IDENTIFICAÇÃO AUTOMÁTICA DE TOPOLOGIA EM REDES TCP/IP [1]

Alexandre Valente Duarte Ferreira [2]
Denilson Marcelino Costa [3]
Estevão Oscar Mognatto Junior [4]
Guilherme Henrique Sousa Santos [5]
Henrique Bruno Mariano Pinto [5]
Ivan da Costa Vieira [6]
Lucas Zinato Carraro [7]
Túlio Magno Quites Machado Filho [8]

Resumo
Com a expansão dos sistemas de automação e sua integração cada vez maior com os sistemas industriais de gestão, conhecer a topologia das redes responsáveis pela interligação desses sistemas se tornou um aspecto essencial para possibilitar à equipe de manutenção rápidas respostas para falhas. Além disso, a constante mudança nos ambientes, com o acréscimo de mais sistemas e equipamentos, faz com que a tarefa de levantamento da topologia fique cada vez mais complicada. Neste artigo serão apresentados alguns métodos e implementações de formas de descobrimento automático de topologia na camada de rede e na camada física, visando resolver grande parte desse problema sem a necessidade de intervenção humana.
Palavras-chave: Topologia; SNMP; Redes; Automação.

AUTOMATIC TOPOLOGY MAPPING OF TCP/IP NETWORKS

Abstract
With the spread of the automation systems and its rising integration with the industrial management systems, to know the topology of the networks that connect these systems has become an essential aspect to provide the maintenance team with real-time answers for failures. Besides, the frequent architecture changes, due to the increase of more systems and equipment, make the task of discovering the topology even more complicated. This article shows some methods and implementations of automatic topology discovering in the network layer and in the physical layer, intending to solve a considerable part of the problem without human intervention.
Key words: Topology; SNMP; Networks; Automation.

[1] *Contribuição técnica ao XI Seminário de Automação de Processos, 3 a 5 de outubro, Porto Alegre-RS*
[2] *Engenheiro Eletricista, Gerente de Produto da ATAN Sistemas, Belo Hte – MG, Brasil.*
[3] *Mestre em Ciência da Computação, Developer Leader da ATAN Sistemas, Belo Hte – MG, Brasil.*
[4] *Cientista da Computação, Software Designer ATAN, Belo Hte – MG, Brasil.*
[5] *Graduando em Ciência da Computação, Software Designer ATAN, Belo Hte – MG, Brasil.*
[6] *Graduando em Engenharia de Controle e Automação, Software Designer ATAN, Belo Hte – MG, Brasil.*
[7] *Cientista da Computação, Gerente de Suporte ATAN, Belo Horizonte – MG, Brasil.*
[8] *Graduando em Engenharia Elétrica, Software Designer ATAN, Belo Hte – MG, Brasil.*

1 INTRODUÇÃO

A integração entre Tecnologia de Automação e Tecnologia de Informação permite que a linha de produção consiga responder satisfatoriamente às exigências do nível de gestão do negócio. A Tecnologia de Automação trouxe o benefício de tornar a produção mais eficiente através do controle e otimização, enquanto a Tecnologia da Informação permite que os dados gerados sejam analisados e relacionados em tempo real.

Uma forma encontrada para que tais tecnologias trabalhem juntas foi a conexão dessas através das redes locais de computadores. Tais redes fornecem conectividade para um grande número de aplicações de missão crítica na área industrial e as redes corporativas interconectam as redes locais para integração total nas organizações. Em vista do cenário colaborativo criado por essa realidade, as empresas desenvolveram uma grande dependência da disponibilidade dessas redes para serem bem sucedidas em seus negócios.

O termo topologia, no contexto de redes de comunicação, refere-se ao *layout* físico da rede. Conhecer a topologia da rede é fundamental para garantir sua confiabilidade, performance e para reduzir seu custo de manutenção. Por exemplo, num caso de falha em um elemento de rede qualquer ou mesmo de sobrecarga de um ponto de acesso, o conhecimento da topologia permite a identificação rápida do ponto em questão, bem como das implicações desse problema. Como no ambiente industrial as mudanças são constantes, manter o controle manual do *layout* da rede é inviável, e, portanto, é importante determinar de forma automática como a rede está realmente desenhada.

Os métodos para descobrimento de topologia são divididos em três grupos: passivos, ativos e híbridos. Os algoritmos de métodos passivos inferem a topologia da rede através de consulta às tabelas mantidas nas entidades de controle da rede (p.ex., *switches* e roteadores), sendo normalmente baseados em **DNS** e **SNMP**. Porém nem todos os elementos, principalmente os legados, suportam tais protocolos. Já os algoritmos ativos inferem a topologia da rede com base em seu comportamento, inserindo pacotes de prova e analisando a resposta desses. Embora uma abordagem ativa possa sempre ser aplicada, ela pode fornecer resultados ruins, devido a alguns pacotes de prova ter tráfego impedido por algumas políticas de segurança de rede. Finalmente, há os métodos híbridos, que mesclam as duas abordagens acima.

O objetivo desse trabalho é descrever a implementação de heurísticas e algoritmos para descobrimento automático de topologia visando solucionar esse problema. Serão apresentados os métodos utilizados para o descobrimento da topologia de uma rede local.

2 MÉTODOS PASSIVOS

Denomina-se metodologias passivas para identificação de topologia àquelas que se restringem à leitura de tabelas fornecidas pelos dispositivos de rede (*switches*, *hubs*, roteadores). Há, basicamente, duas técnicas que se encaixam nessa nomenclatura, usando os protocolos **DNS** e **SNMP**.

O servidor **DNS** de um domínio mantém um banco de dados mapeando todos os nomes nesse domínio para os endereços **IP** correspondentes. Através de um comando *zone transfer* é possível obter uma lista de hosts no domínio. Essa lista

pode não estar completa, visto que *hosts* que obtém seu endereço IP via **DHCP** não constarão no servidor **DNS.**[1]

Via **SNMP**, pode-se obter os dados das tabelas de roteamento fornecida pelos roteadores de camada três e nas *Address Forwarding Tables* (**AFT`s**) fornecidas pelos *switches* (camada dois). As tabelas de roteamento permitem montar a topologia na camada três de forma simples, como conseqüência do fato de que roteadores precisam explicitamente conhecer seus pares para executar sua função básica. A topologia física (em camada dois) porém, representa um desafio maior, uma vez que *switches* se comunicam com seus pares apenas de forma limitada e mantém como estado apenas suas **AFT's**, usadas para mapear os pacotes para a porta de saída correta. A organização de redes em múltiplas sub-redes também representa um problema adicional, na medida em que é possível que elementos com conexão física direta pertençam a sub-redes diferentes, situação na qual um elemento pode ser completamente transparente para seus vizinhos físicos imediatos.[2]

A identificação de topologia usando metodologias passivas possui algumas limitações importantes. A identificação de topologia em camada dois usando **SNMP** pressupõe a completeza das tabelas **AFT** dos dispositivos de rede nessa camada, algo que é difícil de se garantir. Esses dispositivos possuem um mecanismo de "envelhecimento" que remove das tabelas os endereços com longo período de inatividade (o intervalo usual para exclusão é de 5 minutos); se um *switch* não recebe pacotes de uma determinada fonte a intervalos menores do que este, então é possível que os dados dessa fonte não estejam presentes na tabela. Há maneiras de se contornar essa limitação, como, por exemplo, provocar um *flood* na rede, para preencher as tabelas, ou mesmo trabalhar com dados incompletos, mas estas também possuem limitações. Além disso, não é possível garantir que **SNMP** esteja universalmente habilitado. Black et al.[3] argumentam que em redes pequenas é comum o uso de dispositivos sem suporte à **SNMP**, e que mesmo em grandes redes é possível que alguns dispositivos na periferia da rede sejam não-gerenciáveis. Outra preocupação diz respeito à segurança: é comum que **DNS** *Zone Transfers* e **SNMP** estejam desabilitados em redes como forma de minimizar algumas vulnerabilidades.

3 MÉTODOS ATIVOS

É uma forma de determinar um nó na rede dinamicamente através da análise de pacotes gerados por elementos da própria rede. As informações podem ser extraídas diretamente ou indiretamente do pacote, através da implementação de algoritmos adequados a cada tipo de pacote recebido, passível de ser analisado.

Alguns dos métodos ativos são baseados nas ferramentas providas pelo **ICMP**: *ping e traceroute*. O *ping* é um pacote de baixo *overhead* que exige uma resposta do destinatário que, ao respondê-la, identifica seu estado de conexão à rede. Já o *traceroute* é a ferramenta que determina a rota do dispositivo local até um dispositivo alvo, através do envio de pacotes com o campo *Time To Live* incrementados progressivamente a partir de uma unidade. O campo **TTL** é decrementado por cada roteador encontrado e, caso se torne nulo, uma resposta é enviada ao remetente, possibilitando o conhecimento de todos os roteadores.

Os algoritmos dos métodos que utilizam **ICMP** baseiam-se na seguinte estratégia para descobrir o layout da rede: criar uma lista temporária dos possíveis dispositivos da rede e, através do *ping*, determinar se cada um deles está conectado

atualmente à rede e. Além disso, define-se quais os nós existentes entre ambos os *hosts*, caso algum deles responda:

- envia-se um *ping* a todos os endereços **IP** da sub-rede a qual este equipamento pertence para encontrar novos nós;
- usa-se heurísticas para encontrar dispositivos. As heurísticas baseiam-se em observações de situações comuns, como, por exemplo, de que em uma sub-rede, com máscara de 24 bits, o endereço **IP** do roteador geralmente termina em "1" ou que é provável encontrar endereços **IP** em seqüência.

Uma das vantagens desses métodos é sua aplicação na maioria das redes **TCP/IP** devido ao suporte ao protocolo de controle de rede **ICMP**, que é normalmente habilitado, mesmo em redes onde **SNMP** é desabilitado por razões de segurança. É fato que a ferramenta *ping* desse protocolo é a maneira mais simples de descobrir se um dispositivo está conectado à rede.

Uma das desvantagens desses métodos é o custo elevado em relação a recursos de rede, visto que é necessário inserir uma série de pacotes de teste causando sobrecarga na rede. Além disso, o processo é lento. Métodos ativos ainda estão sujeitos ao problema de resolução de *aliases*, que consiste em identificar que duas interfaces distintas pertencem a um mesmo elemento de rede. Outro problema associado a eles é o de reconstruir corretamente a identificação de sub-rede e a máscara de rede.

4 ENCONTRANDO A TOPOLOGIA DE UMA REDE LOCAL

Apresenta-se aqui um algoritmo para determinar a topologia de uma rede local. Uma rede local é composta por *hosts* e elementos de rede. Um *host* é um *end-point* da rede, por exemplo, um computador, uma impressora, etc., que não participa ativamente dos processos de distribuição de tráfego na rede. Dessa forma, os elementos de rede são os dispositivos que efetivamente executam a distribuição do tráfego, tais como *switches*, *bridges* e *hubs*.

Para se definir a topologia da rede, pode-se ignorar, inicialmente, os *hosts*, analisando-se apenas a interligação entre os elementos de rede. Uma vez definida a topologia de conexão entre os elementos de rede, é relativamente simples adicionar os *hosts* a ela.

No cenário apresentado, assume-se como domínio um conjunto ***S*** de *switches* tal que todo *switch* conhecido no caminho entre qualquer par de *switches* em ***S*** pertence a ***S***. Para fins de simplificação, será definido *switch* qualquer dispositivo de camada dois gerenciável cuja **AFT** está disponível (incluindo *switches* e *bridges*). *Hubs* são os dispositivos não-gerenciáveis ou cujas **AFT's** não são disponíveis (incluindo *hubs*, barramentos, *switches* sem suporte a **SNMP** e *switches* com suporte a **SNMP** desabilitado).

Uma topologia é um grafo em árvore, $G = (V, A)$ onde ***V*** é o conjunto de elementos de rede ($S \subseteq V$) e ***A*** é o conjunto de interligações entre esses elementos. É importante notar que ***V*** contém potencialmente *hubs*, que não estão em ***S***.

Definiremos:

- v_i como a ***i***-ésima porta do elemento de rede ***v***.
- $\eta_v(u)$ é função que retorna a porta do elemento ***v*** através da qual esse enxerga ***u***.
- $P_{u,v}$ é o conjunto de portas no caminho que liga ***u*** a ***v***.

- $Q_{u,v}$ é uma partição de $P_{u,v}$ que define uma ordem relativa de portas nesse caminho.

A entrada para o algoritmo será uma lista de *switches* gerenciáveis e as **AFT's** completas para esses *switches*. O algoritmo é composto de duas etapas. Primeiramente determina-se o caminho entre cada par de *switches* em ***S***. Em seguida, define-se a topologia propriamente dita com base nos caminhos encontrados.

Será mostrado o funcionamento do algoritmo através de um exemplo.

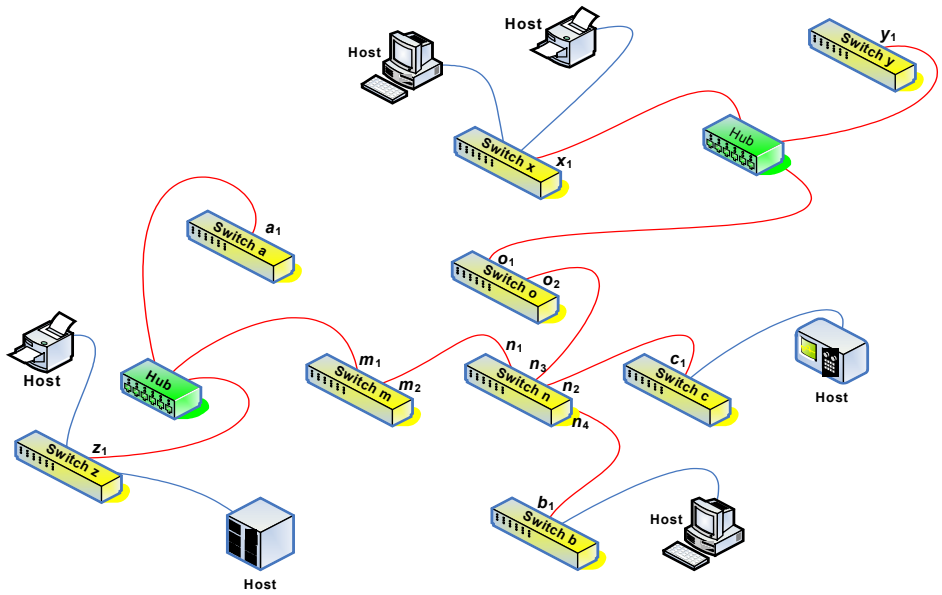

Figura 1: Exemplo de cenário para descobrimento de topologia

4.1 Encontrando o Caminho entre um Par de Elementos de Rede

Seja o par de elementos (**z, c**) na rede mostrada na Figura 1. O objetivo é encontrar $P_{z,c}$ e $Q_{z,c}$. Uma porta x_i pertence à $P_{z,c}$ se e somente se:

- $x_i = \eta_z(c)$
- $x_i = \eta_c(z)$
- $\eta_k(z) \neq \eta_k(c)$ e ($x_i = \eta_k(c)$ ou $x_i = \eta_k(z)$)

Ou seja, se ela é a porta de saída de ***z*** em direção à ***c***, a porta de chegada em ***c*** para tráfego vindo de ***z*** ou uma porta intermediária no caminho. Uma porta intermediária é aquela em que um terceiro elemento enxerga tráfego de ***z*** (ou ***c***), dado que esse elemento enxerga tráfego de ***z*** e de ***c*** em portas distintas. Para o exemplo, tem-se:

$$P_{z,c} = \{z_1, m_1, m_2, n_1, n_2, c_1\}$$

Definido o conjunto de portas que pertencem ao caminho, necessita-se agora encontrar uma partição $Q_{z,c}$ desse conjunto que obedeça às seguintes propriedades:

- Todo elemento de $Q_{z,c}$ é um conjunto unitário
- Se a porta x_i precede a porta x_j no caminho, então $\{x_i\}$ precede $\{x_j\}$ em $Q_{z,c}$

Essa partição será calculada de forma iterativa. Tomando-se como partição inicial:

$$Q^0_{z,c} =< P_{z,c} >=< \{z_1, m_1, m_2, n_1, n_2, c_1\} >$$

Que equivale a partição trivial, que é composta apenas pelo próprio conjunto. A primeira maneira para refinar essa partição é notar que o caminho necessariamente começa em ***z*** e termina em ***c***, de forma que a ordem das portas nesses elementos é definida. Isso fornece:

$$Q^1_{z,c} =< \{z_1\}, \{m_1, m_2, n_1, n_2\}, \{c_1\} >$$

Resta definir a ordem relativa entre os elementos do conjunto $\{m_1, m_2, n_1, n_2\}$. Para tanto, será aplicado o algoritmo de refinamento de forma recursiva. Ainda não pode-se afirmar nada sobre a ordem relativa de ***m*** e ***n*** no caminho entre ***z*** e ***c***. Logo, precisa-se calcular os dois caminhos:

$$Q^1_{n,m} =< \{n_1\}, \{m_2\} >$$

$$Q^1_{m,n} =< \{m_2\}, \{n_1\} >$$

Necessita-se agora determinar qual dessas partições pertence ao caminho entre ***z*** e ***c***. Para tanto, define-se uma restrição adicional, que é determinar a ordem relativa entre as portas de um mesmo elemento no caminho. Basta observar que, como o caminho é orientado de **z** para *c*, então, para um dado elemento ***m*** no caminho, $\eta_m(z)$ precede $\eta_m(c)$. Isso fornece, para o exemplo, duas restrições R_1 e R_2:

- $R_1 =< \{m_1\}, \{m_2\} >$
- $R_2 =< \{n_1\}, \{n_2\} >$

Logo, conclui-se que o caminho entre z e c será dado pela partição:

$$Q^2_{z,c} =< \{z_1\}, \{m_1\}, \{m_2\}, \{n_1\}, \{n_2\}, \{c_1\} >$$

4.2 Inferindo a Topologia a partir dos Caminhos Encontrados

Existe uma conexão direta entre duas portas x_i e y_j se e somente se existe um caminho onde x_i preceda y_j e não existe nenhum caminho onde haja portas intermediárias entre x_i e y_j. Com base nessa propriedade, é possível identificar a topologia da rede a não ser pela identificação de dispositivos não-gerenciáveis.

Para esse segundo caso, basta notar que se há duas ou mais portas diretamente conectadas a uma dada porta z_k, então necessariamente existe um *hub* no qual estão ligadas todas essas portas e z_k.

5 CASOS DE USO

As informações obtidas através do descobrimento da topologia da rede possuem grande valor para o departamento responsável por seu gerenciamento e manutenção. A gama de aplicações possíveis é enorme, mas alguns casos devem receber atenção especial:

5.1 Dashboard para a Manutenção

A simplificação do gerenciamento de uma rede é essencial e esta tarefa necessita de ferramentas aprimoradas para atingir seu objetivo. A partir das informações obtidas da topologia da rede, uma aplicação poderia apresentar dados sobre seu estado atual, sua saúde, as conexões ativas entre os diversos dispositivos e até relacionar estes dados a mapas geográficos.

Dados como estes podem facilitar a busca por um ponto responsável por falhas, e agilizar o processo de manutenção. Além disso, estas informações podem ser adaptadas para facilitar uma manutenção preventiva, já que poderia simplificar a previsão da sobrecarga de um dado nó na rede ou até um certo desbalanceamento de pacotes em links redundantes.

Um outro exemplo importante é possibilitar a execução de testes de segurança, visto que permitiria aos técnicos responsáveis visualizar *hosts* intrusos em tempo real, possibilitando aprimorar e testar a eficiência de uma rede *wireless*.

5.2 Acompanhamento da Carga de Rádio-bases em um Sistema de Operação *Wireless*

Várias aplicações de supervisão e operação são hoje construídas sobre plataformas *wireless*, que possibilitam ao operador acessar, a qualquer instante, a partir de um dispositivo móvel, informações importantes da planta e atuar diretamente no processo. Esse tipo de aplicação é muito sensível ao bom funcionamento da rede sem fio e não são desejáveis problemas como dificuldades de conexão e tráfego extremamente lento. Um dos motivos que podem causar esses problemas é a sobrecarga de um dos pontos de acesso.

Uma forma de se ter conhecimento se que ponto de acesso está sobrecarregado, e evitar essa situação, é através da descoberta da topologia da rede. Conhecendo-se a topologia em tempo real, é possível dividir a carga da rede entre os vários pontos de acesso e evitar esses problemas.

6 CONCLUSÕES

Tendo em vista a importância de se conhecer de forma automática a topologia da rede e a existência atual de várias tecnologias e métodos que podem auxiliar nessa tarefa, a tendência é que surjam cada vez mais produtos voltados para o mercado de automação que façam esse trabalho. Utilizando produtos com essa característica, as equipes de engenharia e manutenção terão um importante auxílio na tarefa cada vez mais complexa de se manter os sistemas de rede corretamente integrados e executando suas tarefas de forma ininterrupta e confiável.

Na abordagem adotada, considera-se apenas os caminhos habilitados na topologia. O uso de *Spanning Tree Protocol* torna difícil identificar caminhos redundantes, que são desabilitados. Dessa forma, pode-se modelar a topologia como uma árvore.

O algoritmo apresentado é confiável a medida que os elementos de rede na topologia analisada sejam gerenciáveis e possam fornecer **AFT's** completas, requerimentos que não são triviais. É possível descobrir elementos não-gerenciáveis, não necessariamente todos, desde que se tenha acesso à maior parte das informações relevantes sobre os demais elementos gerenciáveis.

REFERÊNCIAS

1 SIAMWALLA, R.; SHARMA, R.; KESHAV, S.**Discovering Internet Topology**. Cornell University: Julho de 2008.Disponível em: <http://www.cs.cornell.edu/skeshav/papers.html> Acesso em: 4 mai. 2007.

2 BEJERANO, Yigal; BREITBART, Yuri; GAROFALAKIS, Minos; RASTOGI, Rajeev. **Physical Topology Discovery for Large Multi-Subnet Networks**. Bell Labs Tech. Memorandum: Julho de 2002. Disponível em: < http://www.ieee-infocom.org/2003/papers/09_02.PDF> Acesso em: 2 mai. 2007.

3 BLACK, Richard ; DONELLY, Austin; FOURNET, Cédric. **Ethernet Topology Discovery without Network Assistance**. Microsoft Research,Cambridge,United Kingdon: Maio de 2004. Disponível em: <http://research.microsoft.com/network/topology-CUCL-20040408.ppt> Acesso em: 4 mai. 2007.