UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIA

ESPECIALIZAÇÃO EM TELEINFORMÁTICA E REDES DE COMPUTADORES

THIAGO CESAR DUTRA DE FREITAS

SEGMENTAÇÃO DA REDE DE DADOS DE UMA FÁBRICA DE COMPONENTES TECNOLÓGICOS

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA

2015

THIAGO CESAR DUTRA DE FREITAS

SEGMENTAÇÃO DA REDE DE DADOS DE UMA FABRICA DE COMPONENTES TECNOLÓGICOS

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Teleinformática e rede de computadores, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR

Orientador: Prof. Lincoln Herbert Teixeira

CURITIBA

2015

RESUMO

FREITAS, Thiago Cesar D. de, **Segmentação da rede de dados de uma fábrica de componentes tecnológicos.** 45 páginas, monografia (Especialização em Teleinformática e Redes de Computadores) – Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Este trabalho discute sobre as características da infraestrutura de rede, necessária para segmentar a rede de uma fábrica de montagem de componentes de técnologia. Apresenta-se um caso de uma rede não segmentada, onde haviam vários problemas de rede parada, fazendo com que a produção fosse afetada. Um novo projeto foi proposto, onde foi apresentado uma nova topologia segmentando com Vlans, as para isso seria necessário a aquisição de novos switches. Conceitos de topologia de rede segmentada, qualidade dos serviços, características dos equipamentos, segurança e redes virtuais são discutidos a fim de explorar toda necessidade da infraestrutura para suportar uma rede totalmente segmentada.

Palavras-chave: Redes Segmentadas, DHCP, VTP, Roteamento Estático. ..

ABSTRACT

FREITAS, Thiago Cesar D. de. **Segmentation of the data network of a factory technological components.** 45 pages, monograph (Specialization in Teleinformática and Computer Networks) - Federal Technological University of Paraná. Curitiba, 2015.

This work discuss about the characteristics of the network infrastructure necessary to segment the network of an assembly plant technology components. It presents a case of non-segmented network, which had various problems stop net, making production was affected. A new project has been proposed, where a new topology targeting with Vlans was displayed, for that would require the acquisition of new switches. Segmented network topology concepts, quality of services, equipment features, security and virtual networks are discussed in order to explore all need the infrastructure to support a fully segmented network.

Keywords: Segmented networks, DHCP, VTP, Static Routing. ..

LISTA DE SIGLAS

ARP - Address Resolution Protocol

DHCP - *Dynamic Host Configuration Protocol*

IEEE - Institute of Electrical and Eletronics Engineers

IP – Internet Protocol

GBIC - Gigabit Interface Converter

Gbps – Giga bits per Second

LAN – Local Area Network

MAC - Media Access Control

Mbps - Megabits per Second

NBR – Brazilian Standard

OSI - Open Systems Interconnection

RFC - Request for Comments

STP – Spanning Tree Protocol

TCP - *Transmission Control Protocol*

TCP/IP - Transmission Control Protocol over Internet Protocol

VLAN – Virtual Local Access Network

VTP – VLAN Trunk Protocol

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

Sumário

1. INTRODUÇÃO

Este trabalho irá discutir a melhoria com a segmentação de redes dentro de uma indústria de produção de equipamentos que precisam de IP. Será mostrado que uma rede com uma grande área de conflito de broadcast, pode deixar a rede com uma instabilidade e lentidão, muitas vezes deixando a empresa parada sem faturamento. Neste estudo será abordado, os aspectos importantes do projeto de rede, como topologia, hierarquia, e segmentação. A base teórica do trabalho serve de referência para as discussões e entendimento das tomadas de decisão sobre a tecnologia adotada. Ao final, espera-se que este trabalho possa contribuir para um melhor entendimento das práticas a serem adotas no planejamento e concepção das novas infraestruturas de redes estruturadas.

1.1 TEMA

Com o crescimento desordenado das redes de comunicação e seus serviços tem gerado um grande aumento de fluxo de dados nas redes locais. A redes se tornaram muito importantes para o cotidiano de todas as pessoas e as exigências dos usuários em relação aos sistemas que utilizam redes de comunicação, se tornaram maiores (SHI;SJöDIN, 2007). A configuração e localização de equipamentos e dos protocolos dever ser ajustados da melhor maneira possível com a intenção de criar uma rede de comunicação que cumpra os propósitos para os quais ela está projetada (DOOLEY, 2002). A infraestrutura de uma rede local pode, em algumas situações, não conseguir suprir a demanda computacional de seus usuários. Com isso, torna-se necessário uma reestruturação lógica das redes de comunicação, de forma a aproveitar os recursos já existentes e proporcionar um melhor desempenho e maior facilidade nas atividades de gerenciamento. Essa reformulação é possível por meio da segmentação virtual de redes de comunicação, ou seja, a criação de *Virtual Local Area Network* (VLAN). O termo VLAN refere-se à criação de redes locais virtuais em um mesmo equipamento ou conjunto de

equipamentos de rede. Em segmentos de redes *Ethernet* muito extensos, as VLANs podem reduzir os domínios de colisão, melhorando consideravelmente o desempenho (IEEE SOCIETY COMPUTER, 2006).

1.2 DELIMITAÇÃO DA PESQUISA

A pesquisa, será relacionada à segmentação de rede através do uso de VLANs, abrange os principais conceitos da tecnologia. Serão abordados os conceitos básicos sobre VLAN, protocolo 802.1q, roteamento entre VLANs, *Access Control List*(ACL), sobre o protocolo VLAN Trunk Protocol (VTP) e sobre criação de vários Pools DHCP. Além dos conceitos, é apresentado um cenário de um projeto já aplicado em uma indústria de montagem de computadores, bem como os comandos necessários para a configuração dos equipamentos.

1.3 PROBLEMA

Com o crescimento da companhia de montagem de computadores, percebeu-se que a rede de comunicação estava muito grande e com um único domínio de colisão gigantesco, com isso estava ocasionando parada dentro da linha de produção, pois. por mais que a rede fosse de grande extensão, estava limitada pelo range DHCP, com isso ocorria falhas de distribuição de IPs e travamento nos switches.

> Foi observado que a rede atual e a grande quantidade de dispositivos montados pertenciam ao mesmo domínio de broadcast. Pacotes de dados enviados a todos os dispositivos de uma rede são chamados de Broadcast (KUROSE, 2006). O trafego broadcast é necessário para o bom funcionamento da rede, mas limitar o tamanho do domínio de broadcast em uma LAN traz benefícios de desempenho, segurança e privacidade. (FILIPPETTI, 2014).

1.4 OBJETIVO

A seguir, serão apresentados os objetivos, geral e específico, pretendidos com o projeto de pesquisa.

1.4.1 OBJETIVO GERAL

Realizar um estudo sobre a atual estrutura da rede de comunicação da indústria de montagem de computadores, e propor uma solução de segmentação da rede utilizando VLANs.

1.4.2 OBJETIVOS ESPECIFICOS

Os objetivos específicos são:

- Compreender como funciona uma rede segmentada por VLAN;
- Propor a criação de sub-redes.
- Propor a criação de VLANs conforme características da organização;
- Propor a criação de um domínio VTP;
- Relacionar protocolos que serão utilizados;
- Propor vários Pools DHCP;
- Criar um ambiente de simulação conforme a proposta apresentada;
- Apresentar as configurações necessárias para a implementação da proposta.

1.5 JUSTIFICATIVA

Dentro da fábrica existem um grande número de computadores fixos e outro numero de produzidos por dia, com isso ocorriam várias paradas diárias por estouro DHCP e muitos travados por ter placas de rede com defeito durante a produção. Quando ocorrem essas falhas, o departamento de suporte

precisa dar uma atenção especial para que a linha de produção não fique inoperante.

Sendo assim, foi realizado um estudo para segmentar a rede, apartando a linha de produção das demais redes da fábrica, mas caso alguém necessite de um dado da linha de produção, consiga comunicar com a rede apartada. A ideia é fazer uma produção de vários equipamentos durante o dia sem estouro do range DHCP e sem paradas na rede por travamento de equipamentos que por ventura venham a ter falhas.

Para que a rede não entre em colapso, foram tomadas algumas medidas como adquirir switches totalmente gerenciáveis, no caso foram comprados Switches CISCO 2960X, para que pudesse criar VLANs e de fato segmentar, sabendo onde é o ponto que está afetando a rede, deixando essa porta em estado desligado.

1.6 PROCEDIMENTOS METODOLOGICOS

Para o desenvolvimento desse projeto foram usadas as seguintes metodologias:

- Pesquisa bibliográfica de referência clássica sobre redes de computadores
- Pesquisa bibliográfica sobre redes VLAN.
- Para a simulação foi necessário o software Packet Tracer desenvolvido pela empresa Cisco

1.7 FUNDAMENTAÇÃO TEÓRICA

Os conceitos e protocolos, abordados e estudados no transcorrer desta monografia, são fundamentados na literatura relacionada à área de telecomunicações e redes de computadores.

1.8 ESTRUTURA

O trabalho está dividido em 4 capítulos e 1 apêndice. O capítulo 2 aborda conceitos básicos segmentação de rede, protocolo VTP, serviço DHCP e descrição de roteamento. O capítulo 3 traz uma visão geral da infraestrutura de rede de uma fábrica de produção de equipamentos de tecnologia, ao qual se propõe a adoção de uma rede segmentada. Neste capítulo também é apresentada a proposta de uma rede local hierárquica e segmentada para a fábrica. E por final, o capítulo 4 apresenta as conclusões e considerações finais sobre o trabalho proposto. Os comandos utilizados executados para a criação do cenário em simulador são relacionados e explicados no apêndice A.

2. REFERENCIAL TEORICO

Neste capitulo será abordado os conceitos necessários para a compreensão do funcionamento de redes locais virtuais (VLAN), será apresentado o conceito básico de VTP, como também o serviço DHCP e descrição sobre roteamento estático.

2.1 REDES LOCAIS VIRTUAIS

Uma rede local, LAN (Local Area Network), era definida com o uma rede de computadores fisicamente conectados e localizados em uma mesma área geográfica. Nos dias de hoje, podemos defini-la como um único domínio de colisão e de mesma propriedade e tendo como limite geográfico o roteador da rede. Isto quer dizer que se um usuário transmite informações através da LAN e esta informação pode ser recebida por qualquer outro dispositivo da rede. Essas transmissões têm como limite o roteador da rede.

Para Tanenbaum e Wetherall (2011), o crescimento das redes LAN, acima de 500 dispositivos, abrigados num mesmo local, pode gerar alguns problemas, entre eles, três principais no seu gerenciamento: o tráfego de *broadcasting*, a velocidade e a segurança. A busca de uma solução física, separando as redes de acordo com a estrutura organizacional, pode gerar uma inflexibilidade na rede (TANENBAUM e WETHERALL, 2011). Por esta razão, surgiu o conceito de separação lógica das redes, ou seja, criar redes logicamente separadas sem alterar sua disposição física.

As VLANs surgiram da necessidade de uma maior flexibilidade nas redes de computadores, por não possuírem limitações físicas, podendo ser organizadas de formas variadas. Uma VLAN, ou rede virtual, é um grupo de estações e servidores que se comunicam independente de sua localização física ou de topologia, como se fosse um único domínio de broadcast, ou uma mesma rede lógica (FELLIPETTI, 2014)

O conceito de VLANSs, surge como uma resposta a alguns problemas. VLANs, essencialmente, são domínios lógicos definidos em switches. É uma forma de conseguirmos segmentar um grande domínio de broadcast (uma LAN) sem a necessidade de utilizarmos elemento de camada 3 (como um router) (FILIPPETTI, 2014).

Máquinas associadas a uma VLAN apenas podem enxergar frames originados por equipamentos que pertencem a mesma VLAN. Isso implica que broadcast gerados em uma VLAN ficarão contidos aquele domínio. Máquinas associadas a outras VLANs não terão acesso a esses frames, mesmo que estejam fisicamente conectadas ao mesmo switch (FILIPPETTI, 2014).

Para que seja entendido VLAN, basicamente precisamos entender o conceito de departamentos dentro de uma empresa, onde possui RH, financeiro, produção, TI, entre outros. Esses departamentos fazem atividades independentes, mas uma hora ou outra vão precisar se comunicar com outro departamento, com isso entramos no conceito de camada 3, que seria o roteamento para a outra área que poderia ser a outra VLAN.

2.2. PROTOCOLO VTP

A Cisco criou o VLAN Trunck Protocol para gerenciar e manter a consistência de todas as VLANs configuradas em uma rede. Para permitir que protocolo VTP gerencie as VLANs em uma rede é necessária, antes, a definição de um domínio VTP. Um domínio VTP nada mais é do que um conjunto de switches que trocarão informações VTP entre si (FILIPPETTI,2014).

O VTP é um protocolo de propriedade da Cisco que está disponível na maioria dos produtos Cisco Catalyst Series.

Para manter a conectividade das Vlans em toda a estrutura do switch, as Vlans devem ser configuradas em cada switch. O protocolo VTP (Vlan Trunking Protocol) da Cisco garante um método mais fácil para a manutenção de uma configuração de Vlan consistente em toda a rede comutada.

Usado para distribuir e sincronizar informações de identificação das Vlans configuradas em toda a rede comutada. As configurações estabelecidas em um único servidor VTP são propagadas através do enlace tronco para todos os switches conectados na rede (NETWORK LESSONS).

Como diz FELLIPETTI, para comunicação de um domínio VTP necessita ter um servidor e clientes para que possa existir esse domínio, caso tenha um equipamento fora desse domínio estarão fora.

Na figura 1, essa imagem expressa bem o que seria esse domínio

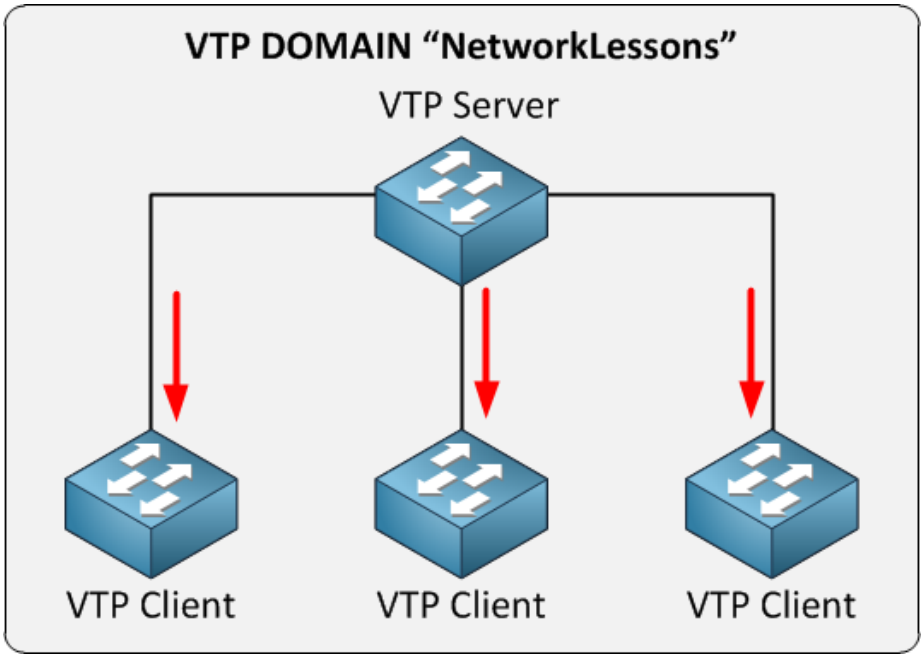

Figura 1 – NETWORK LESSONS.

O interessante desse protocolo ativo na rede é caso algum switch ou roteador seja conectado e esse esteja fora do domínio VTP, a rede irá identificar e fazer um bloqueio a ele, ou seja, no aspecto prático irá desligar a porta do switch que ele foi ligado.

2.3. SERVIÇO DHCP

Dynamic Host Configuration Protocol (DHCP) é um protocolo cliente/servidor que fornece automaticamente um host de IP (Internet Protocol) com seu endereço IP e outras informações de configuração relacionados, como o gateway padrão e máscara de sub-rede. As RFCs 2131 e 2132 definem DHCP como um padrão Internet Engineering Task Force (IETF) com base em Bootstrap Protocol (BOOTP), um protocolo com o qual o DHCP compartilha muitos detalhes de implementação. O DHCP permite que os hosts obtenham informações de configuração de TCP/IP necessárias de um servidor DHCP (TECHNET,2015).

Sem o uso do DHCP, o administrador da rede e a sua equipe teriam que configurar, manualmente, as propriedades do protocolo TCP/IP em cada dispositivo de rede (genericamente denominados hosts). Com o uso do DHCP esta tarefa pode ser completamente automatizada (BATTISTI,2015).

Em uma rede com centenas ou até mesmo milhares de estações de trabalho, configurar o TCP/IP manualmente, em cada estação de trabalho é uma tarefa bastante trabalhosa, que envolve tempo e exige uma equipe técnica para executar este trabalho. Além disso, sempre que houver mudanças em algum dos parâmetros de configuração (como por exemplo uma mudança no número IP do servidor DNS), a reconfiguração terá que ser feita manualmente em todas as estações de trabalho da rede. Por exemplo, imagine que o número IP do Default Gateway teve que ser alterado devido a uma reestruturação da rede. Neste caso a equipe de suporte teria que ir de computador em computador, alterando as propriedades do protocolo TCP/IP, para informar o novo número IP do Default Gateway, isto é, alterando o número IP antigo do Default Gateway para o novo número (BATTISTI,2015).

2.4. ROTEAMENTO ESTÁTICO

Roteamento é o processo utilizado pelo roteador para encaminhar um pacote para uma determinada rede de destino. Este processo é baseado no

endereço IP de destino, os dispositivos intermediários utilizam este endereço para conduzir o pacote até seu destino final (BATTISTI, 2015).

O roteamento estático para rede LAN apresenta vantagens pois são equipamentos que ficam em pequena localidade, caso fosse uma empresa com uma localidade muito maior o ideal seria deixar o roteamento dinâmico afim de que a rede tivesse vários caminhos. Nesse caso a rede é pequena para expressar tal complexidade.

Segundo FELIPPETTI as vantagens do roteamento estático é o menor consumo de memória e CPU no router, não há utilização de largura de banda para troca de informações de roteamento entre os routers e o maior controle de rede.

Também segundo FELIPPETTI as desvantagens da rede com roteamento estático é que o administrador necessita de profundos conhecimentos da rede como um todo, para cada uma das redes novas adicionadas, o administrador necessita anunciar em cada roteador da rede, a nova rota que o mesmo necessita seguir.

3. APLICAÇÃO DO PROJETO

Para o desenvolvimento desse projeto surgiu com a experiência vivida em outras companhias a qual existiam redes já segmentadas e com alta performance, onde, se viu a necessidade de aplicar nessa companhia a segmentação, pois na mesma, estava ocorrendo paradas da produção por falhas de rede.

Dentro da companhia existia um ambiente com uma rede com o domínio de broadcast onde poderia ter mais de 65 mil hosts, ou seja, um /16. Com isso o domínio de colisão da rede se tornava muito grande.

3.1 INFRAESTRUTURA ANTIGA

A infraestrutura antiga da fábrica consistia em uma rede toda com cabo UTP e switches todos sem gerenciamento e com velocidade de 100 MB.

Essa rede era uma rede apresentando uma configuração onde o core era o gateway de uma grande rede que no caso era uma rede 10.11.0.0 com máscara 255.255.0.0, como mostrado na figura abaixo.

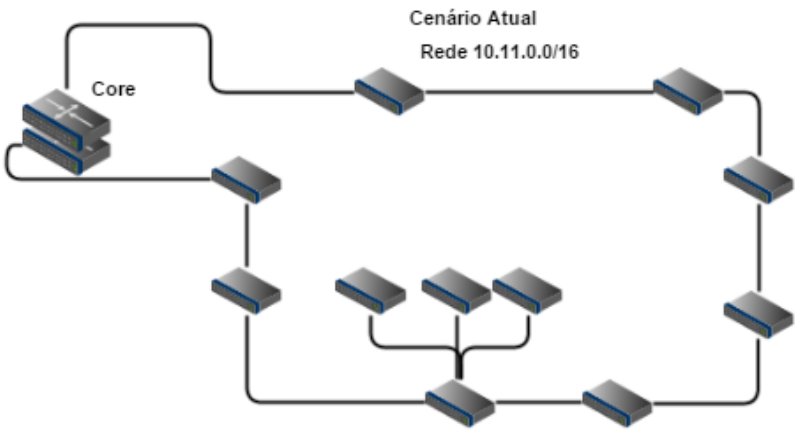

Figura 2 - Cenário Antigo

A segmentação da rede entendia-se que se o servidor DHCP entregasse apenas 512 IPs não teria falhas na comunicação pois estava

limitando a distribuição de IPs pelo serviço DHCP do SO, como mostrado na imagem abaixo exemplo de uma unidade da companhia que ainda não foi aplicado segmentação lógica, esse era o mesmo escopo na fábrica, onde todas as maquinas receberiam IP do DHCP, quando fosse servidor colocaria manualmente no range de servidores já definido na implantação da rede, que seria 10.11.10.0/16.

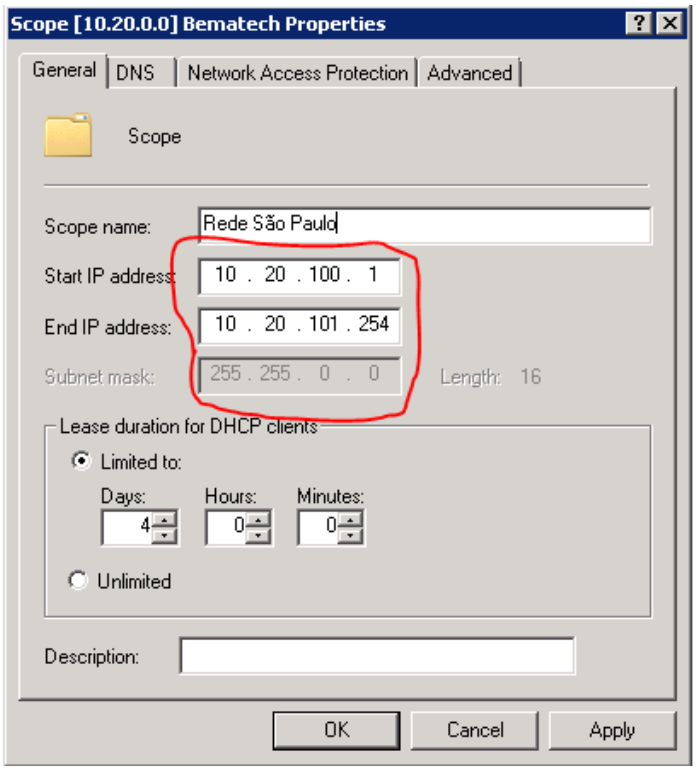

Figura 3 - Exemplo de pool DHCP

3.2 ESTRUTURA FISICA

Os switches antigos eram todos sem gerenciamento e com velocidade de 100 MB, onde podia teoricamente colocar qualquer equipamento na rede, ou seja, como a empresa é uma fábrica que produz equipamentos de tecnologia, sempre, alguém conectava roteadores paralelos que possuíam um serviço DHCP interno, com isso entregavam endereço da IP diferente do que

era projetado e fazia com que a rede ficasse com 2 DHCP entregando endereços diferentes.

3.3 TOPOLOGIA

Foi realizado um estudo da topologia aplicada na rede, onde verificou-se que a forma utilizada era a mais adequada sendo que, a que vinha sendo aplicada tínhamos uma redundância da rede pois estava em forma de anel, a sugestão foi colocar fibra interligando todo o anel da rede.

3.4 SWITCHES

Para que a rede fosse totalmente gerenciada foi escolhido colocar switches Cisco 2960X 48 portas, pois eles possuem todas as portas Gigabit e são gerenciáveis podendo aplicar todo o nível de controle necessário na rede como Spanning tree nas portas, desabilitando-os caso coloquem equipamentos previamente não autorizados pela equipe de infraestrutura de TI.

3.5 SEGMENTAÇÃO DA REDE

Foi realizado um estudo verificando quais áreas deveriam estar totalmente separadas do ambiente, no princípio foi realizado um estudo de separar apenas a rede de produção do restante. Mas após levantamentos, montamos a seguinte estrutura:

```
SJCORE01#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/1, Gi0/3, Gi0/4, Gi0/5
                                                 Gi0/6, Gi0/7, Gi0/8, Gi0/9
                                                 Gi0/10, Gi0/14, Gi0/15, Gi0/18
                                                 Gi0/19, Gi0/21, Gi0/22, Gi0/25
                                                 Gi0/26, Gi0/27
2    FABRICA                           active
3    TESTES                            active
4    ALMOXARIFADO                      active
5    LABORATORIOS                      active
6    IMPRESSAO                         active
7    WIRELESS                          active
8    VIDEOCONFERENCIA                  active
9    VOZ                               active
10   DEFAULT                           active    Gi0/13, Gi0/16, Gi0/17, Gi0/20
11   SERVIDORES                        active    Gi0/11, Gi0/12
12   RELOGIOS                          active
13   FabricaTeste                      active
14   Bilbao                            active
100  LOGCER                            active
200  GERENCIA                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Figura 4 - VLANS no Core

Onde a mesma tinha as seguintes configurações de rede:

ID	Nome	IP	Mascara	Gateway
2	FABRICA	10.11.100.0	255.255.255.0	10.11.100.1
3	TESTES	10.11.101.0	255.255.255.0	10.11.101.1
4	ALMOXARIFADO	10.11.102.0	255.255.255.0	10.11.102.1
5	LABORATORIO	10.11.103.0	255.255.255.0	10.11.103.1
6	IMPRESSÃO	10.11.30.0	255.255.255.0	10.11.30.1
7	WIRELESS	10.11.150.0	255.255.255.0	10.11.150.1
8	VIDEOCONFERENCIA	10.11.160.0	255.255.255.0	10.11.160.1
9	VOZ	10.11.170.0	255.255.255.0	10.11.170.1
10	DEFAULT	10.11.10.0	255.255.255.0	10.11.10.11
11	SERVIDORES	10.11.20.0	255.255.255.0	10.11.20.1
12	RELOGIOS	10.11.40.0	255.255.255.0	10.11.40.1
13	FABRICA_TESTE	10.11.110.0	255.255.255.0	10.11.110.1

Tabela 1 - VLANS Aplicadas

Com essa rede vimos que era a ideal pois estariam todos os ambientes da fábrica separados com sua rede distinta e se comunicando por roteamento. Dessa forma necessita de vários pools DHCP para facilitar a administração.

3.6 DHCP

Para a implantação do serviço DHCP foi estabelecido que seria utilizado o serviço do Windows 2008 R2, com isso precisaria informar ao switch core qual seria o local que ele falaria que o dispositivo iria requisitar o IP, Foi utilizado o comando *ip helper-address*.

3.6.1 POOLS DHCP

Foram criados alguns pools DHCP para cada rede, mas a grande estratégia estava na distribuição de IP dentro da rede FABRICA, uma que tínhamos reduzido a entrega de 512 dispositivos para apenas 250.

Durante a configuração, foi marcado que os IPs seriam renovados a cada 30 minutos. Assim teríamos sempre novos equipamentos sendo testados nessa rede, conforme é mostrado nas figuras abaixo.

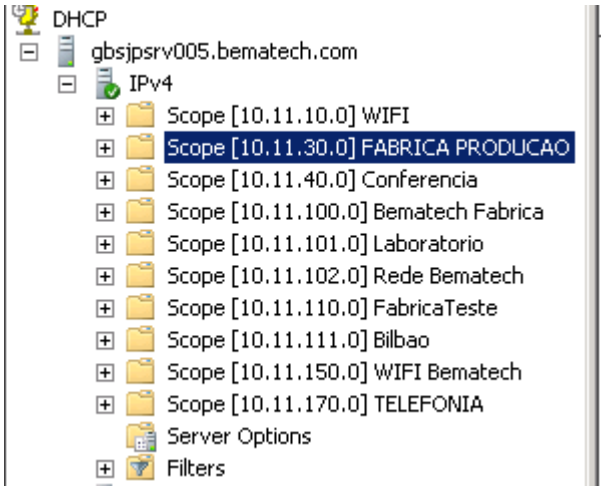

Figura 5 - POOL DHCP Fábrica

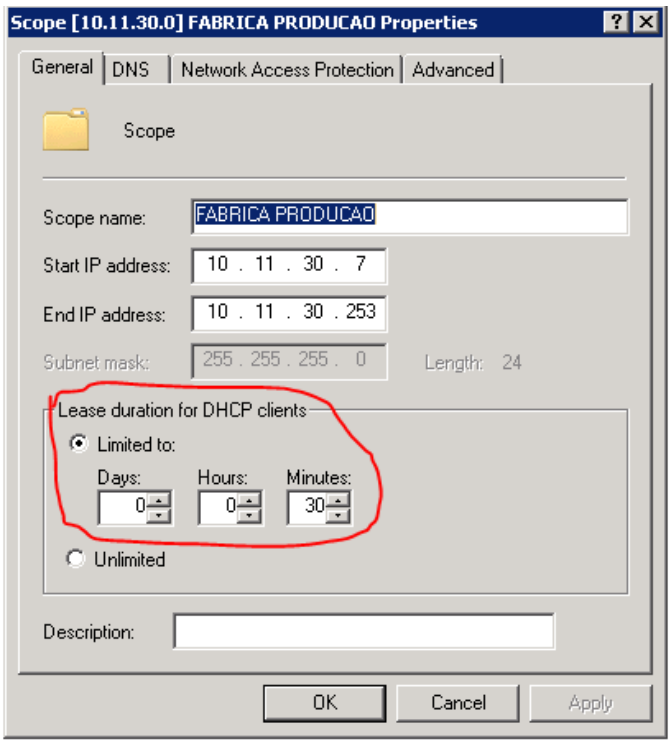

Figura 6 - Tempo de renovação IP Produção

Como nas outras redes temos poucos dispositivos, colocamos um tempo de renovação de 8 horas. Dessa forma o dispositivo terá o mesmo IP durante o dia de trabalho, sem alteração. Esse exemplo é mostrado na figura abaixo:

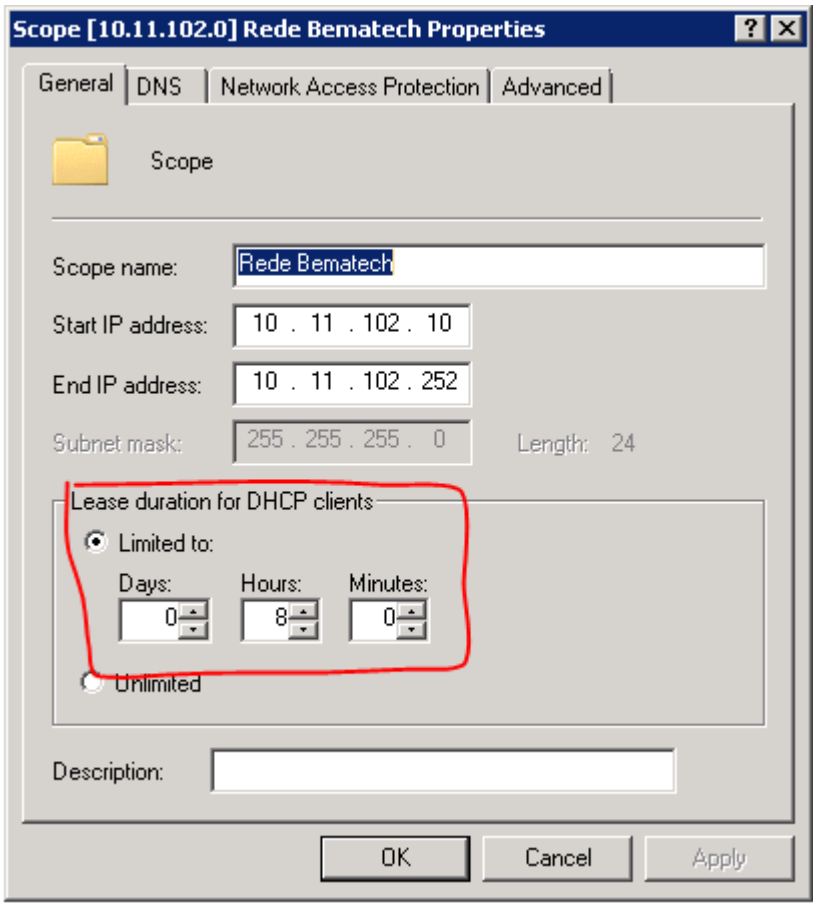

Figura 7 - Tempo de renovação IP Rede Default

Todos os equipamentos dessa maneira estavam se comunicando entre si, mas ainda tinham a necessidade de comunicarem entre as redes da fábrica, com isso houve a necessidade de criar o roteamento estático.

3.7 ROTEAMENTO ESTÁTICO

O caminho para comunicação foi criado de forma que todas as redes internas se comunicassem, deixando apenas isolado o domínio de broadcast, para que a zona de colisão fosse menor do que tinha no início, onde a rede era abrangente, com mais de 65 mil hosts possíveis.

Abaixo segue a figura de como ficaram as rotas apresentadas no switch core.

```
SJCORE01#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.11.10.50 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.11.10.50
      10.0.0.0/8 is variably subnetted, 38 subnets, 4 masks
S        10.1.1.0/24 [1/0] via 10.11.10.4
S        10.10.0.0/16 [1/0] via 10.11.10.10
C        10.11.10.0/24 is directly connected, Vlan10
L        10.11.10.2/32 is directly connected, Vlan10
C        10.11.20.0/24 is directly connected, Vlan11
L        10.11.20.2/32 is directly connected, Vlan11
C        10.11.30.0/24 is directly connected, Vlan6
L        10.11.30.2/32 is directly connected, Vlan6
C        10.11.40.0/24 is directly connected, Vlan12
L        10.11.40.2/32 is directly connected, Vlan12
C        10.11.100.0/24 is directly connected, Vlan2
L        10.11.100.2/32 is directly connected, Vlan2
C        10.11.101.0/24 is directly connected, Vlan3
L        10.11.101.2/32 is directly connected, Vlan3
C        10.11.102.0/24 is directly connected, Vlan4
L        10.11.102.2/32 is directly connected, Vlan4
C        10.11.103.0/24 is directly connected, Vlan5
L        10.11.103.2/32 is directly connected, Vlan5
C        10.11.110.0/24 is directly connected, Vlan13
L        10.11.110.2/32 is directly connected, Vlan13
C        10.11.111.0/24 is directly connected, Vlan14
L        10.11.111.2/32 is directly connected, Vlan14
C        10.11.160.0/24 is directly connected, Vlan8
L        10.11.160.2/32 is directly connected, Vlan8
C        10.11.170.0/24 is directly connected, Vlan9
L        10.11.170.2/32 is directly connected, Vlan9
```

Figura 8 - Lista de Roteamento Estático

Aplicando essas rotas, toda a rede realiza a comunicação entre si e sem afetar a performance da mesma.

4. CONCLUSÃO

Após a aplicação da segmentação da rede percebeu-se que a rede não apresentou mais falhas e nem paradas durante o período de produção. Foi comprovado que existiam equipamentos ultrapassados e sem a capacidade de processamento e técnica para suportar uma produção de equipamentos de tecnologia.

Assim que foram instalados switches Cisco 2960x percebeu-se a grande melhora de performance na rede, pois a mesma foi planejada para que somente equipamentos que recebem IPs possam estar na rede. Dessa forma evitamos que roteadores não homologados possam ser ligados, pois todas as portas estão habilitadas para ficar desligadas caso tenha um equipamento estranho na rede.

Para verificar como a rede ficou pode-se na figura abaixo mostrando através de imagem a segmentação da rede como foi realizada.

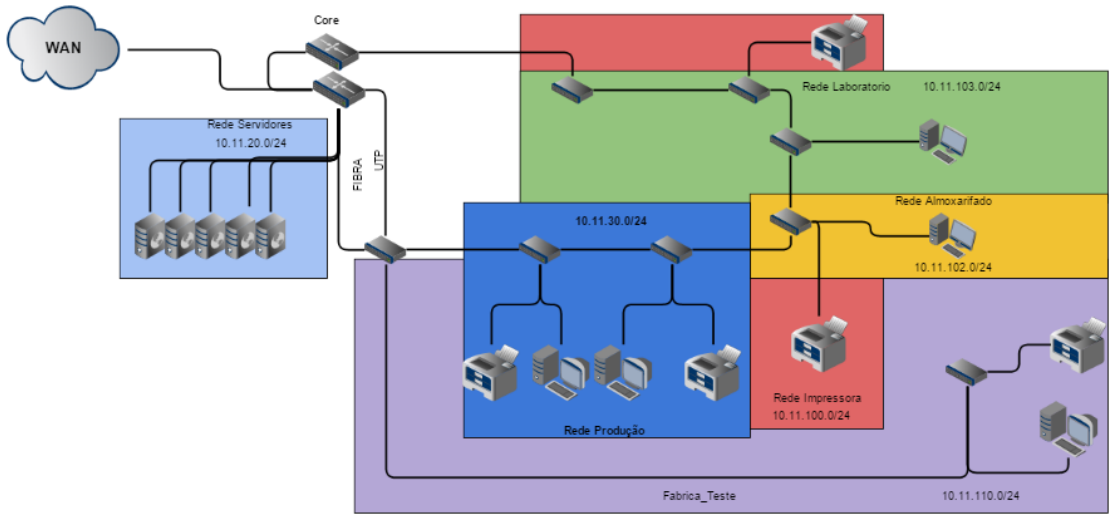

Figura 9 - Topologia de Rede Atual

BIBLIOGRAFIA

BATTISTI,J. http://juliobattisti.com.br/artigos/windows/tcpip_p9.asp, JULHO 2015

DOOLEY, K. Designing Large-Scale LANs. 1. ed. Sebastopol, CA, USA: O'Reilly Associates, Inc., 2002. 385 p. ISBN 0-596-00150-9.

FILIPPETTI, M. AURELIO, *CCNA 5.0 – guia completo de estudo. FLORIANOPOLIS, BRASIL:* Visual Books, 2014. 544 p. ISBN: 978-85-7502-284-9

IEEE SOCIETY COMPUTER. IEEE Std 8021Q. In: *IEEE Standard for Local and metropolitan área networks – Virtual Bridge Local Area Networks. [S1.:s.n.], 2006. p. 303. ISBN 0-7381-4877-6.*

KUROSE, James F., ROSS, Keith W., Redes de computadores e a *Internet*: Uma abordagem top-down. São Paulo: Pearson Addison Wesley, 2006. 634 p.

NETWORK LESSONS, https://networklessons.com/switching/introduction-to-vtp-vlan-trunking-protocol, JULHO 2015.

SHI, L.; SJöDIN, P. A VLAN Ethernet Backplane for Distributed. *IEEE Comunications Magazine, p. 42-45, 2007.*

TANENBAUM, Andrew S., WETHERALL, David J. Computer Networks. 5ª.ed. Boston: Pearson, 2011.

TECHNET, *https://technet.microsoft.com/library/dd145320(v=ws.10).aspx, JULHO 2015.*

ANEXO 1

Configuração do Switch Core Cisco 3750

showtec tec run

Building configuration...

Current configuration : 14893 bytes

Last configuration change at 11:58:16 BRZ Thu Jul 16 2015 by admin

! NVRAM config last updated at 12:16:53 BRZ Thu Jul 16 2015 by admin

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

hostname SJCORE01

boot-start-marker

boot-end-marker

no logging console

enable password 7 02422A7B244701221C43591D25

username admin privilege 15 secret 4 842lolAjVXsVx3kW4VKP1CF5pud8y9JoxuY2dCl6RPg

aaa new-model

aaa authentication login default enable local

aaa authentication enable default enable

aaa session-id common

clock timezone BRZ -3 0

```
 clock summer-time BRZ-DST recurring 3 Sun Oct 0:00 3 Sun Feb 0:00
 system mtu routing 1500
 vtp mode transparent
 ip routing
 no ip domain-lookup
 ip domain-name FABRICA.com
key chain hsrp1
key 0
key-string 7 0526261C35495C584B56
password encryption aes
crypto pki trustpoint TP-self-signed-85762432
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-85762432
revocation-check none
rsakeypair TP-self-signed-85762432
crypto pki certificate chain TP-self-signed-85762432
certificate self-signed 01
quit
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-1005 priority 0
vlan internal allocation policy ascending
vlan 2
name FABRICA
vlan 3
name TESTES
```

```
vlan 4
name ALMOXARIFADO
vlan 5
name LABORATORIOS
vlan 6
name IMPRESSAO
vlan 7
name WIRELESS
vlan 8
name VIDEOCONFERENCIA
vlan 9
name VOZ
vlan 10
name DEFAULT
vlan 11
name SERVIDORES
vlan 12
name RELOGIOS
vlan 13
name FabricaTeste
vlan 14
name Bilbao
vlan 100
name LOGCER
vlan 200
name GERENCIA
```

track 1 ip sla 1 reachability

ip ssh version 2

interface Port-channel1

description ## UPLINK - SJCORE02 ##

switchport trunk encapsulation dot1q

switchport mode trunk

interface GigabitEthernet0/1

description ## UPLINK SW1 ##

switchport trunk encapsulation dot1q

switchport mode trunk

switchport nonegotiate

spanning-tree portfast

interface GigabitEthernet0/2

description Gbsjpsw031_GI1/0/1

switchport trunk encapsulation dot1q

switchport mode trunk

interface GigabitEthernet0/3

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/4

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/5

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/6

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/7

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/8

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/9

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/10

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/11

switchport access vlan 11

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/12

description SERVER028_Eth1

switchport access vlan 11

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/13

switchport access vlan 10

switchport mode access

```
spanning-tree portfast
interface GigabitEthernet0/14
switchport mode access
spanning-tree portfast
interface GigabitEthernet0/15
switchport mode access
switchport nonegotiate
spanning-tree portfast
interface GigabitEthernet0/16
description ## ROUTER-MPLS ##
switchport access vlan 10
switchport mode access
switchport nonegotiate
spanning-tree portfast
interface GigabitEthernet0/17
description FORTIGATE1
switchport access vlan 10
switchport mode access
spanning-tree portfast
interface GigabitEthernet0/18
switchport mode access
spanning-tree portfast
interface GigabitEthernet0/19
switchport mode access
spanning-tree portfast
interface GigabitEthernet0/20
```

description FORTIGATE1

switchport access vlan 10

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/21

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/22

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/23

description Conexao com SWSJPCORE03 - Gi0/2

switchport trunk encapsulation dot1q

switchport trunk allowed vlan 10,100

switchport mode trunk

interface GigabitEthernet0/24

description ## UPLINK - SJCORE02 ##

switchport trunk encapsulation dot1q

switchport mode trunk

channel-group 1 mode on

interface GigabitEthernet0/25

switchport trunk encapsulation dot1q

switchport mode trunk

interface GigabitEthernet0/26

interface GigabitEthernet0/27

interface GigabitEthernet0/28

```
description ## UPLINK - SJCORE02 ##
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode on
interface Vlan1
no ip address
shutdown
interface Vlan2
description FABRICA
ip address 10.11.100.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.100.1
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
interface Vlan3
description TESTES
ip address 10.11.101.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.101.1
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
interface Vlan4
```

```
description ALMOXARIFADO
ip address 10.11.102.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.102.1
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
interface Vlan5
description LABORATORIOS
ip address 10.11.103.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.103.1
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
interface Vlan6
description IMPRESSAO
ip address 10.11.30.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.30.1
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
```

```
interface Vlan7
description WIRELESS
ip address 10.11.150.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.150.1
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
shutdown
interface Vlan8
description VIDEOCONFERENCIA
ip address 10.11.160.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.160.1
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
interface Vlan9
description VOZ
ip address 10.11.170.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.170.1
standby 1 priority 255
```

```
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
interface Vlan10
description DEFAULT
ip address 10.11.10.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.10.11
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
interface Vlan11
description SERVIDORES
ip address 10.11.20.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.20.1
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
interface Vlan12
description RELOGIOS
ip address 10.11.40.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.40.1
```

```
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
interface Vlan13
description FabricaTeste
ip address 10.11.110.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.110.1
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
interface Vlan14
description Bilbao
ip address 10.11.111.2 255.255.255.0
ip access-group 101 out
ip helper-address 10.11.20.5
standby 1 ip 10.11.111.1
standby 1 priority 255
standby 1 preempt
standby 1 authentication md5 key-chain hsrp1
interface Vlan100
ip address 10.13.100.1 255.255.255.240
interface Vlan200
description GERENCIA
ip address 10.11.200.2 255.255.255.0
```

ip access-group 101 out

ip helper-address 10.11.20.5

standby 1 ip 10.11.200.1

standby 1 priority 255

standby 1 preempt

standby 1 authentication md5 key-chain hsrp1

no ip http server

ip http authentication local

ip http secure-server

ip route 10.12.0.0 255.255.0.0 10.11.10.10 track 1

ip route 10.20.0.0 255.255.0.0 10.11.10.10 track 1

ip route 10.22.0.0 255.255.0.0 10.11.10.10 track 1

ip route 10.10.0.0 255.255.0.0 10.11.10.10 track 1

ip route 10.130.0.0 255.255.0.0 10.11.10.10 track 1

ip route 192.168.128.0 255.255.224.0 10.11.10.10 track 1

ip route 0.0.0.0 0.0.0.0 10.11.10.50

ip route 10.1.1.0 255.255.255.0 10.11.10.4

ip route 10.155.0.0 255.255.255.0 10.20.10.12

ip route 10.156.164.0 255.255.255.0 10.20.10.50

ip route 10.200.0.0 255.255.0.0 10.11.10.10

ip route 10.201.20.0 255.255.255.0 10.11.10.10

ip sla 1

icmp-echo 10.200.10.12 source-interface Vlan10

threshold 5

frequency 10

ip sla schedule 1 life forever start-time now

logging trap debugging

logging host 10.200.20.3

access-list 101 deny ip 10.11.0.0 0.0.255.255 10.1.1.0 0.0.0.255 log

access-list 101 permit ip any any log

access-list 102 permit ip 10.13.100.0 0.0.0.15 10.200.0.0 0.0.255.255 log

snmp-server community BEMATECH RO

snmp-server community private RW

snmp-server community public RO

snmp-server location "DATACENTER CURITIBA"BEMATECH_SJ-CORE01

snmp-server contact suporte.redes@bematech.com.br

snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart

snmp-server enable traps flowmon

snmp-server enable traps transceiver all

snmp-server enable traps call-home message-send-fail server-fail

snmp-server enable traps tty

snmp-server enable traps eigrp

snmp-server enable traps ospf state-change

snmp-server enable traps ospf errors

snmp-server enable traps ospf retransmit

snmp-server enable traps ospf lsa

snmp-server enable traps ospf cisco-specific state-change nssa-trans-change

snmp-server enable traps ospf cisco-specific state-change shamlink interface

snmp-server enable traps ospf cisco-specific state-change shamlink neighbor

snmp-server enable traps ospf cisco-specific errors

snmp-server enable traps ospf cisco-specific retransmit

snmp-server enable traps ospf cisco-specific lsa

snmp-server enable traps cluster

snmp-server enable traps fru-ctrl

snmp-server enable traps entity

snmp-server enable traps cpu threshold

snmp-server enable traps power-ethernet police

snmp-server enable traps rep

snmp-server enable traps vtp

snmp-server enable traps vlancreate

snmp-server enable traps vlandelete

snmp-server enable traps flash insertion removal

snmp-server enable traps port-security

snmp-server enable traps auth-framework sec-violation

snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-guest-vlan

snmp-server enable traps envmon fan shutdown supply temperature status

snmp-server enable traps bgp

snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency

snmp-server enable traps config-copy

snmp-server enable traps config

snmp-server enable traps config-ctid

snmp-server enable traps event-manager

snmp-server enable traps hsrp

snmp-server enable traps ipmulticast

snmp-server enable traps isis

snmp-server enable traps msdp

snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message

snmp-server enable traps energywise

snmp-server enable traps vstack

snmp-server enable traps bridge newroot topologychange

snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency

snmp-server enable traps syslog

snmp-server enable traps ipsla

snmp-server enable traps ike policy add

snmp-server enable traps ike policy delete

snmp-server enable traps ike tunnel start

snmp-server enable traps ike tunnel stop

snmp-server enable traps ipsec cryptomap add

snmp-server enable traps ipsec cryptomap delete

snmp-server enable traps ipsec cryptomap attach

snmp-server enable traps ipsec cryptomap detach

snmp-server enable traps ipsec tunnel start

snmp-server enable traps ipsec tunnel stop

snmp-server enable traps ipsec too-many-sas

snmp-server enable traps mac-notification change move threshold

snmp-server enable traps vlan-membership

snmp-server enable traps errdisable

snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down

line con 0

privilege level 15

logging synchronous

line vty 0 4

exec-timeout 0 0

privilege level 15

logging synchronous

transport input ssh

line vty 5 15

exec-timeout 0 0

privilege level 15

logging synchronous

transport input ssh

ntp source Vlan1

ntp server 10.200.20.139

end