Seção: Tutoriais Banda Larga

Redes IP I: Comparativo entre IPv4 e IPv6

Nesta seção veremos alguns detalhes importantes quanto a comparação do IPv4 ao IPv6. Em resumo o IPv6 se diferencia em endereços quase ilimitadas, aumento da mobilidade, melhor desempenho, características de segurança superiores como visualizado na tabela abaixo.

Tabela 2: Comparativo entre IPv4 e IPv6

IPV4	IPV6
Endereço de 32bits	Endereço de 128bits
Suporte opcional de IPSec	Suporte obrigatório de IPSec
Nenhuma referência a capacidade de QoS (*Quality of Service)*	Introduz capacidades de QoS utilizando para isso o campo Flow Label
Processo de fragmentação realizada pelo router	A fragmentação deixa de ser realizada pelos routers e passa a ser processada pelos *host* emissores
O cabeçalho inclui os campos de opção	Todos os campos de opção foram mudados para dentro do campo *extension header*
O *Adress Resolution Protocol* (ARP), utiliza requisitos do tipo *Broadcast*	O ARP foi abandonado, sendo substituídos pelas mensagens *Neibhbor Discovery*
Internet Resolution Management Protocol (IGMP) é utilizado para gerir relações locais de sub-redes	O IGMP fio substituído por mensagens *Multcast Listner Discovery*
Os Endereços de *Broadcast* são utilizados para enviar tráfego para todos os *host* de uma rede	Deixa de existir o endereço de *Broadcast,* para utilizar endereços *multicast*
O endereço tem de ser configurado manualmente	Adição de funcionalidades de autoconfiguração
Suporta pacotes de 576 bytes, passiveis de serem fragmentados	Suporta pacotes de 1280 bytes, sem fragmentação

Fonte: ***http://www.techsutram.com/2009/03/differences-ipv4-vs-ipv6.html***

Cabeçalho

Como podemos verificar na Figura 6, a estrutura do protocolo IPv6 foi bem resumida em relação ao seu antecessor, sendo que muitos campos foram removidos ou tiveram seus nomes alterados.

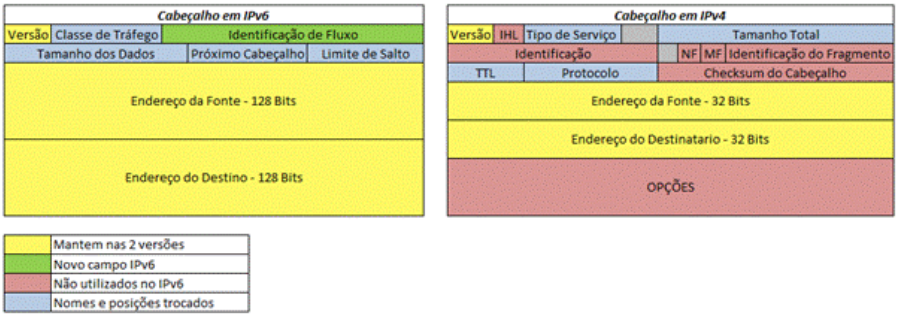

Figura 9: Cabeçalho dos Protocolos IPv4 e IPv6 e suas alterações
Fonte: ***http://rafaelantunesavila.wordpress.com/author/rafaelantunesavila/***

Conforme verificado os campos *Internet header length*, Identificação, NF, MF, Identificação do Fragmento, *Checksum* do Cabeçalho e Opções foram removidos, em contra partida o campo Identificação de Fluxo foi adicionado ao IPv6. Os campos Tipo de serviço, Tamanho total, TTL e Protocolo tiveram seus nomes trocados e posições alteradas, já os campos Endereços da Fonte e endereços do Destino mantiveram nas duas versões, mas suportando uma quantidade de armazenamento maior no IPv6.

Segurança

Hoje, em 2012, são aproximadamente trinta anos de uso do protocolo IPv4 comparado a treze anos do IPv6, mas com uma adoção muito tímida pelo mercado, sendo assim muito cedo a definição de segurança para o novo protocolo. Com a adoção cada vez maior do IPv6, as vulnerabilidades serão publicadas e corrigidas em uma velocidade cada vez maior [5].

Os principais objetivos de segurança do IPv6 são iguais aos objetivos de segurança em qualquer infraestrutura de redes. Estes incluem: robustez da infraestrutura; autenticação, confidencialidade e integridade; não rejeição explícita, controle de acesso e contabilização e registro. Em IPv6, para atingir estes objetivos, tem de ser verificadas diversas ameaças existentes e, dentre elas, serão discutidas sete: pesquisa de pontos fracos em gateway e hosts, pesquisa de endereços *multicast*, acesso não autorizado, exposição de pontos fracos devido ao NAT e pontos fracos do próprio, firewall, ataques de desempenho com cabeçalhos fragmentados, pontos fracos do protocolo e ataques do tipo *Denial of Service (DDoS)* [43].

Segundo Charles M. Kozierok, o IPsec (extensão do protocolo IP cujo objetivo é ser o método padrão para fornecer privacidade ao usuário) não é um protocolo único, mas sim um conjunto de serviços e protocolos que fornecem uma solução de segurança completa para uma rede IP. Esses serviços e protocolos combinados fornecem vários tipos de proteções. IPsec funciona na camada IP, pode fornecer essas proteções para qualquer protocolo TCP seja ele maior que a camada de aplicativo / IP ou protocolo sem a necessidade de métodos adicionais de segurança, o que é uma grande vantagem.

O IPsec inclui as seguintes características:

- Criptografia de dados do usuário de privacidade;
- Autenticação da integridade de uma mensagem para assegurar que ele não é alterada em uma rota;
- Proteção contra certos tipos de ataques de segurança, tais como ataques de repetição entre outras. Como foi parte integrante para o IPv6, seu suporte é obrigatório, ao contrário do que ocorria com o IPv4, no qual seu suporte é opcional;

Há recomendações de segurança para o uso do protocolo IPv6, como:

- Não utilizar endereços óbvios, filtrar mensagens ICMPv6 não essenciais
- Utilizar IPSEC sempre que precisar de uma comunicação segura entre máquinas IPv6;
- Usar endereços IPv6 *unique* local (FC00::/7);
- No IPv4 bloquear as faixas não alocadas;

ICMPv4 vs ICMPv6

De acordo com Adilson Florentino, para suportar esses novos recursos, o protocolo ICMPv6 tem um papel muito importante. Além de continuar a exercer as mesmas funções de seu antecessor ICMPv4, ele também desempenha as funções dos protocolos ARP, RARP e IGMP. Ele é muito importante, pois se deixarmos o *firewall* (dispositivo que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede de computadores)das estações de trabalho bloquearem toda e qualquer mensagem ICMPv6, a rede simplesmente irá parar de funcionar, pois são mensagens desse tipo responsáveis pela descoberta de vizinhança, atribuições de endereços *Stateless* (atribuição automática de endereços de rede sem necessidade de servidor DHCP e/ou configurações manual nas máquinas) e pela descoberta de roteadores e *gateways* (máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos) em rede IPv6.

Protocolo de descoberta de vizinhança

O protocolo de descoberta de vizinhança foi desenvolvido sob a finalidade de resolver os problemas de interação entre nós vizinhos em uma rede. Para isso ele atua sobre dois aspectos primordiais na comunicação IPv6, a autoconfiguração de nós e a transmissão de pacotes.

No caso da autoconfiguração dos nós, o protocolo fornece suporte para a realização de três funcionalidades:

- ***Parameter Discovery*:** atua na descoberta por um nó de informações sobre o enlace (como MTU) e sobre a Internet(como *hop limit*).
- ***Address Autoconfiguration*:** trabalha com a autoconfiguração *stateless* de endereços nas interfaces de um nó.
- ***Duplicate Address Detection*:** utilizado para descobrir se o endereço que se deseja atribuir a uma interface já está sendo utilizado por outro nó da rede.

Já no caso da transmissão de pacotes entre nós, o suporte é dado para a realização de seis funcionalidades:

- ***Router Discovery*:** trabalha com a descoberta de roteadores pertencentes ao enlace.
- ***Prefix Discovery*:** implementa a descoberta de prefixos de redes do enlace, cuja finalidade é decidir para onde os pacotes serão direcionados numa comunicação (se é para um roteador especifico ou direto para um nó do enlace).
- ***Address Resolution*:** descobre o endereço físico através de um endereço lógico IPv6.
- ***Neighbor Unreachability Detection*:** permite que os nós descubram se um vizinho é ou se continua alcançável, uma vez que problemas podem acontecer nos nós como na rede.
- ***Redirect:*** permite ao roteador informar ao nó uma rota melhor ao ser usado para enviar pacotes a determinado destino.
- ***Next-Hop Determination***: algoritmo para mapear um endereço IP de destino em um endereço IP de um vizinho para onde o trafego deve ser enviado [19].

A descoberta de vizinhança substitui ARP (protocolo de resolução de endereços), descoberta de roteador ICMP e ICMP redirecionado, que são usados no IPv4. Ele também fornece funcionalidades adicionais. A seguinte lista mostra como os hosts, roteadores e nós utilizam a descoberta de vizinhança:

- Hosts utilizam para descobrir roteadores vizinhos, endereços, prefixos endereço e outros parâmetros.
- Os roteadores utilizam da descoberta de vizinhança para informar aos hosts de um melhor próximo salto para um endereço de destino específico.
- Nós usam descoberta de vizinhança para descobrir o endereço da camada de um nó vizinho no qual um pacote IPv6 está sendo encaminhado e também para determinar quando o endereço da camada de um nó vizinho foi alterado, e se os pacotes IPv6 podem ser enviados e recebidos de um nó vizinho [20].

DHCPv4 vs DHCPv6

DHCP é a sigla para *Dynamic Host Configuration Protocol*. Trata-se de um protocolo utilizado em redes de computadores que permite a estes obterem um endereço IP automaticamente, sem que o usuário precise configurar manualmente cada host [21].

É importante frisar que, além do endereço IP, também é necessário atribuir outros parâmetros a cada computador (*host*) que passa a fazer parte da rede. Com o DHCP isso também é possível. Pode-se passar à máquina-cliente informações como máscara de rede, endereços de servidores DNS (*Domain Name Server*), nome que o computador deverá assumir na rede (por exemplo, *infowester, infowester1* e assim por diante), rotas, etc [30].

As duas principais diferenças entre DHCPv4 e DHCPv6 são as seguintes:

- No modelo administrativo o DHCPv4 permite que para cada interface e administração é alocado em uma interface lógica e no DHCPv6 essa configuração não é necessária. Este protocolo é habilitado em uma dada interface física.
- DHCPv4 o servidor DHCP fornece a máscara de sub-rede para cada endereço. Uma opção *hostname* define o nome do nó de todo o sistema. Já no DHCPv6 a máscara de sub-rede é fornecida por anúncios ao roteador, não havendo a opção DHCPv6 *hostname* [22].

QoS

Por definição, a Qualidade de Serviço (Quality of Service – QoS) de uma rede é garantida pelos componentes da rede e equipamentos utilizados, estando baseada em um mecanismo fim-a-fim de garantir a entrega das informações e que deve atuar na comunicação dos equipamentos envolvidos visando o controle dos parâmetros de Qualidade de Serviço [23].

Num primeiro momento, o termo "Qualidade de Serviço" pode ser entendido como sendo um requisito das aplicações para a qual exige-se que determinados parâmetros (atrasos, vazão, perdas, etc) estejam dentro de limites bem definidos (valor mínimo e valor máximo). Entretanto, a garantia de Qualidade de Serviço em redes de computadores envolve vários níveis de atuação em diversos tipos de equipamentos e tecnologias, ou seja, esses parâmetros não estão localizados em apenas um único equipamento ou componente da rede. Considerando esse fato, a Qualidade de Serviço deve atuar em todos os equipamentos, camadas de protocolo e entidades envolvidos [23].

A implementação de QoS no IPv4 é baseada nas portas TCP e UDP do pacote, o que pode tornar o seu uso não aplicável em algumas situações. Da mesma forma que o IPv4, o IPv6 é um protocolo responsável pelo endereçamento de hosts e roteamento de pacotes entre redes que são baseadas em TCP/IP. Apesar de assustar em um primeiro momento, o IPv6 é um protocolo bem mais simples que o IPv4. O protocolo IPv6 possui um *Flow Label* (etiqueta de controle de fluxo) para priorizar a entrega de pacotes. Isso permite que os hosts se comuniquem utilizando o conceito de QoS para entrega dos pacotes, tornando alguns serviços mais funcionais [24].

O campo Controle de Fluxo permitirá que políticas de QoS sejam aplicadas sem a necessidades de verificação a fundo das camadas superiores do pacote IPv6 para que sejam definidas e implementadas. Por exemplo, pacotes criptografados poderão passar pelo filtro do QoS, pois o campo “Controle de Fluxo” está fora do cabeçalho de transporte. Já os pacotes fragmentados, que por padrão não possuem todas as informações da camada de transporte, poderão ser verificados utilizando o campo “Controle de Fluxo” [5].