

LOOPING DE REDE

Essa será a última demonstração de problemas da camada 2. Nesta simulação será falado do looping de rede. O looping de rede tem um mecanismo de proteção chamado de STP ou Spanning Tree. Essa será a última demonstração de problemas da **camada 2 (Enlace de Dados)**. Nesta simulação, será abordado o **looping de rede**.

O looping de rede possui um mecanismo de proteção chamado **STP (Spanning Tree Protocol)** — um protocolo fundamental que evita que caminhos redundantes criem ciclos infinitos. Porém, alguns equipamentos permitem **desabilitar o Spanning Tree**, ou simplesmente não possuem essa função. Nesses casos, o loop pode ocorrer facilmente, causando impactos sérios no funcionamento da rede.

O que é um looping de rede?

“Um loop de rede é um ciclo incorreto no qual os pacotes ficam circulando indefinidamente entre dispositivos, criando congestionamento, lentidão e instabilidade geral. Isso acontece quando existem múltiplos caminhos físicos entre dois dispositivos e os switches não sabem para onde enviar o tráfego, formando um ciclo infinito.”

Quando um loop acontece, os sintomas mais comuns são:

- **Rede extremamente lenta ou paralisada**
- **Perdas de pacotes**
- **Aumento repentino de broadcast e multicast (“tempestade de broadcast”)**
- **Dispositivos desconectando e reconectando**
- **CPU dos switches vai ao máximo**
- **Equipamentos travam ou reiniciam**

Por que o STP é importante?

O **Spanning Tree Protocol** detecta caminhos redundantes e **bloqueia** automaticamente um deles, mantendo apenas um caminho operacional. Isso impede que o loop aconteça.

Existem variações modernas do STP, como:

- **RSTP (Rapid Spanning Tree Protocol)** – mais rápido
- **MSTP (Multiple Spanning Tree Protocol)** – permite múltiplas árvores
- **Loop Detection** – proteção adicional em switches domésticos

Em uma rede sem STP, um simples cabo conectado de forma incorreta pode derrubar toda a estrutura de rede.

Como identificar um loop?

Um técnico pode identificar looping pelos seguintes indícios:

1. **Portas LAN piscando rapidamente e de forma constante**
2. **CPU do equipamento no máximo**
3. **Navegação instável ou impossível**
4. **Pacotes ARP se repetindo em grande volume (Wireshark mostra repetição contínua)**
5. **Vários dispositivos com IP duplicado momentaneamente**
6. **Reclamações simultâneas de vários clientes da mesma rede**

Em rede corporativa, loops podem derrubar ambientes inteiros em segundos.

Como resolver um looping de rede?

Aqui estão as formas mais eficazes:

1. Corrigir fisicamente o loop

A solução mais simples:

Retirar o cabo que está formando o caminho redundante.

Exemplo típico:

- Cliente conecta dois cabos entre o mesmo switch e o roteador
- Cliente liga porta LAN na LAN do próprio roteador
- Switch em cascata com cabos invertidos

2. Ativar o STP, RSTP ou MSTP

Nos switches gerenciáveis, habilite:

- **STP** (Spanning Tree Protocol)
- **RSTP** – recomendado, mais rápido
- **MSTP** – redes avançadas

Isso impede loops futuros.

3. Habilitar “Loop Detection” ou “Loop Prevention”

Muitos equipamentos domésticos possuem recursos simplificados como:

- Loop Detection
- Loop Prevention
- Storm Control

Eles detectam loops e **bloqueiam automaticamente** a porta problemática.

4. Substituir switches não gerenciáveis

Se o cliente tiver um switch barato sem proteção, vale orientar:

- Trocar por um switch gerenciável
- Ou usar um switch com “Loop Prevention”

5. Teste por isolamento

Desligue todos os dispositivos do cliente e ligue um por vez até localizar o circuito que cria o loop.

Conclusão

O looping de rede é um dos problemas mais críticos da camada 2 e, quando ocorre, pode derrubar totalmente uma rede local. Conhecer STP, identificar loops através de ferramentas como **Wireshark**, interpretar o comportamento das portas LAN e entender a topologia do cliente são habilidades fundamentais para técnicos e analistas de suporte de redes.