

RD Press

Guia Básico para Configuração de Switches

Alta Disponibilidade

Switches 3Com, H3C e HPN Serie-A

Diego Dias

RD PRESS

Guia Básico para Configuração de Switches – Alta Disponibilidade

© RD Press
Rotadefault.com.br
Comutadores.com.br

Autor: Diego Dias
Revisão: Millena Mota

Índice

| | |
|---|----|
| Introdução à Alta Disponibilidade de Switches Ethernet | 7 |
| Gateway e Roteamento..... | 10 |
| Alta Disponibilidade..... | 10 |
| Spanning-Tree..... | 12 |
| Resumo:Como funciona uma Rede Ethernet..... | 13 |
| Eleição do Switch Root..... | 16 |
| Forçando o Switch Root da Rede..... | 17 |
| Display STP..... | 18 |
| Evolução do STP (802.1d)..... | 19 |
| Explicando um pouco mais sobre o Rapid Spanning-Tree..... | 21 |
| Edge | 22 |
| Point-to-Point | 23 |
| Quais portas foram bloqueadas ou encaminham dados?..... | 24 |
| Custo das portas | 26 |
| Multiple Spanning-Tree | 31 |
| Configurando o MSTP..... | 33 |
| Posicionamento do Switch Root na topologia | 35 |
| Troubleshooting STP..... | 36 |
| Estudo de Caso 1..... | 37 |
| Link Aggregation..... | 40 |
| Configurando o Link Aggregation | 42 |
| Configuração para Comware 5 | 42 |
| Configuração para Comware 3 | 43 |
| Verificando o Link Aggregation..... | 44 |
| Configurando o Link Aggregation entre Cisco e HPN | 45 |
| Detalhes importantes para a agregação de portas em Switches ... | 48 |
| Estudo de caso 2..... | 49 |
| VRRP | 52 |
| Utilizando o VRRP | 54 |
| Eleição do Switch Master | 55 |
| VRRP Modo de Preempção | 57 |

| | |
|---|----|
| VRRP Load Balance | 58 |
| Configurando o VRRP Load Balance..... | 58 |
| Display para visualizar o modo do VRRP | 59 |
| Utilizando o VRRP com o MSTP | 60 |
| Estudo de caso 3 | 62 |
| IRF & XRN..... | 64 |
| Arquitetura IRF e XRN | 67 |
| Configurando o IRFv2, IRF e XRN | 68 |
| Configuração para o IRv2 | 69 |
| Display IRFv2 | 72 |
| Auto-update para o IRFv2 | 72 |
| Configuração para o IRF em Switches 3Com 4800G | 73 |
| Auto-update para o IRF em Switches 3Com 4800G | 75 |
| Display IRF..... | 75 |
| Agregação de portas para o IRF para Switches 4800G | 76 |
| Configuração para o XRN | 77 |
| Configuração do XRN para Switches 3Com 5500 | 78 |
| Display XRN | 81 |
| Problemas na conexão entre os Switches do IRF (IRF Split) | 82 |
| Configurando MAD com LACP | 83 |
| Configurando MAD com BFD | 85 |
| Após a correção da falha..... | 87 |
| Apêndice A..... | 89 |

Quem deve ler esse livro?

Esse livro pode ser utilizado por técnicos ou administradores de Switches Ethernet da 3Com, H3C e HPN Serie-A, familiarizados com a configuração de VLANs e a comunicação entre as redes.

O ebook também servirá para administradores com formação Cisco que desejam por necessidade profissional gerenciar um ambiente com diversos vendedores.

Apesar do título do livro ser **Guia Básico para Configuração de Switches – Alta Disponibilidade**, o conteúdo abordado no eBook poderá ser relacionado à materiais de Certificação de Nível Intermediário como HP ASE Network Infrastructure e CCNP da Cisco. Mas o foco não são os exames de certificação, e sim os comandos e cenários do dia-a-dia de um administrador de Redes.

Agrego a esse material minhas experiências como administrador de redes de pequeno e médio porte, incluindo a administração de Data Centers.

O Livro inclui estudos de caso para análise de topologias similares a cenários reais, trabalhando de forma progressiva desde o gerenciamento de uma rede com Spanning-Tree, LACP, VRRP até a utilização de Stacking/Clusterização (XRN ou IRF) de Switches para prover redundância na rede local.

Agradecimentos

A atividade de escrever o segundo eBook foi muito prazerosa. Houve uma boa aceitação do primeiro livro, muitos contatos e novas amizades que surgiram.

Assim como no volume anterior, não consegui exemplificar nesse material tudo o que gostaria, mas a conclusão do material é uma grande vitória.

Gostaria de agradecer aos meus amigos do Rota Default: Roger Sales e Ricardo Amaral, pela amizade e companherismo.

Gostaria de agradecer também ao colaborador indireto do Rota Default Paulo Roque, pela troca de experiência e desafios; e aos amigos da HP.

Para finalizar, quero agradecer a minha Mãe, quero agradecer a minha companheira (muito paciente) Millena Mota pela ajuda na revisão do material, e louvar a Deus pela compreensão e entendimento a cada dia sobre a vida e pela paz!

*Grandes coisas fez o SENHOR por nós, pelas quais estamos alegres. **Salmos 126:3***

Introdução à Alta Disponibilidade de Switches Ethernet

Este capítulo é uma breve introdução à necessidade da Alta Disponibilidade para a LAN

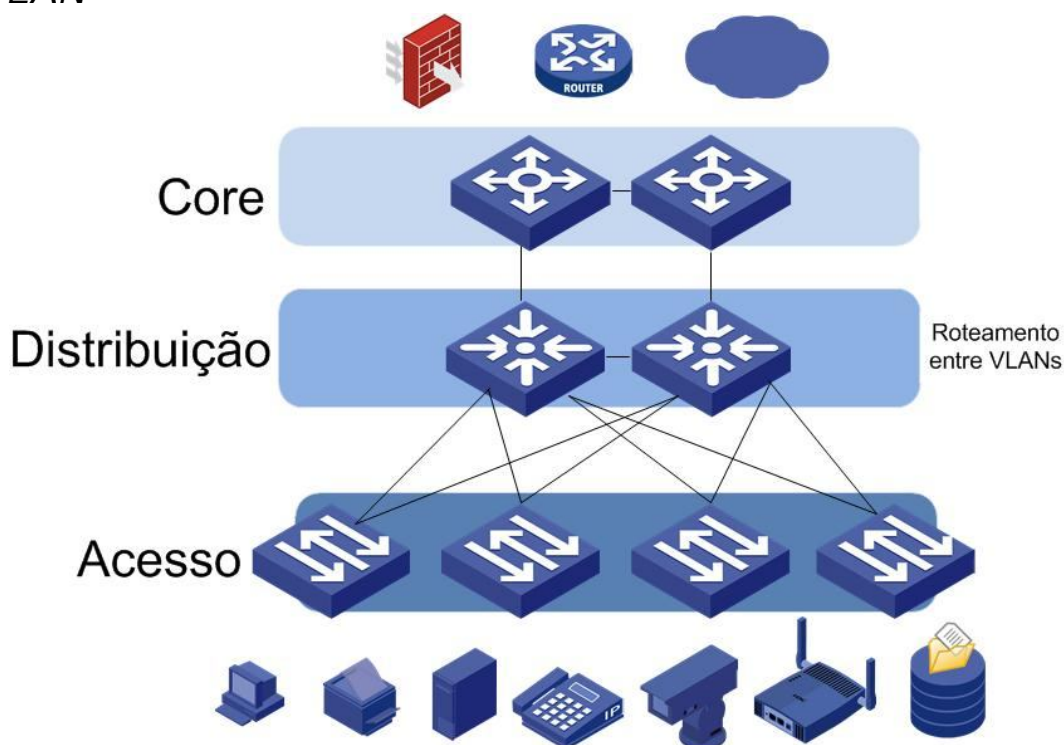
Uma rede de computadores consiste em 2 ou mais dispositivos interligados entre si, de modo a compartilhar recursos físicos e lógicos por um padrão de endereçamento lógico, para troca de informações.

Para a comunicação de diversos equipamentos em uma Área de Rede Local (LAN), utilizamos dispositivos que proveem uma quantidade necessária de portas para acesso aos computadores, servidores e etc, como os Switches.

Com a demanda de redes altamente disponíveis e confiáveis, faz-se necessário a criação de uma topologia de rede resiliente, com caminhos e equipamentos redundantes oferecendo maior tempo de atividade e eliminando pontos únicos de falha.

Os serviços oferecidos aos clientes internos e externos das Empresas necessitam de funcionamento 24 horas por dia, 7 dias por semana e 365 dias por ano, com o SLA de noventa e nove por cento de disponibilidade, oferecido para se ganhar vantagem de mercado.

Exemplo 1-1 *Disposição Hierárquica em camadas para os equipamentos da LAN*



A função básica de um Switch é encaminhar pacotes IP, baseado na leitura de endereço MAC do cabeçalho Ethernet, montando uma tabela de endereços MAC pela monitoração de mensagens trocada pelos equipamentos antes de iniciarem a sua comunicação.

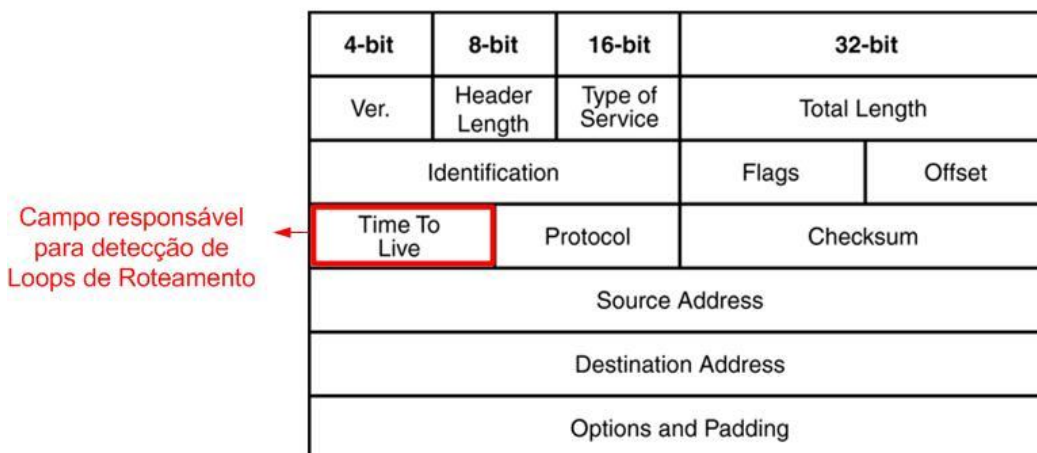
Com o passar dos anos diversas funções foram atribuídas aos Switches Ethernet, tornando-os equipamentos estratégicos para Rede Local, incluindo funções de roteamento de alto desempenho, Stacking/ Clusterização, Balanceamento de tráfego, Firewall, Qualidade de Serviço, etc. **A redundância em uma Rede Local tornou-se item indispensável para os dias atuais**, permitindo a criação de caminhos de redes com equipamentos redundantes.

Apesar do cabeçalho IP possuir mecanismo para detecção de Loop na rede, como o campo TTL, a comunicação entre equipamentos dentro da mesma sub-rede (provida pelo Switch Ethernet) **não utiliza-se dessas informações (do cabeçalho IP)**, e sim, campos do cabeçalho Ethernet, sendo assim, a informação não é lida e o loop não é identificado. Nesse cenário, para Alta Disponibilidade, o loop lógico ocasionado pelo loop

físico derrubaria a rede com um dos comportamentos conhecidos como tempestade de Broadcast.

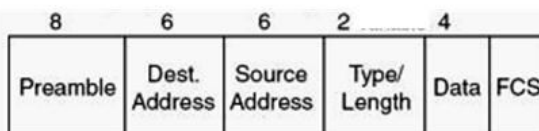
Exemplo 1-2 *Comparação do Cabeçalho IP e do Cabeçalho Ethernet*

Cabeçalho IP



Cabeçalho Ethernet

Ausência de Campo para detecção de Loops



Para eliminar o loop lógico (ocasionado pelo loop físico) faz-se necessário a utilização de protocolos auxiliares para resolver a questão.

O protocolo mais utilizado para detecção de loops na LAN (e também um dos mais "odiados") é o Spanning-Tree (STP), as vezes denominado como um "mal necessário".

Há anos prevemos a substituição do STP com protocolos como o TRILL ou SPB, mas a grande parte das Redes Locais é ainda totalmente dependente de protocolos com variações do STP como o PVST, RSTP e o MSTP.

Alguns cenários também incluem a utilização de protocolos proprietários para topologia em anel com o RRPP, protocolos para


agregação de portas como o LACP, “Stacking” ou features em cenários específicos como o Smart-Link e/ou Monitor-Link.

Termos como SDN (Software Defined Networking), descrevem uma arquitetura que separa o Plano de Dados do Plano de Controle. Com o SDN, o Plano de Controle é administrado em um Software Centralizado separado do equipamento de rede e é independente de soluções e protocolos dos fabricantes (desde que soluções abertas sejam utilizadas), abrindo um caminho para a customização da Rede Local e o surgimento de novas soluções.

Gateway e Roteamento

Com a função de Gateway também atribuída aos Switches para Roteamento entre VLANs, o protocolo VRRP (Virtual Router Redundancy Protocol) tornou-se uma ferramenta importante para a redundância de Switches que atuam como Gateway das VLANs, mantendo o roteamento de pacotes mesmo em caso de falhas em um dos Switches.

Técnicas de “Clusterização” ou também conhecida como “Stacking” de Switches com os protocolos XRN, IRF e IRF versão 2, também são utilizadas como alternativas para facilitar a administração e estabilidade da LAN com o Switch “slave” assumindo a função principal na falha do “master”.

 ***O termo Stacking/Empilhamento também é utilizado para denominar a ação de conectar um Switch ao outro via UpLink. Nesse eBook, utilizaremos o termo para identificar a administração de 2 ou mais Switches como um único equipamento.***

Alta disponibilidade

Uma rede bem estruturada, segmentada em camadas como Core, Distribuição e Acesso, ou com o Núcleo Colapsado somente com as camadas de Core e Acesso (para os Switches) facilita a disposição de novos equipamentos na LAN, além da estrutura física necessária, como

cabeamento, energia elétrica e a redundância de equipamentos, incluindo também a parte lógica.

Nesse volume focaremos as principais features para prevenção de Loop como Spanning-Tree (802.1d, 802.1w e 802.1s), Link-Aggregation (802.3ad), alta disponibilidade do Gateway utilizando o VRRP e o empilhamento de Switches com as features proprietárias da 3Com/H3C/HP (XRN, IRF e IRFv2), que acrescentam maior inteligência aos dispositivos.

Boa leitura!

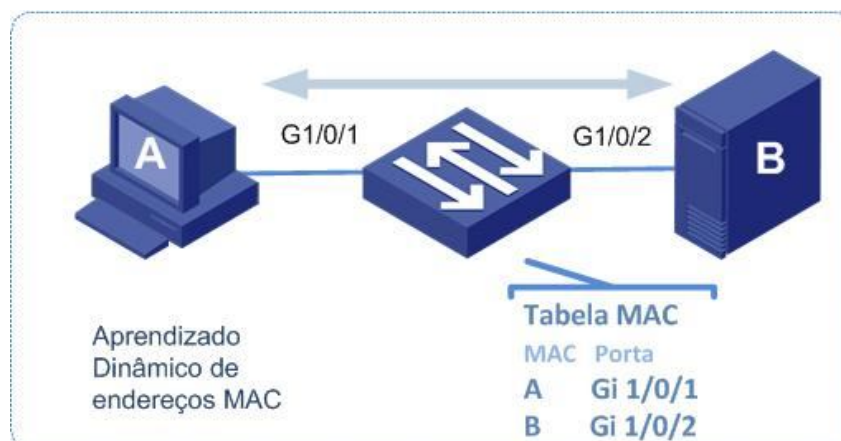
Spanning-Tree

O Protocolo Spanning-Tree é responsável por uma rede livre de loops e com caminhos redundantes em caso de falha no link principal...

O sucesso do protocolo Ethernet em Switches deve-se a sua função Plug&Play do protocolo para o funcionamento em uma Rede Local. Com pouca ou quase nenhuma configuração, é possível estabelecer a comunicação de todos os equipamentos de uma empresa, imaginando que a rede utilize um servidor DHCP, por exemplo.

A inteligência dos Switches Ethernet vem da capacidade de monitorar as mensagens trocadas entre dispositivos da rede (como os computadores) e montar uma tabela com o mapeamento de endereços MAC vinculado às portas do Switch.

Exemplo 2-1 *Comportamento Plug&Play de um Switch Ethernet*



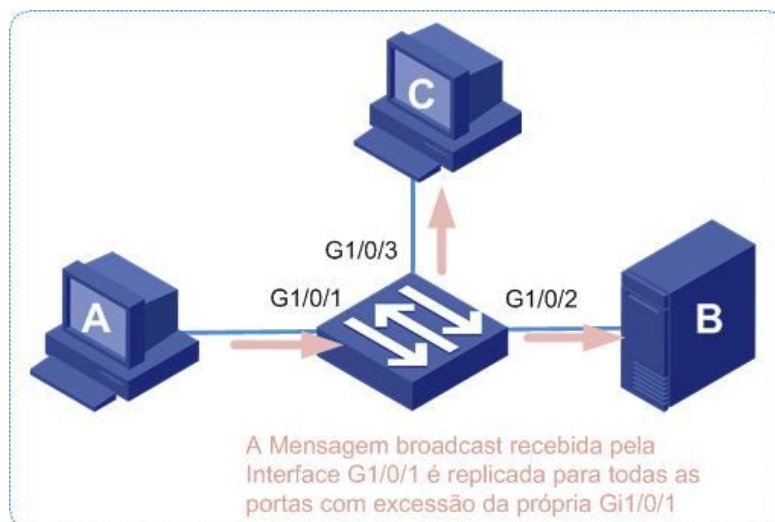
Resumo: Como funciona uma rede Ethernet?

As mensagens trocadas entre computadores para descoberta dinâmica de hosts com endereço IPv4 para comunicação, possuem comportamento Broadcast .

O Switch, ao receber uma mensagem Broadcast, encaminha a informação para todas as portas, exceto para a porta que recebeu a mensagem inicial.

Já para os host com endereços em IPv6, as mensagens para descoberta de vizinhos e roteadores são em endereços Multicast, mas o comportamento inicial da mensagem é muito similar (para um Switch) a uma mensagem Broadcast.

Exemplo 2-2 Comportamento do Switch ao receber uma mensagem Broadcast



O que é um loop Ethernet?

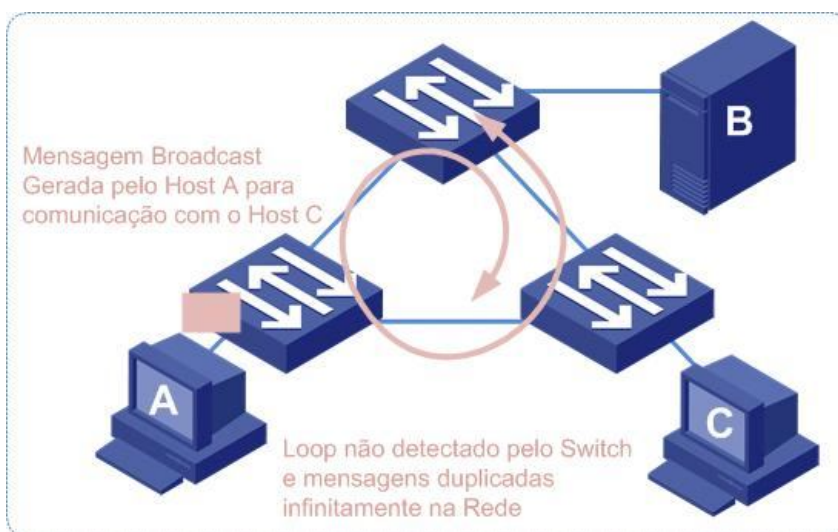
Toda vez que um Switch recebe um frame Ethernet, faz uma busca em sua tabela MAC para encaminhar o "pacote" para a interface correta. **Caso a informação não exista ou seja Broadcast ou Multicast para a rede local, ela é inundada para todas as portas.**

" Quando um Switch recebe um broadcast, ele o repete em cada porta (exceto naquela em que foi recebido). Em um ambiente com loop, os broadcasts podem ser repetidos infinitamente" (Gary A. Donahue , Network Warrior, O'Reilly, 2007, p.59)

O comportamento de flooding (inundação, em uma tradução livre) é essencial para a comunicação entre equipamentos da rede local e o aprendizado dinâmico de endereços via Switch.

A partir do momento que a nossa LAN torna-se complexa, o comportamento de flooding do Switch torna-se um problema para caminhos redundantes na comunicação entre equipamentos da rede.

Exemplo 2-3 Loop Ethernet gerado pela redundância de caminhos



A mensagem broadcast gerada pelo **host A** para o **host C**, ao chegar ao Switch é encaminhada para todas as portas, e o comportamento continua a ser replicado por todos os Switches da rede infinitamente.

STP (Spanning-Tree)

O Protocolo Spanning-Tree utiliza um algoritmo para detecção de caminhos alternativos colocando as interfaces redundantes em modo temporário de bloqueio, eliminando o loop lógico.

A grande maioria dos Switches do mercado já vem com o Spanning-Tree habilitado.

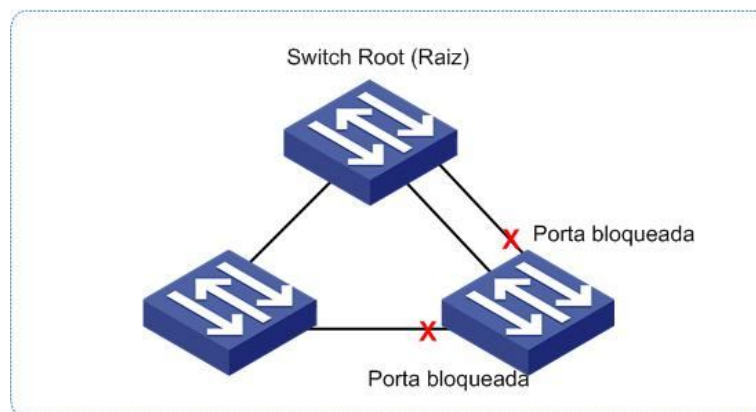
Ao tirarmos um Switch da caixa e colocarmos na rede, haverá a comunicação com todos os outros Switches para convergência e eliminação lógica de caminhos redundantes, favorecendo o comportamento Plug&Play do Protocolo Ethernet.

Todo Switch da LAN , ao iniciar, encaminha e recebe informações sobre os outros Switches da rede através da troca de mensagens chamadas BPDUs (Bridge Protocol Data Units). Os BPDUs são os responsáveis pelo correto funcionamento do algoritmo do Spanning-Tree e são encaminhados a cada 2 segundos em todas as portas.

O Objetivo do STP é eliminar loops na rede com a negociação de caminhos livres através do Switch Root (Raiz). Dessa forma é garantido que haverá apenas um caminho para qualquer destino com bloqueio dos caminhos redundantes. **Se houver falha no enlace principal, o caminho em estado de bloqueio torna-se o principal.**

O algoritmo do STP (chamado STA) deve encontrar um ponto de referência na rede (Root) e determinar os caminhos disponíveis, além de detectar os enlaces redundantes e bloqueá-los.

Exemplo 2-4 Escolha do Switch Root pelo STP e a eleição dos caminhos bloqueados.



Sempre será escolhido pelos Switches o melhor caminho até o Switch Root para encaminhamento de dados.

A utilização do STP é geralmente imperceptível devido ao fato da convergência e da troca de mensagens do protocolo ocorrer sem a necessidade de configurações adicionais.

Atualmente a grande maioria dos Switches Ethernet do mercado, como Cisco, 3Com, Procurve, HPN, Dell e etc., possuem o Spanning-Tree ativo ou a possibilidade de ativação do protocolo.

Eleição do Switch Root

A idéia básica por trás do algoritmo Spanning-tree é que os Switches transmitam mensagens entre si que os permitam calcular uma nova topologia, livre de loops.

As mensagens BPDU's geradas, contêm informações de configuração suficientes para que os Switches elejam para quais portas encaminharão os dados, baseando-se em custo do caminho, informações do Switch e informações da porta. Pois é pensado no algoritmo que uma porta com custo de 100Mb é estatisticamente mais "lenta" que uma interface de 1Gb para grande vazão de dados.

O valor principal para eleição do Root (comparado entre todos os Switches da LAN) é o valor **Bridge ID**, composto da prioridade e do **endereço MAC do Switch**. Por default todos os Switches vêm de fábrica com o valor da Prioridade para **32768**. Vence a eleição quem tiver a menor prioridade, e, em caso de empate, é verificado o endereço MAC do dispositivo.

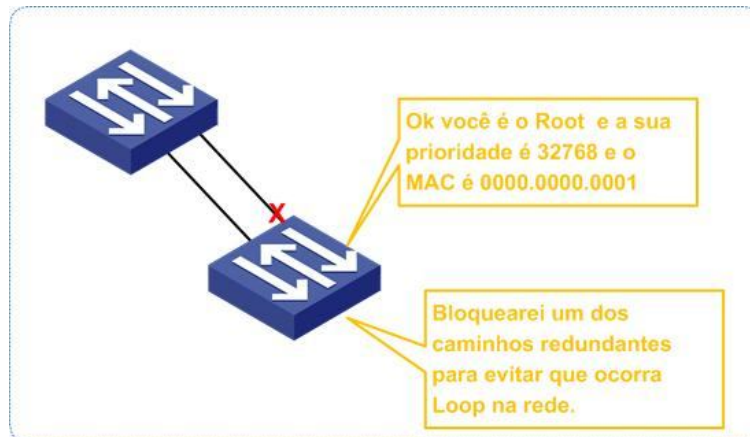
Mesmo que os Switches da rede local tenham escolhido um Switch como Root, caso um novo equipamento encaminhe um **BPDU Superior** (com melhor valor de Bridge ID), a topologia deverá convergir a partir do novo Switch Raiz.

Exemplo 2-5 Troca de mensagens entre os Switches para eleição do Root.



Após a eleição, se houver algum caminho redundante, o mesmo será bloqueado!

Exemplo 2-6 *Após eleição do Switch Root, os caminhos redundantes são bloqueados nos Switches não-Root*



Baseado nas informações do **Bridge ID** dentro dos BPDUs, os switches são capazes de:

- Para o **Switch Root**:
 - Eleger um Switch único, entre todos da LANs, para ser o Root Bridge (Raiz).
- Para os **Switches não-Root**:
 - Calcular a distância do caminho mais curto para o Raiz (Root Bridge).
 - Eleger uma porta designada (**designated port**) para cada segmento.
 - Eleger a porta root (**root port**) que dá o melhor caminho para Root.
 - As portas não selecionadas serão colocadas em estado de **bloqueio**.

Forçando o Switch Root da rede

As melhores práticas sugerem a configuração do Switch Core da rede como Root utilizando o comando **stp root primary** que alterará a prioridade para o valor 0 (zero), forçando o dispositivo a ser o Raiz.

A escolha deverá ser estratégica pela posição privilegiada do equipamento na rede, melhor arquitetura, processamento, etc.

Exemplo 2-7 Alterando o Bridge Priority do Switch

```
<Switch> system-view  
[Switch] stp root primary  
! Forçando a prioridade do Switch (Bridge Priority) para o  
valor 0 (zero)
```

Uma segunda maneira de alterar a prioridade Switch é pela utilização do comando **stp priority 4096** (sempre escolha valores múltiplos de 4096)


Obs: Se houver mais de um Switch com a prioridade 0, vence a eleição quem possuir o menor endereço MAC.

Display STP

O comando **display stp** exibe informações como o valor do Bridge ID (Bridge priority e endereço MAC) do Switch e do Root, timers, etc.

Exemplo 2-8 Verificando o valor do Bridge ID (Bridge Priority e o endereço MAC) do Switch e do Switch Root da LAN.

```
[Switch]display stp  
-----[CIST Global Info][Mode STP]-----  
CIST Bridge : 32768.0000-0000-1234  
! Lista a Prioridade do Switch como 32768 e o endereço MAC  
0000-0000-1234  
Bridge Times : Hello 2s MaxAge 20s FwDly 15s MaxHop 20  
CIST Root/ERPC : 0.0000-0000-abcd/ 20000  
! A linha exibe a prioridade do Switch Root da Topologia  
como 0 (zero nesse caso) e o endereço MAC 0000-0000-abcd  
<saída omi ti da>
```

 Algumas versões do Comware 5 para os Switches HPN série A, possuem como padrão o STP desabilitado.

Exemplo 2-9 *Verificando se o STP está desabilitado no Switch e habilitando o protocolo.*

```

<Switch> system-view
[Switch] display stp
Protocol Status      : disabled
Protocol Std.        : IEEE 802.1s
Version              : 3
Bridge-Prio.         : 32768
MAC address          : 000f-e203-0200
Max age(s)           : 20
Forward delay(s)    : 15
Hello time(s)        : 2
Max hops             : 20
! Identificando que o STP está desabilitado no Switch
[Switch] stp enable
%Jun 18 16:21:10:253 2012 Switch MSTP/6/MSTP_ENABLE: STP is
now enabled on the device.
! Habilitando o Spanning-Tree no Switch e a mensagem de log
exibida na console
[Switch] display stp
-----[CIST Global Info][Mode MSTP]-----
CIST Bridge          : 32768.000f-e203-0240
<saída omitida>

```

Evolução do STP (802.1d)

A versão inicial do protocolo Spanning-tree chamada de 802.1d começou a tornar-se ineficiente com o passar dos anos, conforme as exigências de disponibilidade e desempenho da rede aumentavam. Em casos de falha do enlace principal, a convergência poderia levar até 50 segundos para o link redundante (em estado de bloqueio) gerando um grande tempo de instabilidade em toda a rede.

O IEEE atualizou a versão do protocolo e resolveu alguns problemas, como o tempo de convergência, e foi bem aceito pelo mercado, sendo chamado de Rapid Spanning-Tree (RSTP/802.1w).

A versão melhorada do protocolo evoluiu o tempo de convergência de forma significativa **para resultados práticos de até 2 (dois) segundos.**

