Protocolo IPV4

Conceitos Gerais

1. Introdução

- A camada de rede está diretamente relacionada à transferência de pacotes (que é o PDU desta camada) entre origem e destino, através de saltos entre os dispositivos intermediários na rede, geralmente roteadores.

- Diferente da camada de enlace, que trata a comunicação entre dispositivos adjacentes ou que compartilham o meio, a camada de rede possibilita uma visão fim a fim, isto é, da origem ao destino.

- Entretanto, é importante diferenciar que a sua operação ocorre nó a nó até que o pacote chegue ao seu destino.

- Vale lembrar que a camada de rede tem como propósito oferecer serviços para a camada superior, que no caso é a camada de transporte.

2. Relembrando o Modelo OSI e TCP/IP

- A imagem abaixo mostra um resumo das camadas do modelo OSI

Camadas do OSI

1. **Física**
   Transmite bits (0 e 1) no meio físico (cabos, sinais elétricos).
2. **Enlace de Dados**
   Cuida da comunicação entre dispositivos na mesma rede (MAC, frames, detecção de erro).
3. **Rede**
   Responsável pelo **endereçamento lógico e roteamento** (IP).
4. **Transporte**
   Garante entrega correta dos dados (TCP/UDP, controle de erro e fluxo).
5. **Sessão**
   Controla abertura, manutenção e encerramento de conexões.
6. **Apresentação**
   Tradução de dados (compressão, criptografia, formatação).
7. **Aplicação**
   Interface com o usuário (HTTP, FTP, DNS).

2. Relembrando o Modelo OSI e TCP/IP

- A imagem abaixo mostra um resumo das camadas do modelo TCP/IP

Camadas do TCP/IP:

1. **Acesso à Rede**

   Equivalente às camadas Física + Enlace do OSI.
2. **Internet**

   Equivalente à camada de Rede (IP, roteamento).
3. **Transporte**

   Igual ao OSI (TCP/UDP).
4. **Aplicação**

   Junta Aplicação + Apresentação + Sessão do OSI.

3. Protocolo IPV4

- O protocolo **IP** é um dos dois protocolos chaves da arquitetura TCP/IP, sendo este da camada de Rede ou Inter-Redes. É amplamente utilizado na Internet como protocolo padrão na definição dos pacotes que serão roteados.

- Atualmente, ainda é mais utilizado em sua versão 4, ou IPv4. Veremos mais adiante a “nova” versão 6, ou IPv6, que tendo a aumentar sua utilização ao longo do tempo, principalmente com o o crescimento da IOT.

- O protocolo IP possui seu PDU definido como datagramas IP. É um protocolo extremamente simples, não confiável e não executa operações de detecção e recuperação de erros, ficando a cargo das camadas superiores (TCP por exemplo).

- Possui uma garantia apenas da integridade do cabeçalho do pacote. Utiliza como critério de entrega o método de **melhor esforço (best effort)**.

3. Protocolo IPV4

- O modelo **Best-Effort** significa que o protocolo IP faz **o melhor esforço possível para entregar os pacotes**, mas **não garante nada**.

- Desta forma, quando um nó envia os dados na rede, o IP tenta entregar os pacotes ao destino, mas **não garante que eles vão chegar, n**em garante **ordem, tempo ou integridade.**

- Na prática, quando um pacote IP é enviado, ele é roteado pela rede (passa por vários roteadores). Cada roteador decide o melhor caminho naquele momento.

- Se houver problemas (congestionamento, falha, etc.), o pacote pode ser descartado, chegar atrasado ou fora de ordem.

3. Protocolo IPV4

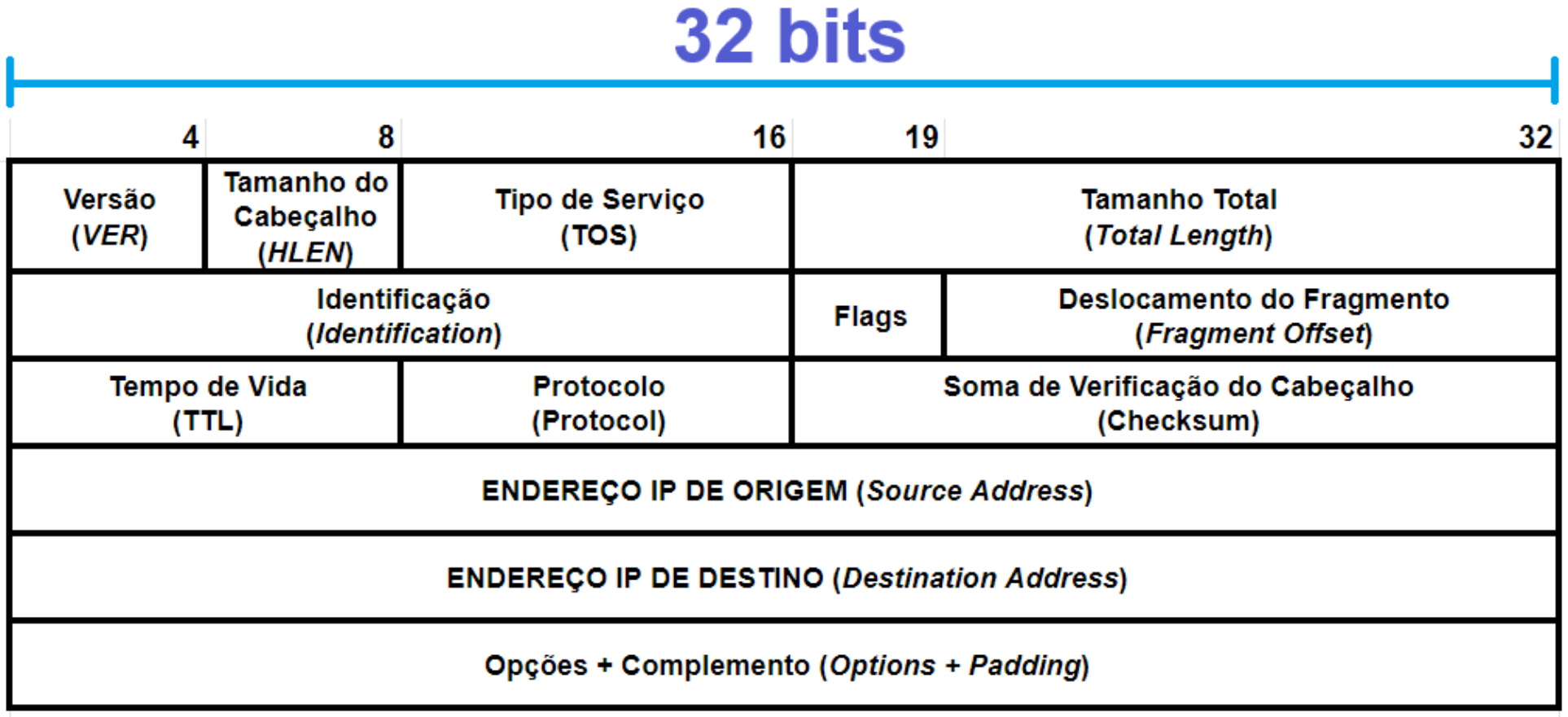
- No modelo Best-Effort, o IP **não garante**: Entrega dos pacotes, Ordem correta, Controle de congestionamento, Controle de fluxo e Retransmissão.

- O protocolo IP é simples e rápido. Ele deixa a responsabilidade para **camadas superiores**, principalmente o **TCP (Transmission Control Protocol)**.

- O TCP resolve os problemas do Best-Effort: Reenvia pacotes perdidos, Ordena os pacotes e Garante entrega confiável.

4. Protocolo IPV4

- O protocolo possui uma estrutura de cabeçalho de 20 bytes de tamanho mínimo, podendo chegar até 60 bytes com os seus campos opcionais de tamanho variável. A imagem abaixo mostra a estrutura do cabeçalho:



4. Protocolo IPV4

- Analisando os campos do cabeçalho:

Ver - Version (4 bits): Responsável por informar a versão do protocolo IP utilizado: IPv4 (0100 em binário) ou IPv6 (0110 em binário).

IHL - Information Header Length (4 bits): Devido ao tamanho variável do cabeçalho do datagrama IP de 20 bytes a 60 bytes, precisa ser informado o tamanho para tratamento do protocolo.

Service Type ou TOS (Type of Service) (8 bits): Serve para indicar como aquele pacote deve ser tratado na rede. Ele define a prioridade ou qualidade de serviço (QoS) do pacote. Nem todo tráfego é igual. Por exemplo: Chamada de voz → precisa ser rápida (baixa latência). Hoje o TOS virou **DSCP (Differentiated Services Code Point),** ele ocupa **6 bits** do campo e define classes de prioridade.

0 → tráfego normal (best-effort)
EF (Expedited Forwarding) → voz (VoIP)
AF (Assured Forwarding) → vídeo, streaming
CS (Class Selector) → classes de prioridade

4. Protocolo IPV4

Total Lenght: Este campo define o tamanho total do datagrama IP (cabeçalho + dados). Pode variar de 20 bytes a 65535 bytes.

Identifier (16 bits): Campo de identificação do pacote IP. Quando há fragmentação de pacote, é através desse identificador que o destino consegue definir quais fragmentos pertencem a determinado pacote original.

Flag: controla se tem fragmento ou não.

Fragment Offset (13 bits): Indica em que posição o fragmento do pacote deve ser colocado para reordenar o pacote final.

4. Protocolo IPV4

Time to Live – TTL: Contém o tempo de vida do pacote na rede em função da quantidade de saltos que este pode dar. Geralmente começa com 32, 64 ou 128 e a cada nó (roteador) que o pacote passa esse valor é decrementado até chegar a 0, caso em que o pacote será descartado. Seu tempo de vida útil máximo com 8 bits é de 255 saltos.

Protocol (8bits): Indica qual protocolo da camada superior vai receber os dados (pacotes) enviados. O campo **Protocol** é como um **rótulo no pacote**, determinando se vai para o TCP, ICMP ou UDP por exemplo. A imagem abaixo mostra os principais valores possíveis:

Valor	Protocolo	Função
1	ICMP	Mensagens de erro e diagnóstico (ex: ping)
6	TCP	Comunicação confiável (web, e-mail)
17	UDP	Comunicação rápida (streaming, DNS)

4. Protocolo IPV4

Header Checksum: Campo que utiliza um algoritmo sobre todo o cabeçalho IP permitindo a verificação da integridade do cabeçalho IP. Lembrando que não garante a integridade dos dados.

Source and Destination Address (32 bits): Armazena a informação do endereço IP em sua versão 4 de origem e destino, respectivamente dos endpoints da comunicação.

Options and Padding (Tamanho Variável): Este campo é opcional. Agrega informações adicionais no protocolo IP em relação à fragmentação, medição e monitoramento, controle, segurança entre outros.

5. Endereçamento do IPV4

- Cada dispositivo na rede ou Internet, seja ele um nó simples, servidor ou equipamento de usuário, deve ser identificado para que possa enviar e receber pacote.

- Essa identificação deve ter informações que definam a rede a qual o elemento pertence e um número de host que o diferencia dentro de uma rede. A ideia é similar ao CEP, onde cada número possui uma parcela destinada a uma área ou região, e uma parcela mais específica.

- Esse identificador é denominado **endereço IP**, endereço lógico ou endereço de rede. Teoricamente, este endereço é único e possui uma visibilidade global na rede. O endereço IP é composto por 32 bits.

6. Formato do Endereço IP

- O **IPv4** usa o endereço IP como uma **identificação única de um dispositivo na rede**. Cada dispositivo (PC, celular, servidor) precisa de um “endereço”, que é o IP.

- Um endereço IP possui **4 números (octetos), que variam de 0 até 255.** Uma parte do IP faz referência a identificação da rede, e a segunda parte ao host (ao computador ou nó específico). Um exemplo de IP: 192.168.1.10

- Apenas olhando o IP, não é possível concluir qual parte identifica a rede e o host. Para isso, é preciso analisar outro elemento conhecido como **máscara de rede**. De forma simples, a máscara determina qual parte do IP identifica a rede e qual parte identifica o dispositivo.

- Por exemplo, em uma situação onde o IP:192.168.1.10 e a Máscara:255.255.255.0, podemos concluir que 192.168.1 é a rede, e 10 é o host. Desta forma, todos os dispositivos desta mesma rede começam com 192.168.1.X

6. Formato do Endereço IP

- Um outro exemplo seria o IP:10.0.0.5 e a Máscara: 255.0.0.0. Neste caso a rede suporta muito mais hosts. Todo host começa com o IP 10.x.x.x.

- Os endereços IP são divididos em classes, conforme a tabela abaixo:

Classe	Faixa de IP	Máscara padrão	Nº de redes	Nº de hosts por rede	Uso principal
A	1.0.0.0 – 126.255.255.255	255.0.0.0 (/8)	Poucas	~16 milhões	Redes muito grandes
B	128.0.0.0 – 191.255.255.255	255.255.0.0 (/16)	Média	~65 mil	Redes médias
C	192.0.0.0 – 223.255.255.255	255.255.255.0 (/24)	Muitas	254	Redes pequenas
D	224.0.0.0 – 239.255.255.255	—	—	—	Multicast
E	240.0.0.0 – 255.255.255.255	—	—	—	Pesquisa/experimental

6. Formato do Endereço IP

- A **Classe D** no IPv4 não é usada para identificar um dispositivo individual. Ela serve para enviar dados para vários dispositivos ao mesmo tempo (grupo).

- Na classe D não existe **máscara de rede tradicional, nem host individual.** Usa protocolos como IGMP (para gerenciar quem participa do grupo).

- Um IP multicast representa um **grupo de dispositivos**. Exemplo: `224.0.0.1,` significa que todos os dispositivos desse grupo devem receber essa mensagem.

- É muito usado em IPTV e streaming. Por exemplo: Um servidor envia um vídeo para **224.1.1.1,** todos os clientes que acessam este grupo recebem ao mesmo tempo.

- Já a classe E é reservada para pesquisas e testes. Não é usada na internet normal e nem é atribuída a dispositivos. É um tipo de “espaço reservado”, quase inexiste no dia a dia.

6. Formato do Endereço IP

- Outro ponto importante para ser descrito é a máscara. Se observarmos o formato 255.255.0.0 (/16). Um IP tem **32 bits** (no IPv4), o **/16** significa: **16 bits são da rede e 16 bits são do host.** Transformando em binário, fica mais claro: 11111111.11111111.00000000.00000000

- Aplicando esta nomenclatura no IP, a ideia é exatamente a mesma. Por exemplo, no IP: `172.16.5.10/16,` significa: Rede → **172.16 e** Host → **5.10**

- Resumindo:

/24 → 255.255.255.0

/16 → 255.255.0.0

/8 → 255.0.0.0

6. Formato do Endereço IP

- Dentro de uma rede no IPv4, existem dois endereços que não podem ser usados por dispositivos: Endereço de rede e o Endereço de broadcast.

- O endereço de rede é o **primeiro IP da rede**. Ele identifica a rede em si (não um dispositivo). Por exemplo: Na rede 192.168.1.0/24, o IP 192.168.1.0 (primeiro IP) é o endereço da rede, e não pode ser usado.

- Assim como o endereço de broadcast (último) também é reservado. No caso do exemplo, o endereço 192.168.1.255 é de broadcast. Sempre que algo é enviado neste endereço, vai para toda a rede.

6. Formato do Endereço IP

- Outro ponto muito importante, é a definição da quantidade de host efetivos em uma rede. Pensando no exemplo anterior, no IP 192.168.1.0/24. Neste caso, apenas os 8 bits finais do endereço representam os hosts.

- Para calcular quantos endereços são possíveis, como 8 bits, fazemos 2^8, o que nos leva a um total de 256 endereços possíveis, logo 256 dispositivos podem ser ligados nesta rede.

- Mas é importante lembrar que dois endereços são reservados, restando então **254 endereços efetivos** para uso por parte dos hosts.

7. Faixa de IP Reservadas

- No IPv4 existem blocos de endereços IP que foram separados exclusivamente para uso interno, ou seja, eles não funcionam diretamente na internet, são usados apenas em redes locais (LAN).

- Desta forma, a Internet possui uma faixa de endereços públicos (válidos globalmente), assim como as redes internas possuem endereços privados (válidos só dentro da rede). A tabela abaixo mostra as faixas de IP reservado para redes internas:

Classe	Faixa privada	CIDR
A	10.0.0.0 – 10.255.255.255	/8
B	172.16.0.0 – 172.31.255.255	/12
C	192.168.0.0 – 192.168.255.255	/16

7. Faixa de IP Reservadas

- Um exemplo prático de endereçamento de uma rede doméstica, podemos definir 192.168.0.1 → roteador, 192.168.0.10 → notebook e 192.168.0.20 → celular. Todos estes dispositivos se comunicam entre si, mas não são visíveis diretamente na internet.

- Já empresas com grande número de dispositivos, costumam usar a faixa **10.x.x.x.**

- Para acessar a internet, é necessário um outro recurso essencial, que é **NAT (Network Address Translation). Ele converte um IP privado para um IP público.**

- Desta forma, o roteador recebe um IP privado (ex: 192.168.0.10), troca por um IP público e envia para a internet.

- Sem faixas de IP privado, teríamos um problema sério com **falta de endereços IPv4.** Então estas faixas privadas ajudam a: Economizar IPs públicos, Aumentar segurança interna e Permitir redes internas grandes.

8. Subredes

- Como vimos anteriormente, em cada classe, é possível criar diversas redes com capacidades variadas e relativamente extensas. Dessa forma, imaginemos um cenário em que um laboratório tenha 10 equipamentos.

- Neste caso, precisaríamos de 10 endereços de rede disponíveis, mais os dois endereços reservados, mais uma reserva para crescimento futuro. Chegaríamos, por exemplo, a no máximo 30 endereços.

- Dessa forma, poderíamos usar um endereço da classe C, que nos permite ter até 256 endereços no total. De imediato notamos o grande desperdício de endereços.

- Por esse motivo, foi criado o conceito de **subrede**. O princípio por trás das subredes reside no fato de se utilizar parte dos bits utilizados para hosts na criação de subredes com capacidades menores que sua rede padrão. Além de ajudar na organização.

8. Subredes

- Desta forma, vamos definir Subrede como **dividir uma rede maior em redes menores.** Vamos utilizar um exemplo de uma empresa: A empresa inteira forma a rede e cada setor (RH, TI, Financeiro) possui sua respectiva subrede. As principais vantagens são:

✔ 1. Organização

Separar setores, departamentos, etc.

✔ 2. Segurança

- Um setor não acessa o outro diretamente
- Pode aplicar regras (firewall)

✔ 3. Desempenho

- Menos "tráfego espalhado"
- Rede mais eficiente

✔ 4. Melhor uso de IPs

Evita desperdício de endereços

8. Subredes

- Para criar uma subrede, o segredo está na máscara. Por exemplo, uma rede original com a configuração 192.168.1.0/24 tem 256 IPs (254 utilizáveis).

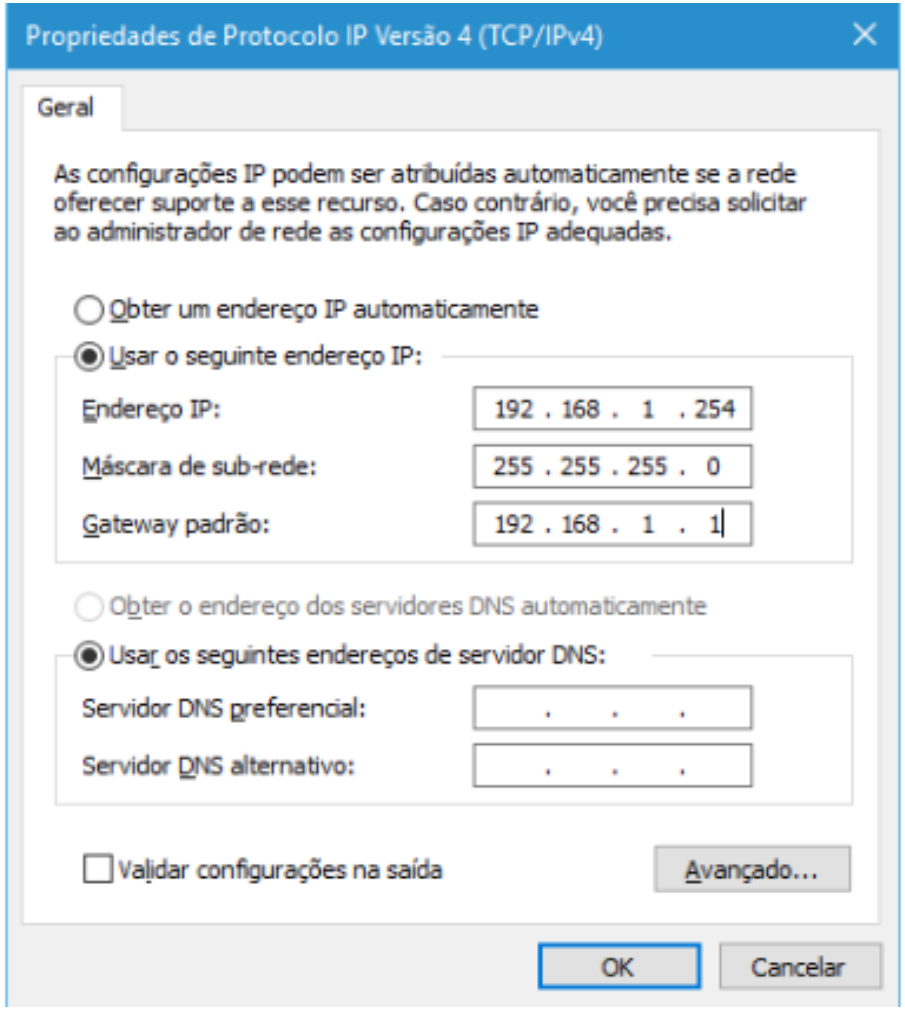
- Mudando para 192.168.1.0/26, agora foram criadas **4 subredes, cada uma com 64 IP's.**

- Colocando **/26** significa que 26 bits são de **rede, o resto é de host. C**omo o IPv4 tem 32 bits, 32 - 26 = 6 bits para hosts. Calculando 2^6 = 64 endereços por subrede.

- Vamos converter: /26 = 11111111.11111111.11111111.11000000. Em decimal, essa máscara fica 255.255.255.192

8. Subredes

- Desta forma, é possível configurar o IP e a máscara do computador:



8. Subredes

- Exemplo: Utilizando um endereço de rede IPv4, para criar 30 sub-redes com 6 hosts cada, deve-se utilizar a máscara Classe C 255.255.255.X, qual o valor de X?

8. Subredes

- Exemplo: Utilizando um endereço de rede IPv4, para criar 30 sub-redes com 6 hosts cada, deve-se utilizar a máscara Classe C 255.255.255.X, qual o valor de X?

- Queremos:
- **30 sub-redes**
- **6 hosts por sub-rede**
- Partindo de uma rede Classe C (no IPv4)
- Máscara base: `255.255.255.0 → /24`

8. Subredes

- Passo 1 – Descobrir quantos bits precisa para hosts:

- Queremos **6 hosts válidos** por subrede.
- Fórmula: $2^h - 2 \geq hosts$
- Testando:
- h = 2 → 2^2 - 2 = 2 (não)
- h = 3 → 2^3 - 2 = 6 (sim)

- Precisamos de **3 bits para hosts**

8. Subredes

- Passo 2 – Descobrir quantos bits precisa para subredes:

- Classe C tem: `/24 → sobram 8 bits (último octeto)`
- Já usamos 3 bits para hosts: `8 - 3 = 5 bits para subredes`

- `Isso gera até 2^5 = 32 subredes`
- Precisamos de 30, então 5 bits para subredes atende

8. Subredes

- Passo 3 – Montar a máscara

- Agora juntamos: 24 bits originais com 5 bits de subrede = `/24 + 5 = /29`

- `/29 = 11111111.11111111.11111111.11111000`
- Resultado: `255.255.255.248`

8. Subredes

- A partir da máscara, podemos começar a configurar as subredes:

- 255.255.255.248 → /29

- O primeiro passo é descobrir o tamanho do bloco:
- Use a regra:
- `256 - último octeto da máscara`
- Nesse caso: `256 - 248 = 8`

- Quer dizer que as subredes “andam” de **8 em 8** no último octeto (0,8,16,24,32,40)

8. Subredes

- A partir da máscara, podemos começar a configurar as subredes:

- 255.255.255.248 → /29

- O primeiro passo é descobrir o tamanho do bloco:
- Use a regra:
- `256 - último octeto da máscara`
- Nesse caso: `256 - 248 = 8`

- Quer dizer que as subredes “andam” de **8 em 8** no último octeto (0,8,16,24,32,40)

8. Subredes

- Agora podemos começar a configurar as subredes:

Subrede 1

- Rede: `192.168.1.0`
- Hosts: `192.168.1.1` → `192.168.1.6`
- Broadcast: `192.168.1.7`

Subrede 2

- Rede: `192.168.1.8`
- Hosts: `192.168.1.9` → `192.168.1.14`
- Broadcast: `192.168.1.15`

8. Subredes

Subrede 3

- Rede: `192.168.1.16`
- Hosts: `192.168.1.17 → 192.168.1.22`
- Broadcast: `192.168.1.23`

Subrede 4

- Rede: `192.168.1.24`
- Hosts: `192.168.1.25 → 192.168.1.30`
- Broadcast: `192.168.1.31`

9. CIDR e VLSM

- O **CIDR** é uma forma de representar redes IP usando **prefixo (/n)** em vez de classes (A, B, C). Anteriormente, as redes de classe C usavam máscara fixa: 255.255.255.0. Com CIDR é possível usar qualquer máscara: `/24`, `/26`, `/30`, etc.

- O CIDR permite melhorar o aproveitamento de IPs e ter redes com tamanhos flexíveis. Por exemplo: Uma rede `192.168.1.0/26`

- O `/26` significa que 26 bits são para definir a rede e 6 bits para hosts (32 - 26). É possível ter 64 endereços de IP (`2^6 = 64 endereços).`

- `Uma rede com 64 endereços pode ter 62 hosts válidos (2 para broadcast e rede). Desta forma, temos a` Rede: 192.168.1.0, Primeiro host: 192.168.1.1, Último host: 192.168.1.62 e Broadcast: 192.168.1.63

9. CIDR e VLSM

- O ideal é sempre definir a estrutura de uma rede perante a quantidade de hosts. Isto é, se for necessária uma rede para 60 usuários, não se usa mais rede classe C, mas sim uma subrede /26.

- O cálculo deve ser feito de forma invertida para os usuários. Se houver 60 hosts, ou seja, endereços efetivos, serão necessários 62 endereços no total para contemplar o endereço de rede e de Broadcast.

- Deve-se calcular qual o valor na base 2 imediatamente superior ao 62. No caso, é o número 64, que corresponde a 26. Logo, será usado 6 bits para hosts e os demais (32 -6 = 26) para definir a rede, sendo então um /26.

- Portanto, pode-se ter máscaras variadas dentro de um bloco de rede padrão. Tal procedimento é chamado de **VLSM (Variable Length Subnet Mask)**.

10. Fragmentação

- Uma capacidade muito importante da camada de rede é a possibilidade de fragmentar os pacotes. A necessidade de fragmentação surge uma vez que a camada de rede recebe pacotes de tamanho superior ao que o enlace ou a rede é capaz de suportar.

- Existem diversos motivos que limitam o tamanho do pacote, entre eles estão o hardware e SO dos equipamentos, protocolos, tamanhos definidos para otimização do tráfego na rede, entre outros.

- A capacidade de suportar determinado tamanho de pacote é chamada de MTU da rede. No protocolo IP, caso haja a fragmentação de pacotes no caminho, estes só serão remontados no destinatário.

- O controle para recombinar estes pacotes é feito no cabeçalho do pacote, com campos específicos para tratar a fragmentação.

10. Fragmentação

- Como exemplo de fragmentação, vamos supor que um pacote chegue a um determinado roteador na rede com tamanho 4000 bytes. No protocolo IP, o cabeçalho possui um tamanho de 20 bytes, logo, de área útil de dados temos 3980 bytes.

- Supondo que a rede seja Ethernet, o MTU é de 1500 bytes (Cabeçalho + Dados), restando 1480 bytes de área máxima de dados. Logo, devemos dividir a área útil de dados original (3980 bytes) em 3 partes (1480 + 1480 + 1020).

- Assim, cada fragmento será acrescido de um cabeçalho e enviado pela rede com MTU de 1500 bytes. Percebam que o último pacote não utilizará toda a capacidade do MTU da rede.

10. Fragmentação

- Outro ponto importante é lembrar dos campos presentes no cabeçalho para tratar a fragmentação, são eles:

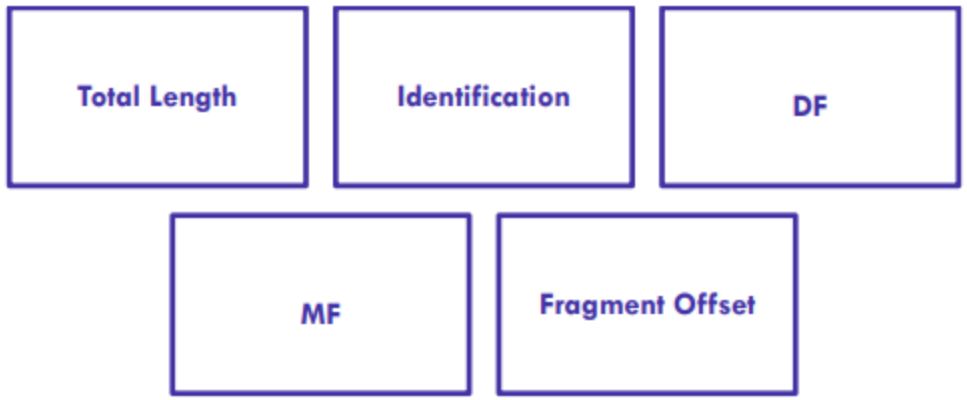
Total Length – o tamanho de cada pacote e definir os espaçamentos entre eles.

Identification – identificador dos pacotes fragmentados.

DF - Campo que define se o pacote pode ou não ser fragmentado

MF - Quando setado, indica que há mais fragmentos para reconstrução do pacote.

Fragment Offset – Ordem dos fragmentos



11. NAT e PAT

- É notório que a quantidade de endereços IP é limitada. Antigamente, 4 bilhões de endereços pareciam ser inesgotáveis. Era plenamente possível atribuir um endereço para cada dispositivo existente na rede.

- Entretanto, atualmente, cada usuário chega a ter acesso a 5 dispositivos distintos que requerem endereço IP (computador do trabalho, celular, tablet, televisão, computador pessoal).

- Além disso, surgiram áreas como IOT, que conectam diversos tipos de máquinas e equipamentos na rede, demandando um grande número de endereços IP.

- Se não fossem os recursos oferecidos pelo **NAT (Network Address Translation) e PAT (Port Address Translation)**, esses endereços já teriam acabado há muito tempo.

11. NAT e PAT

- O **NAT** é uma técnica que permite **traduzir endereços IP privados em IP público,** ou seja, vários dispositivos da rede interna (com IP privado) conseguem acessar a internet (que usa IP público). A ideia principal é “Esconder” vários IPs privados atrás de um IP público.

- Por exemplo, uma rede interna com PC1 → 192.168.1.10 e PC2 → 192.168.1.20 possuem o roteador com IP público) 200.10.10.5.

- Quando o PC1 acessa a internet o NAT faz a conversão de `192.168.1.10 para 200.10.10.5. Para o servidor que hospeda o site, aparece apenas o` IP público.

- Também é possível categorizar o serviço como **NAT estático** (1 IP privado para 1 IP público) ou **NAT dinâmico** (vários IPs privados usam um conjunto de IPs públicos).

11. NAT e PAT

- O **PAT** é um tipo de NAT que usa **portas** para diferenciar conexões. Também é conhecido como **NAT overload**. A ideia é VÁRIOS dispositivos usem **o mesmo IP público ao mesmo tempo.**

- **Por exemplo, uma r**ede interna possui PC1 → 192.168.1.10 e PC2 → 192.168.1.20 com IP público do roteador: 200.10.10.5.

- PC1 acessa um site: `192.168.1.10:5000 → 200.10.10.5:10000` e o PC2 acessa o mesmo site: `192.168.1.20:5001 → 200.10.10.5:10001`

- Observe que eles usam o mesmo IP público, mas as portas são diferentes. O roteador mantém uma tabela para saber diferenciar:

IP privado	Porta interna	IP público	Porta externa
192.168.1.10	5000	200.10.10.5	10000
192.168.1.20	5001	200.10.10.5	10001

11. NAT e PAT

- Em resumo, **NAT** traduz IP privado → IP público e o **PAT** traduz IP + porta → IP público + porta, permitindo que muitos dispositivos compartilharem 1 IP. O PAT é usado na maioria das residências.

Característica	NAT	PAT
Tradução	IP → IP	IP + PORTA
IP público	Pode usar vários	Usa geralmente 1
Quantidade de dispositivos	Limitada	Muitos dispositivos
Uso comum	Empresas	Casas / roteadores

12. NAT Reverso e Balanceamento de Carga

- O **NAT reverso** é quando a tradução acontece no sentido **internet → rede interna**. Desta forma, alguém de fora acessa um IP público e o roteador/firewall redireciona para um servidor interno. Geralmente, o objetivo é "expor" um serviço interno para a internet.

- Por exemplo, a rede interna possui um servidor web → 192.168.1.100 e roteador (IP público): 200.10.10.5.

- Um usuário externo acessa: http://200.10.10.5. Caberá ao NAT reverso fazer a conversão 200.10.10.5 → 192.168.1.100

- Geralmente o NAT reverso é usado em conjunto com um LOAD Balalance para balancear carga. Por exemplo, um cliente acessa IP público, o NAT reverso recebe a requisição e o Balanceador escolhe um servidor para encaminhar a requisição.