USJT - FTCE

Arquitetura OSI
Camada de Enlace
ARP & VLAN

Prof. Me. Ricardo Girnis Tombi

Alunos:

_____

_____

_____

1. Objetivo

Este experimento demonstra o funcionamento do protocolo ARP em uma rede local conectada por um switch, bem como o comportamento da rede quando Vlans são configuradas neste switch.

2. Conceitos Abordados

Arquitetura de Redes OSI, Camada de Enlace, Protocolo ARP e VLAN.

3. Material

- Computadores
- Packet Tracer

4. Teoria

Fonte: LARC/USP 2013

4.1 A Domínio de Colisão e Domínio de Broadcast

Normalmente o uso de um switch permite a separação de domínios de colisão ao criar enlaces dedicados em cada uma de suas portas, ou seja, diferentemente do hub, o switch tem a habilidade de inspecionar os pacotes ingressantes e, identificando a origem e destino, direcioná-lo para o dispositivo correto. Ao direcionar os pacotes apenas para o dispositivo originalmente intencionado, o switch aumenta o desempenho da rede ao diminuir o tráfego de pacotes.

No entanto, os dispositivos conectados por um switch ainda fazem parte da mesma rede local (LAN), e estão sujeitos a pacotes de broadcast, utilizados, por exemplo, para localizar dispositivos na rede. Essas mensagens não são um problema em uma rede pequena, mas para uma grande rede (e.g. grandes corporações) eles podem comprometer o desempenho da mesma e do sistema.

Roteadores podem ser utilizados para separar as redes em diferentes domínios de broadcast e colisão, no entanto, a utilização de roteadores sempre que uma rede precisa ser segmentada em diferentes domínios é desencorajado por diversos motivos: roteadores possuem poucas portas, são dispositivos relativamente caros e aumentam a latência da comunicação uma vez que precisam de mais informações do pacote (são dispositivos de camada 3) para direcioná-los corretamente.

4.2 O Protocolo ARP (*Address Resolution Protocol*)

O Protocolo de Resolução de Endereços (ARP) é o protocolo responsável por fazer a tradução de endereços IP (da camada de rede) para endereço MAC (da camada de enlace). Cada nó em uma sub-rede tem uma tabela ARP que contém mapeamento de endereços IP para endereço MAC. A tabela ARP também contém um campo de tempo de vida (TTL) que indica quando cada mapeamento será apagado da tabela.

Este protocolo é utilizado quando um nó de uma sub-rede quer enviar um datagrama para outro nó na mesma sub-rede. Para isso, a tabela ARP será consultada e, caso não haja nenhum registro na tabela referente ao endereço a que o datagrama se destina, será montado um pacote especial chamado ARP Query. O pacote ARP de consulta e de resposta tem o mesmo formato. Este pacote é enviado por broadcast na camada de enlace e é aguardado a resposta. Todos os nós da sub-rede recebem o pacote ARP e verificam se aquele endereço IP indicado no pacote é o seu, se for, responde acrescentando ao pacote seu endereço MAC. Se não for, simplesmente o descarta. O nó que enviou o ARP recebe a resposta, acrescenta em sua tabela ARP aquele novo registro e já pode enviar o datagrama IP ao nó destino. É interessante saber que o ARP não foi feito especificamente para endereços IP e MAC, ele pode ser utilizado para resolver endereços de rede de outras tecnologias.

4.3 VLANs

Em uma rede tradicional pode-se encontrar diferentes departamentos, como por exemplo, marketing e recursos humanos alocados em um mesmo segmento de rede. Nesse caso, é comum as pessoas estarem trabalhando fisicamente próximas, porém sem a necessidade de uma troca freqüente de comunicação entre os departamentos. Muitas vezes isso não é nem mesmo desejável. Classicamente a forma de separar o tráfego desses departamentos é através de redes físicas distintas para cada departamento, interligadas através de um roteador.

A tecnologia de redes locais virtuais (Virtual Local Area Networks - VLAN) cria uma camada de abstração permitindo que a estrutura lógica da LAN seja independente de sua topologia física. Esse tipo de abordagem traz consigo uma série de vantagens para a pessoa responsável por realizar a manutenção nas estações e nos equipamentos da rede: separação de domínios de broadcast e colisão, isolamento e fácil localização de distúrbios e mais, como será mostrado a frente.

O conceito de VLAN surgiu para que os switches fossem capazes de lidar com diferentes domínios de broadcast simultaneamente. Quando uma VLAN é criada, apenas os membros dessa VLAN poderão enxergar o tráfego nessa rede, confinando inclusive o tráfego de broadcast da rede. Desta forma através de um único equipamento, são criados domínios lógicos separados para cada um dos departamentos evitando dessa forma a interferência direta entre o tráfego das redes.

O emprego de VLAN adiciona ainda a vantagem de permitir que uma única VLAN exista entre diferentes equipamentos. Desta forma se o departamento de marketing, por exemplo, for expandindo, basta acrescentar um novo switch e colocar os novos usuários para trabalharem em conjunto, isto é, na mesma VLAN.

Veja que o departamento pode crescer fisicamente para outros andares. Se uma pessoa não puder ser alocada em um determinado andar, basta mudar a configuração lógica da VLAN. Do ponto de vista dessa pessoa, não haverá nenhuma necessidade de alterar as suas configurações de rede.

É importante notar que apesar dos equipamentos abrigarem diferentes VLANs, a comunicação entre essas VLAN acontece como se estivessem em redes físicas separadas. A única forma para estabelecerem qualquer tipo de comunicação é através do uso de algum equipamento que faça o roteamento do tráfego entre essas redes.

Em resumo, as VLANs apresentam os seguintes objetivos:

- ✓ Confinar os broadcasts dentro de suas próprias VLANs reduzindo o consumo de banda e aumentando o desempenho da rede.
- ✓ Aumentar a segurança da rede, pois ao formar domínios de broadcasts separados, máquinas de diferentes VLANs não podem se comunicar a menos que o tráfego seja roteado na camada 3.
- ✓ Tornar mais flexível a formação de grupos de trabalho virtuais. Uma VLAN pode ser usada para criar grupos que se estendem por diferentes segmentos da rede. Quando a posição física de um equipamento é modificada, dentro da área do seu grupo, o equipamento ainda pode acessar a rede sem a necessidade de modificar as suas configurações de rede. Reconfigurar uma rede torna-se um problema de reconfiguração da lógica dos equipamentos e não de suas conexões físicas.

Observação:

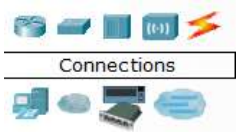
As portas dos switches podem ser configuradas de algumas formas para trabalhar com VLANs, e de uma forma geral serão:

- ✓ **Access**: uma porta de acesso pode pertencer a apenas uma única VLAN e geralmente é conectada ao computador dos usuários.
- ✓ **Trunk**: uma porta trunk pode pertencer a mais de um tipo de VLAN. Ela pode enviar e receber pacotes de diferentes VLANs e é normalmente conectada a outro switch.

5. Procedimento Experimental

a) Abra o programa Packet Tracer.

b) Selecione, no canto inferior esquerdo da tela, os seus equipamentos que formarão sua rede. Arraste os mesmos para a área de trabalho.
- 4 End devices Genéricos (PCs)
- 1 Switch 2960



c) Clique no ícone de conexões e então selecione o cabo *Coper Straight-Through* para conectar os equipamentos.

d) Arraste este cabo até um *End Device*, clique sobre o mesmo e selecione a porta Fast-Ethernet para conexão.

e) Em seguida arraste este cabo até o switch e clique sobre o mesmo. Escolha a porta Fast-Ethernet 0/1 para conexão.

f) Repita os mesmos passos c), d) e e) para conectar os outros 3 *End Device*s ao switch.

Nota: Conecte cada *End Device* pela sua porta Fast-Ethernet e no Switch escolha as portas na forma sequencial.

g) Clique uma vez sobre o PC0 para abrir suas configurações.
Selecione a aba – Config.
Selecione o botão – Interface e então Fast-Ethernet
Configure seu endereço IP no campo IP Configuration. Utilize o valor 10.10.10.10.

h) Repita o item g) para os demais PCs. Utilize os endereço 10.10.10.11; 10.10.10.12; 10.10.10.13.

i) Entre no modo simulação (botão no canto direito inferior da tela)
- ✓ Clique “Edit Filters”, e selecione apenas ICMP e ARP

j) Selecione o PC0, aba Desktop e clique “Command Prompt”

- ✓ Faça um ping para: 10.10.10.13

k) Volte para a tela de Simulação e acione “Auto Capture”

- ✓ Decreva o que ocorre na rede:

_____
_____
_____
_____
_____

l) Clique sobre o switch e selecione a tab Config, e então o botão VLAN Database.

- ✓ Crie duas Vlans: 10 e 20, com os nomes Rede1 e Rede2 respectivamente.
- ✓ Na mesma tela de configuração selecione a interface FastEthernet0/1 e configure a mesma sendo parte da Vlan 10 (Access)
- ✓ Repita o procedimento para a interface FastEthernet0/2
- ✓ Para as interfaces FastEthernet0/3 e 0/4, configure as mesmas para estarem na Vlan 20 (Access).

m) Volte para a tela de Simulação e clique “Reset Simulation”

n) Entre no “Command Prompt” do PC0 e faça um ping para: 10.10.10.11

o) Acione “Auto Capture” e descreva o que ocorre na rede.

_____
_____
_____
_____
_____

p) Entre no prompt do PC0 e descreva o resultado do ping.

_____
_____
_____
_____
_____

q) Assim que o ping terminar, faça novo reset na simulação.

r) A partir do PC3, execute um ping para: 10.10.10.10

s) Acione “Auto Capture” e descreva o que ocorre na rede.

_____
_____
_____
_____
_____

t) Entre no prompt do PC3 e descreva o resultado do ping

_____
_____
_____
_____
_____

u) O que deve ser feito para que os equipamentos possam se comunicar entre as diferentes Vlans

_____
_____
_____

6. Conclusão

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____