

SPANNING TREE: COMO FUNCIONAM STP, RSTP E MSTP EM REDES ETHERNET

Entenda como Spanning Tree, STP, RSTP e MSTP evitam loops, elegem a root bridge, bloqueiam caminhos redundantes e devem ser projetados e testados.

SUMÁRIO

1. O QUE É SPANNING TREE PROTOCOL?	4
1.1. POR QUE OS LOOPS ETHERNET SÃO CRÍTICOS?	4
1.2. REDUNDÂNCIA FÍSICA NÃO SIGNIFICA QUE TODOS OS ENLACES PODEM ENCAMINHAR	4
2. COMO O SPANNING TREE CONSTRÓI A ÁRVORE	5
2.1. ELEIÇÃO DA ROOT BRIDGE	5
2.2. CUSTO DO CAMINHO	5
2.3. PAPÉIS DAS PORTAS	5
3. ESTADOS DAS PORTAS EM STP E RSTP	6
4. STP, RSTP E MSTP: QUAIS SÃO AS DIFERENÇAS?	6
4.1. STP CLÁSSICO	6
4.2. RSTP	6
4.3. MSTP	6
4.4. PVST+, RAPID PVST+ E INTEROPERABILIDADE	7
5. COMO PROJETAR A ROOT BRIDGE	7
5.1. ROOT PRINCIPAL E SECUNDÁRIA	7
5.2. UMA RAIZ POR VLAN OU POR INSTÂNCIA	7
5.3. ROOT BRIDGE DISTANTE DO GATEWAY	7
6. PORTAS DE BORDA E PROTEÇÕES ESSENCIAIS	7
6.1. PORTFAST OU EDGE PORT	8
6.2. BPDU GUARD	8
6.3. ROOT GUARD	8
6.4. LOOP GUARD	8
6.5. BPDU FILTER EXIGE CAUTELA	8
7. SPANNING TREE E LACP	8
8. SPANNING TREE EM ARQUITETURAS HIERÁRQUICAS	9
8.1. DOMÍNIOS LAYER 2 MENORES	9
8.2. ACESSO, DISTRIBUIÇÃO E CORE	9
8.3. NÃO USAR STP PARA COMPENSAR UMA ARQUITETURA INDEFINIDA	9
9. SPANNING TREE EM REDES INDUSTRIAIS	9
10. TEMPORIZADORES E CONVERGÊNCIA	9
11. MUDANÇAS DE TOPOLOGIA E TABELA MAC	10
12. MONITORAMENTO E DIAGNÓSTICO	10
13. COMO DIAGNOSTICAR PROBLEMAS DE SPANNING TREE	10

13.1. VERIFIQUE A RAIZ	10
13.2. VERIFIQUE PAPÉIS E ESTADOS	10
13.3. VERIFIQUE CUSTOS E PRIORIDADES	11
13.4. VERIFIQUE MUDANÇAS RECENTES	11
13.5. VERIFIQUE LACP E TRUNKS	11
14. ERROS COMUNS	11
15. PROJETO, TESTES E COMISSIONAMENTO	11
16. CONCLUSÃO	11
16.0.1. Arquitetura e organização da rede	13
16.0.2. Projeto, switching e ambientes industriais	13
16.0.3. Monitoramento e operação	13
16.0.4. Guias e materiais de aprofundamento	13

O **Spanning Tree Protocol** é o mecanismo que impede loops de camada 2 em redes Ethernet com enlaces redundantes. Ele permite manter caminhos alternativos entre switches, mas bloqueia logicamente as conexões que formariam um ciclo e as reativa quando ocorre uma falha.

Em uma rede sem proteção contra loops, um quadro broadcast, multicast desconhecido ou unicast desconhecido pode circular indefinidamente. Como o Ethernet não possui um campo equivalente ao TTL do IP, o tráfego pode se multiplicar, consumir os enlaces, desestabilizar as tabelas MAC e provocar indisponibilidade generalizada.

Este artigo explica como o Spanning Tree e suas evoluções — **STP, RSTP e MSTP** — elegem a root bridge, calculam caminhos, atribuem papéis às portas, tratam mudanças de topologia e devem ser projetados, protegidos, monitorados e testados.

1. O QUE É SPANNING TREE PROTOCOL?

Spanning Tree Protocol é uma família de protocolos de controle para redes Ethernet comutadas. Seu objetivo é construir uma topologia lógica sem loops sobre uma infraestrutura física que pode possuir múltiplos caminhos.

O protocolo não remove os enlaces redundantes. Ele seleciona um conjunto de portas que permanece encaminhando tráfego e mantém outras portas em estado de descarte ou bloqueio. Quando a topologia muda, a árvore é recalculada e um caminho alternativo pode entrar em operação.

1.1. POR QUE OS LOOPS ETHERNET SÃO CRÍTICOS?

Switches encaminham broadcasts por todas as portas pertencentes à mesma VLAN, exceto pela porta de entrada. Se existir um ciclo entre switches, o mesmo quadro pode retornar por outro caminho e ser novamente replicado.

Os principais efeitos são:

1.2. REDUNDÂNCIA FÍSICA NÃO SIGNIFICA QUE TODOS OS ENLACES PODEM ENCAMINHAR

Dois ou mais enlaces entre switches aumentam a resiliência, mas também podem formar loops. O Spanning Tree calcula uma árvore lógica com caminho único entre os segmentos. Os enlaces excedentes ficam disponíveis para contingência, salvo quando são combinados corretamente em uma agregação lógica, como LACP.

2. COMO O SPANNING TREE CONSTRÓI A ÁRVORE

O processo começa pela troca de **Bridge Protocol Data Units — BPDUs**. Essas mensagens transportam informações utilizadas para eleger a raiz e calcular os melhores caminhos.

2.1. ELEIÇÃO DA ROOT BRIDGE

A root bridge é o ponto de referência da árvore. O switch com menor Bridge ID é eleito como raiz. O Bridge ID combina prioridade e identificador do sistema, normalmente associado ao endereço MAC e, conforme a implementação, à VLAN ou instância.

Deixar a eleição depender dos valores padrão é um erro de projeto. Quando todos os switches possuem a mesma prioridade, o endereço MAC pode decidir a raiz, fazendo com que um equipamento de acesso ou uma posição inadequada assuma função central.

A arquitetura deve definir:

A raiz da rede não deve ser escolhida pelo acaso.

A A3A define root bridge, prioridades, caminhos, agregações e critérios de convergência dentro de uma arquitetura documentada e verificável.

Conhecer o serviço de Projeto de Telecomunicações

2.2. CUSTO DO CAMINHO

Cada interface possui um custo associado à velocidade do enlace. O switch soma os custos até a root bridge e escolhe o caminho de menor custo.

O custo pode ser ajustado para influenciar a seleção, mas mudanças manuais precisam ser documentadas. Configurações isoladas e não registradas tornam o comportamento difícil de prever durante falhas.

2.3. PAPÉIS DAS PORTAS

Os principais papéis são:

A root bridge não possui root port. Suas portas ativas para os segmentos normalmente são designated ports.

3. ESTADOS DAS PORTAS EM STP E RSTP

O STP clássico utiliza os estados blocking, listening, learning, forwarding e disabled. As transições dependem de temporizadores e podem levar dezenas de segundos.

O RSTP simplifica os estados operacionais:

A redução dos estados e o mecanismo de proposta e acordo permitem convergência mais rápida quando os enlaces são ponto a ponto e a topologia está corretamente configurada.

4. STP, RSTP E MSTP: QUAIS SÃO AS DIFERENÇAS?

4.1. STP CLÁSSICO

O STP tradicional foi originalmente associado ao IEEE 802.1D. Ele evita loops, mas depende fortemente de temporizadores para transições. Em redes atuais, sua convergência pode ser lenta para voz, vídeo, sistemas corporativos e aplicações industriais.

4.2. RSTP

O Rapid Spanning Tree Protocol foi introduzido pelo IEEE 802.1w e posteriormente incorporado ao conjunto de normas de bridges. Ele mantém compatibilidade com o STP, mas utiliza novos papéis, estados e mecanismos de sincronização.

O RSTP é normalmente a escolha mínima para redes Ethernet modernas quando ainda existe um domínio Layer 2 com caminhos redundantes.

4.3. MSTP

O Multiple Spanning Tree Protocol permite associar grupos de VLANs a diferentes instâncias de spanning tree. Assim, não é necessário manter uma árvore separada para cada VLAN, e diferentes conjuntos podem utilizar caminhos preferenciais distintos.

Uma região MST é identificada por parâmetros que precisam coincidir entre os switches, incluindo nome, revisão e mapeamento de VLANs para instâncias. Divergências fazem com que os equipamentos sejam tratados como pertencentes a regiões distintas.

4.4. PVST+, RAPID PVST+ E INTEROPERABILIDADE

Ambientes Cisco podem utilizar PVST+ ou Rapid PVST+, mantendo uma instância por VLAN. Isso oferece granularidade, mas aumenta o número de instâncias e BPDUs em redes com muitas VLANs.

Em ambientes multivendor, a interoperabilidade entre PVST, RSTP e MSTP deve ser analisada. A rede não deve depender de pressupostos sobre compatibilidade sem teste e documentação.

5. COMO PROJETAR A ROOT BRIDGE

A raiz deve ser posicionada de acordo com a arquitetura, não pela conveniência da configuração padrão.

Em um campus hierárquico, é comum definir os switches de distribuição ou collapsed core como raiz principal e secundária. O alinhamento com o gateway da VLAN reduz caminhos assimétricos e tráfego desnecessário entre switches.

5.1. ROOT PRINCIPAL E SECUNDÁRIA

O projeto deve definir prioridades explícitas. A secundária precisa estar em posição capaz de assumir a função sem criar gargalos ou caminhos inesperados.

5.2. UMA RAIZ POR VLAN OU POR INSTÂNCIA

PVST permite distribuir VLANs entre diferentes raízes. MSTP permite distribuir instâncias. Esse balanceamento só deve ser utilizado quando os caminhos, gateways e capacidades estiverem alinhados; caso contrário, cria complexidade sem ganho real.

5.3. ROOT BRIDGE DISTANTE DO GATEWAY

Quando a raiz Layer 2 e o gateway Layer 3 estão em lados opostos da topologia, o tráfego pode atravessar enlaces adicionais. Esse desenho aumenta latência, utilização e dependências durante falhas.

6. PORTAS DE BORDA E PROTEÇÕES ESSENCIAIS

O Spanning Tree precisa ser protegido contra conexões indevidas e BPDUs inesperadas.

6.1. PORTFAST OU EDGE PORT

Portas conectadas exclusivamente a endpoints podem entrar rapidamente em forwarding, evitando espera desnecessária. Essa configuração não deve ser aplicada indiscriminadamente em enlaces entre switches.

6.2. BPDU GUARD

BPDU Guard desabilita ou coloca em erro uma porta de borda que recebe BPDU. Ele ajuda a impedir que um switch não autorizado seja conectado a uma porta destinada a usuário, câmera, telefone ou servidor.

6.3. ROOT GUARD

Root Guard impede que uma porta aceite uma raiz superior à esperada. É útil em fronteiras onde um equipamento conectado não deve alterar a root bridge da rede.

6.4. LOOP GUARD

Loop Guard protege contra a condição em que uma porta deixa de receber BPDUs por falha unidirecional e poderia transitar incorretamente para forwarding.

6.5. BPDU FILTER EXIGE CAUTELA

Filtrar BPDUs pode remover a proteção contra loops. O recurso só deve ser utilizado em cenários claramente compreendidos e documentados. Em portas inadequadas, pode permitir que um enlace redundante entre em forwarding sem participação na árvore.

Switching, segmentação e hardening precisam formar uma única arquitetura.

A solução da A3A integra projeto, configuração, Cisco ISE, hardening, monitoramento, implantação e documentação técnica.

Conhecer a solução de Redes Cisco

7. SPANNING TREE E LACP

LACP combina vários enlaces físicos em uma única interface lógica. Para o Spanning Tree, um port-channel corretamente formado é visto como um único enlace.

Os membros precisam possuir parâmetros compatíveis. Quando apenas parte dos enlaces forma a agregação ou quando um lado está agregado e o outro não, podem surgir

bloqueios, inconsistências ou loops.

O projeto deve definir:

8. SPANNING TREE EM ARQUITETURAS HIERÁRQUICAS

A melhor maneira de reduzir riscos é limitar o alcance da camada 2.

8.1. DOMÍNIOS LAYER 2 MENORES

Quanto maior o domínio, maior o número de switches, VLANs estendidas, BPDUs e eventos de mudança de topologia. Fronteiras Layer 3 menores contêm falhas e tornam a convergência mais previsível.

8.2. ACESSO, DISTRIBUIÇÃO E CORE

Em arquiteturas hierárquicas, o Spanning Tree costuma operar principalmente entre acesso e distribuição. O core pode utilizar enlaces roteados, reduzindo dependência de bloqueio Layer 2.

8.3. NÃO USAR STP PARA COMPENSAR UMA ARQUITETURA INDEFINIDA

Spanning Tree é um mecanismo de proteção e convergência. Ele não substitui decisões sobre camadas, redundância, agregação, roteamento e domínios de falha.

9. SPANNING TREE EM REDES INDUSTRIAIS

Redes industriais podem utilizar RSTP ou MSTP, especialmente quando há switches gerenciáveis e topologias em anel ou malha parcial. Entretanto, protocolos industriais como MRP, DLR, PRP e HSR possuem objetivos e comportamentos distintos.

A escolha depende de:

Não se deve misturar mecanismos de redundância sem compreender qual protocolo controla cada enlace e como as fronteiras serão tratadas.

10. TEMPORIZADORES E CONVERGÊNCIA

Alterar hello time, max age ou forward delay sem um projeto consistente pode produzir instabilidade e incompatibilidade.

Em RSTP, a convergência rápida depende da detecção de enlace ponto a ponto, dos papéis das portas e da sincronização entre bridges. Links compartilhados, equipamentos legados ou configuração inconsistente podem forçar comportamento mais lento.

O critério de aceite deve medir o tempo real percebido pelas aplicações, não apenas o momento em que o switch indica forwarding.

11. MUDANÇAS DE TOPOLOGIA E TABELA MAC

Quando uma porta muda de estado, os switches precisam atualizar suas tabelas de encaminhamento. Mudanças frequentes podem provocar flooding temporário e aumento de tráfego.

Eventos repetitivos indicam problemas como:

12. MONITORAMENTO E DIAGNÓSTICO

Uma rede não deve depender apenas de inspeção manual após falha.

Devem ser monitorados:

SNMP, syslog, telemetria e backups de configuração ajudam a identificar mudanças e divergências.

13. COMO DIAGNOSTICAR PROBLEMAS DE SPANNING TREE

O diagnóstico deve começar pela topologia esperada e compará-la com o estado operacional.

13.1. VERIFIQUE A RAIZ

Confirme se a root bridge é o equipamento previsto em todas as VLANs ou instâncias relevantes.

13.2. VERIFIQUE PAPÉIS E ESTADOS

Identifique root ports, designated ports, alternate ports e interfaces inconsistentes. Uma porta bloqueada não é necessariamente defeito; pode ser o resultado correto do cálculo.

13.3. VERIFIQUE CUSTOS E PRIORIDADES

Custos manuais, prioridades de porta e velocidades negociadas incorretamente podem alterar o caminho escolhido.

13.4. VERIFIQUE MUDANÇAS RECENTES

Compare configurações, logs e eventos de topologia. A causa pode estar em uma porta de acesso conectada incorretamente, em um novo switch ou em uma alteração de trunk.

13.5. VERIFIQUE LACP E TRUNKS

Confirme se o port-channel está formado dos dois lados e se VLANs, native VLAN e parâmetros físicos coincidem.

14. ERROS COMUNS

15. PROJETO, TESTES E COMISSIONAMENTO

O projeto deve registrar:

Os testes devem incluir falha de uplink, membro de LAG, switch, fonte e rota física. É necessário registrar perda, tempo de convergência, mudança de papéis, alarmes e recuperação das aplicações.

Redundância só pode ser aceita quando a falha é realmente testada.

A A3A verifica topologia, papéis, convergência, alarmes, perda e recuperação das aplicações em cenários controlados.

Conhecer o serviço de Comissionamento e Aceite Técnico

16. CONCLUSÃO

Spanning Tree continua sendo um controle essencial em redes Ethernet com caminhos redundantes de camada 2. O protocolo precisa ser projetado: raiz, prioridades, custos, portas de borda, proteções, agregações e fronteiras devem ser explícitos.

RSTP oferece convergência mais rápida que o STP clássico. MSTP permite agrupar VLANs em instâncias e controlar diferentes árvores. A escolha deve considerar porte, interoperabilidade, operação e arquitetura.

O objetivo não é apenas impedir loops, mas construir uma rede previsível, observável e testável, capaz de convergir sem criar gargalos ou ampliar o domínio de falha.

- [1] IEEE. IEEE Std 802.1Q — Bridges and Bridged Networks. New York: IEEE.
- [2] IEEE. IEEE Std 802.1D-2004 — Media Access Control (MAC) Bridges. New York: IEEE, 2004.
- [3] IEEE. IEEE Std 802.1w-2001 — Rapid Reconfiguration of Spanning Tree. New York: IEEE, 2001.
- [4] IEEE. IEEE Std 802.1s-2002 — Multiple Spanning Trees. New York: IEEE, 2002.
- [5] CISCO SYSTEMS. Understanding Rapid Spanning Tree Protocol (802.1w). San Jose: Cisco.
- [6] OPPENHEIMER, Priscilla. Top-Down Network Design. 3. ed. Indianapolis: Cisco Press, 2011.

O que é Spanning Tree Protocol? É uma família de protocolos que evita loops em redes Ethernet comutadas, selecionando caminhos ativos e mantendo enlaces redundantes em estado de descarte até que sejam necessários. **Qual é a diferença entre STP e RSTP?** O STP clássico utiliza estados e temporizadores que podem tornar a convergência lenta. O RSTP simplifica os estados e utiliza mecanismos de proposta e acordo para reagir mais rapidamente a mudanças. **Para que serve o MSTP?** MSTP permite mapear grupos de VLANs para diferentes instâncias de spanning tree, reduzindo a quantidade de árvores e possibilitando caminhos preferenciais distintos. **O que é root bridge?** É o switch de referência da árvore. Todos os demais calculam o melhor caminho até ele. A root bridge deve ser definida por prioridade, e não deixada ao acaso. **Uma porta bloqueada pelo STP indica problema?** Não necessariamente. O bloqueio pode ser o comportamento correto para impedir um loop. É necessário comparar o estado com a topologia e o projeto esperados. **PortFast pode ser usado em qualquer porta?** Não. PortFast ou edge deve ser utilizado em portas conectadas a endpoints. Aplicá-lo indiscriminadamente em enlaces entre switches aumenta o risco de loops. **Como LACP se relaciona com Spanning Tree?** Um port-channel LACP corretamente formado é visto pelo Spanning Tree como um único enlace lógico. Configurações inconsistentes entre os lados podem causar bloqueios ou loops. **Como testar o Spanning Tree no comissionamento?** Devem ser simuladas falhas de enlaces, membros de LAG, switches e fontes, registrando papéis das portas, perda, tempo de convergência, alarmes e recuperação das aplicações.

Continue a trilha conforme o ponto que deseja aprofundar: arquitetura, projeto, switching, operação ou documentação.

16.0.1. Arquitetura e organização da rede

16.0.2. Projeto, switching e ambientes industriais

16.0.3. Monitoramento e operação

16.0.4. Guias e materiais de aprofundamento

Sobre a A3A Engenharia de Sistemas

Com 30 anos de história, a A3A Engenharia de Sistemas se consolidou como referência em serviços de Engenharia, oferecendo soluções integradas de Telecomunicações, Segurança Eletrônica, Segurança Digital e Instalações Elétricas.

A empresa atua em todas as etapas do ciclo de Engenharia, desde a elaboração de projetos e consultoria técnica até a implantação, manutenção e retrofit de sistemas, sempre em conformidade com as normas técnicas e melhores práticas do setor.