Utilizando Spanning Tree Protocol como uma estratégia para melhoramento da rede do campus

Raiela Quirino Lima[1], Rômulo Nunes de Oliveira[1]

[1]Universidade Federal de Alagoas (UFAL) – Campus Arapiraca
Avenida Manoel Severino Barbosa, s/n – Bom Sucesso, 57309-005 – Arapiraca – AL

raiela.lima@arapiraca.ufal.br, romulo@nti.ufal.br

Abstract. *The importance of computer networks for companies has become notorious over time: the sending and receiving of information by employees, access to servers and protection of the company dependent on access to network resources. Because of this, there was a concern to prevent the network from becoming inoperative due to natural failures, which can be avoided. For this, an available protection is the implementation of the RSTP protocol in the equipment, which allows a redundant connection between them. In other words, if a path connecting the switches is lost, it is possible to activate an alternative route, preventing the network from being broken. This article discusses the implementation of this protocol in a part of the Campus Arapiraca network.*

Resumo. *A importância das redes de computadores para instituições tornou-se notória ao decorrer do tempo: o envio e recebimento de informações por parte dos funcionários, o acesso a servidores e a proteção da empresa dependem do acesso a recursos da rede. Por conta disso, surgiu a preocupação de evitar que a rede fique inoperante por falhas naturais, que podem ser evitadas. Para isso, uma proteção disponível é a implementação do protocolo RSTP nos equipamentos, que possibilita a conexão redundante entre eles. Ou seja, caso um caminho que conecta os switches seja perdido, é possível ativar uma rota alternativa, evitando que a rede fique desconectada. Este artigo aborda a implementação desse protocolo em uma parte da rede do Campus Arapiraca.*

1. General Information

Os computadores conectados em rede tornaram-se um importante mecanismo de disseminação de informações, colaboração e interação, independente da localização geográfica. Ao longo dos anos, como afirma [Catalani 2006], a tecnologia da Internet revolucionou a forma de se trabalhar com os computadores, que deixaram de ser apenas máquinas para armazenar e processar informações, e passaram a ser utilizados como ferramentas de comunicação. Além disso, a evolução dos equipamentos, com a chegada de microcomputadores e celulares, por exemplo, tornou praticamente impossível para a sociedade sobreviver sem o suporte das redes de computadores. Esse fenômeno também afetou o ambiente corporativo, que viu a importância da rede de computadores se intensificar ao passar dos anos. Atualmente, as empresas possuem sistemas de telefonia e de câmeras de segurança, bem como serviços imprescindíveis para o seu funcionamento, dependendo da comunicação via Internet ou de uma infraestrutura robusta de rede interna.

Naturalmente foram surgindo preocupações quanto a esse fenômeno, como o fato de manter a segurança das informações que trafegam na rede, proteger os equipamentos e *softwares* de ataques de terceiros. Assim como prover capacidade à rede de se manter

funcionando mesmo com eventuais problemas naturais, que afetem a integridade da comunicação entre os equipamentos. A esse último problema está atrelado o conceito de resiliência da rede. Segundo a abordagem sistemática sobre o assunto, feita por [Smith *et al.* 2011], resiliência diz respeito à capacidade de uma rede de se defender e manter um nível aceitável de serviço na presença de tais desafios naturais. Este é um problema para o qual as empresas e corporações devem se atentar, uma vez que possuem serviços críticos que não podem ser interrompidos.

Ainda no aspecto de resiliência, é importante falar sobre a redundância em rede de computadores. Esse artigo trata redundância como a duplicidade controlada de rotas que interconectam os diversos *switches*, distribuídos em localidades diferentes da infraestrutura de redes. Elas são importantes porque possibilitam caminhos alternativos caso a comunicação operante entre os dispositivos falhe. Porém precisam ser tratadas, porque senão causam *loop* infinito[1] e o consumo de toda memória dos equipamentos, já que os dados ficam sendo retransmitidos de modo infinito sem chegar ao destino final. É justamente nesse ponto que está o problema: redundâncias não podem estar ativas, mas devem existir. Porque se um *switch* A estiver conectado a um *switch* B por apenas um caminho e este caminho for quebrado por alguma causa natural, a rede ficará isolada em um dos locais. Mas se houver uma outra via, que possa servir de alternativa, ela poderá ser ativa nessa situação e servir de rota *backup*.

Para possibilitar a redundância sem prejudicar o funcionamento da rede, o *Spanning Tree Protocol* (STP) foi criado com o intuito de eliminar a existência dos *loops*. O aperfeiçoamento deste protocolo surgiu devido a necessidade de diminuir o tempo de convergência da rede. O *Rapid* STP (RSTP) é uma evolução do STP que otimiza o tempo de decisão do protocolo. Há, ainda, uma outra variação, chamada MSTP, que considera não apenas a rede física, mas também a configuração virtual. Ou seja, as VLANs (*Virtual Local Area Network*) existentes também são analisadas para formar a topologia final. No entanto, para redes relativamente pequenas não é necessário considerar a distribuição virtual, sendo suficiente apenas implementar o protocolo RSTP.

Sabendo dos benefícios desse protocolo, foi escolhido implementá-lo em uma parte da rede do campus de Arapiraca, da Universidade Federal de Alagoas. A instituição tem a necessidade de possuir uma rede resiliente, uma vez que é responsável pela comunicação entre docentes, discentes, além de todas as outras pessoas que trabalham nela. Além disso, existem serviços de alta importância que dependem da rede, como a administração e o serviço de monitoramento por câmeras. Tais serviços não podem ficar propensos a falhas simples, como a de não possuir mais de uma alternativa ligando os dispositivos que formam a rede.

A implementação do protocolo foi feita em quatro *switches* da rede, escolhidos justamente devido a importância dos serviços pelos quais são responsáveis. Eles estão localizados em locais muito relevantes da universidade: NTI (Núcleo de Tecnologia da Informação), que recebe o *link* principal de Internet e onde estão todos os servidores; Administração 1, onde está localizada a sala de segurança, lugar em que acontece o monitoramento em tempo real de todas as câmeras do campus; Administração 2, possuindo salas de coordenações de cursos e de monitoria, além de outros serviços; e

[1] Diferentemente dos roteadores, os *switches* não decrementam o campo TTL (*Time To Live*), presente no cabeçalho dos pacotes que trafegam na rede. Dessa forma, os pacotes tendem a serem propagados infinitamente entre os equipamentos conectados em uma topologia cíclica.

Guarita, que possui as câmeras que registram todas as entradas e saídas do campus.

2. Referencial Teórico

O *Spanning Tree Protocol* implementa o algoritmo definido pelo padrão IEEE 802.1D e sua configuração é feita nos *switches*. A [Hojjat et al. 2016] define a forma de funcionamento do protocolo dizendo que os *switches* configurados com o protocolo trocam mensagens BPDU (*Bridge Protocol Data Unit*) com outros *switches* para detectar *loops* e, em seguida, removê-lo ao desligar interfaces selecionadas. Este algoritmo garante que haja apenas um caminho ativo entre dois dispositivos de rede, embora possa existir mais de uma alternativa os ligando fisicamente.

Quando este protocolo está implementado, não há necessidade de configuração manual, caso a comunicação entre dois *switches* seja perdida. Isso porque ele provê a capacidade desses equipamentos trocarem mensagens entre si, contendo informações sobre o seu estado de funcionamento. Dessa forma, quando percebem que estão sem comunicação com algum lugar, se organizam em uma nova topologia e decidem reativar uma rota alternativa, se houver. Novamente, fica claro a importância da redundância: quando um caminho falhar, outro deve existir e estar disponível para entrar em funcionamento, de modo que a conexão não seja perdida por muito tempo.

A definição dada em [Extreme 2014] continua, explicando que a chave desse protocolo é que todos os *switches* da rede elejam um dispositivo raiz, que se torne o ponto central da rede. Essa eleição é feita escolhendo o *switch* que possuir menor valor no campo *Bridge* ID (campo que é formado por um valor de prioridade do dispositivo e seu endereço MAC (*Media Access Control*)). Todas as outras decisões da rede, como qual porta bloquear e qual porta colocar no modo de encaminhamento, são tomadas na perspectiva desta ponte raiz. Quando existem VLANs implementadas, cada uma deve ter sua própria raiz porque cada VLAN é um domínio de transmissão separado. As raízes para as diferentes VLANs podem residir em um único *switch* ou em vários.

O STP permite que as portas assumam cinco estados, sendo eles: *Forwarding*, *Learning*, *Listening*, *Blocking* e *Disabled*. Ou seja, para que uma porta desativada possa funcionar, será necessário passar por todos esses cinco estados. Isso deixa a rede com um tempo de convergência muito alto. O RSTP, sendo um aperfeiçoamento do STP e funcionando com algoritmo similar, excluiu três estados, deixando a convergência mais rápida. O RSTP tem apenas três estados de portas: *Forwarding*, *Learning* e *Discarding*.

Existem alguns trabalhos na literatura que visam demonstrar o desempenho do protocolo quanto a capacidade de prover a resiliência da rede. O artigo escrito por [Pallos *et al.* 2007] traz uma análise do tempo do RSTP em ambientes reais, mostrando que a convergência da rede acontece, em topologias pequenas, na ordem de segundos e até milissegundos para alguns casos. Além de expor as definições e o funcionamento de protocolos de árvore de abrangência, usados para deixar a rede resiliente, o artigo de [Willis 2019] realiza um comparativo do RSTP com o STP em termos de tempo de convergência. Há um debate sobre a falta da capacidade dos *switches* de salvar a topologia escolhida quando são desligados da rede e comparação com protocolos que usam outros algoritmos. Entende-se, no entanto, que esse protocolo é o que tem menor custo para ser implementado e atende bem às necessidades de uma rede de pequeno porte.

3. Método

O método utilizado para chegar na implementação do protocolo na parte escolhida da rede da Universidade, seguiu as seguintes etapas:

1. Estudo preliminar teórico sobre o protocolo que será utilizado.
2. Levantamento sobre os *switches* que compõem a rede (marca, modelo, *firmware*), além de verificar a situação dos armários de TI que comportam tais dispositivos.
3. Estudo do manual e guia de usuário dos *switches*, uma vez que isso é primordial para entender como está definida a configuração do protocolo desejado, já que cada fabricante tem seus comandos próprios. Além disso, pequenas diferenças podem existir de acordo com o fabricante do *switch*. Alguns possuem até uma versão própria do protocolo.
4. Configuração do protocolo em cada *switch*.
5. Realização de testes.

4. Implementação da solução

Depois da realização do passo 2, foi constatado que o campus possui dispositivos das marcas *Extreme Networks, Planet* e *TP-Link*, distribuídos em vários locais. Apesar de possuir aparelhos de três marcas, foi notado que o centro da rede está inteiramente conectado com *switches Extreme*, sendo estes os que possuem maior número. Os *Planets* e o *TP-Link* foram usados estrategicamente na borda da rede, ou seja, esses equipamentos não são potenciais causadores de *loops* se estiverem com seus vizinhos configurados corretamente. Com isso, a atenção ficou voltada no primeiro momento à configuração do centro da rede. Dessa forma, os *Planets* e *TP-Link* ficaram com função de retransmitir os de BPDUs dos demais *switches*.

A rede abordada no estudo está distribuída em 4 nós, que guardam no mínimo um *switch*, sendo estes nós relacionados à locais do campus, como foi falado anteriormente. Entende-se por nó, nesse trabalho, o local que possui um armário de TI (Tecnologia da Informação), contendo no mínimo um *switch*. Em cada um desses nós há pelo menos um equipamento fazendo a comunicação entre si e entre os equipamentos do seu respectivo local, sejam eles computadores, telefones VoIPs, roteadores, *hubs* ou qualquer outro. Quando há mais de um *switch* em um desses nós, eles estão configurados para trabalharem empilhados: conectados entre si e configurados para operarem juntos como uma unidade.

Com esse levantamento feito, começou a execução do passo 3: o estudo do manual do fabricante do *switch*, visando entender como estava disponível a configuração e funcionamento do protocolo. A partir de então foi documentado os comandos que seriam necessários para implementar o RSTP. Graças ao estudo do manual da *Extreme*, foi visto que seria necessário considerar as VLANs existentes na rede, dividindo-as em domínios, com cada domínio tendo uma ou mais VLANs.

Com a fundamentação teórica, o levantamento das marcas dos *switches* e o estudo do manual, pode-se partir para a configuração manual em cada equipamento. Na Figura 1 estão representados como os quatro equipamentos selecionados serão conectados, formando uma topologia em anel, ou seja, um circuito fechado, em série. Vale ressaltar que o cenário escolhido da rede não contém, a priori, redundância porque, como foi citado, a rede da universidade não possuía nenhum tratamento para possibilitar isso.

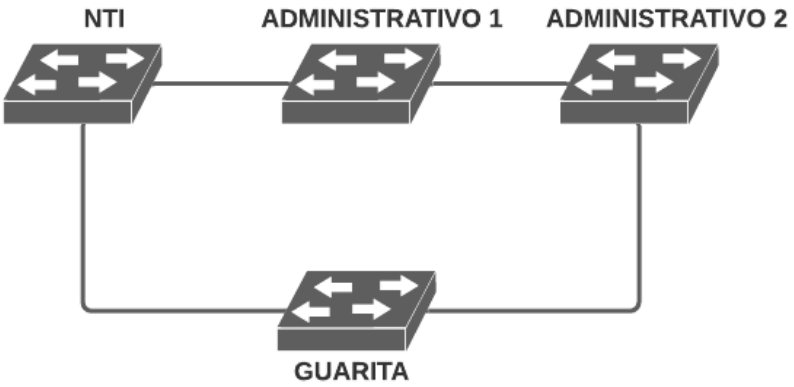

Figura 1. Cenário físico de como os *switches* foram conectados

É válido salientar que a Figura 1 mostra apenas o caminho físico das ligações entre os equipamentos. O protocolo desabilita um desses caminhos logicamente, impedindo que ele funcione até que seja necessário (quando houver algum problema em outro caminho que estava ativo ou quando um administrador de rede achar conveniente usá-lo).

O protocolo RSTP precisou ser configurado em cada um desses *switches* descritos anteriormente. Abaixo segue o passo a passo usado para isso. Os comandos usados, relativos aos equipamentos da marca *Extreme*, estão mostrados na Tabela 1.

Tabela 1. Lista de comandos usados na configuração do RSTP

#	Comando	Explicação
1	*create stpd <stpd_name>*	Cria o domínio do STP
2	*configure stpd <stpd_name> mode [dot1d | **dot1w** | mstp [cist | msti <instance>]]*	Define o modo de operação do domínio. O dot1w é referente RSTP.
3	*configure stpd <stpd_name> default-encapsulation [dot1d | emistp | **pvst-plus**]*	Designa o modo de encapsulamento. Escolheu-se o pvst-plus porque ele tem compatibilidade maior.
4	*configure stpd <stpd_name> add vlan <vlan_name> ports [all | <port_list>]*	Adiciona uma VLAN que fará parte do domínio criado.
5	*configure stpd <stpd_name> tag <stpd_tag>*	Dá uma tag ao domínio do STP, geralmente a mesma da VLAN.

5. Resultados

A implementação do protocolo foi bem sucedida. Como resultado, foi possível conectar toda a rede de teste sem causar *loop*. Isso porque, através do acordo realizado entre os dispositivos, por meio do protocolo implementado, o *link* ligando o *switch* do Administrativo 2 e o da Guarita ficou em estado bloqueado, conforme ilustrado na Figura 2. O que quer dizer que este caminho está obstruído para pacotes convencionais da rede, responsáveis pelos *loops*, e liberado apenas para os quadros BPDUs do protocolo, responsáveis pelo funcionamento do RSTP.

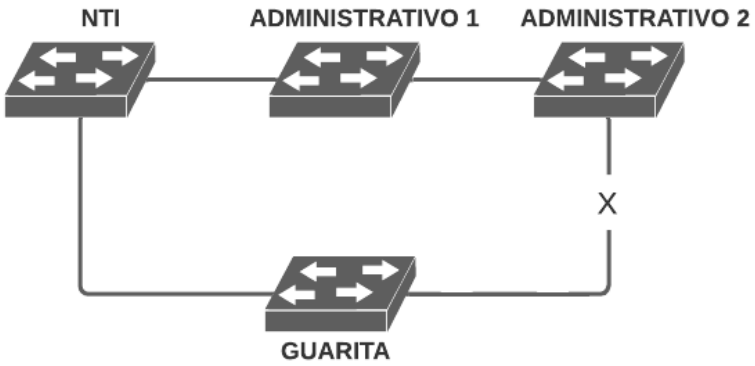

Figura 2. Cenário lógico definido pelo protocolo RSTP

Graças ao comando *show stpd*, descobriu-se que o *switch* localizado no NTI foi o escolhido para ser a raíz dessa topologia. Isso aconteceu de forma natural pelos parâmetros do protocolo, mas utilizou-se do comando que altera o valor do campo *Bridge* ID, atribuindo ao *switch* do NTI um valor menor que padrão. O objetivo é forçar e garantir que em todas as situações a raiz seja de fato o NTI, já que o *link* da Internet e os servidores estão localizados nesse lugar.

Para verificar a conectividade entre os equipamentos da rede, utilizou-se o comando *ping* (*Packet Internet Network Grouper*). O comando obteve respostas de todos os dispositivos, mostrando, inclusive, que as alterações na rede não produziram mudanças significativas no tempo de retorno da requisição. Outro teste realizado foi o de desconectar um caminho que estava ativo, tanto de forma manual quanto com o uso do comando *disable port*, para verificar se o caminho que estava desativado iria demorar para sair desse estado e passar a funcionar. Depois se desfez essa alteração. O resultado para esse teste foi muito satisfatório, mostrando que a transição ocorreu de forma quase instantânea, não tendo nenhuma perda de pacote sendo capturada no *ping*, que ficou em execução continuamente enquanto esses testes eram realizados. Ou seja, a porta previamente bloqueada ficou servindo como uma alternativa, que entrou em funcionamento quando foi necessário.

Vale ressaltar que a escolha de qual porta seria bloqueada seguiu as definições estabelecidas no algoritmo do próprio protocolo. Como está descrito no trabalho de [Pinotti 2009], o RSTP determina o papel de uma porta baseando-se nos pacotes BPDUs trocados entre os dispositivos que formam a rede. Ou seja, o estado que determinada porta vai assumir, depende da comparação entre os valores armazenados na respectiva porta e no BPDU recebido de outros *switches*. Assim sendo, a porta escolhida para se comunicar com o *switch* raiz da topologia é aquela que possuir menor custo. É por isso, então, que o *switch* Guarita se comunica com o dispositivo raiz (NTI, neste caso) de forma direta. Isso tende a trazer uma melhora na performance da rede, já que o RSTP sempre busca deixar os caminhos de menor custo servindo como *link* de comunicação.

6. Conclusão

Com o protocolo implementado nos quatro *switches*, presentes na rede de estudo do trabalho, foi possível formar uma topologia em anel sem a presença de *loop*. Isso deixou a rede resiliente, uma vez que ainda vai funcionar mesmo que algum caminho entre os equipamentos seja interrompido. O RSTP ficou responsável por identificar a presença do

anel, desativar um dos caminhos e manter a rede funcionando logicamente como uma árvore. Dessa forma, caso a comunicação em algum ponto seja perdida, é possível reativar o caminho que estava anteriormente desativado. Isso tudo feito de forma dinâmica graças ao protocolo implementado, o que quer dizer que um técnico não precisará ir *in loco* fazer as alterações.

Com isso, a parte da rede do Campus Arapiraca, da Universidade Federal de Alagoas, ficou mais robusta. O que consequentemente melhora a disponibilidade dos serviços para os sistemas administrativos, de segurança, além do acesso à Internet para os usuários. Futuramente a mesma configuração realizada neste experimento será replicada em toda a rede do campus, visando proporcionar as mesmas características de robustez em mais três anéis formados em outras áreas físicas da instituição.

References

Catalani, L. (2006). E-commerce na prática.

Extreme, N. (2014). *ExtremeXOS Command Reference Guide for Release.* Extreme.

Hojjat, H., Nakhost, H., and Sirjani, M. (2006). Formal verification of the ieee 802.1 d spanning tree protocol using extended rebeca. *Electronic Notes in Theoretical Computer Sicience,* 159:139-154.

Pallos, R., Farkas, J., Moldovan, I., and Lukovszki, C. (2007). Performance of rapid spanning tree protocol in access and metro networks. In *2007 Second International Conference on Access Networks & Workshops,* pages 1-8. IEEE.

Pinotti, I. K. (2009). Desenvolvimento do protocolo rstp-rapid spanning tree protocol. *Trabalho de Conclusão de Curso, Curso de Engenharia de Computação,* FENG/FACIN, PUCRS.

Smith, P., Hutchison, D., Sterbenzm J. P., Scholler, M., Fessi, A., Karaliopoulos, M., Lac, C., and Plattner, B. (2011). Network Resilience: a systematic approach. *IEEE Communications Magazine,* 49(7):88-97.

Willis, P. (2019). *A performance Analysis of the Meshed Tree Protocol and the Rapid Spanning Tree Protocol.* Rochester Institute of Technology.