

Mateus Tomoo Yonemoto Peixoto
Renan Kodama Rodrigues

Trunking e STP

Relatório técnico de atividade prática solicitado pelo professor Rodrigo Campiolo na disciplina de Redes de Computadores II do Bacharelado em Ciência da Computação da Universidade Tecnológica Federal do Paraná.

Universidade Tecnológica Federal do Paraná – UTFPR
Departamento Acadêmico de Computação – DACOM
Bacharelado em Ciência da Computação – BCC

Campo Mourão
Junho / 2018

Resumo

Neste relatório é abordado como foi desenvolvido a atividade prática sobre roteamento utilizando redes virtuais VLAN's (Virtual Local Area Network), de modo que no cenário existam as VLAN's, VLAN1, VLAN2 e VLAN3 onde para cada VLAN está configurado o STP (Spanning Tree Protocol) determinando qual é a VLAN principal e qual é a VLAN secundária, para a comunicação entre as VLANS foi utilizado o modo Trunk conectados à um roteador.

Após a elaboração do cenário como descrito no tópico objetivos, foi possível testar a infraestrutura de rede através do protocolo ICMP (Internet Control Message Protocol) onde os resultados obtidos encontram -se no tópico procedimentos e resultados obtidos. O relatório apresenta também as configurações e ferramentas utilizadas para construir o cenário solicitado, assim como os endereços, equipamentos, tipos de interfaces de redes e cabeamentos, descritos no tópico de materias. **Palavras-chave:** Virtual Local Area Network. Spanning Tree Protocol. Trunk.

Sumário

1	Introdução	4
2	Objetivos	4
3	Fundamentação	5
4	Materiais	5
5	Procedimentos e Resultados	7
	5.1 Procedimentos	7
	5.2 Resultados	10
6	Discussão dos Resultados	10
7	Conclusões	11
8	Referências	11

1 Introdução

Uma rede local virtual VLAN (Virtual Local Area Network), é uma rede logicamente independente onde várias VLANs podem coexistir em um mesmo switch, de forma a dividir uma rede física em mais de uma rede, criando domínios de broadcast separados. Uma VLAN também torna possível colocar em um mesmo domínio de broadcast hosts com localizações físicas distintas e ligados a switches diferentes. O uso de VLAN's também proporciona maior segurança, pois nela é possível separar as redes agrupando máquinas ou hosts que tenham o mesmo propósito, tornando possível separar uma rede administrativa de uma rede operacional, logo ambas as terão permissões diferentes por exemplo. Para manter a conectividade das VLANs em toda a estrutura do switch, as VLANs devem ser configuradas em cada switch, o protocolo VTP da Cisco garante um método mais fácil para a manutenção de uma configuração de Vlan consistente em toda a rede comutada.

2 Objetivos

Os objetivos à serem alcançados para a elaboração desta atividade sobre a comunicação entre VLAN's (Virtual Local Area Network) consistem em:

- Construir o cenário de rede apresentado na figura 1. Para as VLAN1, VLAN2, VLAN3 use os identificadores 10, 20 e 30 respectivamente;

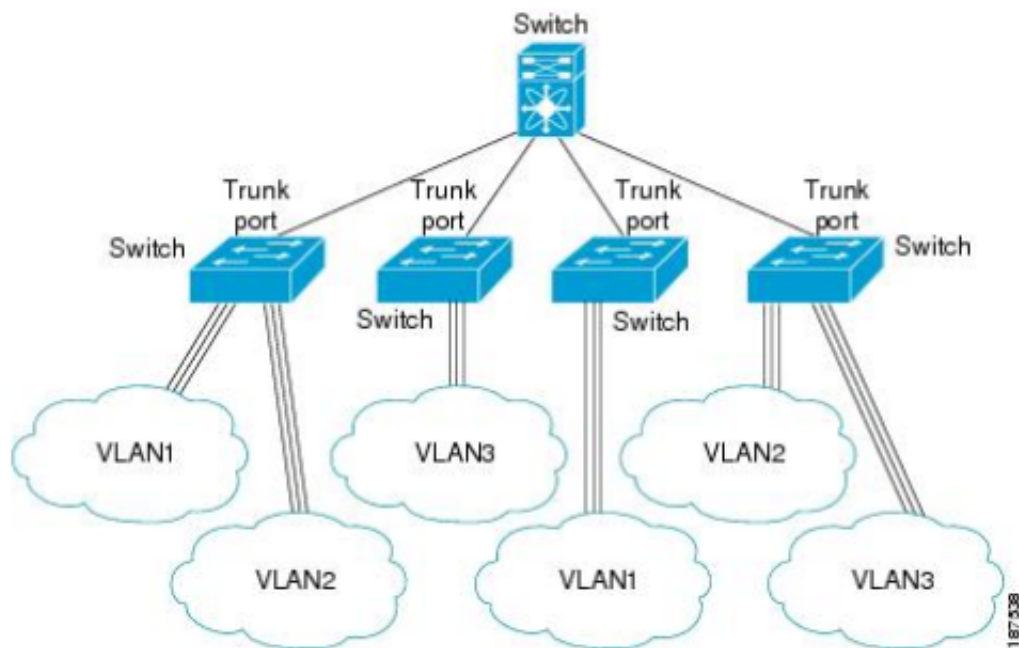


Figura 1: Cenário de rede composto por múltiplas VLAN's (Fonte: Cisco).

- Verificar a conectividade entre VLANs de mesmo identificador;

- Adicionar um gateway conectado ao Switch que interliga todos os outros para possibilitar a conectividade entre as VLANs. Use somente uma porta do switch;
- Verificar a conectividade entre VLANs diferentes;
- Estabelecer redundância entre os switches e configurar o STP para cada VLAN definindo o servidor raiz (primário) e o reserva (secundário);
- Realizar um teste de desconexão entre algum dos switches com o principal e verificar a convergência do STP;

3 Fundamentação

A constituição de VLANs (Virtual Local Area Network) em uma rede física, pode dever-se a questões de organização onde diferentes departamentos/serviços podem ter a sua própria VLAN referindo que a mesma VLAN pode ser configurada ao longo de vários switches, permitindo assim que utilizadores do mesmo departamento/serviço estejam em locais físicos distintos da mesma instituição, ou questões de segurança para que os utilizadores de uma rede não tenham acesso a determinados servidores, ou ainda para questões de segmentação dividindo a rede física em redes lógicas mais pequenas e assim ter um melhor controlo/gestão a nível de utilização/tráfego. Basicamente é uma rede lógica onde podemos agrupar várias máquinas de acordo com vários critérios, como por exemplo grupos de usuários, departamentos, tráfego e etc. As VLANs permitem a segmentação das redes físicas, sendo que a comunicação entre máquinas de VLANs diferentes terá de passar obrigatoriamente por um roteador ou outro equipamento capaz de realizar o encaminhamento, que será responsável por encaminhar o tráfego entre redes (VLANs) distintas (FUZITANI, 2018).

O protocolo VTP utiliza a camada 2 de enlace para adicionar, excluir ou renomear as VLANs. Os pacotes de VTP são enviados em quadros do Inter-Switch Link ou em quadros do IEEE 802.1Q e estes pacotes são enviados ao endereço MAC de destino (CISCO, 2018).

4 Materiais

Para a realização da atividade proposta, foi utilizado como sistema operacional o linux Elementary OS baseado na versão do Ubuntu 16.04, com kernel Linux 4.4.0-127-generic. Para as configurações de hardware da máquina, a atividade proposta foi elaborada em um sistema com um processador CoreTM i5-5200U e CPU com 2.20GHz e com 4.0GB de memória RAM (Random Access Memory), com placa de vídeo NVIDIA Corporation GF117M e com 107.2GB de espaço no HDD (Hard Disk Drive).

Para a elaboração do cenário, foi utilizado o programa Cisco Packet Tracer na versão 7.1, para os elementos presentes no cenário, estes consistem em, um roteador com quatro placas de rede do tipo Giga Ethernet, onde na primeira placa existem duas redes virtuais GigaEthernet 0/0.1 e GigaEthernet 0/0.2, na segunda placa existe apenas uma rede virtual identificada como GigaEthernet 1/0.1, na terceira interface existe apenas uma rede virtual identificada como GigaEthernet 2/0.1 e na quarta interface de rede existem duas redes virtuais identificadas como GigaEthernet 3/0.1 e GigaEthernet 3/0.2, quatro equipamentos switches cada um com vinte e quatro interfaces do tipo Fast Ethernet e duas interfaces do tipo Giga Ethernet, no cenário também está presente os hosts ou máquinas PC's (Personal Computer) cada um com uma placa de rede do tipo Fast Ethernet, para a comunicação entre os dispositivos da rede foi utilizado o cabeamento do tipo straight through (par trançado).

Os comandos utilizados para a configuração dos equipamentos presentes no cenário e suas respectivas funcionalidades são descritas a seguir:

- `#(config) spanning tree vlan [1-4096] root primary` #define a vlan selecionada como primária.
- `#(config) spanning tree vlan [1-4096] root secondary` #define a vlan selecionada como secundária.
- `#(config) interface [Fa0/0.X]` #cria uma rede virtual na interface.
- `#(config-if) encapsulation dot1q [IDVLAN]` #habilita o suporte ao IEEE 802.1q que suporta o uso de VLAN.
- `#(config-if) ip address [IP] [MASK]` #configura um endereço ip e máscara em uma interface.
- `#(config-if) switchport mode access` #configura interface do switch no modo access.
- `#(config-if) switchport mode trunk` #configura interface do switch no modo trunk.
- `#(config-if) switchport access vlan [ID]` #associa uma interface do switch para alguma vlan.
- `#show vlan` #comando para visualizar todas as vlans em um switch.
- `#(config) vlan [ID]` #selecionar vlan.
- `#(config) no vlan [ID]` #remover vlan.
- `#(config-vlan) name [NAME]` #atribuir um nome para a vlan selecionada.

5 Procedimentos e Resultados

5.1 Procedimentos

Primeiramente todos os equipamentos descritos foram inseridos no cenário juntamente com suas ligações como é apresentado pela figura 2.

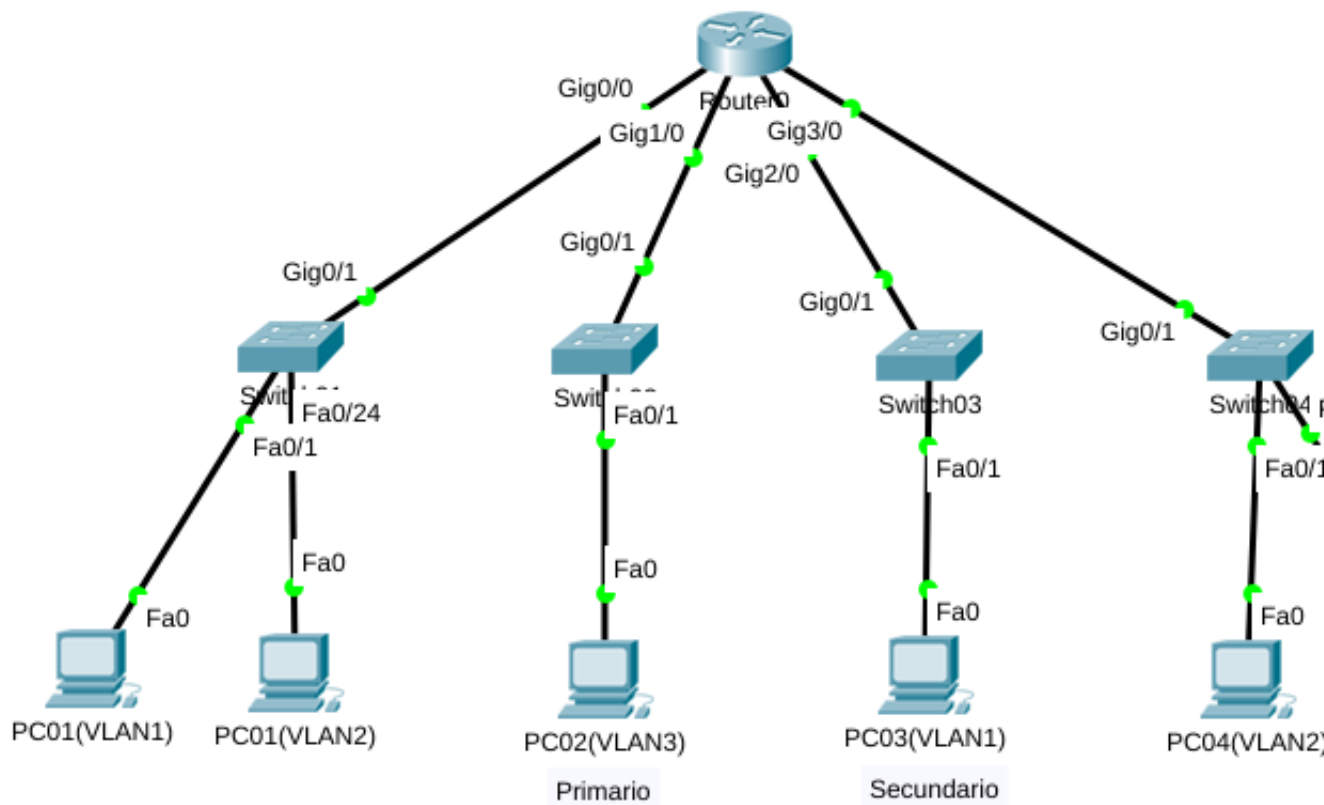


Figura 2: Cenário proposto para a atividade conforme o tópico Objetivos[2]

Logo após a inserção de tais equipamentos, foi realizado as configurações de suas interfaces de rede atribuindo à elas os endereços conforme cada tipo de equipamento, a seguir a Tabela 1 representa a configuração realizada.

Tabela 1: Configuração de endereçamento das interfaces dos dispositivos de rede do cenário elaborado

	Endereço IP	Máscara de Rede	Gateway
PC01(VLAN1)	192.168.0.1	255.255.255.0	192.168.0.254
PC01(VLAN2)	192.168.1.1	255.255.255.0	192.168.1.254
PC02(VLAN3)	192.168.2.1	255.255.255.0	192.168.2.254
PC03(VLAN1)	192.168.3.1	255.255.255.0	192.168.3.254
PC04(VLAN2)	192.168.4.1	255.255.255.0	192.168.4.254
PC04(VLAN3)	192.168.5.1	255.255.255.0	192.168.5.254
Router0 - GigabitEthernet 0/0.1	192.168.0.254	255.255.255.0	—————
Router0 - GigabitEthernet 0/0.2	192.168.1.254	255.255.255.0	—————
Router0 - GigabitEthernet 1/0.1	192.168.2.254	255.255.255.0	—————
Router0 - GigabitEthernet 2/0.1	192.168.3.254	255.255.255.0	—————
Router0 - GigabitEthernet 3/0.1	192.168.4.254	255.255.255.0	—————
Router0 - GigabitEthernet 3/0.2	192.168.5.254	255.255.255.0	—————

Para a configuração dos equipamentos switches, foram selecionadas as portas de entrada e saída para respectivas VLAN's (Virtual Local Area Network) como descritas no tópico de objetivos [2]. Após atribuir as interfaces as respectivas VLAN's, as configurações finais podem ser observadas a seguir pelas figuras 3, 4, 5 e 6. Para as interfaces com tecnologias do tipo GigaEthernet foram configuradas como modo Trunk Protocol, tais portas são usadas para comunicar duas VLAN's distintas.

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Gig0/2
2 20	active	Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Figura 3: Configuração das VLAN's no switch 01.

VLAN Name	Status	Ports
1 default	active	Gig0/2
3 30	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Figura 4: Configuração das VLAN's no switch 02.

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Figura 5: Configuração das VLAN's no switch 03.

VLAN	Name	Status	Ports
1	default	active	Gig0/2
2	20	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11
3	30	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Figura 6: Configuração das VLAN's no switch 04.

As configurações nos roteadores do cenário seguiram da seguinte forma, para cada interface conectada à um equipamento switch, nestas interfaces foram atribuídas redes virtuais, representadas pela figura 7.

Routing Table for Router0				
Type	Network	Port	Next Hop IP	
C	192.168.0.0/24	GigabitEthernet0/0.1	---	0/0
C	192.168.1.0/24	GigabitEthernet0/0.2	---	0/0
C	192.168.2.0/24	GigabitEthernet1/0.1	---	0/0
C	192.168.3.0/24	GigabitEthernet2/0.1	---	0/0
C	192.168.4.0/24	GigabitEthernet3/0.1	---	0/0
C	192.168.5.0/24	GigabitEthernet3/0.2	---	0/0

Figura 7: Configurações das redes virtuais no router0.

5.2 Resultados

Após a elaboração e configuração do cenário proposto, realizamos a verificação da comunicação entre os hosts PC (Personal Computer) da rede hospedados em diferentes VLAN's (Virtual Local Area Network) utilizando o protocolo ICMP (Internet Control Message Protocol) para garantir a comunicação entre os equipamentos. As respostas às solicitações ICMP podem ser observadas na figura 8.
















PDU List Window				
Fire	Last Status	Source	Destination	Type
	Successful	PC01(VLAN1)	PC01(VLAN2)	ICMP
	Successful	PC01(VLAN1)	PC02(VLAN3)	ICMP
	Successful	PC01(VLAN1)	PC03(VLAN1)	ICMP
	Successful	PC01(VLAN1)	PC04(VLAN2)	ICMP
	Successful	PC01(VLAN1)	PC04(VLAN3)	ICMP
	Successful	PC01(VLAN2)	PC02(VLAN3)	ICMP
	Successful	PC01(VLAN2)	PC03(VLAN1)	ICMP
	Successful	PC01(VLAN2)	PC04(VLAN2)	ICMP
	Successful	PC01(VLAN2)	PC04(VLAN3)	ICMP
	Successful	PC02(VLAN3)	PC03(VLAN1)	ICMP
	Successful	PC02(VLAN3)	PC04(VLAN2)	ICMP
	Successful	PC02(VLAN3)	PC04(VLAN3)	ICMP
	Successful	PC03(VLAN1)	PC04(VLAN2)	ICMP
	Successful	PC03(VLAN1)	PC04(VLAN3)	ICMP
	Successful	PC04(VLAN2)	PC04(VLAN3)	ICMP

Figura 8: Respostas as requisições ICMP entre todos os hosts da rede.

6 Discussão dos Resultados

Após a elaboração do cenário com as configurações descritas anteriormente no tópico de objetivos [2], pode-se observar a comunicação entre os equipamentos após a requisição do protocolo ICMP (Internet Control Message Protocol) mesmo que tais dispositivos estejam hospedados em diferentes VLAN's. Tal comunicação só é possível graças às configurações das interfaces dos switches que ligam outros switches estarem habilitadas no modo Trunk e o roteador está configurado também para encapsular os pacotes que são originados em determinadas VLAN (Virtual Local Area Network) através do comando "*(config-if) #encapsulation dot1q [IDVLAN]*". Para toda informação destinada à outra rede, é direcionado para o roteador por meio do gateway padrão das máquinas PC's (Personal Computer), assim o roteador tem a função de repassar a mensagem de uma VLAN, atingindo o equipamento destinado.

7 Conclusões

Através dos protocolos de rede VTP (VLAN Trunking Protocol), tem-se um melhor controle e distribuição das redes, uma vez que políticas de controle podem interagir de forma diferenciada para cada rede virtual criada, criando uma divisão lógica da rede que por sua vez não precisa seguir a mesma divisão física, gerando assim uma estrutura de controle diferenciado para cada VLAN (Virtual Local Area Network) na rede, onde . Acima de tudo, o VTP permite que grandes LANs possam ser divididas em redes menores, aumentando a rapidez e seguranças delas.

8 Referências

- CISCO. *Catalyst 6500 Release 12.2SX Software Configuration Guide*. [S.l.], 2018. Disponível em: <<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500-ios/12-2SX/configuration/guide/book/vtp.html#wp1051097>>. Acesso em: 09.06.2018. Citado na página 5.
- FUZITANI, C. *Fundamentos de Redes de Computadores*. [S.l.], 2018. Disponível em: <<http://frc2013.blogspot.com/2013/10/vlan.html>>. Acesso em: 09.06.2018. Citado na página 5.