódica
- Campo Tempo Alcançável (*Reachable Time*)
  - Tempo em ms de validade de informações guardadas no cache
  - Ex.: tabela de endereços IPv6 x endereços físicos
    - ao final do tempo, procedimento de detecção de inacessibilidade inicia

Mensagem de Anúncio de Roteador

- Campo Temporizador de Retransmissão (*Retransmission Timer*)
  - Período (em ms) entre transmissões não solicitadas de anúncios
  - Permite detectar se o roteador ficou inacessível
- Campo Opções pode conter
  - endereço físico da fonte
  - MTU
  - informação sobre um ou mais prefixos

Mensagem de Solicitação de Vizinho

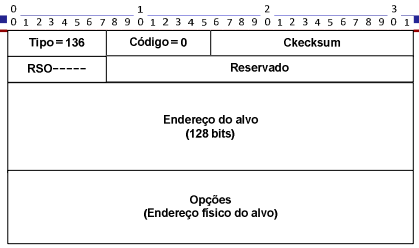


- Obtenção de informações sobre um equipamento vizinho
  - enviada explicitamente ao vizinho
  - ou a um endereço de difusão (corresponde ao ARP Request no IPv4)
- Endereço de Origem
  - Endereço link-local, global, ou não especificado

Mensagem de Solicitação de Vizinho

- Endereço de Destino
  - Endereço Multicast Nó-Solicitado correspondente ao endereço procurado
  - ou endereço do equipamento (caso de detecção de inacessibilidade – NUD)
- Campo Reservado
  - Alinhamento em palavras de 64 bits
- Campo Endereço do Alvo
  - Endereço IPv6 do equipamento procurado
- Campo Opções
  - Endereço físico da fonte
    - deve ser incluído em solicitações multicast
    - pode ser incluído em solicitações unicast
    - não deve ser incluído em solicitações com endereço de origem não especificado

Mensagem de Anúncio de Vizinho

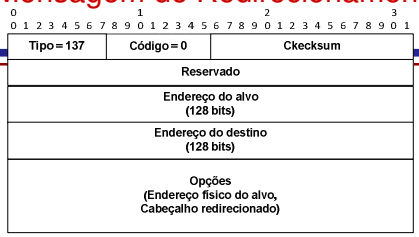


- Enviada em resposta a uma solicitação
  - ou enviada espontaneamente em caso de mudança de endereço físico
  - ou de "status de roteador"
- Corresponde ao ARP Response do IPv4 no caso de determinação do endereço físico

Mensagem de Anúncio de Vizinho

- Bit R (Router flag) = 1: o emissor é um roteador
  - O bit R permite detectar um roteador que se torna um equipamento "normal"
- Bit S (Solicited flag) =1: o anúncio foi enviado em resposta a uma solicitação
- Bit O (Override) =1: o anúncio deve apagar informações anteriores dos caches dos equipamentos, em especial a tabela de endereços físicos
- Campo Endereço do Alvo
  - Se S=1, contém o Endereço do Alvo da mensagem de solicitação à qual este anúncio corresponde
  - Se S=0, contém o endereço IPv6 link-local do equipamento emissor
- Campo Opção
  - Contém o endereço físico do emissor da mensagem

Mensagem de Redirecionamento



- Função de Redirecionamento semelhante ao IPv4
- Também serve para que estações sobre um mesmo meio físico, porém com prefixos diferentes, comuniquem-se diretamente
- Campo Endereço Alvo
  - Endereço IPv6 do equipamento para o qual os pacotes devem ser enviados (próximo salto melhor)
- Campo Endereço Destino
  - Endereço IPv6 do equipamento para o qual o redirecionamento se aplica

Configuração Automática

- Objetivo: Conexão à rede local sem intervenção humana
  - Instalação automática de rotas
    - ICMPv6 Router Solicitation/Announcement
  - Auto-configuração de endereços
- Obtenção de um endereço quando
  - A máquina se conecta à rede pela primeira vez
  - Renumeração da rede, após uma mudança de provedor de rede
- **Processo**
  - Criação de um endereço link-local
  - Verificação da unicidade do endereço link-local
  - Determinação do endereço unicast global

GTA/UFRJ

Configuração Automática

- 2 formas de **determinação do endereço unicast global**:
  - **Autoconfiguração sem estado** (*stateless autoconfiguration*)
    - Útil quando não é necessária gestão administrativa dos endereços atribuídos
  - **Autoconfiguração com estado** (*stateful autoconfiguration*)
    - Útil quando é necessário controle estrito dos endereços atribuídos
    - Realizada pelo protocolo DHCPv6
- Anúncios de Roteador indicam o método utilizado
  - Bit M=0: autoconfiguração sem estado do endereço
  - Bit M=1: o endereço deve ser solicitado a um servidor DHCPv6
  - Bit O=1: além do endereço, informações adicionais disponibilizadas pelo servidor DHCPv6

GTA/UFRJ

Etapas do Procedimento de Autoconfiguração do Endereço

- Criação do endereço link-local
  - (Comunicação com outras máquinas no enlace é possível)
- Recebimento de uma mensagem de anúncio de roteador
  - Determinação do método de obtenção do endereço unicast global
- Autoconfiguração sem estado

  ou
- Autoconfiguração com estado (DHCPv6)

Obs.: Se não houver roteador, autoconfiguração com estado

Duplicate Address Detection (DAD)

- Endereço em estado *provisório* enquanto DAD em execução
- Passos do Algoritmo de Detecção de Endereço Duplicado
  - Entrada no grupo multicast nó-solicitado correspondente
  - Envio de uma mensagem de Solicitação de Vizinho
    - Campo Endereço Alvo: endereço provisório
    - Endereço fonte: endereço IPv6 não especificado (`::/128`)
  - Espera por resposta durante 1 segundo (tempo padrão sugerido)
  - Casos possíveis de acordo com a resposta:
    - Mensagem de anúncio de vizinho é recebida: o endereço provisório já era considerado válido por outra máquina e não pode ser utilizado
    - Mensagem de solicitação de vizinho/DAD é recebida: outro nó pretendia usar o mesmo endereço provisório; este não será utilizado por nenhum dos dois
    - Nenhuma resposta recebida: o endereço passa de provisório a válido

Criação do Endereço Link-local

- Endereço link-local = prefixo + identificador da interface
- Prefixo link-local
  - **`FE80::/64`**
- Identificador
  - EUI-64
- Endereço provisório > DAD > Endereço válido

Autoconfiguração Sem Estado

- Geração do endereço de uma estação a partir de informações locais e informações fornecidas por um roteador
  - Autoconfiguração funciona para estações, não para roteadores
- Endereço global = prefixo + identificador da interface
- Prefixo
  - Opção "Informação sobre Prefixo" das mensagens Anúncio de Roteador
- DAD não é obrigatório, já que foi realizada para escolha do endereço link-local

Propriedades de Segurança

- Confidencialidade dos dados
- Confidencialidade do fluxo de dados
- Autenticação da origem dos dados
- Autenticação mútua de duas entidades
- Integridade dos dados
- Prevenção contra ataques de repetição
- Não repúdio

Principais Formas de Ataque no IP

- IP sniffing
  - "Escuta" do tráfego em trânsito em uma rede
- IP spoofing
  - Falsificação do endereço IP da origem ou do destino
    - "Usurpação" da identidade de outra pessoa
- IP flooding
  - Envio de uma grande quantidade de pacotes, de forma que o tratamento destes pacotes exaure os recursos da máquina sob ataque

Principais Formas de Defesa no IP

- IP sniffing
  - Confidencialidade
- IP spoofing
  - Autenticação/integridade
  - Confidencialidade
  - Detecção de repetição
- IP flooding
  - Limitação das comunicações com/a determinadas estações

Extensões de Segurança no IPv6

- *Authentication Header* (AH)
  - Autenticação
  - Integridade
  - Detecção de ataques de repetição (opcional)
  - Não repúdio (a depender do método de autenticação)
- *Encapsulation Security Payload* (ESP)
  - Confidencialidade
  - Integridade
  - Autenticação
  - Detecção de ataques de repetição
  - Confidencialidade (parcial) do fluxo

Modos de Proteção do IPSec

- Modo Transporte
  - Protege a carga útil do pacote, e alguns campos do seu cabeçalho
- Modo Túnel
  - Protege a comunicação dentro de um túnel IP
  - Ou seja, protege todos os campos do pacote IP original e alguns campos do novo pacote IP que encapsula o pacote original

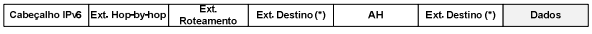
A Associação de Segurança

- Definição
  - Tipo de extensão de segurança do IPv6
  - Serviços e parâmetros de segurança
    - Algoritmo de autenticação e chaves
    - Algoritmo de criptografia e chaves, método de criptografia, ...
    - Tempo de vida da associação de segurança
    - Modo do protocolo IPSec (túnel ou transporte)
- Identificada por um índice de parâmetros de segurança
  - *Security Parameters Index* (SPI)

GTA/UFRJ

Autenticação

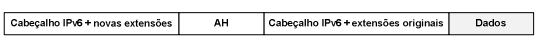
- Extensão AH (*Authentication Header*)
- Modo Transporte
  - Integridade
    - Dados do transporte e campos (cabeçalho e extensões) imutáveis do pacote IP
  - Posicionamento da extensão no pacote:



GTA/UFRJ

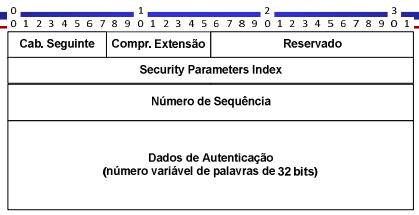
Autenticação

- Extensão AH (*Authentication Header*)
- Modo Túnel
  - Integridade
    - Todo o pacote IP original
    - Campos imutáveis do novo pacote IP que encapsula o original
  - Posicionamento da extensão no pacote:



GTA/UFRJ

Conteúdo da Extensão AH

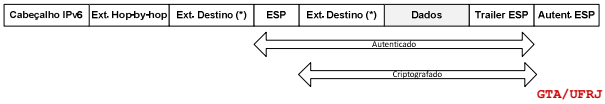


- Comprimento da Extensão em palavras de 32 bits
- SPI identifica a associação de segurança
- Número de sequência
  - Opcional: deve ser preenchido pela origem, mas o destinatário não é obrigado a verificar
- Dados de autenticação
  - Número variável de palavras de 32 bits

GTA/UFRJ

Confidencialidade

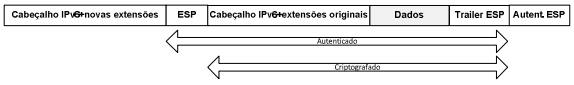
- Extensão ESP (*Encapsulating Security Payload*)
- Modo Transporte
  - Proteção criptográfica
    - Dados, do trailer ESP, e extensão destino (dependendo da sua posição no pacote)
  - Autenticação/integridade
    - Garante toda o conteúdo da extensão ESP, exceto o campo de dados de autenticação ESP
  - Posicionamento da extensão no pacote:



GTA/UFRJ

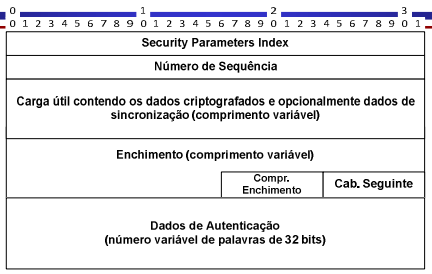
Confidencialidade

- Extensão ESP (*Encapsulating Security Payload*)
- Modo Túnel
  - Proteção criptográfica
    - Sobre todo o pacote IP original
  - Autenticação/integridade
    - Garante toda o conteúdo da extensão ESP, exceto o campo de dados de autenticação ESP
  - Posicionamento da extensão no pacote:



GTA/UFRJ

Conteúdo da Extensão ESP



- SPI identifica a associação de segurança
- Número de sequência

Conteúdo da Extensão ESP

- Carga útil (dados criptografados) pode conter:
  - Cabeçalho IP + Extensões + Dados do transporte
    - (pacote IP completo)
  - Extensão de destino + Dados do transporte
  - Dados do transporte
  - Dados de sincronização dependendo do algoritmo criptográfico
- Enchimento, Comprimento do Enchimento
  - Bits de enchimento se devido ao alinhamento dos dados de criptografia
- Cabeçalho seguinte
  - Indica tipo de dados contidos no primeiro campo da carga útil
- Dados de autenticação
  - Opcional, depende da associação de segurança