Um Sistema Especialista para Auxiliar no Diagnóstico de Problemas Relacionados à Configuração de VLANs em Switches Gerenciáveis

Jorge Janaite Neto[1], **Carlos Nascimento Silla Jr.**[2]

[1] Universidade Estadual Paulista (UNESP)
Campus Marília, SP – Brasil

[2]Universidade Tecnológica Federal do Paraná (UTFPR)
Campus Cornélio Procópio, PR – Brasil

janaite@marilia.unesp.br, carlosjunior@utfpr.edu.br

Abstract. *This paper presents an expert system for an Ethernet network configuration problem. The type of problem addressed in this work is how to configure reconfigurable switches in VLAN segmented ethernet networks.*

Resumo. *Este trabalho apresenta um sistema especialista para um problema de configuração de redes Ethernet. O problema abordado é a configuração de switches gerenciáveis em redes Ethernet segmentadas em VLANs.*

1. Introdução

Dentro do assunto Redes de Computadores, uma das tecnologias mais populares empregadas na implementação de redes locais é a tecnologia *Ethernet*. Desde o seu surgimento, esta tecnologia sofreu várias evoluções para que pudesse suprir as demandas que foram emergindo ao longo dos anos, tais como: facilidade na instalação física, confiabilidade, possibilidade de operar com enlaces distintos, compatibilidade elétrica com cabeamentos já instalados, aumento expressivo da largura de banda, etc. Um dos momentos importantes nesta evolução foi a transição das topologias de redes comutadas, empregando-se *switches*, para as topologias comutadas gerenciáveis, utilizando-se (além dos switches convencionais) os chamados *switches gerenciáveis*; esta evolução conceitual permitiu que as redes Ethernet pudessem ser estendidas em abrangência e número de nós sem prejuízos para a segurança ou mesmo desempenho geral da rede.

Uma situação comum que ocorre em ambientes onde a aquisição dos equipamentos é feita priorizando-se custos imediatos ou mesmo devido a questões de ordem jurídica, como é o caso de órgão públicos no Brasil, é a diversidade de fabricantes, e consequentemente, de sistemas de gerenciamento de ativos (neste caso de Switches Gerenciáveis) com sintaxe ou mesmo modos de configurações incompatíveis entre si. De uma maneira geral, todos que operam diretamente com tais equipamentos necessitam de constante reciclagem de conhecimento, o que torna a curva de aprendizagem de um novo técnico bem acentuada, necessitando de um nível mínimo de proficiência em diversas sintaxes distintas. Para ilustrar a diferença entre duas sintaxes distintas, são apresentadas nas Figuras 1 e 2 dois exemplos de configuração que tem o mesmo objetivo. O objetivo dos exemplos apresentados nas Figuras 1 e 2 são: criar uma *Virtual LAN* (VLAN) estática com a *Vlan Tag* = 22, associar todo o tráfego (*inbound* e *outbound*) da primeira porta física do *Switch Ethernet*

```
<SW-00> system-view
[SW-00] vlan 22
[SW-00-vlan22] description VLAN-TESTE
[SW-00-vlan22] quit
[SW-00] interface GigabitEthernet 1/0/1
[SW-00-GigabitEthernet1/0/1] port link-type access
[SW-00-GigabitEthernet1/0/1] port access vlan 22
[SW-00-GigabitEthernet1/0/1] undo shutdown
[SW-00-GigabitEthernet1/0/1] quit
[SW-00] quit
<SW-00> save
<SW-00> quit
```

Figura 1. Exemplo de sintaxe de comandos em *Switches Ethernet* marca *3com*

```
SW-00> enable
SW-00# configure terminal
SW-00(config)# vlan 22
SW-00(config-vlan)# name VLAN-TESTE
SW-00(config-vlan)# exit
SW-00(config)# interface gigabitEthernet 0/1
SW-00(config-if)# switchport access vlan 22
SW-00(config-if)# no shutdown
SW-00(config-if)# exit
SW-00(config)# exit
SW-00# copy running-config startup-config
SW-00# exit
```

Figura 2. Exemplo de sintaxe de comandos em *Switches Ethernet* marca *CISCO*

a esta VLAN criada e guardar estas configurações para que sejam aplicadas sempre que o equipamento for reinicializado.

Como pode ser observado nas Figuras 1 e 2 , a forma de configurar switchs gerenciáveis de diferentes marcas é realmente muito diferente entre si. Por esse motivo, neste trabalho vamos investigar o desenvolvimento de um Sistema Especialista para auxiliar um técnico em Redes, que não possua conhecimento prévio das linguagens utilizadas na configuração destes equipamentos, a configurar e solucionar problemas relacionados principalmente a configurações de VLAN entre os equipamentos.

No intuito de esclarecer as etapas utilizadas no desenvolvimento do sistema especialista, na seção 2 é apresentada uma revisão de conceitos sobre Redes de Computadores e, mais especificamente na seção 3, conceitos sobre Redes Ethernet. Na seção 4 é apresentada uma breve revisão sobre os conceitos de sistemas especialistas. Na seção 5 é apresentada a principal contribuição deste trabalho que é o sistema especialsita desenvolvido e finalmente, na seção 6 é apresentada uma discussão sobre o uso do sistema e as conclusões deste trabalho. No Anexo A é apresentado o código-fonte do sistema criado.

2. Conceitos de Redes de Computador

Nesta seção é apresentada uma breve revisão contendo alguns termos e conceitos básicos, utilizados entre os diversos profissionais que atuam na área de Redes de Computadores, que nos serão úteis na explicação de conceitos mais elaborados.

2.1. Classificação por Abrangência

As Redes podem ser classificadas empregando-se diversos critérios. Os termos *Local Area Network* (LAN), *Wide Area Network* (WAN), *Metropolitan Area Network* (MAN) e *Campus Area Network* (CAN) adotam basicamente o critério da área de abrangência física para realizar a classificação. A definição das siglas é a seguinte:

LAN: é uma rede limitada a um espaço bem determinado como um prédio ou mesmo um andar de uma edificação e que emprega tecnologias para alcance em pequena distância como Ethernet, IEEE 802.11

WAN: é uma rede, geralmente pertencente a Operadoras de Telecomunicações, empregada para conectar LANs normalmente a grandes distâncias

CAN: é um rede que conecta LANs em um território controlada por uma única autoridade, como fábricas e campus universitário

MAN: também é uma rede que conecta LANs mas essas LANs estão separadas entre si por territórios particulares não pertencentes ao proprietário das LANs

Observe que a distinção entre MAN e CAN é bem tênue, pois apoia-se no fato de que em um campus universitário, ou mesmo um complexo industrial, onde existem diversas construções concentradas em uma mesma região é possível o uso de enlaces ópticos ou wireless entre tais construções de uma maneira simples sem o envolvimento de terceiros sem gerar custos periódicos para a manutenção da rede. No caso da MAN, que esta localizada em alguma cidade, a implantação de links entre as LANs, normalmente, é feita por uma Empresa de Telecomunicações que detém alguma tecnologia já implantada na cidade em questão que alugue os links ponto-a-ponto [Donahue 2007, pp. 4-5].

2.2. Alocação de Recursos

Existem basicamente duas metodologias para a alocação de recursos em uma rede de telecomunicações para transmissão de dados: *Packet Switching* (comutação de pacotes) e *Circuit Switching* (comutação de circuitos).

Em redes que empregam *Circuit Switching*, a comunicação deve ser estabelecida em três etapas: estabelecimento do circuito, conversação e desconexão. A característica principal desta metodologia é a previsibilidade da latência e garantia de banda, pois uma vez estabelecido o circuito, normalmente a rota que os pacotes usarão será sempre a mesma. Isso facilita a implementação de *Quality of Service* (QoS).

A metodologia de *Packet Switching* permite duas formas de comunicação: orientada a conexão e não orientada a conexão. Enquanto que na primeira é necessário o estabelecimento de um canal de comunicação antes de iniciar a conversação, na segunda forma basta transmitir. Uma característica importante do *Packet Switching*, independentemente de estar operando orientado ou não a conexão, é que não há explicitamente alocação de banda nem mesmo garantias de que o roteamento será mantido fixo, consequentemente não há uma previsibilidade de latência. Percebemos aqui claramente que para

haver alguma forma QoS, será necessário auxílio dos ativos de rede envolvidos em toda a trajetória do frame. No caso específico de redes Ethernet, existe a possibilidade de implementar QoS em Layer-2 utilizando-se marcações especiais no *Frame Ethernet* (veja na seção 3.2.3).

3. Redes Ethernet

3.1. Histórico das Redes Ethernet

Os princípios da tecnologia de redes Ethernet foram propostos por Bob Metcalfe em 1973. Ele se baseou em uma rede desenvolvida no final de 1960 pela Universidade do Havaí, chamada *Aloha Network* [Spurgeon and Zimmerman 2014, pp. 4-9]. Nesta proposta inicial já havia o conceito de uma mídia compartilhada entre várias estações mediante o uso do que viria a ser o *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD) [Spurgeon and Zimmerman 2014, pp. 4-9].

O controle de acesso ao meio, também conhecido como *Media Access Control* (MAC), inicialmente foi implementado, conforme já mencionado, com o protocolo CSMA/CD que permitia apenas uma estação transmitir no meio, esta operação é classificada como transmissão *half-duplex*. Isso tornou desnecessária a existência de um controlador central, bastando apenas que as estações fossem conectadas ao meio físico por meio das interfaces de rede chamadas *Network Interface Controller* (NIC) [Spurgeon and Zimmerman 2014, pp. 10-31]. Percebemos que a proposta inicial era que a rede Ethernet não necessitasse de configuração em seus ativos intermediários.

Ao longo dos anos o padrão Ethernet foi evoluindo para suprir as demandas que foram surgindo com o aumento de sua popularidade e uso em áreas cada vez mais abrangentes. Basicamente ele evoluiu para atender a demanda do mercado sob dois itens complementares: nos tipos de meio físico empregados para a comunicação e no aumento da largura de banda [Spurgeon and Zimmerman 2014, pp. 6-9].

A mudança nos tipos de meio físico empregados ocorreu visando aspectos elétricos e físicos. Eletricamente alguns meios de transmissão possuem características necessárias para atender às demandas dos novos padrões, como aumento da frequência de transmissão e melhoria da relação sinal-ruído ou *Signal-to-Noise Ratio* (SNR). Aspectos físicos também influenciaram, tais como facilidade de manuseio e conectorização, resistência à umidade, à tração, etc.

No início das redes Ethernet foi utilizada a mídia do tipo *thick coax cable* (Cabo Coaxial Grosso), posteriormente o *thin coax cable* (Cabo Coaxial Fino) – RG58A/U, e devido a complexidade envolvida no manuseio de cabos coaxiais, estes caíram em desuso sendo substituídos por cabos Twisted-Pair com o uso de HUBs. Observe que mesmo com o uso de HUBs (criando-se uma topologia física de estrela) a topologia lógica de barramento foi mantida [Donahue 2007, pp. 6-11].

No quesito largura de banda, partindo-se do pressuposto de que uma rede de computadores serve para mover informação entre computadores e que esta informação (no caso de uma rede Ethernet) deve estar contida no payload de um *Frame Ethernet*, torna-se necessário uma maneira eficiente de encaminhar estes *Frames Ethernet* para que se obtenha um aumento perceptível da largura de banda efetiva de uma rede.

Durante a evolução histórica do Ethernet percebemos a evolução das formas de transmissão e recepção dos *Frames Ethernet*: inicialmente o uso de um único segmento gerenciado por CSMA/CD, tanto nos enlaces metálicos do tipo cabo coaxial quanto no enlaces metálicos do tipo UTP e STP; posteriormente tivemos a divisão destes grandes segmentos em segmentos menores com o uso de *Bridges* (veja na seção 3.3.1) que permitiram o uso de enlaces heterogêneos (metálico e óptico) que se transformaram, em algumas situações, em segmentos com apenas duas interfaces, o que permitiu a comunicação *full-duplex* (veja na seção 3.3.2).

A largura de banda das redes Ethernet também aumentou bastante, como pode ser observado na tabela 1 [Spurgeon and Zimmerman 2014, pp. 5-9]:

ano	largura de banda	descrição
1972	2,94 Mbp/s	Primeiro experimento Ethernet
1980	10 Mbp/s	DIX - primeiro padrão proprietário
1983	10 Mbp/s	IEEE 802.3 - primeiro padrão aberto
1995	100 Mbp/s	IEEE 802.3u - padrão *Fast Ethernet*
1999	1000 Mbp/s	IEEE 802.3ab - padrão *Gigabit Ethernet*
2003	10 Gb/s	IEEE 802.3ae - primeiro padrão 10GbE
2010	40 Gb/s e 100 GB/s	IEEE 802.3ba - primeiro padrão 40GbE e 100GbE

Tabela 1. Evolução da largura de banda do padrão Ethernet

3.2. Princípios e Fundamentos de Redes Ethernet

Um dos princípios norteadores da tecnologia Ethernet é o do *Best-Effort Delivery*, que significa que a entrega do *Frame Ethernet* não é garantida. Existe apenas a garantia de que se o *Frame Ethernet* for entregue ele chegará livre de erros; nos casos de *Frames Ethernet* incorretos, estes serão descartados silenciosamente, não ocorrendo qualquer tipo de sinalização para o emissor [Spurgeon and Zimmerman 2014, pp. 36-37].

3.2.1. Endereçamento físico

O endereçamento físico dos *Frames Ethernet* é gerenciado utilizando-se identificadores globais únicos de 48-bits conhecidos formalmente por *MAC Address*. Estes identificadores são utilizados em todos os *Frames Ethernet* que trafegam na rede Ethernet e servem para identificar de forma única o nó de origem (campo *Source Address* do *Frame Ethernet*) e o nó de destino (campo *Destination Address* do *Frame Ethernet*) daquele *Frame Ethernet*. Cada NIC possui, geralmente pré-programado pelo próprio fabricante, um desse identificadores únicos associados a ela que é utilizado no campo *Source Address* de todos os *Frames Ethernet* originados a partir daquele NIC.

3.2.2. O Frame Ethernet

O padrão estabelecido pelo *Institute of Electrical and Electronics Engineers* (IEEE) denominado *IEEE 802.3 Ethernet Working Group* (IEEE 802.3) define a estrutura e o momento em que cada estação poderá enviar o *Frame Ethernet*. Originalmente foi definido

pelo padrão DEC-Intel-Xerox (DIX), mas foi posteriormente modificado e aperfeiçoado pelo padrão IEEE 802.3 [Spurgeon and Zimmerman 2014, p. 44].

Existem atualmente três tamanhos de frame, apresentados na tabela 2, sendo obrigatório que uma interface Ethernet suporte no mínimo um deles; há uma recomendação que seja priorizado o suporte ao novo formato (envelope frame).

Padrão de Frame Ethernet	tamanho mínimo	tamanho máximo
DIX Basic Frame	64 bytes	1518 bytes
IEEE 802.3 Basic Frame	64 bytes	1518 bytes
IEEE 802.3 Basic Frame with Q-Tag	64 bytes	1522 bytes
IEEE 802.3 with Envelope prefix and/or Suffix	64 bytes	2000 bytes

Tabela 2. Tamanhos de Frame Ethernet (sem considerar o preâmbulo)

Apesar de existirem quatro padrões de frame, o formato IEEE 802.3 Basic Frame é idêntico, em itens e campos, ao formato DIX Basic Frame, diferenciando-se apenas no conteúdo de alguns campos (ilustrados nas figuras 3 e 4). Em todos os padrões, o payload de Dados/LCC sempre possui o tamanho entre 46 e 1500 bytes, o que caracteriza o padrão Ethernet, desde o seu surgimento, com um *Maximum Transmission Unit* (MTU) básico de 1500 bytes [Spurgeon and Zimmerman 2014, p. 45].

Destination MAC Addr						Source MAC Addr						Type		Payload	Checksum			
1	2	3	4	5	6	1	2	3	4	5	6	1	2	46 ... 1500	1	2	3	4

Figura 3. Frame Ethernet padrão *DIX Basic Frame*

Destination MAC Addr						Source MAC Addr						Type/Len		Payload	Checksum			
1	2	3	4	5	6	1	2	3	4	5	6	1	2	46 ... 1500	1	2	3	4

Figura 4. Frame Ethernet padrão *IEEE 802.3 Basic Frame*

3.2.3. VLAN Tag

Com o aumento do uso das LANs Ethernet e com surgimento de LANs cada vez maiores, tanto em abrangência física quanto em número de equipamentos conectados, a ineficácia do uso de tráfego broadcast começou a ficar cada vez mais evidente. Uma solução desenvolvida para criar mais de um Domínio de Broadcast em uma mesma LAN foi a VLAN.

Um Domínio de Broadcast é a área de uma rede Ethernet onde o broadcast será propagado. Perceba que os broadcasts não estão restritos ao *Switch Ethernet* ou mesmo a VLAN que os originou, pois nada impede a criação (intencional ou mesmo acidental) de uma ligação física entre o tráfego de uma VLAN X com o de uma VLAN Y. Nesta situação hipotética caso os ativos de ambas as VLANs estiverem configurados dentro da

mesma rede IP, em termos de máscara IP, haverá comunicação entre eles [Donahue 2007, p. 8].

A implementação do conceito de VLAN surgiu como diversas soluções proprietárias e não padronizadas entre fabricantes distintos, mas posteriormente foi padronizada pela norma IEEE 802.1Q [Fall and Stevens 2011, pp. 89-91] que estabeleceu uma forma interoperável de marcar a identificação da VLAN nos Frames Ethernet (Figura 5) que, posteriormente, evoluiu para uma forma mais genérica, e totalmente retrocompatível com a introdução do conceito de envelope, no qual a *VLAN Tag* passa a ser um tipo específico de envelope (Figura 6).

Destination MAC Addr						Source MAC Addr						802.1q Tag				Type/Len		Payload	Checksum			
1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	1	2	46 ... 1500	1	2	3	4

Figura 5. Frame Ethernet padrão *IEEE 802.3 Basic Frame with Q-Tag*

Destination MAC Addr						Source MAC Addr						Envelope Prefix	Type/Len		Payload	Envelope Suffix	Checksum			
1	2	3	4	5	6	1	2	3	4	5	6	2 .. 482	1	2	46 ... 1500	0 ... 482	1	2	3	4

Figura 6. Frame Ethernet padrão *IEEE 802.3 with Envelope prefix and/or Suffix*

Uma vantagem implícita em se utilizar *VLAN tagging* conforme definido pelo padrão IEEE 802.1Q é a adição de valores *Class of Service* (CoS) definidos no IEEE 802.1p, utilizado por alguns switches para o controle explícito de congestionamento e priorização de tráfego em *OSI model layer 2* [Spurgeon and Zimmerman 2013, p. 28].

3.3. Equipamentos e tecnologias de Redes Ethernet

3.3.1. Bridges

São equipamentos intermediários utilizados em redes ethernet. Foram criadas, basicamente, para permitir a divisão de um grande segmento de Rede em dois segmentos menores (às vezes, cada segmento possui um tipo de meio distinto, por exemplo: ethernet com cabeamento coaxial e ethernet com cabeamento do tipo UTP)

Dentro da filosofia de não configuração dos ativos, apenas das extremidades da rede, surge o conceito de *Transparent Bridging* que torna a operação da *bridge* invisível para os outros dispositivos conectados à rede. Os *Frames Ethernet* não sofrem qualquer tipo de alteração, sendo apenas encaminhados, quando necessário, ao outro segmento da rede. A decisão sobre o encaminhamento de tráfego é feita baseando-se unicamente no endereço MAC de destino contido em cada *Frame Ethernet*. O encaminhamento de tráfego entre os segmentos ethernet (*traffic forwarding*) é iniciado imediatamente, antes mesmo da *bridge* aprender todos os endereços MAC de ambos os segmentos.

O processo de *Address Learning* ocorre da seguinte forma: cada porta da *bridge*, que também possui um endereço MAC único, está conectada fisicamente a um segmento ethernet distinto. Estas portas operam em modo *promiscuous*, o que significa que elas escutam todo o tráfego daquele segmento. Ao receber um frame em qualquer uma das portas, a *bridge* adiciona o endereço MAC de origem contido naquele frame ethernet

(juntamente com a identificação da porta na qual aquele frame foi recebido) a uma tabela interna do equipamento, chamada *MAC Address Table*. Desta forma, conforme as interfaces vão trocando frames entre si, a *bridge* vai aprendendo quais são os endereços MAC de todas as interfaces conectadas àquela porta que tenham transmitido algum frame [Spurgeon and Zimmerman 2013, pp. 4-5].

Ao receber um frame ethernet a *bridge* verifica se o endereço MAC de destino daquele frame existe em sua *MAC Address Table*, este é o processo de *Traffic Filtering*. Caso exista, o frame é encaminhado para a porta registrada naquela entrada da tabela, porém se a porta registrada na tabela for a mesma porta por onde o frame ingressou ele será descartado. Se o endereço não existir na *MAC Address Table* haverá o *Frame Flooding*, que é o encaminhamento daquele frame recebido para todas as portas, exceto a porta por onde ele ingressou. Em ambos os casos, todas as entradas da *MAC Address Table* possuem um temporizador predefinido que determina o tempo máximo que cada endereço MAC será mantido na tabela, portanto, poderá haver *Frame Flooding* mesmo para endereços MAC já aprendidos que tiveram o seu tempo de vida expirado e, consequentemente, foram removidos da tabela [Spurgeon and Zimmerman 2013, p. 6].

3.3.2. Switches

Um *Switch Ethernet* nada mais é que uma *bridge* com várias portas. Serve para encaminhar frames ethernet entre suas portas, reduzindo o domínio de colisão de cada segmento de rede. Para realizar essa tarefa baseia-se no uso do endereçamento MAC contido em cada frame, conforme estabelecido no padrão IEEE 802.1D [Spurgeon and Zimmerman 2013, p. 1], existindo inclusive switches com interfaces *built-in* ou modular para conectar tipos de redes distintos como Ethernet, *Asynchronous Transfer Mode* (ATM) e *IEEE 802.11 Standard for Wireless LAN Technology* (IEEE 802.11) entre si por meio da Camada 2 (enlace) dos modelos de rede OSI e TCP/IP.

Com a popularização dos switches e na tentativa de melhorar o eficiência da rede, tornou-se comum ligar apenas um dispositivo por porta do *Switch Ethernet* o que permitiu o estabelecimento de comunicação bidirecional simultânea (comunicação *full-duplex*) entre o dispositivo e o *Switch Ethernet*, eliminando-se por completo a possibilidade de colisão de frames naquele segmento de rede. A comunicação *full duplex* foi estabelecida pelo padrão IEEE 802.3x, publicado em 1997 [Spurgeon and Zimmerman 2014, p. 53].

Uma característica peculiar das Bridge e switches é que eles não segmentam o domínio de broadcast, mas podem segmentar o domínio de multicast, porém muitos (geralmente os switches de baixo custo) optam por tratar o multicast L2 como sendo broadcast L2, ou seja, realizando *flood* dos *Frames Ethernet* [Spurgeon and Zimmerman 2013, p. 8].

3.3.3. Redes Gerenciáveis Ethernet - Switches Multilayer

Existem *Switches Ethernet* que possuem a capacidade de interpretar e tratar dados da terceira camada, denonimada Camada de Rede segundo o modelo OSI [Fall and Stevens 2011, p. 9]. Estes equipamentos, que podem ser considerados Roteado-

res, são conhecidos popularmente como Switches Multilayer ou mesmo Switches Layer 3. É nesta categoria que se encontram os Switches Gerenciáveis

Como estes *Switches Ethernet* possuem a capacidade de tratar a terceira camada, muitos deles fazem o chamado *IGMP Snooping*, que consiste em interpretar as mensagens *Internet Group Management Protocol* (IGMP) trocadas entre Hosts e Routers, utilizadas para gerenciar grupos IPv4 multicast. É este recurso que permite ao *Switch Ethernet* otimizar em *Layer 2* o tráfego multicast configurado em *Layer 3*.

Nesta seção foi apresentado um único exemplo (a capacidade de efetuar *IGMP Snooping*) dentre os diversos recursos que estes *Switches Ethernet* possuem. Em termos gerencias é possível perceber que a adição deste tipo de ativo permite redes Ethernet mais complexas, extensas e, se configurados adequadamente, mais seguras com um melhor aproveitamento das bandas de transferência disponíveis nos enlaces.

3.4. Topologias

A vantagem em utilizar *Switches Ethernet* em uma rede é a melhora no desempenho devido ao encaminhamento mais racional do tráfego e à redução, e até eliminação, do domínio de colisão de cada segmento de rede. Um outra vantagem é a possibilidade de conectar entre si segmentos de rede que estão operando em velocidade de transmissão distintas, pois cada porta do *Switch Ethernet* geralmente é capaz de operar em diversas velocidades previstas no padrão. Quando o número de *Switches Ethernet* aumenta significativamente, o impacto do tráfego nos *uplinks* crescem expressivamente, surgindo então a necessidade de um design mais robusto das interconexões dos *Switches Ethernet*. Um dos designs mais populares para topologia física é o chamado *Hierarchical Network Design* ou simplesmente Design Hierárquico.

Na topologia de Design Hierárquico, são definidas três camadas: *Core Layer*, *Distribution Layer* e o *Access Layer* (Figura 7). No caso de uma rede CAN, no *Core Layer*, que está no *DataCenter* da Instituição, situam-se os *Switches Ethernet* de alto desempenho que interconectam todos os prédios entre si; na camada de *Distribution* situam-se os *Switches Ethernet* de médio desempenho, alojados na sala de telecomunicações de cada prédio, que interconectam os diversos *Switches Ethernet* de distribuição situados nos diversos *racks* instalados dentro das salas e/ou corredores daquele prédio ao *Core Layer*. Os *Switches Ethernet* do *Access Layer* são responsáveis pela conexão de todos os dispositivos de rede de um determinado prédio ao *Distribution Layer*, é neles que estão conectados os pontos embutidos ou sobrepostos em paredes e similares (que receberão por meio de um *patch coord* a conexão do equipamento final) [Spurgeon and Zimmerman 2013, pp. 34-36]. Observe que a camada de acesso está conectada diretamente à camada de distribuição, não há interconexão dos *Switches Ethernet* de acesso entre si, evitando a criação de caminhos horizontais entre os *Switches Ethernet* envolvidos, facilitando o trabalho do *Spanning Tree Protocol* (STP).

Esta mesma topologia pode ser simplificada (Figura 8), onde o *Core Layer* e o *Distribution Layer* são colapsados em uma única camada, daí o nome *Two-Tier Collapsed-Core*, sendo esta camada conectada diretamente ao *Access Layer*. Esta topologia é empregada quando o número de *Switches Ethernet* de acesso não é elevado a ponto de justificar a existência de uma sala de telecomunicações dentro da edificação, existindo apenas um *Rack* de centralização contendo os *Switches Ethernet* de acesso, cascateados ou empilha-

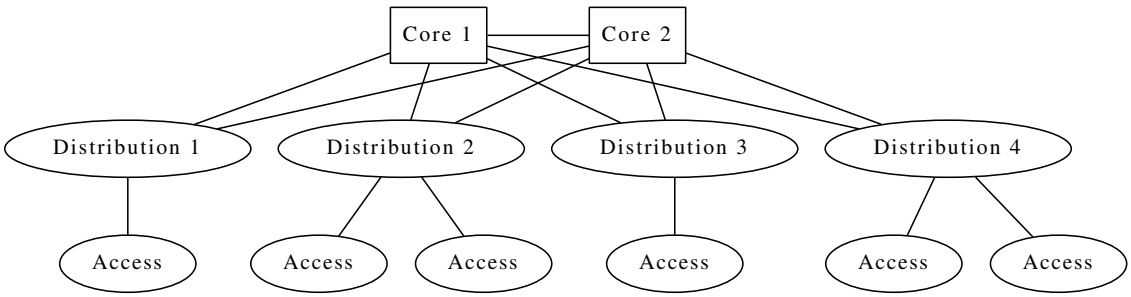

Figura 7. Topologia de Rede *Three-Tier*: *Core Layer*, *Distribution Layer* e *Access Layer*

dos, e um enlace direto para o *Data Center* que contém a camada *Core+Distribution*.

Uma característica interessante que surge ao empregarmos o Design Hierárquico é que obtemos uma rede puramente comutada, na qual os *Switches Ethernet Core* (ou *Core+Distribution*) possuirão em sua *MAC Address Table* todos os endereços MAC de todos os dispositivos finais conectados na camada de acesso (desde que tenham enviado algum frame e que o cronômetro da tabela ainda não tenha expirado).

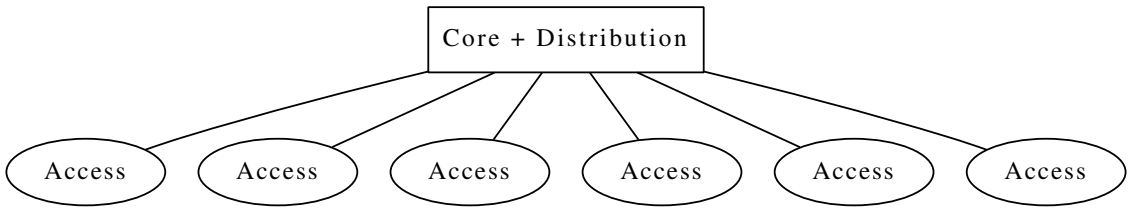

Figura 8. Topologia de Rede *Two-Tier Collapsed-Core*: *Core+Distribution Layer* e *Access Layer*

4. Sistemas Especialistas

4.1. Teorias e Conceitos

Sistemas Especialistas "são programas de computador que procuram atingir soluções de determinados problemas do mesmo modo que especialistas humanos, se estiverem sob as mesmas condições" [LIA 1995, p. 4]

A arquitetura mais convencional para um sistema especialista, segundo os autores do *ExpertSINTA* [LIA 1995], é a que emprega *variáveis*, *objetivos* e *regras de produção* (*production rules*). Estas regras basicamente são um conjunto de testes condicionais no formato *IF...THEN...* onde a condição é composta por um ou mais testes interligados por meio de conectivos lógicos *AND* ou *OR*. A base do conhecimento representa a informação que o Sistema Especialista possui, ela é representada por meio de fatos e regras de produção.

As variáveis servem como conhecimento dinâmico a ser inferido e utilizado durante a execução do Sistema Especialista. Elas podem ser univaloradas ou multivaloradas. Todas as variáveis não numéricas possuem associado a elas um conjunto de valores predefinidos, elas poderão assumir apenas estes valores ou o valor "desconhecido". As

```
Variavel multivalorada RESULTADO
   valores possiveis: conclusaoA, conclusaoX, conclusaoJ
Variável univalorada SITUACAO1
   valores possíveis: aaa, bbb, [desconhecida]
Variável univalorada SITUACAO2
   valores possíveis: xxx, yyy, [desconhecida]

Regra1: Se    SITUACAO1 == aaa
        Entao RESULTADO = conclusaoA
Regra2: Se    SITUACAO2 == xxx
        Entao RESULTADO = conclusaoX

Objetivo: solucionar RESULTADO
```

Figura 9. Exemplo de solução multivalorada

variáveis univaloradas podem armazenar apenas um único valor daquele conjunto predefinido de valores possíveis, um exemplo de uso bem comum é o conjunto de valores "sim", "não"; observe que as variáveis numéricas sempre serão do tipo univaloradas. As variáveis multivaloradas podem assumir mais de um valor pertencente aquele conjunto predefinido de valores.

Os chamados "objetivos" são as variáveis que devem ser solucionadas, ou seja, são aquelas variáveis que precisamos saber todos os valores possíveis que elas poderiam assumir mantendo-se a relação lógica previamente definida durante o treinamento do Sistema Especialista. Veja que solucionar uma variável multivalorada pode resultar em um subconjunto do conjunto de valores possíveis dela, com fatores de confiança provavelmente distintos. Quando não é possível chegar a um resultado, a variável receberá o valor chamado "desconhecido". Na Figura 9 podemos ver um exemplo desta solução multivalorada, onde naquele caso se SITUACAO1 = "aaa" e SITUACAO2 = "bbb", RESULTADO será simutâneamente: conclusaoA CNF (grau de confiança da SITUACAO1) e conclusaoB CNF (grau de confiança da SITUACAO2).

Uma forma de associar novos valores às variáveis (produzir novos fatos) é mediante o uso de alguma interface de comunicação com o mundo externo, geralmente uma *Graphical User Interface* (GUI) questionando o usuário do sistema e oferecendo a possbilidade de escolha de um (no caso das variáveis univaloradas) ou múltiplos (no caso das variáveis multicaloradas) valores dentro do conjunto de valores válidos para a variável em questão. Uma outra forma de associar novos valores às variáveis (produzir novos fatos) é utilizando regras de produção, adicionando valores no caso de variáveis multivaloradas ou substituindo valores no caso das variáveis univaloradas, note que a regra de produção só será ativada, produzindo seus efeitos, se todas as premissas da regra forem satisfeitas.

Em um Sistema Especialista o conhecimento é armazenado na forma de fatos e regras de produção. Os fatos são conhecimentos prévios, já inseridos na base de conhecimento do Sistema Especialista durante o seu treinamento ou inferidos por meio das regras de produção, ou seja, as regras de produção podem gerar novos fatos na base de conhecimento do Sistema Especialista.

Em termos sintáticos, uma regra de produção é composta por um conjunto de premissas e suas conclusões. Conforme já mencionado, as premissas da regra são as condições necessárias para que a regra seja ativada e faça com que suas conclusões sejam executadas, alterado-se a base de conhecimento.

O ato de produzir novos fatos utilizando-se regras de produção é denominado inferência. Ao tentar solucionar uma variável (encontrar todos os valores ou o valor válido para ela dentro da lógica definida) podemos nos deparar com outras variáveis desconhecidas que serão necessárias para que possamos ativar determinadas regras de produção que irão produzir a solução que precisamos. Neste caso, para que possamos solucionar a variável inicial, necessitamos solucionar primeiramente outra variável ou outras variáveis que são requisitos para atingirmos uma solucão para o problema inicial. Perceba que este processo é recursivo, pois estas variáveis que são requisitos também podem possuir suas dependências com outras variáveis e assim sucessivamente, formamos uma espécie cadeia de requisitos e dependências entre as diversas variáveis. Uma das técnicas empregadas para solucionar este tipo de problema é a inferência por *Back-Chaining* que parte dos objetivos, que são as variáveis que precisamos solucionar e avança através das dependências até chegar a algum resultado, percorrendo todos os caminhos válidos no grafo de dependências.

4.2. ExpertSINTA

A ferramenta utilizada neste trabalho foi o *ExpertSINTA*, classificado como uma shell para sistemas especialistas, definida por seus autores como:

> O *ExpertSINTA* é uma ferramenta computacional que utiliza técnicas de Inteligência Artificial para geração automática de sistemas especialistas. Esta ferramenta utiliza um modelo de representação do conhecimento baseado em regras de produção e probabilidades [LIA 1995].

Todo o funcionamento do *ExpertSINTA* baseia-se nos conceitos: Variáveis, Objetivos, Regras e Interfaces. A técnica de inferência empregada é a inferência por *Back-Chaining*, que falamos na seção 4.1 [LIA 1995, pp. 9-11].

As variáveis, no caso do *ExpertSINTA*, também possuem um fator de confiança associado a cada valor que influencia no cálculo final das probabilidades das respostas; observe que este recurso não foi utilizado neste trabalho, por isso na explicação que segue não haverá mais menção aos fatores de confiança (CNF).

Uma forma de associar novos valores às variáveis (produzir novos fatos) é com o uso do que o *ExpertSINTA* chama de "Interface", que nada mais é que uma pergunta, na forma de texto predefinido, feita para o usuário do sistema sobre qual ou quais os valores que uma determinada variável possui, existindo a possibilidade do usuário manter a variável com o valor "desconhecido".

<conectivo>	<atributo>	<operador>	<valor>
NÃO / E / OU	variável instanciada	= / < / <= / <>	valores possíveis

Figura 10. Regra de produção no *ExpertSINTA*: estrutura das *premissas da regra*

Um outra forma de associar novos valores às variáveis é utilizando-se regras de produção (seção 4.1). No *ExpertSINTA* as premissas da regra de produção seguem a estrutura demonstrada na Figura 10, perceba que esta estrutura de condições pode ser repetida mais de uma vez, bastado utilizar um conectivo entre elas (no caso da primeira premissa, apenas o conectivo "NÃO" é válido). Após as premissas temos as conclusões, que seguem a estrutura demonstrada na Figura 11.

<atributo>	=	<valor>	<grau de confiança>
nome da variável	operador de atribuição	um dos valores possíveis para a variável	porcentagem de confiabilidade

Figura 11. Regra de produção no *ExpertSINTA*: estrutura das *conclusões*

Podemos ver na figura 12 um exemplo de regra de produção, na qual a variável "TESTE ip e vlan ok" terá associado o valor "falha" apenas se as seguintes condições forem satisfeitas: a variável "PERG conhece a vlan?" esteja resolvida para o valor "nao", a variável "AFIRM mac conhecido" esteja resolvida para o valor "sim" e a variável "PERG mac/vlan existe no core" esteja resolvida para o valor "nao". No caso específico da implementação discutida aqui, optou-se por utilizar o prefixo "PERG" para variáveis que serão resolvidas por uma "interface" e o prefixo "MSG" para variáveis que utilizam uma "interface" apenas para fornecer orientações ao usuário, sempre resolvendo para o valor "ok".

```
SE PERG conhece a vlan? = nao
E AFIRM mac conhecido = sim
E MSG descobrir vlan no core = ok
E PERG mac/vlan existe no core = nao
ENTAO TESTE ip e vlan ok = falha
```

Figura 12. Exemplo de uma regra de produção do sistema desenvolvido no *ExpertSINTA*

5. Um Sistema Especialista para auxiliar na configuração de Redes Ethernet gerenciáveis heterogêneas

Nesta seção apresentamos a principal contribuição deste trabalho, a criação de um sistema especialsita para auxiliar na configuração de VLANs em uma rede Ethernet gerenciável heterogenia.

As configurações destas redes ethernet gerenciaveis heterogenias são baseadas em uma rede com enlaces metálicos Cat6a, topologia *Collapsed-Core*, classificação de abrangência CAN, onde a LAN de cada prédio está ligada por meio de enlace óptico a um Switch Multilayer que age como o Switch CORE. Para a implementação desta proposta foi utilizada a shell *ExpertSINTA* [LIA 1995], treinada na sintaxe de comandos de Switches Gerenciaveis fabricados pela 3com, modelo 4500G.

Na implementação feita para testes práticos, o ambiente físico objeto é composto por switches de acesso marca 3com modelo 4500G e o Switch Core é também da marca 3com modelo 4800. A rede é toda segmentada em VLANs (ao todo são mais de 20

VLANs) utilizando 15 classes C de IPv4 completas, o que disponibiliza um pouco mais de 2700 números IPv4 para serem utilizados em ativos de rede.

A topologia de *Collapsed-Core* torna a rede totalmente comutada e permite que os endereços MAC sejam facilmente rastreados. O mesmo principio aqui empregado poderia ser estendido para redes roteadas, porém a técnica empregada para a localização do hardware por meio do endereçamento físico (endereço MAC), que será discutida mais adiante neste parágrafo, seria aplicável apenas dentro de cada segmento comutado, devendo o operador se conectar a interface de gerência do roteador pertencente aquele segmento. A técnica de rastreio e identificação dos pontos baseia-se justamente na peculiaridade já mencionada (seção 3.4) que redes com topologia hierárquica possuem: todos os endereços MAC dos dispositivos conectados aparecerão na *MAC Address Table* do Switch CORE. Esta técnica parte do princípio de que após um ativo ser conectado a qualquer *Switch Ethernet* de acesso, caso este ativo tente enviar algum frame de broadcast (o que geralmente ocorre, pois o Sistema Operacional daquele ativo tentará obter um IP por meio de DHCP Request, nos casos de ativos configurados para obter automaticamente as configurações de rede) o endereço MAC dele aparecerá na *MAC Address Table* do *Switch Ethernet* core. No caso de uma rede segmentada em várias VLANs, além da porta, aparecerá no Switch CORE o número da VLAN (lembre-se que cada VLAN deve ser identificada na tabela de MACs)

Como prova conceitual, foi implementado um procedimento rotineiro de *troubleshooting* que consiste em configurar adequadamente a VLAN quando um ativo de rede (neste caso, um aparelho VoIP ou mesmo um computador) são conectados fisicamente a um outro ponto de rede e, como a camada de acesso não esta configurada, acabam não funcionando. Observe que na prática isto ocorre com grande frequência, pois sempre há o deslocamento físico de tais equipamentos entre salas/departamentos e também, no dia a dia não há uma forma eficiente de se manter um mapeamento adequado e confiável a respeito da correspondência na identificação do ponto com o *Switch Ethernet* e porta que pertence aquele ponto.

O Sistema Especialista criado pelo *ExpertSINTA* baseia-se no conceito de *Back-Chaining*, ou seja, partimos de uma lista de hipóteses sobre o provável motivo do não funcionamento adequado do ativo e por meio de perguntas e respostas dirigidas ao técnico que estiver utilizando o sistema o Sistema Especialista buscará, por meio de inferência, uma sugestão de solução. Em meio as perguntas, alguns comandos vão sendo sugeridos para que o técnico digite-os no terminal e consiga obter a resposta de algumas perguntas mais complexas. A listagem completa do sistema aqui proposto pode ser visualizada no Anexo A.

6. Conclusões

Discutimos neste trabalho a ideia de empregar um Sistema Especialista treinado em algumas sintaxes de comandos utilizados em *Switches Ethernet* gerenciáveis para auxiliar um Técnico em Redes a configurar e solucionar problemas em redes gerenciávies heterogenias. Os resultados alcançados neste experimento foram animadores, demonstrando a viabilidade de uma implementação mais extensa que englobe outros modelos de equipamentos bem como outros fabricantes.

Uma proposta futura é a de automatizações mais agressivas, onde ao invés de

orientar um técnico a digitar no terminal os comando sugeridos para obter algumas das respostas ao questionamentos propostos, o próprio Sistema Especialista se comunica com o terminal do *Switch Ethernet*, executa os comandos e obtém as respostas das quais precisa. Poderíamos até pensar em sistemas totalmente automatizados, nos quais o Sistema Especialista consiga se comunicar com o terminal do *Switch Ethernet* enviando comandos, fazendo análises dos resultados e enviando novos comandos até que o problema seja automaticamente solucionado.

Referências

Donahue, G. A. (2007). *Network Warrior*. USA: O'Reilly, 1st edition.

Fall, K. R. and Stevens, W. R. (2011). *TCP/IP Illustrated, Volume 1: The Protocols*. USA: Addison-Wesley, 2nd edition.

Gansner, E. R., Koutsofios, E., and North, S. (2010). *Drawing graphs with dot*. Disponível em: http://www.graphviz.org/pdf/dotguide.pdf. Acesso em 15.AGO.14.

LIA (1995). *Manual do Expert Sinta v1.1 - Uma ferramenta visual para criação de sistemas especialistas*. Laboratório de Inteligência Artificial da Universidade Federal do Ceará (LIA). Disponível em: http://www.lia.ufc.br/ bezerra/exsinta. Acesso em 12.AGO.14.

Spurgeon, C. E. and Zimmerman, J. (2013). *Ethernet Switches*. USA: O'Reilly, 1st edition.

Spurgeon, C. E. and Zimmerman, J. (2014). *Ethernet The Definitive Guide. Designing and Managing Local Area Networks*. USA: O'Reilly, 2nd edition.

A. Código-fonte completo do sistema especialista desenvolvido

```
1
2  VARIAVEIS UNIVALORADAS
3
4    AFIRM faixa conhecida
5    AFIRM ip conhecido
6    AFIRM ip dentro da faixa da vlan
7    AFIRM mac conhecido
8    AFIRM vlan conhecida
9    AFIRM vlan esta correta
10
11   MSG como alterar a vlan
12     Valores:      ok
13   MSG como alterar o ip
14     Valores:      ok
15   MSG como descobrir a faixa
16     Valores:      ok
17   MSG como descobrir o ip
18     Valores:      ok
19   MSG como descobrir o mac
20     Valores:      ok
21   MSG descobrir vlan no core
22     Valores:      ok
23
24   PERG conhece a faixa
25   PERG conhece a vlan
26   PERG conhece mac
27   PERG conhece o ip
28   PERG ip dentro da faixa da vlan
29   PERG mac/vlan existe no core
30   PERG vlan esta correta
31
32   TESTE ip e vlan ok
33     Valores:
34       sucesso, alterado o ip
35       falha, problemas de configuracao ou fisico
36       sucesso
37       sucesso, alterada a vlan
38
39
40 OBJETIVOS
41     TESTE ip e vlan ok
42
43
44 REGRAS
45
46   Regra 1
47   SE AFIRM ip dentro da faixa da vlan = Sim
48   ENTAO TESTE ip e vlan ok = sucesso CNF 100%
49
50   Regra 2
51   SE PERG conhece a vlan = Sim
52   ENTAO AFIRM vlan conhecida = Sim CNF 100%
53
54   Regra 3
55   SE PERG conhece a vlan = Nao
56   E  AFIRM mac conhecido = Sim
57   E  MSG descobrir vlan no core = ok
58   E  PERG mac/vlan existe no core = Sim
59   ENTAO AFIRM vlan conhecida = Sim CNF 100%
60
61   Regra 4
62   SE PERG conhece a vlan = Nao
63   E  AFIRM mac conhecido = Sim
64   E  MSG descobrir vlan no core = ok
65   E  PERG mac/vlan existe no core = Nao
66   ENTAO TESTE ip e vlan ok = falha, problemas de configuracao ou fisico CNF 100%
67
68   Regra 5
69   SE PERG conhece mac = Sim
```

```
70    ENTAO AFIRM mac conhecido = Sim CNF 100%
71
72    Regra 6
73    SE PERG conhece mac = Nao
74    E  MSG como descobrir o mac = ok
75    ENTAO AFIRM mac conhecido = Sim CNF 100%
76
77    Regra 7
78    SE PERG conhece o ip = Sim
79    ENTAO AFIRM ip conhecido = Sim CNF 100%
80
81    Regra 8
82    SE PERG conhece o ip = Nao
83    E  MSG como descobrir o ip = ok
84    ENTAO AFIRM ip conhecido = Sim CNF 100%
85
86    Regra 9
87    SE AFIRM ip conhecido = Sim
88    E  AFIRM faixa conhecida = Sim
89    E  PERG ip dentro da faixa da vlan = Sim
90    ENTAO AFIRM ip dentro da faixa da vlan = Sim CNF 100%
91
92    Regra 10
93    SE AFIRM ip conhecido = Sim
94    E  AFIRM faixa conhecida = Sim
95    E  PERG ip dentro da faixa da vlan = Nao
96    ENTAO AFIRM ip dentro da faixa da vlan = Nao CNF 100%
97
98    Regra 11
99    SE PERG conhece a faixa = Sim
100   ENTAO AFIRM faixa conhecida = Sim CNF 100%
101
102   Regra 12
103   SE PERG conhece a faixa = Nao
104   E  MSG como descobrir a faixa = ok
105   ENTAO AFIRM faixa conhecida = Sim CNF 100%
106
107   Regra 13
108   SE AFIRM ip dentro da faixa da vlan = Nao
109   E  PERG vlan esta correta = Sim
110   ENTAO AFIRM vlan esta correta = Sim CNF 100%
111
112   Regra 14
113   SE AFIRM ip dentro da faixa da vlan = Nao
114   E  PERG vlan esta correta = Nao
115   ENTAO AFIRM vlan esta correta = Nao CNF 100%
116
117   Regra 15
118   SE AFIRM ip dentro da faixa da vlan = Nao
119   E  AFIRM vlan esta correta = Nao
120   E  MSG como alterar a vlan = ok
121   ENTAO TESTE ip e vlan ok = sucesso, alterada a vlan CNF 100%
122
123   Regra 16
124   SE AFIRM ip dentro da faixa da vlan = Nao
125   E  AFIRM vlan esta correta = Sim
126   E  MSG como alterar o ip = ok
127   ENTAO TESTE ip e vlan ok = sucesso, alterado o ip CNF 100%
128
129
130 PERGUNTAS
131
132   Variavel:MSG como alterar a vlan
133   Pergunta:"instrucoes sobre como alterar a vlan"
134
135   Variavel:MSG como alterar o ip
136   Pergunta:"instrucoes sobre como alterar o ip"
137   Motivo: "Como alterar o IP: Maquina Windows
138     "Iniciar -> Painel de Controle -> Central de Rede e Compartilhamento -> (escolher a
          interface)
```

```
    "propriedades -> TCP/IP v4 -> propriedades -> usar o seguinte endereco IP

  Variavel:MSG como descobrir a faixa
  Pergunta:"instrucoes sobre como descobrir a faixa"
  Motivo: "Como descobrir a faixa de IPs valida dentro de uma VLAN
  "**********************************
  "
  "conecte-se ao switch core e utilize o seguinte comando:
  "<core.sw> display Vlan-Interface VLAN
  "onde VLAN = numero da vlan que voce estiver consultando

  Variavel:MSG como descobrir o ip
  Pergunta:"Instrucoes sobre como descobrir o IP"
  Motivo:"Como descobrir o IP da maquina:
  "**************************************
  "Maquina Windows:
  "Iniciar -> Executar ... -> cmd.exe
  "ipconfig /all

  Variavel:MSG como descobrir o mac
  Pergunta:"instrucoes sobre como descobrir o mac"
  Motivo:"Como descobrir o MAC Address da maquina
  "**************************************
  "Maquina Windows:
  "Iniciar -> Executar... -> cmd.exe
  "ipconfig /all

  Variavel:MSG descobrir vlan no core
  Pergunta:"instrucoes sobre como descobrir a vlan no core"
  Motivo:"Como descobrir a VLAN associada a um ponto
  "consultando o switch Core (3com serie 4500/4800)
  "*******************************************
  "conecte-se ao switch core e utilize o comando abaixo,
  "como resposta obtera a VLAN
  "<core.sw> display mac-address MAC_ADDR
  "exemplo:
  "display mac-address 0102-0304-0506

  Variavel:PERG conhece a faixa
  Pergunta: "Voce sabe qual e a faixa de IPs valida dentro da VLAN
    associada ao ponto (fisico) de rede onde o ativo esta conectado?"

  Variavel:PERG conhece a vlan
  Pergunta:"Voce sabe qual VLAN esta realmente associada ao ponto (fisico) de rede onde
      o ativo esta conectado?"

  Variavel:PERG conhece mac
  Pergunta:"Conhece o endereco fisico (mac address) da interface do ativo?"

  Variavel:PERG conhece o ip
  Pergunta:"Voce sabe qual o IP que o ativo possui?"

  Variavel:PERG ip dentro da faixa da vlan
  Pergunta:"O IP que o ativo possui esta dentro da faixa associada aquela VLAN?"

  Variavel:PERG mac/vlan existe no core
  Pergunta:"A busca pelo MAC do dispositivo no switch CORE retornou alguma VLAN?"

  Variavel:PERG vlan esta correta
  Pergunta:"A VLAN esta correta (de acordo com a politica de gerencia da Rede)?"
```