MULTICAST EM REDES BASEADAS EM *SWITCHS*

O *switch* é um dispositivo de diversas portas, com cada uma delas podendo ser conectada a várias estações (sob a forma de uma LAN), ou a uma única estação. A sua função é segmentar uma rede muito grande em LAN's menores e menos congestionadas, de forma a melhorar o desempenho da rede. Esse aumento de performance é obtido fornecendo a cada porta do *switch* uma largura de banda dedicada. No caso de redes locais diferentes serem conectadas em cada uma dessas portas, pode-se transmitir dados entre essas LAN's conforme o necessário. O *switch* também provê uma filtragem de pacotes entre LAN's que estejam separadas. **Erro! A origem da referência não foi encontrada.**

Os *switchs* que operam na camada 2 enviam, por padrão, todo o tráfego multicast a todas as portas pertencentes à rede de destino. Este comportamento reduz a eficiência do *switch*, além de contradizer o principal propósito do equipamento que é o de limitar o tráfego às portas que querem a informação.

Na próxima Figura 16 é mostrada uma rede local com multicast habilitado e núcleo baseado em *switchs*, com vários tipos diferentes de dispositivos conectados.

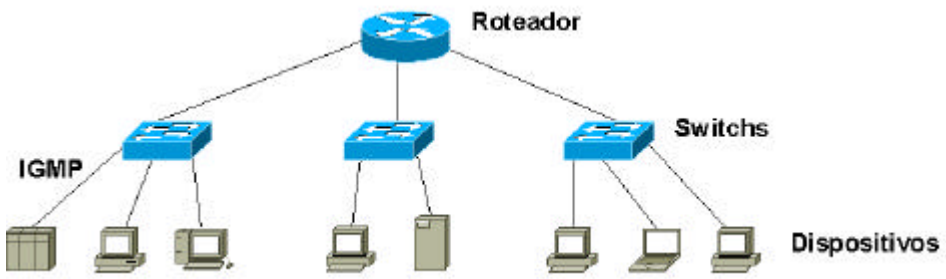

Figura 1: Mostra uma rede local multicast com núcleo baseado em *switchs*, com vários tipos diferentes de dispositivos conectados.

Esta característica do IP multicast em *switchs* camada 2 pode ser tratada de maneira eficiente através de três métodos, IGMP *Snooping*, *Cisco Group Management*

Protocol – CGMP e *Router-Port Group Management Protocol* – RGMP. O IGMP *Snooping* e o CGMP são utilizados em sub-redes roteadas que possuem receptores ativos, ambos dependem das mensagens de controle do IGMP que são enviadas entre roteadores e receptores, enquanto que o RGMP é utilizado em segmentos que só possuam roteadores. Na Figura 17 abaixo são indicadas as áreas de atuação dos protocolos IGMP *Snooping*, CGMP dentro de uma rede local com multicast habilitado.

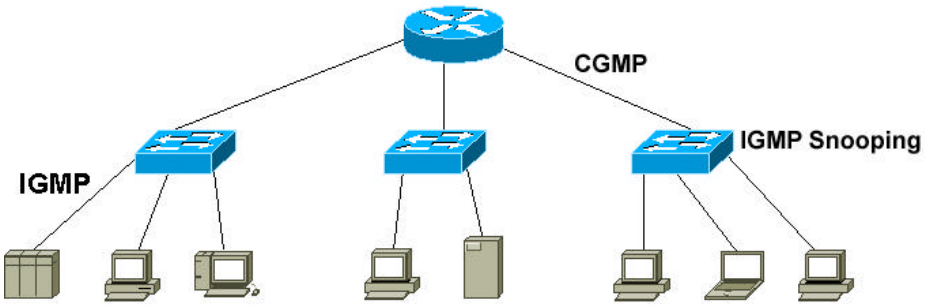

Figura 2: Mostra a área de atuação dos protocolos IGMP *Snooping*, CGMP dentro de uma rede local multicast.

Na Figura 17 abaixo é indicado a área de atuação do protocolo RGMP.

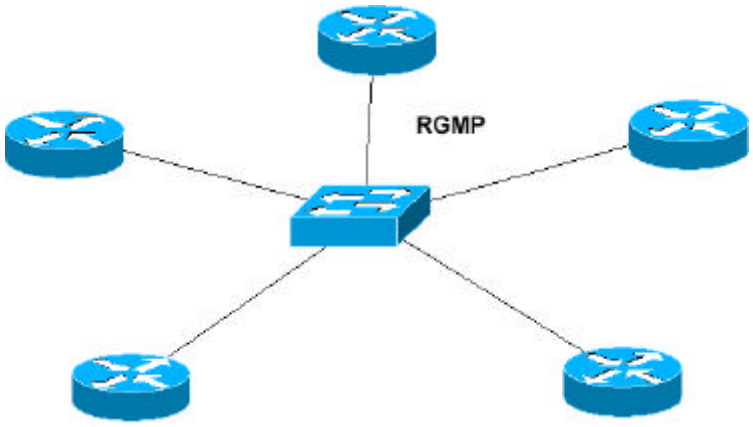

Figura 3: Segmento de rede que só contem roteadores.

IGMP *SNOOPING*

É um método de confinamento do IP multicast que é executado em *switchs* de camada 2. Tem seu princípio de funcionamento baseado no exame de algumas informações da camada 3 contidas nas mensagens IGMP de saída e de união aos grupos, trocadas entre o roteador e os dispositivos da rede.

Quando o *switch* verifica a existência de uma mensagem de união, encaminhada por um dispositivo, a um determinado grupo ele adiciona a porta referente àquele dispositivo a uma tabela correlacionando porta e grupo multicast. Quando é verificada uma mensagem de saída do grupo, a entrada correspondente da tabela é removida.

Uma vez que as mensagens IGMP são pacotes multicast, o *switch* camada 2 não tem capacidade de distingui-las dos pacotes multicast com dados. Assim, um *switch* executando IGMP *Snooping*, para descobrir se existe alguma mensagem de controle fica obrigado a verificar todas as mensagens multicast que chegam a ele.

Se o IGMP *Snooping* for executado em um *switch* com pequeno poder de processamento a sua performance será muito afetada quando houver uma grande taxa de tráfego de dados.

CISCO GROUP MANAGEMENT PROTOCOL – CGMP

É um protocolo desenvolvido pela Cisco que permite aos *switchs Catalyst* obter informações do IGMP nos roteadores Cisco, possibilitando-os a tomada de decisões na camada 2. Deve ser configurado nos roteadores multicast e nos *switchs* camada 2.

Através do CGMP o tráfego IP multicast é enviado somente as portas do *switch* que possuem receptores para o tráfego multicast. Todas as portas que não requisitaram tráfego multicast não receberam, com a exceção da portas de conexão com os roteadores multicast, pois estas devem receber todo o tráfego dos pacotes multicast.

O funcionamento básico pode ser descrito como: uma mensagem de relatório de um grupo específico é enviada ao roteador passando pelo *switch* sem nenhum processamento extra. O roteador recebe e processa esta mensagem normalmente, cria uma mensagem CGMP de união e a envia ao *switch*. Ao receber a mensagem CGMP de união o *switch* acrescenta a porta a sua tabela de memória de conteúdo-endereçado – *content-addressable memory* para o grupo. Todo o tráfego subseqüente daquele grupo será encaminhado àquela porta para o receptor. Na Figura 19 a seguir é mostrado o caminho das mensagens no funcionamento do CGMP.

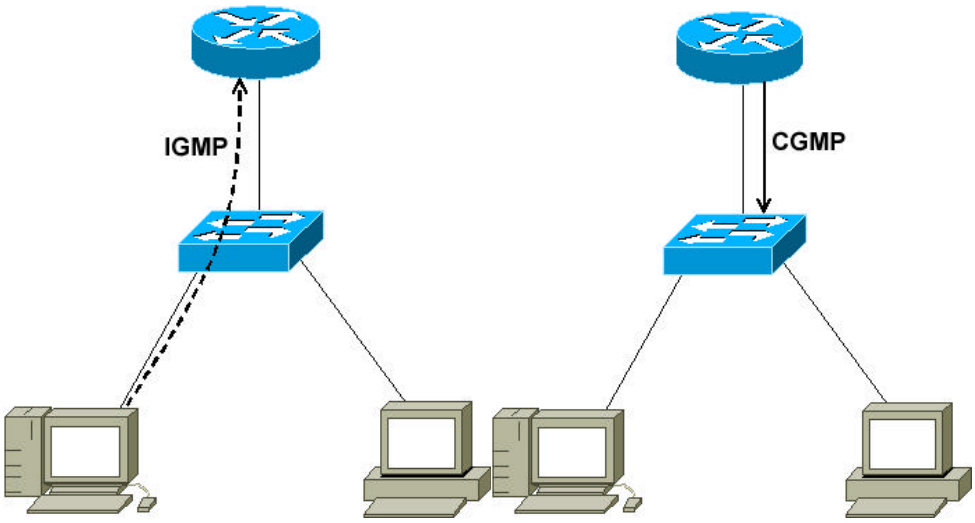

Figura 4: Funcionamento do CGMP.

ROUTER-PORT GROUP MANAGEMENT PROTOCOL – RGMP

Roteadores não enviam mensagens IGMP de relatório, com isso o CGMP e o IGMP *Snooping* não podem ser utilizados para controlar o tráfego multicast em *switchs* pertencentes a um *backbone Ethernet* de *switchs*. Os roteadores enviam mensagens *Protocol Independent Multicast* - PIM de união e poda para o tráfego multicast na camada 3. O PIM será descrito no decorrer deste estudo.

O funcionamento básico pode ser descrito como: o roteador indica a intenção de receber tráfego multicast enviando uma mensagem RGMP de união a um grupo específico. O *switch* então adiciona a porta referente àquele roteador na sua tabela de encaminhamento daquele grupo, um processo similar ao do CGMP. Como conseqüência todo o tráfego multicast daquele grupo será encaminhado somente as portas que efetuaram alguma indicação. Quando o roteador não necessitar mais do tráfego multicast ele envia uma mensagem RGMP de saída do grupo e o *switch* retira o encaminhamento da tabela.