

STP, RSTP e MSTP

Atividade 1 - Segundo Bimestre

Abigail Sayury Nakashima e Miguel de Campos Rodrigues Moret

Redes de Computadores II

1.1 Introdução

Um loop de rede ocorre quando há uma conexão entre duas portas de uma tomada de rede. Essa ligação cria um loop de rede Ethernet. Tal situação pode ser accidental ou intencional, em caso de necessidade de conferir falhas na infraestrutura da rede.

Esse tipo de ocorrência deve ser feito com cautela, pois apresenta alguns problemas que afetam o desempenho da rede:

- **Broadcast storm**, onde quadros de broadcast são retransmitidos de forma excessiva na rede, pois os switches retransmitem quadros em broadcast através de suas demais portas. Quando há um caminho fechado, os quadros são retransmitidos continuamente pelos switches, inundando a rede e consumindo sua capacidade.
- **Instabilidade na tabela MAC nos switches**, pois cada switch tem uma tabela que mapeia endereços físicos MAC de dispositivos para as portas correspondentes. Essa tabela indica a porta por onde um quadro deve ser retransmitido para que chegue ao endereço MAC de destino. Como essa tabela é dinâmica, ela é constantemente atualizada e sobreescrita, criando conflitos.
- **Múltiplos quadros repetidos recebidos em cada host**, pois cada quadro recebido também precisa ser processado, o que gera carga adicional para o equipamento final no tempo de processamento desses quadros repetidos.

A fim de impedir que loops em redes façam circular pacotes continuamente, foi criado o protocolo STP, ou Protocolo Spanning Tree, que soluciona o problema de loops em redes LAN, conferindo redundância à rede e bloqueando alguns caminhos, garantindo que os dados se movam eficientemente.

Nas próximas seções deste trabalho serão tratados, de forma mais aprofundada, os protocolos STP, RSTP e MSTP, conceitos fundamentais para compreensão do funcionamento e entendimento dos protocolos, a arquitetura de rede proposta para a segunda parte do trabalho e o plano de endereçamento IP e VLANs definido.

1.2 Protocolos STP, RSTP e MSTP

Como apresentado anteriormente, o protocolo STP foi desenvolvido para resolver problemas de redundância em redes Ethernet, sendo um protocolo padrão aberto e que impede broadcast storms, instabilidade da tabela MAC, loops e quadros múltiplos repetidos. Desde o seu desenvolvimento ocorreram atualizações: Rapid STP, ou RSTP, e Multiple STP, ou MSTP, que melhoraram o STP.

1.2.1 STP

O Spanning Tree Protocol foi definido inicialmente no padrão IEEE 802.1D. Foi o primeiro protocolo criado para evitar loops em redes Ethernet com caminhos

redundantes. Seu funcionamento é baseado em uma árvore livre de ciclos, onde apenas um caminho lógico pode ser selecionado entre dois pontos de uma rede. Ele envolve quatro etapas principais:

- Eleger uma Root Bridge, que vai ser a raiz da árvore livre de ciclos.
- Encontrar topologias que possuem ciclos, enviando mensagens chamadas de BPDU, que, baseadas nelas, os switches encontram as partes com ciclos da topologia.
- Configurar os papéis das portas. Quando identificando um ciclo, cada switch coloca quantas portas de switch forem necessárias para que a topologia fique sem loops.
- Re-convergir em volta de falhas. Os switches continuam a trocar mensagens para acompanhar as conexões e a disponibilidade de switches adjacentes. Se um link cair, os switches executam os passos 2 e 3 novamente para ter certeza de que a nova topologia seja livre de ciclos.

1.2.2 RSTP

O Rapid STP foi criado pois o tempo para ser inicializado era muito grande, levando 50 segundos para um cliente se conectar para que pudesse então se comunicar em uma rede de dois switches conectados. Antigamente, esse tempo de até minutos era aceitável, mas atualmente isso é inaceitável.

A solução, que é o RSTP, foi que ele não depende de temporizadores para definir se deve colocar uma interface no estado de encaminhamento. Ao invés disso, o RSTP usa um handshake explícito para negociar o papel da porta e o estado, e esse é o mecanismo que faz o protocolo rápido. Essa versão converge mais rápido que o STP sem nenhuma configuração especial.

1.2.2.1 O que torna o processo do protocolo rápido É um processo de sincronização que aumenta a velocidade de convergência do RSTP comparado ao STP, e eles seguem os seguintes passos:

1. Quando uma porta de um switch (swi1) inicializa-se pela primeira vez, ela começa como uma porta designada no estado de bloqueio e começa a enviar BPDU com um conjunto de bits de proposta, informando que esse switch quer se tornar a ponta designada para o segmento, incluindo o Bridge ID e o papel da porta.
2. Quando o outro switch (swi2) recebe o BPDU com a flag de proposta, ele começa um processo de sincronização, e é considerado sincronizado se estiver ou em estado de bloqueio ou se for uma porta de fronteira. Para alcançar esse estado, o switch temporariamente move todas as portas que não são de fronteira para o estado de bloqueio e checa se o BPDU recebido não está em conflito com os papéis das próprias portas.
3. Quando a checagem é completa, esse switch (swi2) seleciona um papel de porta e dá seguimento para colocar essa porta em estado de encaminhamento, o que então faz com que ela envie uma BPDU de volta para o

swi1, com uma flag de consentimento.

4. Quando o swi1 recebe a BPDU com a flag de consentimento, ele sabe que a proposta foi aceita e move a porta designada para o estado de encaminhamento.

Esse processo de proposta e consentimento é muito rápido porque não depende de temporizadores STP, levando cerca de 0,3 segundos para começar o tráfego de encaminhamento.

1.2.2.2 Papéis de Portas do RSTP O RSTP seleciona o switch com o menor valor de prioridade de bridge como a root bridge e então define os seguintes papéis para cada porta:

- Porta root, o caminho de menor custo para alcançar a root bridge.
- Porta designada, a porta que conecta o switch com o melhor caminho para o segmento específico até a root bridge.
- Porta alternativa, o caminho de backup para a root bridge caso a porta atual falhe.
- Porta backup, a porta de backup para a porta designada.
- Porta desabilitada, porta que não participa na spanning tree.

1.2.2.3 Estados das Portas do RSTP **Discarding:** estado em que a porta descarta todos os frames que estão vindo e não aprende endereços MAC, combinando os estados Disabled, Blocking e Listening do STP.

Learning: estado em que a porta ainda descarta todos os frames que estão vindo, mas começa a aprender endereços MAC.

Forwarding: a porta encaminha frames baseado nos endereços MAC que já aprendeu e continua a aprender.

1.2.3 MSTP

O MSTP foi apresentado pelo padrão IEEE 802.1s, sendo baseado em seu antecessor RSTP, mas oferecendo a possibilidade de criar múltiplas árvores em uma única rede, melhorando a escalabilidade e a eficiência.

Cada árvore é uma instância, e cada instância pode ter sua própria root bridge e topologia de encaminhamento, assim como pode ser associada com uma ou mais VLANs, o que significa que diferentes VLANs podem seguir diferentes caminhos dentro de uma mesma rede física, sendo útil para redes maiores que precisam de maior flexibilidade e redundância.

1.2.3.1 Implementação de um protocolo MSTP A fim de ter implementado é necessário seguir os seguintes passos:

1. Definir a região MST, que é um grupo de switches que utilizam o MSTP e têm os mesmos parâmetros de configuração (nome, número de revisão e o mapeamento VLAN por instância), sendo crucial configurar para todos os switches regionais.

2. Configurar a instância MST (número, root bridge, papéis de porta).
3. Configurar a fronteira MST, que é o ponto em que a região se conecta a outra região ou a uma rede não MST, sendo necessário configurar para cada fronteira (CIST e CST).

1.2.3.2 Vantagens e Desvantagens O protocolo auxilia a reduzir instâncias de Spanning Trees e BPDUs, o que pode ajudar na redução do uso da CPU e memória nos switches, além de melhor utilizar links redundantes e balancear a carga, assim como simplificar a configuração da rede e oferecer compatibilidade com versões anteriores como STP e RSTP.

Entretanto, é necessário bom planejamento para evitar caminhos subótimos e ciclos, requerendo configuração consistente em todos os switches, e nem sempre suporta dispositivos legados ou de terceiros que não implementaram MSTP.

1.3 Conceitos Fundamentais

Embora os protocolos apresentem variações em desempenho e funcionamento, todos compartilham um conjunto de conceitos fundamentais que definem como a topologia livre de loops é construída. A seguir serão apresentados os principais elementos comuns aos protocolos da família Spanning Tree.

1.3.1 Root Bridge

A Root Bridge é o elemento central da Spanning Tree. Ela representa o ponto de referência de toda a topologia lógica e é escolhida através de um processo de eleição entre todos os switches que participam do protocolo.

A Root Bridge sempre possui o menor Bridge ID e, a partir dela, os demais switches calculam os caminhos de menor custo para chegarem à raiz, determinando o papel das portas e como o tráfego será encaminhado.

1.3.2 Bridge ID

O Bridge ID é a identificação única de cada switch e é composto por dois elementos: a prioridade do bridge e o endereço MAC do switch. O valor mais baixo representa o switch mais preferencial. Esse identificador é usado durante a eleição da Root Bridge e na determinação dos caminhos da topologia.

1.3.3 Eleição

O processo de eleição é responsável por determinar qual switch será a Root Bridge. Os switches elegem com base no Bridge ID, sendo escolhido aquele com o menor valor. Quando um switch inicializa-se, ele não sabe o valor do ID de todos os outros switches da topologia e então se elege como Root Bridge. Quando ele recebe um BPDU com um BID root menor que o dele, ele imediatamente para de anunciar-se como root e começa a encaminhar o valor do Root Bridge superior.

1.3.4 Path Cost

O Path Cost é o custo associado às portas dos switches e depende da velocidade do enlace. Quanto maior a largura de banda, menor é o custo. Esse valor é utilizado para calcular o caminho mais eficiente até a Root Bridge. Em caso de múltiplas rotas possíveis, o caminho com o menor custo total é selecionado como o caminho principal.

1.3.5 Port States

Para evitar loops, os switches operam suas portas em estados específicos que definem como cada porta participa da Spanning Tree. Discarding, Learning e Forwarding foram os estados explicados no RSTP, mas para o STP são cinco estados: Disabled, Blocking, Listening, Learning e Forwarding.

O primeiro não participa nos cálculos; o segundo ocorre na primeira inicialização, não encaminhando nenhum tráfego e apenas aguardando por BPDUs, aprendendo a topologia sem causar loops; o terceiro não encaminha frames, mas começa a enviar e receber BPDUs, auxiliando a anunciar sua presença e a se preparar para se unir à topologia; o quarto é a fase em que começa a aprender os endereços MAC observando os frames encaminhados, mas ainda sem encaminhar tráfego; e, finalmente, o quinto estado ocorre quando a porta é selecionada para ser parte da topologia sem loops, podendo tanto enviar quanto receber frames e BPDUs.

Esse estados são fundamentais para controlar o encaminhamento e garantir que a topologia lógica esteja estável antes de permitir o tráfego completo.

1.3.6 Detecção de Loops

Assim que a eleição do root é completada, os switches começam a identificar loops. Os switches entendem que há um loop quando recebem BPDUs da Root Bridge por mais de uma interface; portanto, se receberem esses BPDUs por mais de uma porta, deve haver um loop, e essa porta deve ser colocada no estado de blocking.

1.3.7 Convergência

A convergência ocorre quando todos os switches da rede finalizam seus cálculos, selecionam os papéis das portas e ajustam seus estados, resultando em uma topologia estável e livre de ciclos. Tanto no STP quanto em suas versões mais modernas, esse processo garante que, mesmo com redundância física, a rede mantenha uma rota lógica confiável para o tráfego.

1.4 Objetivos Gerais e Específicos

Os objetivos deste trabalho estão divididos em um objetivo geral e objetivos específicos, conforme descritos a seguir.

1.4.1 Objetivo Geral

Projetar e configurar uma rede corporativa de médio porte utilizando STP, RSTP e MSTP, analisando seu comportamento, tempos de convergência e desempenho em situações de falha.

1.4.2 Objetivos Específicos

- Compreender o funcionamento dos protocolos STP, RSTP e MSTP.
- Criar uma topologia de rede redundante em laboratório ou ambiente de produção.
- Implementar e comparar os três protocolos em cenários distintos ou iguais.
- Medir o tempo de convergência e estabilidade da rede (mesmo em redes simuladas).
- Propor boas práticas para ambientes corporativos com múltiplas VLANs (item não obrigatório).

1.5 Arquitetura de Rede Proposta

A arquitetura de rede proposta para este projeto foi planejada visando redundância, escalabilidade e fácil gerenciamento. O ambiente simulado representa uma rede corporativa de médio porte, em que múltiplas VLANs coexistem e diferentes funções de camada de acesso, distribuição e núcleo são distribuídas entre os switches da infraestrutura.

A topologia geral é composta por:

- **2 switches de Core**, responsáveis pelo processamento central do tráfego, pela coordenação da topologia lógica dos protocolos STP, RSTP e MSTP e pela interligação entre os principais segmentos da rede.
- **2 switches de Distribuição**, atuando como camada intermediária entre o núcleo e os pontos de acesso, agregando enlaces redundantes e auxiliando no controle do fluxo entre os diferentes setores da rede.
- **10 hosts distribuídos**, utilizados para representar estações de trabalho e validar o funcionamento dos protocolos em condições próximas às de um ambiente corporativo real.

A rede foi estruturada seguindo o modelo hierárquico tradicional, permitindo observar o comportamento dos protocolos de Spanning Tree de maneira organizada. Os switches de Core desempenham o papel central na convergência da topologia, atuando como referências primária e secundária no cálculo da árvore livre de loops. Os switches de Distribuição formam caminhos alternativos e designados conforme as decisões dos protocolos, garantindo redundância e estabilidade no tráfego. Já os hosts representam os dispositivos finais conectados à arquitetura, permitindo a análise do encaminhamento, da convergência e das possíveis alterações na rede durante testes práticos.

A seguir, apresenta-se um diagrama conceitual da topologia da rede:

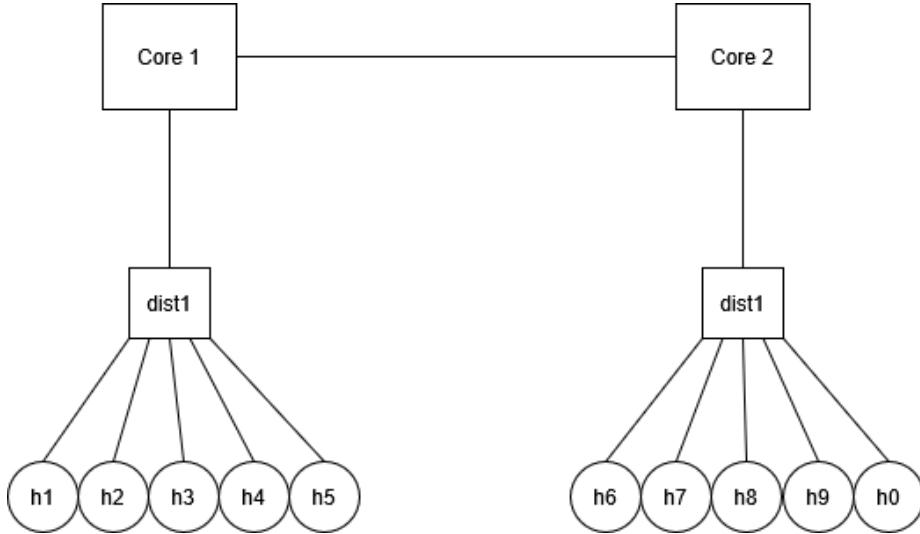


Figure 1: Diagrama Conceitual

Essa arquitetura permite observar o comportamento dos protocolos em situações de falha simulada, cortes de enlaces, mudanças de papéis de porta e análise do tempo de convergência em cada camada.

1.6 Endereçamento de IP e Esquema de VLANs

O endereçamento IP e a definição de VLANs são componentes essenciais para a organização lógica da rede, permitindo que os dispositivos sejam distribuídos de forma estruturada e que o tráfego seja segmentado conforme as necessidades operacionais da infraestrutura. A segmentação por VLANs possibilita separar departamentos, funções ou grupos específicos de equipamentos, reduzindo o domínio de broadcast e aumentando a segurança e o desempenho.

A definição de um esquema de VLANs permite que o tráfego seja isolado em nível de camada 2, enquanto o plano de endereçamento IP garante que cada segmento possua sua própria faixa de endereços, facilitando o roteamento, o controle de acesso e o gerenciamento geral da rede. Em ambientes corporativos, essas divisões lógicas auxiliam na organização do tráfego, na aplicação de políticas de rede e no suporte a múltiplos serviços simultaneamente.

Além disso, a presença de VLANs influencia diretamente o comportamento dos protocolos STP, RSTP e MSTP, uma vez que a topologia lógica pode variar conforme os segmentos configurados. Protocolos como o MSTP, por exemplo, permitem associar múltiplas VLANs a diferentes instâncias da spanning tree, otimizando caminhos redundantes e distribuindo a carga entre enlaces disponíveis.

Dessa forma, o endereçamento IP e o esquema de VLANs constituem a base

para uma infraestrutura organizada, segura e preparada para operar de maneira eficiente em conjunto com os mecanismos de prevenção de loops analisados neste trabalho.

Parte prática

2.1 - Rede Projetada

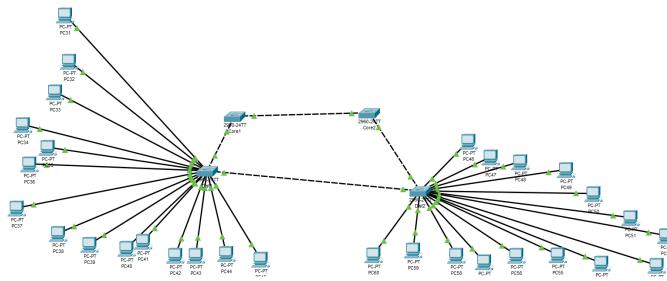


Figure 2: Topologia da rede projetada

2.2 — Configuração das VLANs

Configuração geral das VLANs

```
enable
conf t
vlan 10
  name ADMIN
vlan 20
  name FINANCEIRO
vlan 30
  name TI
end
```

Core1

```
enable
conf t
interface range fa0/1-2
  switchport mode trunk
  switchport trunk native vlan 1
exit
```

Core2

```
enable
```

```
conf t
interface range fa0/1-2
switchport mode trunk
switchport trunk native vlan 1
exit
```

Dist1

```
enable
conf t
interface range fa0/1-2
switchport mode trunk
switchport trunk native vlan 1
exit
```

```
interface range fa0/3-7
switchport mode access
switchport access vlan 10
exit
```

```
interface range fa0/8-12
switchport mode access
switchport access vlan 20
exit
```

```
interface range fa0/13-17
switchport mode access
switchport access vlan 30
exit
```

```
end
write
```

Dist2

```
enable
conf t
interface range fa0/1-2
switchport mode trunk
switchport trunk native vlan 1
exit
```

```
interface range fa0/3-7
switchport mode access
switchport access vlan 10
exit
```

```

interface range fa0/8-12
  switchport mode access
  switchport access vlan 20
exit

interface range fa0/13-17
  switchport mode access
  switchport access vlan 30
exit

end
write

```

2.3 — Protocolos de Spanning Tree

STP (IEEE 802.1D)

Em todas os switchs

```

conf t
spanning-tree mode pvst
end
wr

```

Conclusões

- **Root Bridge:** Core1
- **Portas bloqueadas:** Dist2 (Fa0/2)
- **Portas de encaminhamento:** todas as demais portas
- **Tempo de convergência:** 30–50 s

RSTP (IEEE 802.1w)

```

conf t
spanning-tree mode rapid-pvst
end
wr

```

No Core1:

```

conf t
spanning-tree vlan 1 priority 4096
end
wr

```

Nos demais (Core2 e Distribuição):

```

conf t
spanning-tree vlan 1 priority 32768
end
wr

```

Conclusões

- **Root Bridge:** Core1
- **Portas bloqueadas:** Core1 (Fa0/2)
- **Portas de encaminhamento:** todas as demais portas
- **Tempo de convergência:** 1–5 s

MSTP (IEEE 802.1s)

Os modelos de switches utilizados no simulador não oferecem suporte ao modo MSTP. No entanto, teoricamente os resultados esperados seriam:

- **Root Bridge:** Core1
- **Portas bloqueadas:** Core1 (Fa0/2)
- **Portas de encaminhamento:** todas as portas no Core1
- As demais portas seriam classificadas como *root* e *designated*
- **Tempo de convergência:** 1–5 s

Conclusão

Para os testes foi feito o ping entre dois computadores pertencentes a mesma LAN (10) mas em switchs de distribuição diferentes (Dist1 e Dist2) e para testar o teste de conexão foi cronometrado o tempo que os pacotes demoravam para voltar a serem enviados corretamente O protocolo RSTP se mostrou o melhor para a situação.

Referências Bibliográficas

PYNET LABS. **What Is Spanning Tree Protocol (STP) and How It Works?** Disponível em: <https://www.pynetlabs.com/spanning-tree-protocol-explained/>. Acesso em: 16 nov. 2025.

GLMTEC. **Entenda O Loop De Rede E Como Preveni-lo.** Disponível em: <https://glmtec.com.br/entenda-o-loop-de-rede-e-como-preveni-lo/>. Acesso em: 16 nov. 2025.

IFSC. **Redes locais: Caminhos Fechados Em LANs (loops).** Disponível em: https://moodle3.ifsc.edu.br/mod/book/view.php?id=312208&chapterid=56881&lang=pt_br. Acesso em: 16 nov. 2025.

IVANOV, I. **How Spanning-Tree works?** Disponível em: <https://www.networkacademy.io/ccna/spanning-tree/how-stp-works>. Acesso em: 16 nov. 2025.

IVANOV, I. **Introduction to Rapid PVST+.** Disponível em: <https://www.networkacademy.io/ccna/spanning-tree/introduction-to-rapid-pvst>. Acesso em: 16 nov. 2025.

PYNET LABS. **What Is Spanning Tree Protocol (STP) and How It works?** Disponível em: <https://www.pynetlabs.com/spanning-tree-protocol-explained/>. Acesso em: 16 nov. 2025.

PYNET LABS. **What Is MSTP Protocol (Multiple Spanning Tree Protocol)?** Disponível em: <https://www.pynetlabs.com/what-is-mstp-protocol/>.

TECNOLOGIA MAISVCH. **Compreendendo Os Protocolos STP, RSTP, PVST E MSTP: Principais Diferenças E Benefícios - Maisvch Technology.** Disponível em: <https://maisvch.com/pt/blog/qual-e-a-diferenca-entre-stp-mstp-pvst-e-rstp/>. Acesso em: 16 nov. 2025.

TP-LINK. **Práticas Recomendadas Para Evitar Loops De Rede Com a Solução Omada SDN | TP-Link Brasil.** Disponível em: <https://www.tp-link.com.br/support/faq/3898/>. Acesso em: 16 nov. 2025.

ZEYA, S.; KALAWAT, A. **Identificar E Solucionar Problemas De Flaps/Loop MAC Em Switches Cisco Catalyst.** Disponível em: https://www.cisco.com/c/pt_br/support/docs/lan-switching/spanning-tree-protocol-stp-8021d/221722-troubleshoot-mac-flaps-loop-on-cisco-cat.html. Acesso em: 16 nov. 2025.