**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.

**IPX/SPX**

O protocolo Internetwork Packet Exchange/Sequenced Packet Exchange – IPX/SPX é um conjunto de protocolos de rede para redes de sistemas operacionais Novell Netware¹ inicialmente. Assim como o UDP/IP o IPX é um protocolo de datagrama usado para comunicações sem conexões.

O SPX é um protocolo da camada de transporte (camada 4 do modelo OSI) utilizados em redes Novell Netware. A camada IPX fica sobre o topo da camada IPX(camada 3) e fornece serviços orientados a conexão entre dois nós da rede. É usado principalmente em aplicações cliente/servidor.

O IPX/SPX foi concebido como uma alternativa para o protocolo TCP/IP e é variante do Xerox Network Systems (XNS)².

¹Novell Netware: Foi o primeiro sistema operacional desenvolvido para servidores. Surgiu em 1983 inovando ao invés de usar o compartilhamento de disco, usar o compartilhamento de arquivos. Liderava o espaço mundial no mercado de servidores até os anos 90 onde começou a perder espaço para o Linux e servidores Microsoft, como o Windows NT.

²XNS: Protocolo criado pela Xerox nos anos 70, sendo um protocolo bastante similar ao TCP/IP.

**SAP**

O Service Advertising Protocol é um componente do protocolo IPX/SPX usado para a adição e remoção de serviços de rede dinamicamente, como por exemplo, servidores de arquivo e impressoras. Ele é um método usado por um nó provedor de serviços em uma rede (como um servidor de arquivos ou um servidor de aplicações) para informar a outros nós de uma rede que ele se encontra disponível para acesso. Quando um servidor é inicializado, ele utiliza o protocolo para anunciar seus serviços; quando o mesmo servidor é desativado, ele utiliza o protocolo para anunciar que não se encontra mais disponível.

**NETBEUI/SMB**

Por volta de 1984 a IBM criou uma API (Application Programming Interface) para conectar seus computadores em rede chamada Network Basic Input/Output System – NetBIOS. A API NetBIOS prove para a aplicação um design rudimentar para conexão e o compartilhamento de dados com outros computadores. É interessante pensar na NetBIOS como extensões de chamadas padrões de rede da API BIOS. Com a BIOS, cada chamada de baixo nível está confinada ao hardware da máquina local e não precisa de ajuda alguma para ir ao seu destino. Originalmente a NetBIOS tinha que trocar instruções com computadores através de IBM PC ou redes Token Ring. Era então requerido um protocolo de transporte de baixo nível para carregar as requisições de um computador para o outro.

No final de 1985 a IBM lançou tal protocolo, que integrava a API NetBIOS. Era o NetBIOS Enhanced User Interface - NetBEUI . O NetBEUI foi desenvolvido para pequenas LANs (com menos de 255 nós, o que era uma restrição prática em 1985) e permitia que cada máquina na rede clamasse um nome (até 15 caracteres) que não estivesse já sendo utilizado por outra máquina. O protocolo NetBEUI era muito popular entre aplicativos de rede incluindo aqueles que rodam sobre Windows para Workgroups. Mais tarde implementações do NetBIOS sobre o protocolo IPX da Novell surgiram, competindo então com o NetBEUI.

O SMB – Service Message Block,é um protocolo de compartilhamento de arquivos em rede que permite que os aplicativos de um computador leiam e gravem em arquivos e solicitem serviços dos programas do servidor em uma rede de computadores. O protocolo SMB pode ser usado sobre seu protocolo TCP/IP ou outros protocolos de rede. Utilizando o protocolo SMB, um aplicativo (ou o usuário de um aplicativo) pode acessar arquivos ou outros recursos em um servidor remoto. Isso permite que os aplicativos leiam, criem e atualizem arquivos no servidor remoto. Ele também pode se comunicar com qualquer programa do servidor que esteja configurado para receber uma solicitação de um cliente SMB.

**APPLETALK**

É um conjunto de protocolos de rede desenvolvido pela Apple por volta de 1984 para ser usado nos seus Macintosh’s.

O propósito do AppleTalk era permitir que vários usuários compartilhassem recursos, como arquivos e impressoras. Os dispositivos que fornecem esses recursos são chamados de servidores, enquanto os dispositivos que utilizam esses recursos (como um usuário de computador Macintosh) são chamados clientes. Por esse motivo, o AppleTalk é uma das primeira implementações de um sistema distribuído cliente-servidor.

O AppleTalk foi projetado com sua interface de rede transparente. Isso significa que a interação entre os computadores e os servidores de rede requer uma pequena interação da parte do usuário. Além disso, as efetivas operações dos protocolos AppleTalk são invisíveis para os usuários finais, que veem somente o resultado dessas operações. Existem duas operações de AppleTalk: AppleTalk Fase 1 e AppleTalk Fase 2.

O AppleTalk Fase 1, que é a primeira especificação do AppleTalk, foi desenvolvida no começo dos anos 80, restritamente para o uso em grupos de trabalhos locais. Assim, a Fase 1 apresenta duas limitações principais: seus segmentos de rede que não podem conter mais do que 127 hosts e 127 servidores e podem suportar somente redes não-estendidas.

O AppleTalk Fase 2, a segunda implementação Apple Talk otimizada, foi projetada para utilização em internet works maiores. A Fase 2 soluciona as principais limitações do AppleTalk Fase 1 e contém vários aperfeiçoamentos em relação à Fase 1. Em particular, a Fase 2 permite qualquer combinação de 253 hosts ou servidores em um mesmo segmento de rede.

**PPP**

O protocolo ponto a ponto (PPP) é um conjunto de protocolos padrão que permite a interoperação de programas de software de acesso remoto de diferentes fornecedores. Uma conexão ativada por PPP pode discar para redes remotas através de qualquer servidor PPP padrão da indústria. O PPP também permite que um servidor de acesso remoto receba chamadas e forneça acesso de rede a programas de software de acesso remoto de outros fornecedores compatíveis com os padrões PPP.

**PPPoE**

Utilizando o PPPoE e um modem de banda larga, os usuários de LAN podem obter acesso autenticado individual a redes de dados de alta velocidade. Ao combinar a Ethernet e o protocolo PPP, o PPPoE proporciona uma maneira eficiente de criar uma conexão separada com um servidor remoto para cada usuário. Acesso, cobrança e serviços escolhidos são gerenciados com base em cada usuário, e não em cada site. Os clientes podem criar conexões dial-up e de discagem por demanda usando o PPPoE.