

PROBLEMA DE MTU / FRAGMENTAÇÃO

Esta será a última simulação de **camada 3** apresentada no curso. Não porque não existem outras falhas nessa camada, mas porque, segundo o instrutor, o conteúdo coberto até aqui já é suficiente para o suporte técnico. O assunto desta etapa é um problema muito comum, mas muitas vezes negligenciado: **falhas de MTU**, que levam à **fragmentação de pacotes**.

O que é fragmentação de pacotes?

Todo pacote IP possui um tamanho máximo. Em redes tradicionais, o tamanho máximo de um pacote IP (MTU) é **1500 bytes**. Quando se utiliza **PPPoE**, o cabeçalho PPPoE consome **8 bytes**, reduzindo o MTU efetivo para:

$$1500 - 8 = 1492 \text{ bytes}$$

Assim, quando usamos autenticação PPPoE, o maior pacote que pode ser transmitido sem fragmentação é de **1492 bytes**.

Quando utilizamos IPoE, essa redução *não* ocorre, pois o cabeçalho PPPoE não está presente.

Quando ocorre a fragmentação?

Se um pacote de **1500 bytes** precisa passar por um equipamento (por exemplo, uma ONT) que só aceita pacotes de **1492 bytes**, então:

1. A ONT **quebra** o pacote original em pedaços menores.
2. Reenvia esses pedaços.
3. O destino precisa **remontar** o pacote completo.

Esse processo é conhecido como **fragmentação de pacote**.

Problemas causados pela fragmentação

A fragmentação pode gerar diversos problemas, como:

- **Redução de velocidade**, pois aumenta o processamento na ONT ou roteador.
- **Perda de pacotes**, se o destino não aceitar fragmentação.
- **Sites lentos ou que não carregam**, especialmente serviços mais sensíveis.
- **Instabilidade geral**, quando o MTU está abaixo do recomendado.
- **Carga excessiva no hardware**, principalmente em ONTs mais simples.

Quanto menor o MTU configurado, maior será o número de fragmentações e maior será a perda de desempenho.

E no IPv6?

No **IPv6**, o comportamento é diferente:

- O **roteador não fragmenta** pacotes
- Quem ajusta o tamanho é o próprio **host de origem**, usando um mecanismo chamado *Path MTU Discovery*.
- Se algum equipamento não aceitar determinado tamanho, ele devolve uma mensagem pedindo para reduzir o MTU.

Assim, o IPv6 **não sofre dos mesmos problemas** de fragmentação que o IPv4.

A simulação feita pelo instrutor

Para evitar interferência, o instrutor desligou o **IPv6** do computador, garantindo que apenas o IPv4 influenciasse o teste.

Pontos importantes:

- A maioria dos sites aceita fragmentação entre **1480 e 1492 bytes**.
 - Abaixo de **1480 bytes**, problemas começam a aparecer.
 - Algumas ONTs lidam muito mal com MTUs baixos, deixando sites **extremamente lentos** ou inacessíveis.
 - É importante configurar o MTU **exatamente como o provedor definiu**.
-

Testando MTU via CMD

Para testar MTU sem permitir fragmentação:

```
ping [IP] -f -l [tamanho]
```

Onde:

- -f = não fragmentar.
- -l = tamanho do pacote (payload).

Exemplo:

```
ping 10.0.57.255 -f -l 1500.
```

Como 1500 bytes não passam em PPPoE, o pacote falhará. A partir daí, deve-se **reduzir o valor** até encontrar o maior tamanho que passa sem fragmentar.

Se a ONT estiver configurada para **1492**, você deve encontrar um número próximo desse valor, lembrando que o tamanho no ping representa apenas o *payload*, portanto haverá variação.

Tudo o que você reduzir no MTU da ONT deve ser proporcionalmente ajustado no teste até encontrar o valor real.

Conclusão

Problemas de MTU podem causar lentidão e perda de acesso a sites específicos. Por isso, precisam ser analisados com cuidado, sempre respeitando o MTU definido pelo provedor e testando adequadamente para evitar fragmentação indevida.

Como Resolver Problemas de MTU?

Para resolver problemas de MTU, o objetivo principal é **garantir que todos os dispositivos na sua rede concordem com o mesmo tamanho de pacote** e evitar a fragmentação. O processo envolve descobrir o valor de MTU ideal para o seu caminho de rede específico e aplicá-lo ao seu roteador e dispositivos.

Aqui está um guia passo a passo:

1. Descubra o Valor de MTU Ideal

Você precisa realizar um teste de "ping" usando o prompt de comando (Windows) ou terminal (macOS/Linux) para descobrir o maior pacote que pode ser enviado sem fragmentação. O valor padrão a ser testado é 1500, e você diminuirá a partir daí.

No Windows:

1. Abra o **Prompt de Comando** (pesquise por cmd no menu iniciar).
2. Digite o seguinte comando, substituindo google.com pelo endereço do servidor que você deseja testar (pode ser o endereço IP do seu provedor):

```
bash
```

```
ping google.com -f -l 1500
```

Use code with caution.

1. -f: Define o bit "Não Fragmentar" (Do Not Fragment), forçando a falha se o pacote for muito grande.

2. -l 1500: Define o tamanho inicial do pacote para 1500 bytes.

3. Analise o resultado:

1. Se você receber a mensagem "O pacote precisa ser fragmentado, mas o DF está definido" (ou "Packet needs to be fragmented but DF set"), o tamanho é muito grande.

2. **Diminua o tamanho do pacote** (ex: 1472, 1400, 1350) e repita o comando até obter uma resposta bem-sucedida.

4. **Calcule o MTU ideal:** Quando encontrar o maior tamanho de pacote que funciona (ex: 1472 bytes), **adicione 28 bytes** (esses 28 bytes são para os cabeçalhos IP e ICMP, que são invisíveis no teste de ping).

1. *Exemplo:* $1472 + 28 = \mathbf{1500}$ (neste caso, o padrão é o ideal).

2. *Exemplo 2:* Se o maior tamanho que funcionou foi 1432, seu MTU ideal é $1432 + 28 = \mathbf{1460}$.

2. Ajuste as Configurações de MTU

Depois de encontrar o valor ideal, você precisará aplicá-lo onde o problema está ocorrendo.

A. No Roteador (Recomendado)

Alterar o MTU no roteador aplica a correção para todos os dispositivos conectados àquela rede.

1. Acesse a interface de administração do seu roteador (geralmente digitando 192.168.0.1 ou 192.168.1.1 no navegador).
2. Procure por configurações de **WAN**, **Rede (Network)** ou **Internet**.
3. Encontre um campo chamado **MTU** ou **Tamanho do pacote**.
4. Insira o valor ideal que você calculou (ex: 1460 ou 1500) e salve as configurações.
5. **Reinicie o roteador.**

B. No Seu Dispositivo Específico (Alternativo)

Se você não puder acessar o roteador, ou se o problema for apenas em um computador específico, você pode ajustar o MTU localmente.

No Windows (usando Prompt de Comando como Administrador):

1. Abra o **Prompt de Comando** como Administrador (clique com o botão direito no menu iniciar e selecione "Prompt de Comando (Admin)" ou "Windows PowerShell (Admin)").
2. Primeiro, anote o nome exato da sua interface de rede (ex: "Ethernet" ou "Wi-Fi") usando este comando:

```
bash
```

```
netsh interface ipv4 show subinterfaces
```

Use code with caution.

3. Defina o novo valor de MTU (substitua Valor_MTU_Ideal e "Nome da Interface"):

```
bash
```

```
netsh interface ipv4 set subinterface "Nome da Interface"  
mtu=Valor_MTU_Ideal store=persistent
```

Use code with caution.

No macOS:

1. Vá para **Preferências do Sistema > Rede**.
2. Selecione sua conexão ativa (Wi-Fi ou Ethernet), clique em **Avançado...**
3. Vá para a aba **Hardware** ou **Ethernet**.
4. No menu suspenso **Configurar**, selecione **Manual**.
5. Em **MTU**, selecione **Personalizado** e insira o valor ideal.

3. Verifique a Solução

Após aplicar a mudança e reiniciar os equipamentos, repita o teste de ping do passo 1. Agora, com o MTU configurado corretamente, o teste com o valor ideal não deve mais reportar a mensagem de fragmentação e a sua conexão deve estar mais estável e rápida.

E Se Tiver Com o IPv6 Ligado Junto Do IPv4?

Em um cenário de suporte técnico onde o problema de MTU persiste em um ambiente misto IPv4/IPv6, e a causa raiz não é óbvia, o diagnóstico requer uma abordagem sistemática e focada na visibilidade do caminho da rede.

O objetivo é isolar onde os pacotes estão sendo silenciosamente descartados ("*black-holed*") em vez de fragmentados ou devolvidos.

Aqui está um plano de ação estruturado para um técnico de suporte:

Passo a Passo para o Suporte Técnico

Fase 1: Diagnóstico e Coleta de Dados

1. Confirmação do Escopo (Dual Stack):

1. Verifique se o cliente está de fato usando *dual stack* (IPv4 e IPv6 simultaneamente). Use ferramentas como o `ipconfig` ou `ifconfig` no dispositivo do cliente para confirmar a atribuição de ambos os tipos de endereços.

2. Verificação do Comportamento do PMTUD (Path MTU Discovery):

1. O problema de MTU é quase sempre um problema de PMTUD quebrado (BPMPD - Broken PMTUD). Isso ocorre porque algum firewall no caminho está bloqueando as mensagens ICMP Type 3 Code 4 (Destination Unreachable - Fragmentation Needed).

2. **A ação chave é testar se o ICMP está passando.**

3. Executar Testes de Ping Agressivos:

1. Vá além do teste de ping simples. Use ferramentas de diagnóstico de rota que variam o tamanho do pacote, como o mtr ou tracert avançado.

2. **No Windows:**

bash

Teste o MTU com DF bit configurado (como feito antes)

ping destino.com.br -f -l 1500

Use code with caution.

3. **No Linux/macOS (mais robusto para IPv6):**

bash

Use ping6 com o flag -M do para forçar "do not fragment"

ping6 -M do -s 1480 google.com

Use code with caution.

4. **O que procurar:** Observe exatamente em qual *hop* (salto de roteador) a resposta para de vir quando você atinge um determinado tamanho de pacote. Isso aponta o dispositivo problemático.

Fase 2: Isolamento e Resolução de Problemas

Se você identificar o hop problemático, as ações de resolução são:

1. **Checar o Firewall do Cliente:**

1. O bloqueio de ICMP pode estar no próprio computador do cliente (Windows Defender, McAfee, etc.). Desative temporariamente o firewall do cliente para testar se o problema desaparece. Se sim, reconfigure o firewall para permitir ICMP.

2. **Checar o Roteador/CPE do Cliente (Prioridade Máxima):**

1. Acesse o equipamento do cliente. A maioria dos problemas acontece aqui.

2. Procure especificamente por configurações de firewall no roteador que possam estar bloqueando o ICMP. Muitas vezes há uma caixa de seleção como "Block ICMP" ou "Enable SPI Firewall" que é muito restritiva.
3. Se o bloqueio de ICMP não for a causa, a solução é **forçar um MTU menor** no roteador do cliente, como discutido anteriormente (usando o valor calculado de 1460, por exemplo, que é um valor "seguro" que geralmente funciona).

3. Soluções Alternativas (Se o ISP for o culpado):

1. Se os testes de tracert ou mtr indicarem que o problema ocorre *depois* que o tráfego sai da rede do cliente e entra na rede do Provedor de Internet (ISP), o cliente não pode resolver o problema sozinho.
2. Nesse caso, o suporte deve **abrir um chamado interno** para a equipe de engenharia de rede do ISP, fornecendo os dados exatos do mtr/tracert (qual IP bloqueou e qual tamanho de pacote), para que eles corrijam a configuração do firewall ou do MTU em seus *routers* de borda.

Resumo do Plano de Ação

O segredo para o suporte técnico é não adivinhar. Use as ferramentas de ping e tracert com a opção "Do Not Fragment" ativada para **localizar exatamente onde o pacote morre** e, a partir daí, aplicar a correção (abrir portas ICMP no firewall ou forçar um MTU menor no roteador do cliente).