

IPv4

1. Introdução

Um endereço IPv4 é um endereço hierárquico de 32 bits, composto por uma parte da rede e uma parte do host. Ao determinar a parte da rede versus a parte do host, deve-se observar o fluxo de 32 bits.

Os bits na parte de rede do endereço devem ser iguais em todos os dispositivos que residem na mesma rede. Os bits na parte de host do endereço devem ser exclusivos para identificar um host específico dentro de uma rede. Se dois hosts tiverem o mesmo padrão de bits na parte de rede especificada do fluxo de 32 bits, esses dois hosts residirão na mesma rede.

Parte de rede	Parte de host
192.168.10	.10

Os endereços IPv4 começam como binários e são difíceis de gerenciar, logo, administradores de rede os convertem em decimal. Cada endereço é composto por uma string de 32 bits dividida em quatro seções, chamadas de octetos. Cada octeto tem 8 bits (1 byte) separados por um ponto. Aprender a converter binário em decimal requer uma compreensão da notação posicional, isso significa que um dígito representa valores diferentes, dependendo da posição que ocupa na sequência de números. Para usar o sistema posicional, associe um determinado número a seu valor. O exemplo abaixo ilustra o número 1234.

	Milhar	Centena	Dezena	Unidade
Valor posicional	1000	100	10	1
Número decimal	1	2	3	4
Cálculo	$1 * 1000$	$2 * 100$	$3 * 10$	$1 * 4$
Junte-os...	1000	+200	+30	+4

O resultado é 1234.

A tabela abaixo ilustra a conversão do número 11000000 em binário para decimal.

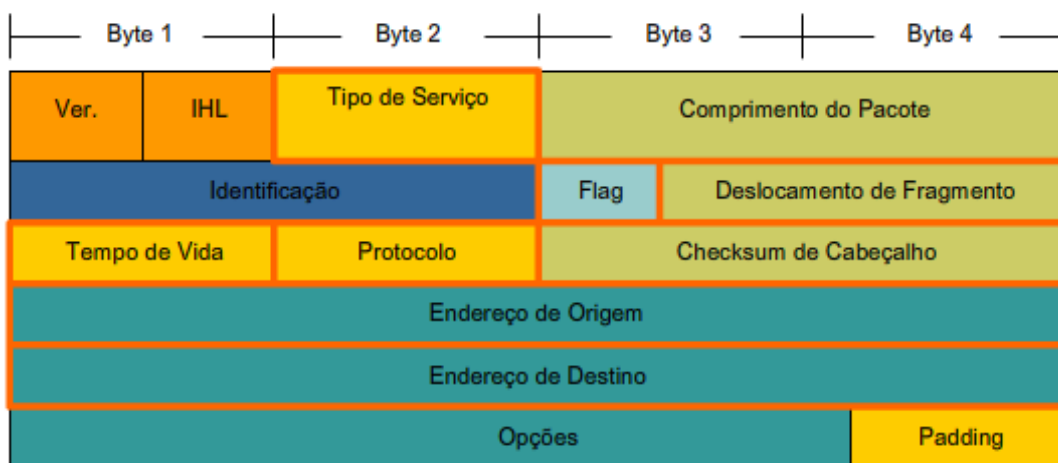
Valor posicional	128	64	32	16	8	4	2	1
Binário	1	1	0	0	0	0	0	0
Cálculo	$1 * 128$	$64 * 1$	$0 * 32$	$0 * 16$	$0 * 8$	$4 * 0$	$2 * 0$	$1 * 0$
Adicione-os	+128	+64	0	0	0	0	0	0

O resultado é 192

Para converter um endereço IPv4 binário em seu equivalente decimal com pontos, divida o endereço IPv4 em quatro octetos de 8 bits, em seguida, aplique o valor posicional binário ao primeiro octeto do número binário e calcule de acordo. Repita o processo até o último octeto.

É preciso saber como converter um endereço IPv4 decimal com pontos para binário. Uma ferramenta útil é a tabela de valores posicionais binários. O número do octeto é igual ou superior ao bit mais significativo? Se sim, adicione um binário 1 no valor posicional e subtraia do número decimal. Se não for, adicione o binário 0 ao valor posicional. Repita esse processo até o número 1.

O cabeçalho do pacote IPv4 é usado para garantir que esse pacote seja entregue para sua próxima parada no caminho para seu dispositivo final de destino. O cabeçalho de um pacote IPv4 consiste em campos com informações importantes. Estes campos contêm números binários que são examinados pelo processo da camada 3.



Os valores binários de cada campo identificam várias configurações do pacote IP. Os diagramas de cabeçalho de protocolo, cuja leitura é feita da esquerda para a direita, de cima para baixo, disponibilizam uma visualização para consulta.

2. Versão

Contém um valor binário de 4 bits definido como 0100 que identifica isso como um pacote IPv4.

2.1 Serviços diferenciados (DS)

O campo DS tem tamanho de 8 bits e é usado para determinar a prioridade de cada pacote. Os seis bits mais significativos do campo são os bits do ponto de código de serviços diferenciados (DSCP) e os dois últimos são os bits de notificação de congestionamento.

2.2 Tempo de vida (TTL)

Contém um valor binário de 8 bits usado para limitar a vida útil de um pacote. O dispositivo de origem do pacote IPv4 define o valor TTL inicial. É diminuído em um cada vez que o pacote é processado por um roteador. Se o campo TTL for decrementado até zero, o roteador

descartará o pacote e enviará uma mensagem ICMP de tempo excedido para o endereço IP de origem. O roteador deve recalcular a soma de verificação do cabeçalho.

2.3 Protocolo

Este campo é usado para identificar o próximo nível de protocolo. O valor binário de 8 bits indica o tipo de carga de dados que o pacote está carregando, o que permite que a camada de rede transfira os dados para o protocolo apropriado das camadas superiores. Valores comuns incluem ICMP, TCP e UDP. Checksum de cabeçalho é usado para detectar corrupção no cabeçalho IPv4.

2.4 Endereço IPv4 de origem

Contém um valor binário de 32 bits que representa o endereço IPv4 de origem do pacote. O endereço de origem IPv4 é sempre um endereço unicast.

2.5 Endereço IPv4 de destino

Contém um valor binário de 32 bits que representa o endereço IPv4 de destino do pacote. O endereço IPv4 destino é um endereço unicast, multicast ou broadcast.

O IPv4 enfrenta atualmente 3 grandes problemas estão descritos abaixo.

- **Esgotamento de endereço IPv4:** O IPv4 tem um número limitado de endereços públicos exclusivos disponíveis. Conexões sempre ativas e o potencial de crescimento de regiões menos desenvolvidas têm aumentado a necessidade de mais endereços.
- **Falta de conectividade ponto a ponto:** NAT é uma tecnologia comumente implementada em redes IPv4. É uma forma de vários dispositivos compartilharem um único endereço IPv4 público. No entanto, como o endereço IPv4 público é compartilhado, o endereço IPv4 de um host de rede interna fica oculto. Isso pode ser problemático para tecnologias que exigem conectividade de ponta a ponta.
- **Maior complexidade da rede:** Embora o NAT tenha ampliado a vida útil do IPv4, ele só se destinava a ser um mecanismo de transição para o IPv6. O NAT tem suas várias implementações, cria complexidade adicional na rede, criando latência e dificultando a solução de problemas.

Os endereços IPv4 públicos são endereços globalmente entre os roteadores do Provedor de Serviço de Internet (*ISP*). No entanto, nem todos os endereços IPv4 disponíveis podem ser usados na Internet. Existem blocos de endereços que são usados pela maioria das organizações para atribuir endereços IPv4 a hosts internos.

Os endereços IPv4 privados não são exclusivos e podem ser usados internamente em qualquer rede. Estes endereços privados são definidos no RFC 1918.

A maioria das redes internas, de grandes empresas e redes domésticas, usa endereços IPv4 privados para endereçar todos os dispositivos internos (*intranet*), incluindo hosts e roteadores. No entanto, os endereços privados não são globalmente roteáveis.

Antes que um ISP possa encaminhar esse pacote, ele deve traduzir o endereço IPv4 de origem, que é um endereço privado para um endereço IPv4 público usando NAT. O NAT é usado para converter entre endereços IPv4 privados e IPv4 públicos. Isso geralmente é feito no roteador que conecta a rede interna à rede ISP. Os endereços IPv4 privados na Intranet da organização serão traduzidos para endereços IPv4 públicos antes do encaminhamento para a Internet.

Existem determinados endereços que não podem ser atribuídos aos hosts. Há também endereços especiais que podem ser atribuídos a hosts, mas com restrições quanto ao modo como interagem na rede.

3. Endereços de loopback (127.0.0.0/8 ou 127.0.0.1 a 127.255.255.254)

Os endereços de loopback são mais comumente identificados como apenas 127.0.0.1. Esses são endereços especiais usados por um host para direcionar o tráfego para si próprio.

3.1 Endereços link local (169.254.0.0/16 ou 169.254.0.1 a 169.254.255.255)

Os endereços locais de link são mais conhecidos como endereços de endereçamento IP privado automático ou endereços auto-atribuídos. Eles são usados por um cliente DHCP do Windows para auto-configurar no caso de não existirem servidores DHCP disponíveis. Endereços de link local podem ser usados em uma conexão ponto a ponto, mas não são comumente usados para esse fim.

Em 1981, os endereços IPv4 foram atribuídos usando o endereço classful. A RFC dividiu os intervalos de unicast em classes específicas da seguinte maneira.

- **Classe A (0.0.0.0/8 até 127.0.0.0/8):** Projetado para suportar redes extremamente grandes com mais de 16 milhões de endereços de hosts. A classe A usou um prefixo /8 com o primeiro octeto para indicar o endereço de rede e os três octetos restantes para endereços de host
- **Classe B (128.0.0.0/16 até 191.255.0.0/16):** Projetado para suportar as necessidades de rede de tamanho moderado a grande, com até aproximadamente 65.000 endereços de host. A classe B usou um prefixo fixo de /16 com os dois octetos de alta ordem para indicar o endereço de rede e os dois octetos restantes para endereços de host.
- **Classe C (192.0.0.0/24 até 223.255.255.0/24):** Projetado para suportar redes pequenas com um máximo de 254 hosts, a classe C usou um prefixo fixo de /24 com os três primeiros octetos para indicar a rede e o octeto restante para os endereços de host.