UNVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRONICA
CURSO DE ESPECIALIZAÇÃO EM SOFTWARE LIVRE APLICADO A TELEMATICA

DANIEL ERNESTO WAGNER

SEGMENTAÇÃO E ROTEAMENTO DE VLAN'S EM SERVIDORES LINUX UTILIZANDO O PROTOCOLO 802.1Q

MONOGRAFIA

CURITIBA - PR
2012

DANIEL ERNESTO WAGNER

SEGMENTAÇÃO E ROTEAMENTO DE VLAN'S EM SERVIDORES LINUX UTILIZANDO O PROTOCOLO 802.1Q

Monografia apresentada ao Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de "Especialista em Software livre aplicado a telemática." -
Orientador: Prof. Dr. Kleber Nabas

CURITIBA - PR

2012

RESUMO

WAGNER, Daniel Ernesto. Segmentação e roteamento de vlan's em servidores linux utilizando o protocolo 802.1q. 2012. 31 f. Monografia (Especialização em Software Livre Aplicado a Telemática) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

Devido a necessidade de aumentar a segurança, privacidade e melhorar o desempenho da rede com a otimização dos recursos venho com a proposta de utilizar a segmentação através da criação de vlan's, aumentando a segurança e privacidade das informações contidas em cada sub-rede criada, aprimorando a utilização de uma DMZ para utilização de equipamentos e serviços comuns a varias sub-redes e ate mesmo acesso externos as dependências do departamento, utilizando a customização do kernel do sistema operacional linux, dando suporte ao protocolo IEEE 802.1Q assim reconhecendo em uma única interface ethernet as TAG`'s de VID assim podendo um único equipamento fazer todo o trabalho de redirecionamento, interconexão, serviço de servidor de DHCP e ainda regras de filtragem através de software livre, não utilizando hardware ou software proprietário.

Para isso os procedimentos relacionados nesse material indicarão as formas e recursos necessários para atingir esse objetivo.

Palavras Chaves: Vlan. 802.1Q. Linux. Roteamento.

ABSTRACT

WAGNER, Daniel Ernesto. Segmentation and routing vlan's Linux servers using the 802.1q protocol. 2012. 31 f. Monograph (Specialization in Open Source Software Applied to Telematics) - Graduate Program in Technology, Federal Technological University of Paraná. Curitiba, 2012.

Because of the need to increase security, privacy and improve network performance by optimizing resources come with the proposal to use the segmentation by creating vlan's, increasing security and privacy of information contained in each subnet created, improving the use of a DMZ for use of equipment and services common to several subnets and even access external dependencies department, using the customization of linux operating system kernel, supporting IEEE 802.1Q protocol thus recognizing a single interface the ethernet `TAG 's VID so one device can do the whole job redirection, interconnection, service and DHCP server still filtering rules through free software, not hardware or using proprietary software.
For related procedures that indicate that material forms and resources needed to achieve this goal..

Key Words: Vlan. 802.1Q. Linux. Routing.

SUMÁRIO

Lista de Figuras

Lista de Tabelas

1. INTRODUÇÃO

Devido a necessidade de segmentação de rede e otimização dos recursos a proposta será a segmentação através da criação de vlan's e fazer todo o trabalho de roteamento, interconexão, regras de filtragem através de software livre, não utilizando hardware ou software proprietário.

Com a segmentação ira trazer maior segurança e privacidade das informações para cada laboratório, sendo compartilhados as informações e os recursos somente com quem há de direito, essa segmentação também diminui o domínio de *broadcast* diminuindo o problema de interferência estranhas ao ambiente, tais como servidores de DHCP não autorizados, sniffers de rede, etc.

A criação de uma DMZ torna possível o compartilhamento seguro de serviços e equipamentos tais como servidores de licenças de softwares, compartilhamentos de arquivos comuns para varias sub-redes, utilização comunitária de serviços de impressão.

Um serviço de DHCP otimizado para atender todas as sub-redes otimiza melhor a administração, pois concentra em um único hardware, o que facilita também a implementação de novos serviço sem a necessidade de replicação para a as varias sub-redes.

Nesta monografia serão abordados as fases e procedimentos necessários para alcançar o objetivo completo da proposta, melhorando e otimizando a infra-instrutora de rede atual.

Obs.: Os endereçamentos IP apresentados foram suprimidos ou alterados por motivo de segurança e privacidade do departamento a pedido do orientador e coordenador do departamento.

2. OBJETIVOS

Fazer a segmentação de varias redes através de Vlan's (Virtual Local Network) com um único servidor que irá rotear as redes, distribuir os endereçamentos de rede via DHCP e fazer o compartilhamento da internet para todas as redes, dispondo de uma limitação de equipamentos e espaço físico utilizando do software livre como a ferramenta principal para a implantação do cenário

2.1 Cenário atual

O departamento Citec possui um Roteador/Firewall (equipamento microcomputador desktop com sistema operacional Linux) com duas interfaces de rede, a primeira com o endereço 200.XXX.XXX.XXX/24 que esta ligada a rede 200.XXX.XXX.0/24 do campus Curitiba da UTFPR, a segunda interface está configurada com o endereço 200.XXX.XXX.XXX/24 gerando a rede com endereçamentos de IP's validos do Citec. Partindo desta segunda interface será conectada da um switch separado em duas VLan's onde, a Vlan_1 servirá para ligar os equipamentos de rede interna com endereço privados, e a Vlan_2 servirá para ligar os equipamentos com endereçamentos públicos de rede.

Existe um segundo computador desktop fazendo o roteamento e NAT (Network Address Translation) interno da rede, esse computador com duas interfaces de rede, a primeira interface com endereçamento 200.XX.XXX.XXX/24 ligado ai switch na Vlan_2, e a segunda interface configurada com o endereçamento 192.168.100.254 ligado no switch na Vlan_1

A partir das portas configuradas na Vlan_1 desse switch é feita o cascateamento para os demais switch's. Como demonstrado na Figura 1

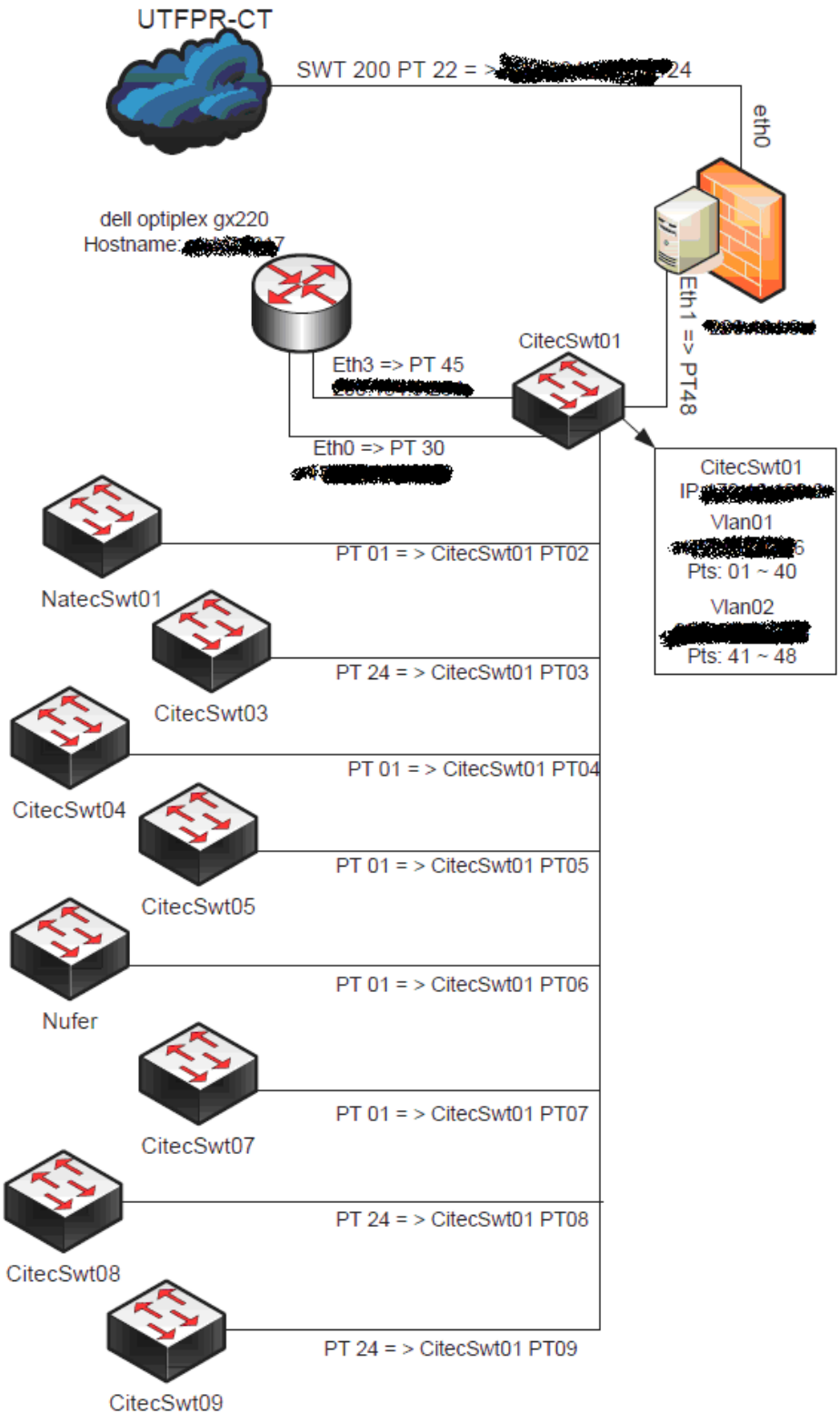

Figura 1 - Cenário Atual
Fonte: Autoria Própria

2.2 Proposta de implantação

Escopo

A proposta é segmentar a rede interna separando as várias salas de aulas por Vlan's e sub-redes diminuindo o domínio de *broadcast* e aumentando *a segurança e privacidade de cada seguimento de sub-rede*, sendo que cada seguimento ira possuir uma com sua faixa de IP, mas todas utilizando o mesmo serviço de DHCP (Dynamic Host Configuration Protocol), assim diminuindo os custos de implantação.

Ainda criar uma DMZ (*demilitarized zone* ou *zona desmilitarizada*) para acesso comum a todas as sub-redes onde poderá ser instalado serviços, servidores, impressoras, etc. que poderão ser acessadas de todas as sub-redes e também acessadas externamente, tudo controlado através do firewall.

Toda a arquitetura utilizada será feita através de Software livre, tanto o Sistema Operacional dos equipamentos utilizados, quanto os serviços instalados possibilitando assim futuras implementações de novos serviços, podendo ser customizada de forma para atender diversas funcionalidades especificas que possam surgir conforme representado na figura abaixo.

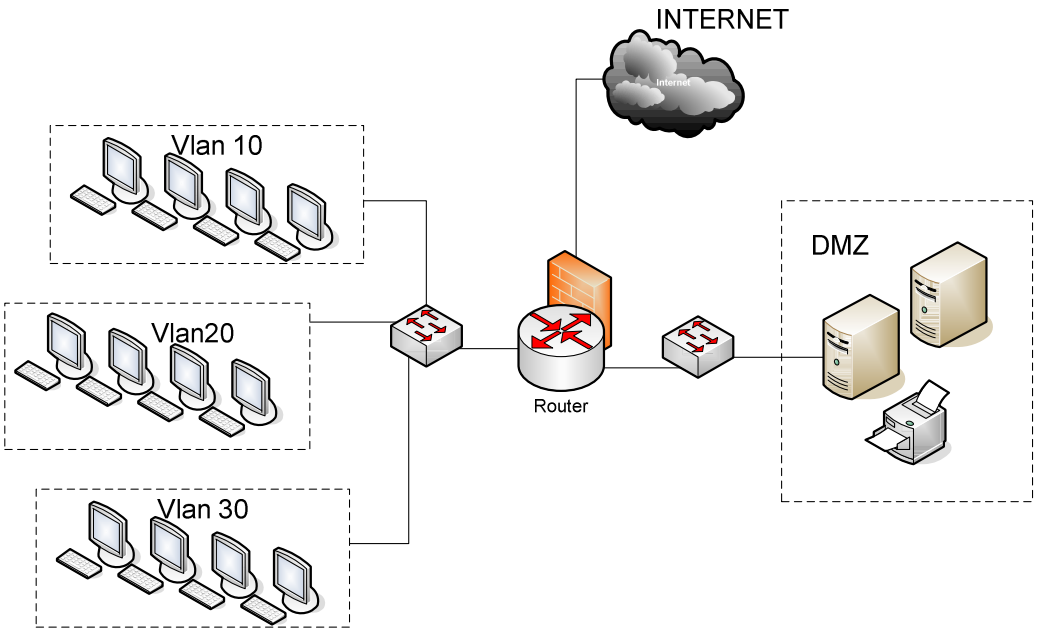

Figura 2 - Proposta de implantação
Fonte: Autoria Própria

3 JUSTIFICATIVA

Em uma rede comutada padrão os pacotes são transmitidos em *broadcast* por todos os dispositivos conectados a rede, utilizando um switch o processo comutação na camada 2 (camada de enlace) diminui o domínio de colisão criando segmentos individuais para cada dispositivo, porem assim mesmo, todos os dispositivos conectados no segmentos ficam visíveis uns aos outros podendo trocar informações. Quanto maior o número de dispositivos e usuários, maior o volume de *broadcast* e pacotes de cada dispositivo tem de ser processado e transmitido pela rede.

Utilizando a especificação do padrão IEEE 802.1Q, é possível a criação de Vlan's (*Virtual Local Area Network*) onde será segmentada a rede trazendo um quadro com algumas vantagens.

- Redução do domínio de *broadcast.*
- Agrupamento lógico de usuários e dispositivos
- Organização pode ser feita por localidade, função ou grupo, independentemente da localização física do dispositivo.
- Aumenta a segurança e melhora o gerenciamento da rede local
- Possibilita melhor escalabilidade e flexibilidade da rede

Com a concentração de todo o redirecionamento de endereços IP's das inúmeras sub-redes, otimizando os equipamentos em um único equipamento, alem de economia financeira com o hardware utilizado e a energia elétrica, ainda existe uma economia considerável com o espaço físico para acomodação desses equipamentos, também existe uma facilidade maior com a gerencia pois a configuração está concentrada.

A utilização do Software Livre permite muitas alterações futuras e implementações de novos serviços sem grandes mudanças de equipamentos.

4 METODOLOGIA

4.1 Protocolo IEEE 802.1Q

O protocolo de redes virtuais opera no modelo OSI na camada 02, camada de enlace ou ligação de dados

A figura abaixo representa o frame do cabeçalho dentro da camada de enlace

Endereço de destino	Endereço de Origem	802.1Q Vlan Tag	Tipo	Dados	Frame Check CRC

Figura 03 - Cabeçalho do protocolo IEEE 802.1Q
Fonte: Autoria Própria

Com a inclusão da TAG de 4 bytes ao frame original do quadro ethernet, com isso a checagem de erro do campo "Frame CHECK" e feito com base em um novo calculo.

Com a inclusão do número da VLAN adicionado no campo TAG, a informação de identificação da VLAN (VID) pode ser reconhecido entre

Os dispositivos que se comunicam entre o mesmo seguimento pertencendo a mesma VLAN não necessitam receber a TAG de identificação sendo denominadas untagged. Alguns dispositivos com interfaces de rede não são compativeis com o protocolo IEEE 802.1Q, quando isso ocorre, a interface simplesmente descarta a frame tagged não compreendido ignorando a informação da TAG de VLAN

Os Switchs com a porta configurada com TRUNK ao receber a informação do frame TAG ao repassar o quadro para à Vlan de destino acaba removendo o campo com a marcação da TAG.

4.2 Criação das VLan's

O protocolo IEEE 802.1Q permite a inclusão de uma TAG de identificação de VLan entre 1 e 4094 para cada frame transmitido, com isso e possível atribuir uma VID a cada VLan que deseja-se criar.

Existe dois métodos de associação de VLan,

Associação dinâmica, consiste em designar a qual Vlan o dispositivo irá se associar automaticamente através de um software especifico de gerenciamento, essa associação seria feita através do endereço físico do dispositivo (MAC) ou através de um Login.

Associação estática, consiste em designar uma determinada porta do switch e atribuí-la a determinada VLan, esse método e mais utilizado por ser mais prático o gerenciamento não sendo necessário o cadastramento de dispositivos a ingressar na rede. Isso de certa forma e mais seguro também, pois hoje e possível clonar ou alterar o endereçamento físico dos adaptadores de rede, possibilitando o ingresso a outra sub-rede sem a devida autorização.

Desta forma será utilizado no projeto o sistema de associação estática com links de acesso *(Access Link)* para os dispositivos e links de transporte *(Trunk Links)* para a interligação entre os Switch's e para a comunicação com o equipamento que fará a função de roteamento.

O modo de operação da interface de rede para o funcionamento da Vlan consiste ativar a leitura do cabeçalho do frame TAG com a informação do VID ou o modo UNTAG, que ignora o cabeçalho do frame com a identificação de VID, desta forma fica definida a forma que cada porta do equipamento irá se comportar para a comunicação com cada dispositivo ou interface conectada a ele.

As portas dos equipamentos de rede que estarão ligadas diretamente aos dispositivos clientes deverão estar configurada de modo *access link* ou seja de modo *untag*

As portas dos equipamentos de rede que estarão servido como uplink para interconectar os vários switch's e a ligação com o equipamento que estará fazendo a função de roteamente deverá estar configurada de mode *Trunk Links* ou seja com as TAG's de identificação de VID

4.3 Endereçamentos IP

Para que a comunicação na camada 3 (camada e rede) entre as Vlan's aconteça é necessário que cada sub-rede tenha uma faixa diferente de endereçamento de rede, caso isso não ocorra a comunicação entre as sub-redes nunca acontecerá, pois o roteamento acontece somente passando de uma faixa de rede para outra utilizando o gateway como porta de saída da rede.

Sendo assim será utilizado o endereçamento com o seguinte esquema conforme a tabela 1

VID	Rede
Vlan_10	192.168.0.0/24
Vlan_11	192.168.1.0/24
Vlan_12	192.168.2.0/24
Vlan_13	192.168.3.0/24
Vlan_14	192.168.4.0/24
etc ...	

Tabela 01- Endereços de VLan's
Fonte: Autoria Própria

Compilação e preparação do kernel do Sistema operacional pra que a placa de rede tenha suporte ao padrão IEEE 802.1Q, podendo assim ser conectada a uma porta do tipo trunk no switch.

Configuração as rotas locais para que uma rede não tenha acesso a outra, apenas possibilitando o trafego de saída das varias redes somente para a internet.

Configuração do serviço de dhcp (Dinamic Host Configuration Portocol) para que reconheça as varias redes e distribua o endereçamento entre as diversas vlan's

4.4 Kernel

A compilação do kernel se faz necessária em algumas distribuições por que a leitura do rotulo do frame (TAG) que identifica o VID da Vlan pela interface ethernet não ser padrão em todas as distribuições, após habilitar o novo suporte ao protocolo IEE 802.1q a interface de rede deverá fazer a leitura desses rotulo do frame (TAG).

4.5 Redirecionamento

Firewall

Com o Firewall e possível liberar ou bloquear o transito de pacotes da interface de rede de uma forma seletiva, bloqueando, liberando ou redirecionando os pacotes conforme necessário, em sistemas Linux esse trabalho do firewall a filtragem dos pacotes e tratado diretamente pelo kernel do sistema operacional, sendo assim não existe intervalo de tempo entre o carregamento do sistema operacional e a ativação do firewall.

O framework integrado ao Kernel do Linux e identificado com *netfilter*.

Os sistemas linux utilizam a ferramenta "iptables" para manipular as ações do filtros de pacotes e NAT para o protocolo IP versão 4 do firewall.

Existem 2 modos de operação filtragem de pacotes no firewall, modo Stateful e Stateless.

Firewall Stateless

Os firewall's que trabalham do modo de filtro de pacote são conhecidos como *Stateless* tratam cada pacote roteado pelo firewall de modo individual a medida que são trafegados, verificando inclusive as informações da camada de enlace e camada de rede, sem fazer análise das camadas superiores.

Firewall Statefull

Os firewall's que trabalham em modo de sessão são conhecidos como *Stateful*, desse modo é feita a analise e do pacote e guardado a informação do estado de cada conexão fazendo uma previsão de legitimidade de resposta. Deste modo de operação alem do firewall trabalhar com as camadas de enlace e de rede, ele também opera analisando a camada de transporte, oferecendo maior segurança no filtro de pacotes por fazer a analise em uma camada mais alta. Porem isso acaba exigindo um recurso de hardware maior.

A partir do kernel 2.4 o netfilter trabalha com a filtragem no modo statefull.

5 Procedimentos

5.1 Preparação do hardware

O Hardware utilizado para fazer a função de roteador deverá ser um computador com pelo menos 03 (três) interfaces de rede

A primeira para receber o link externo, no caso o endereçamento fornecido pelo campus Curitiba da UTFPR.

A segunda será conectada a uma Vlan exclusiva da DMZ onde servirá para interconectar a uma rede de endereçamento público

A terceira placa de rede estará ligada a uma porta do switch que deverá estar configurada de modo que receba todas as vlan's disponíveis pelo departamento, esta mesma interface de rede deverá reconhecer a TAG das Vlan's

O Switch deverá ter suporte ao protocolo IEEE 802.1Q.

A interligação da rede será feita conforme apresentado na figura a seguir.

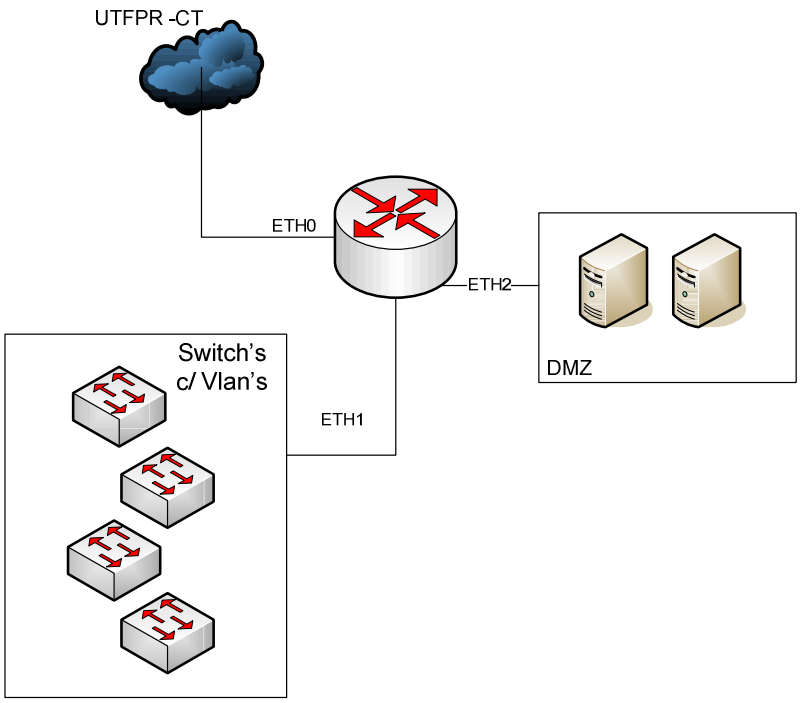

Figura 4 - Demonstrativo de ligação do hardware
Fonte: Autoria Própria

5.2 Escolha da distribuição do SO

A escolha da distribuição Debian do Sistema Operacional e dada pela sua forma de licença que não faz discriminação contra fins de utilização, podendo ser usada de forma acadêmica, administrativa e comercial sem restrição alguma, o que proporciona maior facilidade de implantações e estudos futuros.

5.3 Compilação do Kernel

O Kernel do Linux a partir do 2.4 já possui suporte ao protocolo IEEE 802.1Q, algumas distribuições se torna necessário fazer a re-compilação com os seguintes opções.

```
[*] Network options->802.1Q VLAN support

      <*> Network options->packet socket

      <*> Network options->socket filtering
```

Pode ser feita a compilação de duas formas, através de incorporação interna ou através de carregamento do módulo.

Ainda se faz necessário a instalação de um pacote de aplicativos que no debian recebe do nome de "*vlan - user mode programs to enable VLANs on your ethernet device*s" pode ser instalado via utilitário "*apt-get*" por se tratar de um pacote que se encontra no repositório oficial da distribuição.

O suporte ao *netfilter* também é nativo do sistema linux a partir do kernel 2.4 o modulo do kernel que deve estar habilitada para a implementação do redirecionamento

```
[*] CONFIG_NETFILTER
```

5.4 Tabela de redirecionamento

A tabela a seguir foi extraída do redirecionamento atual da rede.

Destino	Roteador	Mascara	Interface	Vlan_ID
200.X.X.0	0.0.0.0	255.255.255.0	Eth0	
200.X.X.0	0.0.0.0	255.255.255.0	Eth2	
192.168.0.0	0.0.0.0	255.255.255.0	Eth1.10	Vlan_10
192.168.1.0	0.0.0.0	255.255.255.0	Eth1.11	Vlan_11
192.168.2.0	0.0.0.0	255.255.255.0	Eth1.12	Vlan_12
192.1688.3.0	0.0.0.0	255.255.255.0	Eth1.13	Vlan_13
0.0.0.0	200.XXX.XXX.XXX	0.0.0.0		

Tabela 02- Endereços de redirecionamento atual
Fonte: Autoria Própria

5.5 Regras de Firewall

O local onde as regras do firewall são armazenadas são denominada de CHAINS, os principais onde as principais já embutidas como padrão são INPUT para dados que chegam ao firewall, OUTPUT para dados que estão saindo a partir do firewall e FORWARD para dados que são redirecionados para outra interface de rede ou outra maquina.

A tabela de *FILTER (filtro)* e a principal tabela do firewall nela será definido as regras que definirão se o pacote será aceito ou bloqueado ou re-encaminhados pelo firewall a outro destino.

A tabela *NAT (Network address translation ou tradução de endereço de rede)* e a tabela de regras de operações de tradução de endereço de rede ou porta de serviços, tanto de destino como origem.

A**cesso à DMZ**

Baseado nas regras já existentes foi gerado uma tabela de regras para acesso a rede com endereçamentos públicos que será utilizado com DMZ.

A regra padrão para acesso a DMZ será de bloqueio geral, liberando somente o acesso do host específico, ou seja o firewall ira "*whitelist"* trabalhar com lista branca ou lista segura bloqueando todo e qualquer trafego não autorizado.

A tabela a seguir especifica uma lista de host que tem acesso a redes externas e acesso comum a todas as redes internas. Existe também acesso permitindo a toda outra rede de outro departamento.

Tabela de regras de acesso a DMZ

ACCEPT	all	200.XXX.XXX.1	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.2	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.3	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.4	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.15	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.16	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.20	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.21	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.25	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.60	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.80	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.81	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.82	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.89	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.99	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.100	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.120	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.206	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.207	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.254	0.0.0.0/0
DROP	all	200.XXX.XXX.0/24	0.0.0.0/0
ACCEPT	all	200.XXX.XXX.0/24	200.17.96.0/24

Tabela 03- Regras de acesso a DMZ
Fonte: Autoria Própria

5.6 Implementação de serviço DHCP

O sistema operacional ira tratar cada Vlan como sendo uma interface de rede, criando uma interface virtual para cada vlan criada, portando deve ser feita a definição o endereçamento IP para cada interface

Como o sistema reconhece as Vlan's como interfaces de rede dever ser informado ao serviço de DHCP cada vlan's criadas como se fosse uma interface de rede diferente, sendo assim se faz necessário informar ao serviço quais interfaces ele deve distribuir o endereçamento.

```
# Arquivo dhcp3-server
        Interfaces = "eth1.10 eth1.20 eth1.30"
```

Informando todas as interfaces virtuais para que o serviço de DHCP ira fornecer os endereçamentos de rede.

Configurando várias sub-redes do DHCP nesse caso deve-ser configurado uma chave de subnet para cada vlan, alterando o endereçamento IP conforme casa sub-rede já deveinida.

```
# Arquivo dhcpd.conf
      subnet 192.168.x.0 netmask 255.255.255.0 {
      range 192.168.x.1 192.168.x.253;
      option routers 192.168.x.254;
      option broadcast-address 192.168.x.255;
      option domain-name-servers 192.168.x.254;
      }
```

A figura abaixo demonstra a propagação do serviço de DHCP pelas Vlan's criadas.

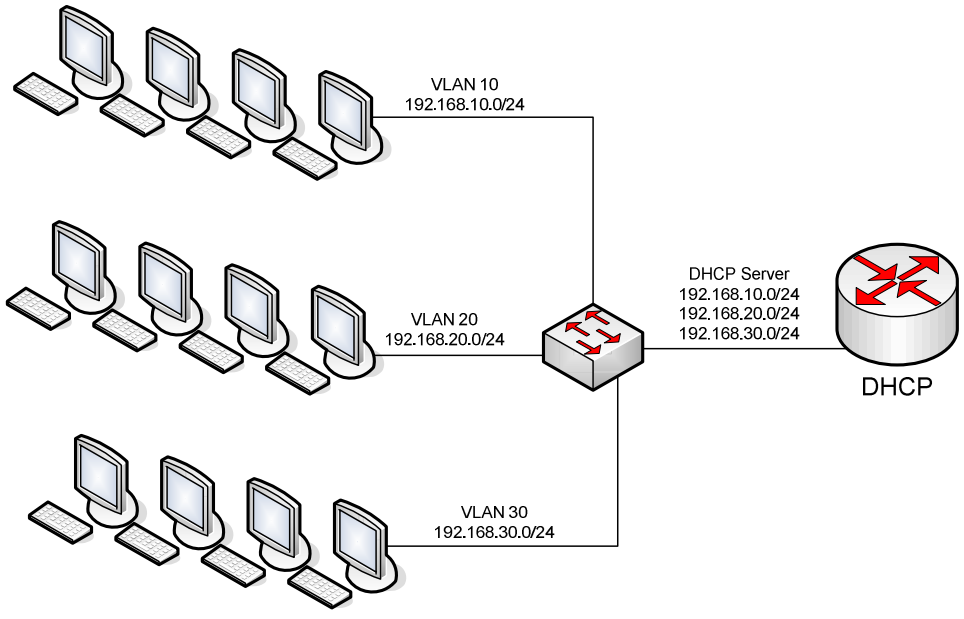

Figura 5 - Demonstrativo da propagação do DHCP
Fonte: Autoria Própria

6. RECURSOS NECESSÁRIOS

Switch's gerenciáveis com suporte ao protocolo 802.1Q para ser colocado no core da rede.

Computador para fazer a função de firewall e roteador de rede com as seguintes características.

03 (duas) interfaces de rede ethernet com suporte a protocolo IEEE 802.1Q preferencialmente Gigabit.

Processamento e memória compatível com o número de nós de rede.

Refrigeração adequada ao equipamento.

Sistema operacional com o kernel 2.4 ou superior para compatibilidade à customização do suporte ao protocolo IEEE 802.1Q

.

7. CONCLUSÃO

Com todo o processo de implantação dos procedimentos descritos a conclusão foi que a segmentação da rede com a utilização de Vlan's torna a rede mais estável e segura e escalonável pois a concentração do serviço de DHCP em um único equipamento acaba com a necessidade de fornecer um equipamento para cada sub-rede fazer esse serviço, diminuindo o custo total da infra-instrutora e possibilitando a fácil criação de novos grupos de trabalhos isolado. A criação de uma DMZ viabiliza o compartilhamento de serviços e equipamentos comuns a vários grupos de trabalhos independentemente a qual sub-rede o usuário pertence.

Outra grande vantagem de fazer-se a segmentação e roteamento das VLAN'S em um equipamento utilizando software livre e a liberdade para poder fazer futuras instalações de outras ferramentas para auxiliar a rede de forma rápida e com um custo reduzido, sem a necessidade de fazer a compra de equipamentos caros para fazer um teste de implementação de um serviço, que nem sempre existe a disponibilidade imediata de recursos financeiros ou não existe tempo hábil para realizar compra de equipamentos específicos sem perda de produtividade do ambiente.

REFERENCIAS

TANENBAUM, A. **Redes de Computadores**. Rio de Janeiro: Campus, 2003.

PRITCHARD, S.; PESSANHA, B. G.; LANGFELDT, N.; DEAN, J.; STANGER, J.; **Certificação Linux LPI - Nível 1**; 2ª Edição, Alta Books, 2007.

PRITCHARD, S.; PESSANHA, B. G.; LANGFELDT, N.; DEAN, J.; STANGER, J.; **Certificação Linux LPI - Nível 2**; 2ª Edição, Alta Books, 2007

http://antropologia.codigolivre.org.br/debian/node8.html; 10/12/2012

TANENBAUM, A. S.; **Sistemas Operacionais Modernos**; 3ª Edição, Pearson Prentice Hall, 2009.

FILIPPETTI, Marco Aurélio. CCNA 4.1: Guia Completo de Estudos. Florianópolis: Visual Books, 2008.

UTFPR. **Normas para elaboração de trabalhos Acadêmicos**. Curitiba: UTFPR, 2008

MOTA FILHO, João Eriberto, **Descobrindo o Linux**; 2ª Edição, São Paulo, 2007

Anexos

Anexo 01

Tabela 04 - ndereços de hosts liberados para acesso

Acesso	Protocolo	Endereço Origem	Endereço destino
DROP	all	192.168.X.X/24	0.0.0.0/0
ACCEPT	all	192.168.X.X	0.0.0.0/0
ACCEPT	all	192.168.X.X	0.0.0.0/0
ACCEPT	all	192.168.X.X	0.0.0.0/0
ACCEPT	all	192.168.1.199	0.0.0.0/0
ACCEPT	all	192.168.1.200	0.0.0.0/0
ACCEPT	all	192.168.1.211	0.0.0.0/0
ACCEPT	all	192.168.1.212	0.0.0.0/0
ACCEPT	all	192.168.1.213	0.0.0.0/0
ACCEPT	all	192.168.1.214	0.0.0.0/0
ACCEPT	all	192.168.1.215	0.0.0.0/0
ACCEPT	all	192.168.1.218	0.0.0.0/0
ACCEPT	all	192.168.1.220	0.0.0.0/0
ACCEPT	all	192.168.1.244	0.0.0.0/0
ACCEPT	all	192.168.1.245	0.0.0.0/0
ACCEPT	all	192.168.1.246	0.0.0.0/0
ACCEPT	all	192.168.1.247	0.0.0.0/0
ACCEPT	all	192.168.1.248	0.0.0.0/0
ACCEPT	all	192.168.1.249	0.0.0.0/0
ACCEPT	all	192.168.1.250	0.0.0.0/0
ACCEPT	all	192.168.1.254	0.0.0.0/0
ACCEPT	all	192.168.11.79	0.0.0.0/0
DROP	all	192.168.13.0/24	0.0.0.0/0
ACCEPT	all	192.168.13.11	0.0.0.0/0
ACCEPT	all	192.168.13.12	0.0.0.0/0
ACCEPT	all	192.168.13.13	0.0.0.0/0
ACCEPT	all	192.168.13.14	0.0.0.0/0
ACCEPT	all	192.168.13.15	0.0.0.0/0
ACCEPT	all	192.168.13.2	0.0.0.0/0
ACCEPT	all	192.168.13.20	0.0.0.0/0
ACCEPT	all	192.168.13.21	0.0.0.0/0
ACCEPT	all	192.168.13.22	0.0.0.0/0
ACCEPT	all	192.168.13.23	0.0.0.0/0
ACCEPT	all	192.168.13.24	0.0.0.0/0
ACCEPT	all	192.168.13.25	0.0.0.0/0
ACCEPT	all	192.168.13.254	0.0.0.0/0
ACCEPT	all	192.168.13.8	0.0.0.0/0
ACCEPT	all	192.168.13.80	0.0.0.0/0
ACCEPT	all	192.168.13.99	0.0.0.0/0
DROP	all	192.168.14.0/24	0.0.0.0/0
ACCEPT	all	192.168.14.156	0.0.0.0/0
ACCEPT	all	192.168.14.182	0.0.0.0/0
ACCEPT	all	192.168.14.183	0.0.0.0/0

ACCEPT	all	192.168.14.184	0.0.0.0/0
ACCEPT	all	192.168.14.185	0.0.0.0/0
ACCEPT	all	192.168.14.186	0.0.0.0/0
ACCEPT	all	192.168.14.187	0.0.0.0/0
ACCEPT	all	192.168.14.188	0.0.0.0/0
ACCEPT	all	192.168.14.189	0.0.0.0/0
ACCEPT	all	192.168.14.190	0.0.0.0/0
ACCEPT	all	192.168.14.22	0.0.0.0/0
ACCEPT	all	192.168.14.254	0.0.0.0/0
ACCEPT	all	192.168.14.30	0.0.0.0/0
ACCEPT	all	192.168.14.35	0.0.0.0/0
ACCEPT	all	192.168.14.36	0.0.0.0/0
ACCEPT	all	192.168.14.82	0.0.0.0/0
ACCEPT	all	192.168.14.83	0.0.0.0/0
ACCEPT	all	192.168.14.84	0.0.0.0/0
ACCEPT	all	192.168.14.85	0.0.0.0/0
DROP	all	192.168.16.0/24	0.0.0.0/0
ACCEPT	all	192.168.16.1	0.0.0.0/0
ACCEPT	all	192.168.16.12	0.0.0.0/0
ACCEPT	all	192.168.16.15	0.0.0.0/0
ACCEPT	all	192.168.16.254	0.0.0.0/0
ACCEPT	all	192.168.16.33	0.0.0.0/0
ACCEPT	all	192.168.16.4	0.0.0.0/0
ACCEPT	all	192.168.16.40	0.0.0.0/0
ACCEPT	all	192.168.16.50	0.0.0.0/0
ACCEPT	all	192.168.16.51	0.0.0.0/0
ACCEPT	all	192.168.16.52	0.0.0.0/0
ACCEPT	all	192.168.16.53	0.0.0.0/0
DROP	all	192.168.20.0/24	0.0.0.0/0
ACCEPT	all	192.168.20.200	0.0.0.0/0
ACCEPT	all	192.168.20.254	0.0.0.0/0
DROP	all	192.168.21.0/24	0.0.0.0/0
ACCEPT	all	192.168.21.1	0.0.0.0/0
ACCEPT	all	192.168.21.2	0.0.0.0/0
ACCEPT	all	192.168.21.254	0.0.0.0/0
DROP	all	192.168.22.0/24	0.0.0.0/0
ACCEPT	all	192.168.22.252	0.0.0.0/0
ACCEPT	all	192.168.22.253	0.0.0.0/0
ACCEPT	all	192.168.22.254	0.0.0.0/0
ACCEPT	all	192.168.23.1	0.0.0.0/0
ACCEPT	all	192.168.23.2	0.0.0.0/0
ACCEPT	all	192.168.23.254	0.0.0.0/0
ACCEPT	all	192.168.9.1	0.0.0.0/0
ACCEPT	all	192.168.9.2	0.0.0.0/0
ACCEPT	all	192.168.9.254	0.0.0.0/0
ACCEPT	all	192.168.9.3	0.0.0.0/0
ACCEPT	all	192.168.9.4	0.0.0.0/0
ACCEPT	all	192.168.9.5	0.0.0.0/0
ACCEPT	all	192.168.9.6	0.0.0.0/0
ACCEPT	all	192.168.9.7	0.0.0.0/0
ACCEPT	all	192.168.9.8	0.0.0.0/0
ACCEPT	all	192.168.9.9	0.0.0.0/0

ACCEPT	all	192.168.1.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.2.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.3.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.4.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.5.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.6.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.7.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.8.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.9.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.11.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.12.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.13.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.14.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.15.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.16.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.17.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.20.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.21.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.22.0/24	200.XXX.XXX.15
ACCEPT	all	192.168.23.0/24	200.XXX.XXX.15

Anexo 02

Tabela 05 - Regras atuais do firewall existente

Chain INPUT (policy ACCEPT)					
target	prot	opt	source	destination	
ACCEPT	all	--	192.168.0.0/16	200.XXX.XXX.1	
ACCEPT	all	--	200.XXX.XXX.0/24	200.XXX.XXX.1	
ACCEPT	all	--	192.168.0.0/16	200.XXX.XXX.2	
ACCEPT	all	--	192.168.0.0/16	200.XXX.XXX.3	
ACCEPT	all	--	192.168.0.0/16	200.XXX.XXX.4	
ACCEPT	udp	--	200.XXX.XXX.17	0.0.0.0/0	udp dpt:161
ACCEPT	tcp	--	200.XXX.XXX.17	0.0.0.0/0	tcp dpt:161
ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.1	tcp dpt:53
ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.1	udp dpt:53
ACCEPT	tcp	--	200.XXX.XXX.0/24	200.XXX.XXX.19	tcp dpt:25
ACCEPT	tcp	--	192.168.0.0/16	200.XXX.XXX.19	tcp dpt:25
ACCEPT	icmp	--	192.168.0.0/16	200.XXX.XXX.0/24	
ACCEPT	icmp	--	200.XXX.XXX.0/24	200.XXX.XXX.0/24	
DROP	icmp	--	0.0.0.0/0	200.XXX.XXX.0/24	
DROP	icmp	--	200.134.25.0/24	200.XXX.XXX.0/24	
ACCEPT	udp	--	0.0.0.0/0	0.0.0.0/0	udp dpt:161
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:161
ACCEPT	udp	--	0.0.0.0/0	0.0.0.0/0	udp dpt:162
Chain FORWARD (policy ACCEPT)					
target	prot	opt	source	destination	
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.248	tcp dpt:465
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:465
DROP	all	--	200.XXX.XXX.19	0.0.0.0/0	
DROP	all	--	0.0.0.0/0	200.XXX.XXX.19	
ACCEPT	all	--	200.XXX.XXX.1	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.2	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.3	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.4	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.15	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.16	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.20	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.21	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.25	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.60	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.80	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.81	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.82	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.89	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.99	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.100	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.120	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.206	0.0.0.0/0	

ACCEPT	all	--	200.XXX.XXX.207	0.0.0.0/0	
ACCEPT	all	--	200.XXX.XXX.254	0.0.0.0/0	
DROP	all	--	200.XXX.XXX.0/24	0.0.0.0/0	
ACCEPT	all	--	192.168.1.1	0.0.0.0/0	
ACCEPT	all	--	192.168.1.120	0.0.0.0/0	
ACCEPT	all	--	192.168.1.150	0.0.0.0/0	
ACCEPT	all	--	192.168.1.199	0.0.0.0/0	
ACCEPT	all	--	192.168.1.211	0.0.0.0/0	
ACCEPT	all	--	192.168.1.212	0.0.0.0/0	
ACCEPT	all	--	192.168.1.213	0.0.0.0/0	
ACCEPT	all	--	192.168.1.214	0.0.0.0/0	
ACCEPT	all	--	192.168.1.200	0.0.0.0/0	
ACCEPT	all	--	192.168.1.215	0.0.0.0/0	
ACCEPT	all	--	192.168.1.220	0.0.0.0/0	
ACCEPT	all	--	192.168.1.218	0.0.0.0/0	
ACCEPT	all	--	192.168.1.244	0.0.0.0/0	
ACCEPT	all	--	192.168.1.245	0.0.0.0/0	
ACCEPT	all	--	192.168.1.246	0.0.0.0/0	
ACCEPT	all	--	192.168.1.247	0.0.0.0/0	
ACCEPT	all	--	192.168.1.248	0.0.0.0/0	
ACCEPT	all	--	192.168.1.249	0.0.0.0/0	
ACCEPT	all	--	192.168.1.250	0.0.0.0/0	
ACCEPT	all	--	192.168.1.254	0.0.0.0/0	
DROP	all	--	192.168.1.0/24	0.0.0.0/0	
ACCEPT	all	--	192.168.9.1	0.0.0.0/0	
ACCEPT	all	--	192.168.9.2	0.0.0.0/0	
ACCEPT	all	--	192.168.9.3	0.0.0.0/0	
ACCEPT	all	--	192.168.9.4	0.0.0.0/0	
ACCEPT	all	--	192.168.9.5	0.0.0.0/0	
ACCEPT	all	--	192.168.9.6	0.0.0.0/0	
ACCEPT	all	--	192.168.9.7	0.0.0.0/0	
ACCEPT	all	--	192.168.9.8	0.0.0.0/0	
ACCEPT	all	--	192.168.9.9	0.0.0.0/0	
ACCEPT	all	--	192.168.9.254	0.0.0.0/0	
ACCEPT	all	--	192.168.13.2	0.0.0.0/0	
ACCEPT	all	--	192.168.13.8	0.0.0.0/0	
ACCEPT	all	--	192.168.13.11	0.0.0.0/0	
ACCEPT	all	--	192.168.13.12	0.0.0.0/0	
ACCEPT	all	--	192.168.13.13	0.0.0.0/0	
ACCEPT	all	--	192.168.13.14	0.0.0.0/0	
ACCEPT	all	--	192.168.13.15	0.0.0.0/0	
ACCEPT	all	--	192.168.13.20	0.0.0.0/0	
ACCEPT	all	--	192.168.13.21	0.0.0.0/0	
ACCEPT	all	--	192.168.13.22	0.0.0.0/0	
ACCEPT	all	--	192.168.13.23	0.0.0.0/0	
ACCEPT	all	--	192.168.13.24	0.0.0.0/0	
ACCEPT	all	--	192.168.13.80	0.0.0.0/0	
ACCEPT	all	--	192.168.13.99	0.0.0.0/0	
ACCEPT	all	--	192.168.13.254	0.0.0.0/0	
ACCEPT	all	--	192.168.13.25	0.0.0.0/0	
DROP	all	--	192.168.13.0/24	0.0.0.0/0	
ACCEPT	all	--	192.168.14.22	0.0.0.0/0	

ACCEPT	all	--	192.168.14.30	0.0.0.0/0	
ACCEPT	all	--	192.168.14.35	0.0.0.0/0	
ACCEPT	all	--	192.168.14.36	0.0.0.0/0	
ACCEPT	all	--	192.168.14.82	0.0.0.0/0	
ACCEPT	all	--	192.168.14.83	0.0.0.0/0	
ACCEPT	all	--	192.168.14.84	0.0.0.0/0	
ACCEPT	all	--	192.168.14.85	0.0.0.0/0	
ACCEPT	all	--	192.168.14.156	0.0.0.0/0	
ACCEPT	all	--	192.168.14.182	0.0.0.0/0	
ACCEPT	all	--	192.168.14.183	0.0.0.0/0	
ACCEPT	all	--	192.168.14.184	0.0.0.0/0	
ACCEPT	all	--	192.168.14.186	0.0.0.0/0	
ACCEPT	all	--	192.168.14.187	0.0.0.0/0	
ACCEPT	all	--	192.168.14.185	0.0.0.0/0	
ACCEPT	all	--	192.168.14.188	0.0.0.0/0	
ACCEPT	all	--	192.168.14.190	0.0.0.0/0	
ACCEPT	all	--	192.168.14.189	0.0.0.0/0	
ACCEPT	all	--	192.168.14.254	0.0.0.0/0	
DROP	all	--	192.168.14.0/24	0.0.0.0/0	
ACCEPT	all	--	192.168.16.1	0.0.0.0/0	
ACCEPT	all	--	192.168.16.4	0.0.0.0/0	
ACCEPT	all	--	192.168.16.12	0.0.0.0/0	
ACCEPT	all	--	192.168.16.15	0.0.0.0/0	
ACCEPT	all	--	192.168.16.33	0.0.0.0/0	
ACCEPT	all	--	192.168.16.40	0.0.0.0/0	
ACCEPT	all	--	192.168.16.50	0.0.0.0/0	
ACCEPT	all	--	192.168.16.51	0.0.0.0/0	
ACCEPT	all	--	192.168.16.52	0.0.0.0/0	
ACCEPT	all	--	192.168.16.53	0.0.0.0/0	
ACCEPT	all	--	192.168.16.254	0.0.0.0/0	
DROP	all	--	192.168.16.0/24	0.0.0.0/0	
ACCEPT	all	--	192.168.20.200	0.0.0.0/0	
ACCEPT	all	--	192.168.20.254	0.0.0.0/0	
DROP	all	--	192.168.20.0/24	0.0.0.0/0	
ACCEPT	all	--	192.168.21.1	0.0.0.0/0	
ACCEPT	all	--	192.168.21.2	0.0.0.0/0	
ACCEPT	all	--	192.168.21.254	0.0.0.0/0	
DROP	all	--	192.168.21.0/24	0.0.0.0/0	
ACCEPT	all	--	192.168.22.252	0.0.0.0/0	
ACCEPT	all	--	192.168.22.253	0.0.0.0/0	
ACCEPT	all	--	192.168.22.254	0.0.0.0/0	
DROP	all	--	192.168.22.0/24	0.0.0.0/0	
ACCEPT	all	--	192.168.23.1	0.0.0.0/0	
ACCEPT	all	--	192.168.23.2	0.0.0.0/0	
ACCEPT	all	--	192.168.23.254	0.0.0.0/0	
ACCEPT	all	--	192.168.11.79	0.0.0.0/0	
ACCEPT	tcp	--	192.168.6.0	0.0.0.0	tcp dpt:1723
ACCEPT	all	--	200.XXX.XXX.0/24	200.17.96.0/24	
ACCEPT	all	--	192.168.0.0/16	200.17.96.0/24	
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.25	tcp dpt:4711
ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.25	udp dpt:4711
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.25	tcp dpt:4662

ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.25	udp dpt:4662
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.25	tcp dpt:4672
ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.25	udp dpt:4672
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.25	tcp dpt:8080
ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.25	udp dpt:8080
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.25	tcp dpt:80
ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.25	udp dpt:80
DROP	tcp	--	0.0.0.0/0	200.XXX.XXX.15	tcp dpt:21
DROP	tcp	--	0.0.0.0/0	200.XXX.XXX.15	tcp dpt:3128
ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED
ACCEPT	all	--	192.168.1.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.2.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.3.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.4.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.5.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.6.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.7.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.8.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.9.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.11.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.12.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.13.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.14.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.15.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.16.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.17.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.20.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.21.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.22.0/24	200.XXX.XXX.15	
ACCEPT	all	--	192.168.23.0/24	200.XXX.XXX.15	
ACCEPT	all	--	200.XXX.XXX.16	200.XXX.XXX.15	
ACCEPT	all	--	200.XXX.XXX.80	200.XXX.XXX.15	
ACCEPT	all	--	200.XXX.XXX.25	200.XXX.XXX.15	
ACCEPT	tcp	--	200.186.32.166	192.168.15.15	tcp dpt:22
ACCEPT	tcp	--	0.0.0.0/0	192.168.15.15	tcp dpt:80
ACCEPT	tcp	--	0.0.0.0/0	192.168.15.15	tcp dpt:8080
ACCEPT	tcp	--	0.0.0.0/0	192.168.15.15	tcp dpt:443
ACCEPT	tcp	--	0.0.0.0/0	192.168.15.15	tcp dpt:5432
ACCEPT	tcp	--	0.0.0.0/0	192.168.15.15	tcp dpt:2401
ACCEPT	udp	--	0.0.0.0/0	192.168.15.15	udp dpt:2401
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.15	tcp dpt:53
ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.15	udp dpt:53
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.21	tcp dpt:7788
ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.21	udp dpt:7788
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.16	tcp dpt:53
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.16	tcp dpt:25
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.16	tcp dpt:110
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.16	tcp dpt:143
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.16	tcp dpt:783
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.16	tcp dpt:993
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.16	tcp dpt:80
ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.16	udp dpt:53

ACCEPT	tcp	--	0.0.0.0/0	192.168.17.7	tcp dpt:7788
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.3	tcp dpt:7788
ACCEPT	udp	--	0.0.0.0/0	192.168.17.7	udp dpt:7788
ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.3	udp dpt:7788
DROP	tcp	--	0.0.0.0/0	200.XXX.XXX.120	tcp dpt:53
DROP	udp	--	0.0.0.0/0	200.XXX.XXX.120	udp dpt:53
DROP	tcp	--	0.0.0.0/0	200.XXX.XXX.0/24	tcp dpt:139
DROP	tcp	--	0.0.0.0/0	200.XXX.XXX.0/24	tcp dpt:445
DROP	tcp	--	0.0.0.0/0	200.XXX.XXX.0/24	tcp dpt:135
DROP	tcp	--	200.XXX.XXX.0/24	0.0.0.0/0	tcp dpt:139
DROP	tcp	--	200.XXX.XXX.0/24	0.0.0.0/0	tcp dpt:445
DROP	tcp	--	200.XXX.XXX.0/24	0.0.0.0/0	tcp dpt:135
DROP	tcp	--	0.0.0.0/0	200.XXX.XXX.15	tcp dpt:3128
ACCEPT	icmp	--	192.168.0.0/16	200.XXX.XXX.0/24	
ACCEPT	icmp	--	200.XXX.XXX.0/24	200.XXX.XXX.0/24	
ACCEPT	icmp	--	200.XXX.XXX.0/24	192.168.0.0/16	
DROP	icmp	--	0.0.0.0/0	200.XXX.XXX.0/24	
DROP	icmp	--	0.0.0.0/0	192.168.0.0/16	
DROP	icmp	--	200.134.25.0/24	200.XXX.XXX.0/24	
DROP	icmp	--	200.134.25.0/24	192.168.0.0/16	
ACCEPT	all	--	0.0.0.0/0	192.168.0.0/16	
ACCEPT	all	--	192.168.0.0/16	0.0.0.0/0	
ACCEPT	all	--	0.0.0.0/0	200.XXX.XXX.0/24	
ACCEPT	all	--	200.XXX.XXX.0/24	0.0.0.0/0	
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.249	tcp dpt:48699
ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.249	udp dpt:48698
ACCEPT	udp	--	0.0.0.0/0	200.XXX.XXX.249	udp dpt:48699
ACCEPT	tcp	--	0.0.0.0/0	200.XXX.XXX.249	tcp dpt:48698
Chain OUTPUT (policy ACCEPT)					
Target	prot	opt	source	destination	
ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED