**DHCP**

Dynamic Host Configuration Protocol (DHCP), é um protocolo cliente servidor, que proporciona automaticamente um endereço um Internet Protocol Host (IP Host) com seu endereço IP, máscara de sub-rede, gateway padrão e DNS.

Como o próprio nome sugere, o DHCP é usado para controlar a configuração da rede de um Host através de um servidor remoto.

**ARP**

O Adress Resolution Protocol é um protocolo usado pelo Internet Protocol , especialmente o IPv4, para mapear os endereços IP’s da rede para os endereços de hardware usados pelo protocolo de enlace de dados. Esse protocolo opera abaixo da camada de rede como parte da interface entre a camada de rede e a camada de transporte.

**Estrutura Datagrama IPV4**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 4 | 8 | 12 | 16 | 20 | 24 | 28 |
| Versão | IHL | Tipo de Serviço | | Tamanho Total | | | |
| Identificação | | | | Flags | Fragment Offset | | |
| Time to Live | | Protocolo | | Header Checksum | | | |
| Endereço Fonte | | | | | | | |
| Endereço de Destino | | | | | | | |
| Opções + Paginação (0 ou mais 32-bit palavras) | | | | | | | |
| Dados | | | | | | | |
| *Mais Dados ...* | | | | | | | |

**Versão:** Versão do protocolo IP que determina como interpretar o cabeçalho.

**IHL:** Tamanho do Cabeçalho em um número de 32bits.

**Tipo de Serviço:**  Muitas vezes ignorado pelos roteadores atuais, serve para permitir que o tráfego seja priorizado.

**Tamanho Total:** O tamanho máximo do diagrama inteiro e os dados, sendo que o máximo permitido é 65,535 bytes ou 64KB.

**Identificação, Flags e Fragment Offset:** Estes valores permitem ao datagrama ser fragmentado para transmissão e remontado no destino.

**Time to Live:** Um número inteiro que representa quanto tempo o datagrama permanece vivo. Se chagar a zero é descartado e uma mensagem ICMP é enviada para o host de origem (Explicação mais completa abaixo).

**Protocolo:** Identifica o protocolo da camada de transporte que irá interpretar a seção de dados. Normalmente é TCP ou UDP mas pode apresentar outros valores.

**Header Checksum:** É usado para verificar o cabeçalho, e é recalculado a cada hop houter.

**Endereços e Opções**:São endereços IP’s que representam o endereço de rede o host.

**ICMPv4**

O Internet Control Message Protocol é usado em conjunto com o IP para proporcionar diagnósticos e controlar a informação relacionada com a configuração da camada de protocolo IP e a disposição de pacotes IP.

ICMP prevê a entrega de mensagens de erro e de controle que podem exigir atenção. As mensagens ICMP geralmente são acionadas por:

* A Camada de IP em si;
* Protocolos de Transporte de camada superior(High Layer) - TCP ou UDP;
* Aplicações do usuário.

**TTL**

Como visto dentro da estrutura do datagrama IPV4, TTL ou Time to Live “é o tempo de vida” do pacote IP. Cada vez que é realizado um salto entre roteadores(hop) esse valor é decrescido em 1 e quando chega a zero o pacote IP é descartado. Esse campo também indica um número máximo de saltos entre roteadores permitindo para um pacote.

**ESP**

O Encapsulating Security Payload é o responsável de providenciar autenticação, integridade e confiabilidade de dados sendo assim o que garante a proteção dos dados e fornecedor da proteção do conteúdo da mensagem.

O ESP trabalha em conjunto com os servidos de criptografia IPSec – Esses que são estruturas abertas para a implementação de algoritmos padrão da indústria, como SHA e MD5. O IPSec utiliza algoritmos que produzem identificadores únicos e não falsificáveis para cada pacote, equivalente a uma impressão digital na vida real, assim verificando se um pacote é válido ou se foi alterado e se caso foi alterado, não realiza a entrega dele ao destinatário.

Essa criptografia permite que somente o remetente e o receptor tenham autorização para acessar os dados.

**AH**

O protocolo de autenticação de Cabeçalho - Authentication Header é uma parte do IPSec que autentica a origem dos pacotes (datagramas) de IP’s e garante a integridade dos dados. O AH confirma a origem do pacote e verifica se seu conteúdo não sofreu alterações durante a transmissão. O AH, se configurado, pode ser usado para defender de possíveis ataques usando uma tecnologia chamada Sliding Technologie.