Gabriel Kendy Faria Komatsu - 10816711
João Gabriel de Carvalho Ribeiro - 10783027
Vinicius Alves Matias - 10783052

Relatório do EP2 (simulação)
ACH2026 - Redes de Computadores - Turma 04

Simulação e comparação dos protocolos de roteamento RIP e AODV

São Paulo
Dezembro / 2020

1 - Resumo da Simulação

Neste EP nosso grupo tem como objetivo analisar diferenças entre dois protocolos de roteamento entre roteadores: RIP e AODV. Para tal, testamos diversos cenários com variações entre si com intenção de chegar a uma conclusão relacionando ambos os protocolos.

Para este EP a linguagem utilizada foi C++, o software onde as simulações foram conduzidas foi o ns-3 versão 30.1 e o sistema operacional utilizado foi o Linux Ubuntu 20.04.

2 - Detalhes da implementação

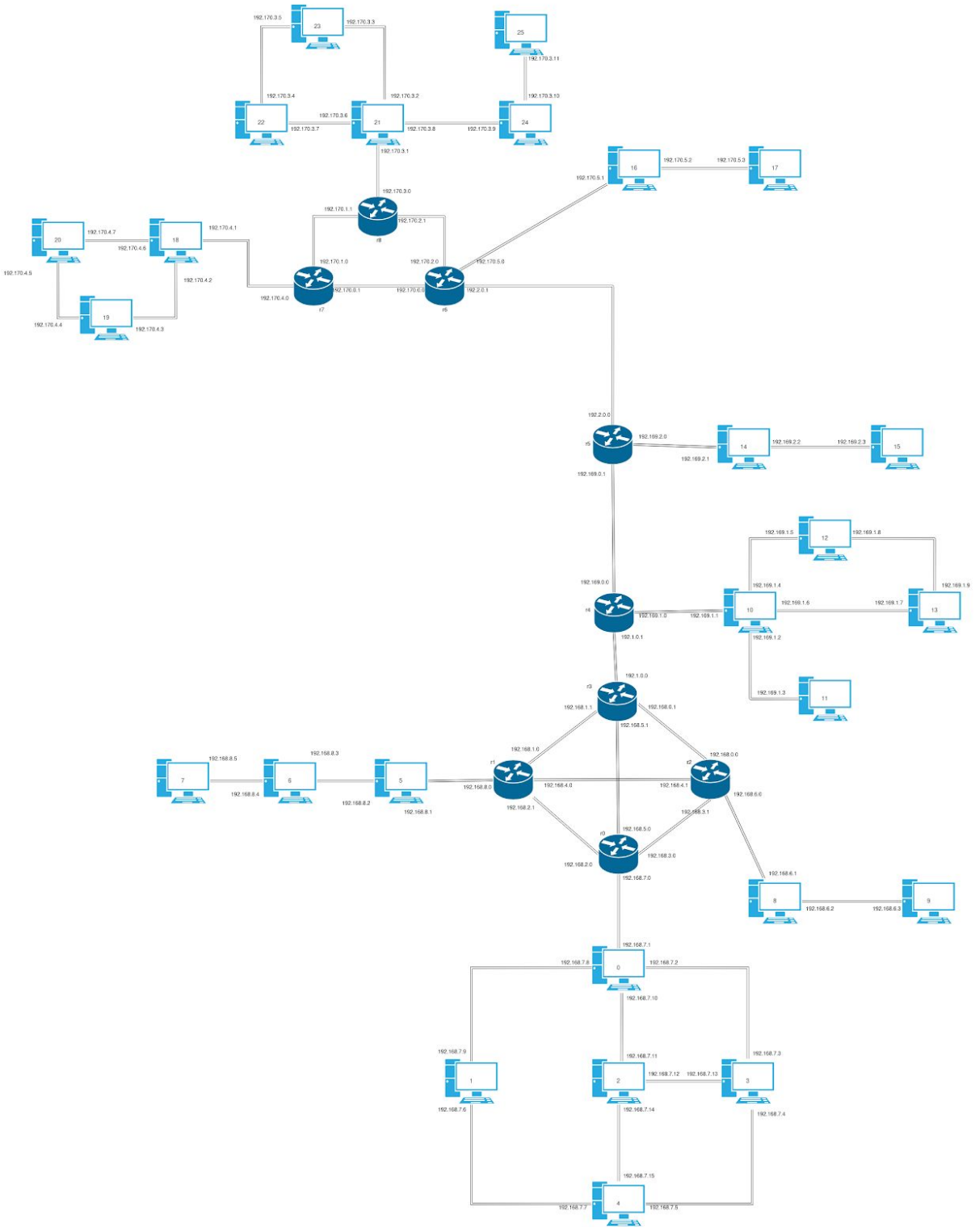

Figura 1 - Topologia da rede (acesso ao arquivo da figura clicando aqui)

A topologia básica da rede consiste em 9 roteadores, com 8 deles conectados às suas próprias sub redes, e 1 interligando roteadores. Os 26 hosts acabaram não se

tornando tão importantes para a análise da simulação, mas continuaram na rede. Os hosts podem utilizar os protocolos IP, TCP e UDP, enquanto os roteadores podem usar os protocolos RIP ou AODV, de acordo com a simulação.

Foi utilizado apenas o protocolo IPv4 para fornecer os IPs da rede. Por padrão, os enlaces entre dois pontos se dão por canais de delay igual à 3 milissegundos (não tendo uma interferência relevante na simulação) e taxa de transmissão de dados de 1Mbps.

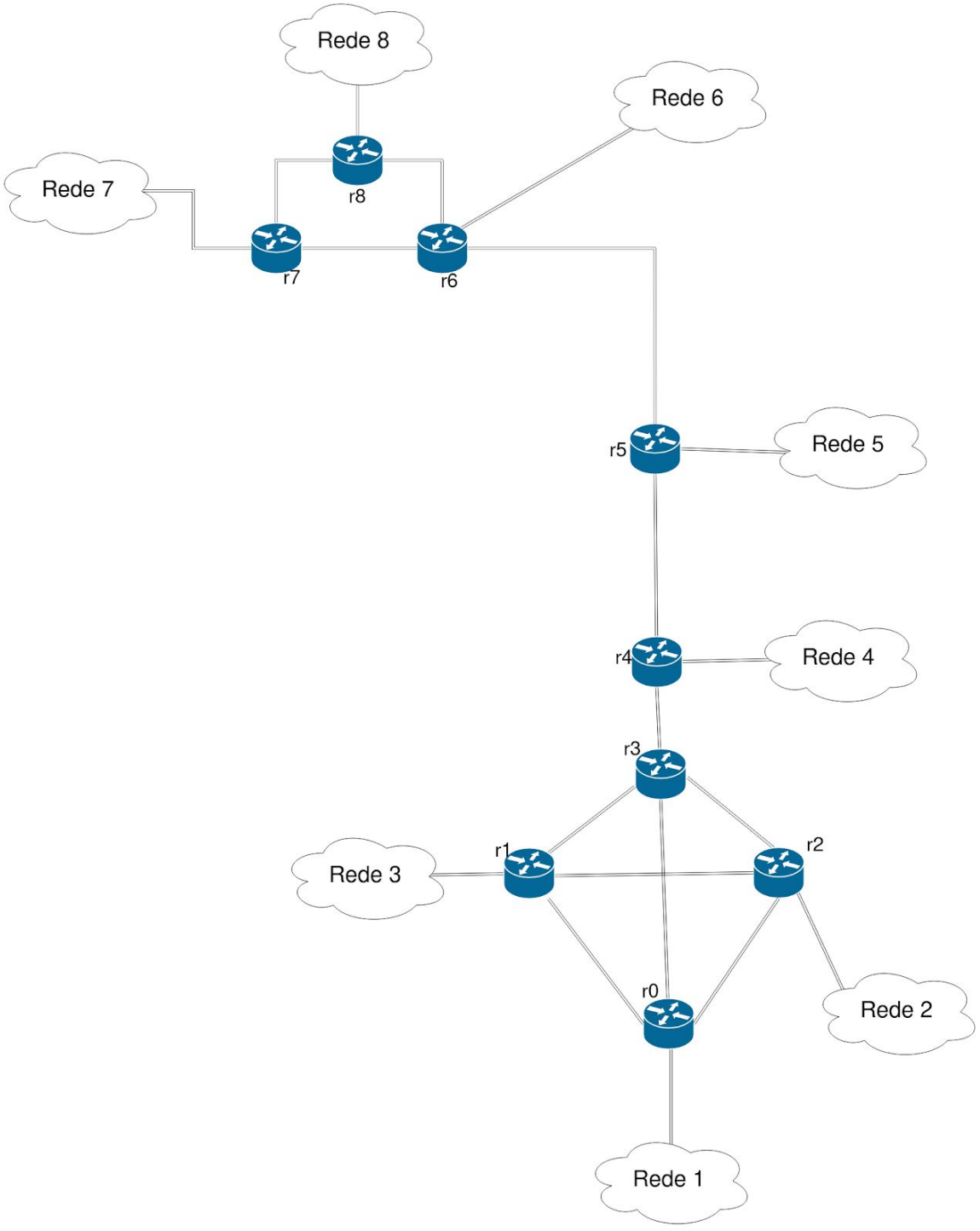

Figura 2 - Topologia resumida

3 - Como compilar e executar

Para EPs de simulação, digam qual é o simulador e se preciso fazer alguma configuração especial antes de carregar e rodar a simulação.

1. Colocar o nosso script na pasta scratch que está dentro da pasta do ns-3.
2. Abrir um terminal na pasta do ns-3, no nosso caso “ns-allinone-3.30.1/ns-3.30.1”.
3. Digitar o comando:
   ./waf --run scratch/sim0_rip
   ./waf --run scratch/sim0_aodv

Note que os scripts possuem .cc como extensão, mas nós somente executamos com o nome do arquivo.

- Os arquivos PCAP são logs feitos para cada nó e suas respectivas conexões (as “arestas” entre nós) dependendo da ordem em que foram instanciados. Para executar os outputs gerados com a extensão .pcap utilize o comando *tcpdump -r arquivo-nó-aresta.pcap*
  - Note que os arquivos foram gerados após compilar o arquivo e serão gerados na pasta ns-allinone-3.30.1/ns-3.30.1
  - Exemplo: tcpdump -r sim1_rip-0-0.pcap vai retornar o cabeçalho UDP do nó 0 com relação a sua conexão com o nó 1. sim1_rip-0-2.pcap é referente à conexão do nó 0 com o nó 3.

- Para executar a animação da simulação no NetAnim (caso deseje), você precisa:
  - Executar o NetAnim (digitando ./NetAnim no diretório netanim-versao do seu ns-3);
  - Escolher então o arquivo simX_protocolo.xml (encontrado no diretório raíz do NS-3 após ter compilado a simulação) pela interface do NetAnim.
  - Exemplo: sim1_aodv.xml

4 - Como ler o código

Os scripts anexados junto ao relatório estão escritos na linguagem C++ e muito bem comentados. Devem ser executados a partir do diretório “ns-allinone-3.30.1/ns-3.30.1” e o script deve estar dentro da pasta “ns-allinone-3.30.1/ns-3.30.1/scratch” usando o comando “./waf --run scratch/redes” do ns-3.

Os “Log do terminal” exibidos durante as simulações na parte de Testes deste relatório foram gerados através de prints das tabelas de roteamento.

Os arquivos estão nomeados como simX_protocolo.cc
Onde:

- X é o número da Simulação
- protocolo é o protocolo usado (rip ou aodv)

Ainda que cada código tenha suas particularidades, eles seguem um fluxo comum:

- Definição dos nós
- Configuração e estabelecimento dos canais entre 2 nós
- Instalação dos protocolos de roteamento específicos nos roteadores (AODV e RIP, além do reconhecimento de IPv4)
- Instalação da Pilha de Internet nas máquinas locais (permite usar IP, TCP e UDP)
- Definição dos endereços IPs dos canais
- Construção da Simulação (definição do método de análise do comportamento dos protocolos)

5 - Testes, Análise e Conclusões

Neste serão comentadas as arquiteturas de cada cenário de simulação, resultados obtidos nos testes e as conclusões da comparação entre os protocolos de roteamento AODV e RIP. O primeiro cenário remete aos fundamentos do uso dos protocolos.

Cenário 0: Princípios

A topologia da rede básica consiste em 9 roteadores, sendo que 8 deles servem de interconexão à alguma rede P2P, enquanto um dos roteadores faz uma interligação entre roteadores, tal como pode ser visualizado na imagem de topologia da rede. Existem 4 configurações para os enlaces, sendo a padrão definida com taxa de transferência de dados de 1Mbps e delay na transmissão de 3ms. Dado esse cenário padrão, será analisado como o protocolo RIP e AODV atuam nessa rede.

RIP

O protocolo RIP (Routing Information Protocol) é utilizado em roteadores para construir uma maneira eficiente de transferir datagramas em um sistema autônomo (AS). Para a simulação corrente, são considerados os 9 roteadores como parte de um mesmo AS sendo que a utilização de um roteamento inter-AS por protocolos como o BGP consideram nos custos dos enlaces políticas locais que não serão consideradas neste cenário.

Roteadores com o protocolo RIP estruturam suas tabelas de roteamento segundo o algoritmo de vetor de distâncias, isto significa que a identificação do caminho mais curto para outro roteador segue um ritmo empírico, onde as novas descobertas de roteadores interferem na tabela corrente, quando é identificado um caminho mais curto para alguma sub rede conectada à um roteador conhecido. As tabelas 1 e 2 mostram a diferença nas tabelas de roteamento no segundo 0 e no segundo 5 para o roteador 0 do AS em questão.

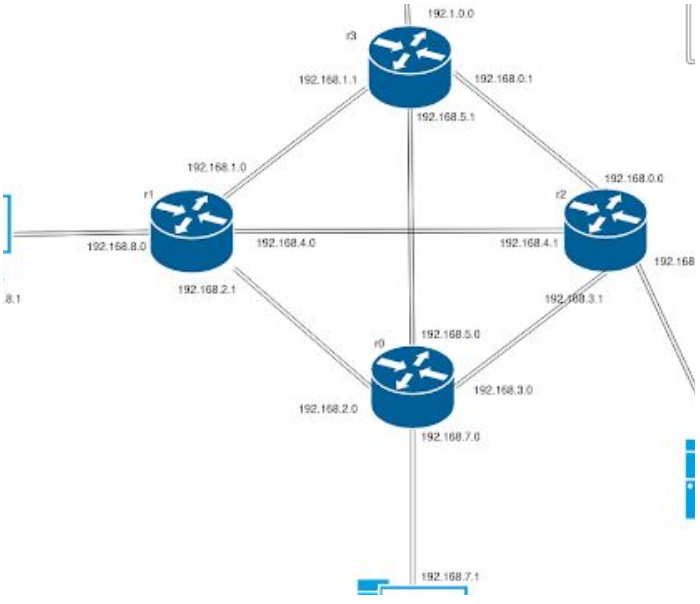

Figura 2 - Recorte da rede (comunicações do roteador 0)

Tabela 1 - Tabela de Roteamento do roteador 0 no segundo 0

Destination	Gateway	Genmask	Flags	Metric	Iface

192.168.2.0	0.0.0.0	255.255.255.0	U	1	1
192.168.3.0	0.0.0.0	255.255.255.0	U	1	2
192.168.5.0	0.0.0.0	255.255.255.0	U	1	4
192.168.7.0	0.0.0.0	255.255.255.0	U	1	5

Tabela 2 - Tabela de Roteamento do roteador 0 no segundo 5

Destination	Gateway	Genmask	Flags	Metric	Iface
192.168.8.0	192.168.2.1	255.255.255.0	UGS	2	1
192.168.1.0	192.168.2.1	255.255.255.0	UGS	2	1
192.169.1.0	192.168.2.1	255.255.255.0	UGS	3	3
192.169.0.0	192.168.5.1	255.255.255.0	UGS	3	3
192.170.5.0	192.168.5.1	255.255.255.0	UGS	5	3
192.170.2.0	192.168.5.1	255.255.255.0	UGS	5	3
192.170.0.0	192.168.5.1	255.255.255.0	UGS	5	3
192.2.0.0	192.168.5.1	255.255.255.0	UGS	4	3
192.169.2.0	192.168.5.1	255.255.255.0	UGS	4	3
192.1.0.0	192.168.5.1	255.255.255.0	UGS	2	3
192.168.6.0	192.168.3.1	255.255.255.0	UGS	2	2
192.168.0.0	192.168.3.1	255.255.255.0	UGS	2	2
192.168.4.0	192.168.3.1	255.255.255.0	UGS	2	2
192.168.2.0	0.0.0.0	255.255.255.0	U	1	1
192.168.3.0	0.0.0.0	255.255.255.0	U	1	2
192.168.5.0	0.0.0.0	255.255.255.0	U	1	3
192.168.7.0	0.0.0.0	255.255.255.0	U	1	4

Como pode ser verificado, a tabela no segundo 0 conhece apenas seus vizinhos, podendo chegar a cada uma das 4 redes visíveis fazendo o repasse à interface de rede correspondente na tabela (Iface). Como não há necessidade de utilizar outros enlaces da rede, é considerado o custo (Metric) de chegar ao destino disponível igual à 1, pois é o custo de um pulo entre a interface de rede que recebe o datagrama e o repasse à interface

de rede que aponta para o enlace de destino. A flag U (up) sozinha significa apenas que a rota para um destino é válida.

Verificando a tabela de roteamento após 5 segundos de simulação notamos que foram adicionados novos endereços IP de destino, isso porque nesses segundos de diferença houve o envio das informações de custos de enlace do roteador 0 aos seus vizinhos, e esses roteadores enviaram os custos para chegar aos seus enlaces conhecidos. Dessa forma, poucos milissegundos após fazer o broadcast entre seus vizinhos, eles farão o mesmo processo enviando também uma mensagem de resposta RIP ao roteador adjacente que era seu vizinho e tinha apenas eles na sua tabela de roteamento, mas agora tem o feedback desse roteador e pode identificar o custo para chegar em um desses novos destinos conhecidos ou um caminho de menor custo para chegar à um endereço já conhecido anteriormente (na primeira atualização não vai haver um menor caminho para chegar à uma interface do próprio roteador, pois já tem custo 1, mas com novos destinos sendo conhecidos por feedback dos outros roteadores envolvidos passará a ser possível essa identificação de menores caminhos).

Além disso, uma tabela com destinos além dos vizinhos diretos do roteador deverá ter outras flags do protocolo RIP, no caso todos os destinos que têm custo maior que 1 (isso quer dizer deve se passar por pelo menos um enlace para chegar no destino) persistem na tabela de roteamento com a flag U (Up) que significa que a rota é válida, G (Gateway) para dizer que o destino está atrelado à outro gateway (ou seja, não é vizinho direto do roteador) e S (Static) para apontar que a rota foi acionada pelo comando route através do NS-3.

Para chegar em um destino direto a outro roteador mas que está visível por essa segunda tabela de roteamento deve-se, primeiramente, escolher o destino. Como exemplo, se um datagrama chegar ao roteador 0 no segundo 5 querendo ir para um IP da subrede de endereço 192.169.0/24 ele deve encontrar na tabela de roteamento esse endereço e, através dela, identificará que o menor caminho será pela interface de rede 3 do roteador 0, que sai do roteador pelo endereço 192.168.5.1 (gateway), que leva à uma interface de rede do roteador 3. O roteador 3 terá outra tabela de roteamento que irá indicar para qual de suas interfaces o datagrama deve ser repassado, agora com custo 2 para chegar ao destino. Após isso, o datagrama estará no roteador cujo custo é 1 para chegar na rede de destino, sendo feito o repasse para chegar na sub rede de destino.

É importante mencionar que outras tabelas de roteamento podem estar sendo populadas enquanto não recebem o feedback de outras mais distantes, que é o caso do roteador 7, como pode ser visto nas tabelas 3 e 4.

Tabela 3 - Tabela de Roteamento do roteador 7 no segundo 0

Destination	**Gateway**	**Genmask**	**Flags**	**Metric**	**Iface**
192.170.0.0	0.0.0.0	255.255.255.0	U	1	1
192.170.1.0	0.0.0.0	255.255.255.0	U	1	2
192.170.4.0	0.0.0.0	255.255.255.0	U	1	3

Tabela 4 - Tabela de Roteamento do roteador 7 no segundo 5

Destination	Gateway	Genmask	Flags	Metric	Iface
192.170.5.0	192.170.0.0	255.255.255.0	UGS	2	1
192.2.0.0	192.170.0.0	255.255.255.0	UGS	2	1
192.170.3.0	192.170.1.1	255.255.255.0	UGS	2	2
192.170.2.0	192.170.1.1	255.255.255.0	UGS	2	2
192.170.0.0	0.0.0.0	255.255.255.0	U	1	1
192.170.1.0	0.0.0.0	255.255.255.0	U	1	2
192.170.4.0	0.0.0.0	255.255.255.0	U	1	3

Ainda que o roteador 7 não tenha recebido o anúncio RIP do roteador 0, ele conseguiu identificar alguns enlaces com custo máximo de 2. Ocorrendo o reconhecimento do roteador 0, a tabela do roteador 7 identifica os menores custos para chegar à algum enlace relacionado ao roteador 0, assim como os roteadores de meio de caminho atualizam suas tabelas também para encontrar um caminho de menor custo pelo algoritmo de vetores de distância.

A atualização da tabela de roteamento está relacionada aos anúncios dos roteadores vizinhos. Quando há uma nova informação de custo ou destino, essa é propagada aos roteadores conhecidos para recalcular a melhor rota. Contudo, depois de um período de tempo as atualizações podem ficar menos frequentes e para impedir que exista a possibilidade de um enlace não estar mais disponível (ou ter aumentado o custo) e continuar na tabela de roteamento que após cerca de 20 segundos sem nenhum feedback de um enlace, os roteadores enviam um novo anúncio RIP aos seus vizinhos para identificar o estado dos enlaces e propogar as verificações.

Para exemplificar, a figura 3 exibe um gráfico com os 6 anúncios RIP que acontecem nos 100 primeiros segundos de simulação do roteador 0 ao roteador 1. Note que os 4 primeiros ocorrem em um curto período de tempo (aproximadamente 12 segundos) que é o período em que se está estudando os roteadores do AS para adicionar na tabela de roteamento, depois desse período as atualizações se tornam menos frequentes e, para verificar se não houveram mudanças nos custo dos enlaces, envia novas mensagens em um intervalo de cerca de 30 segundos.

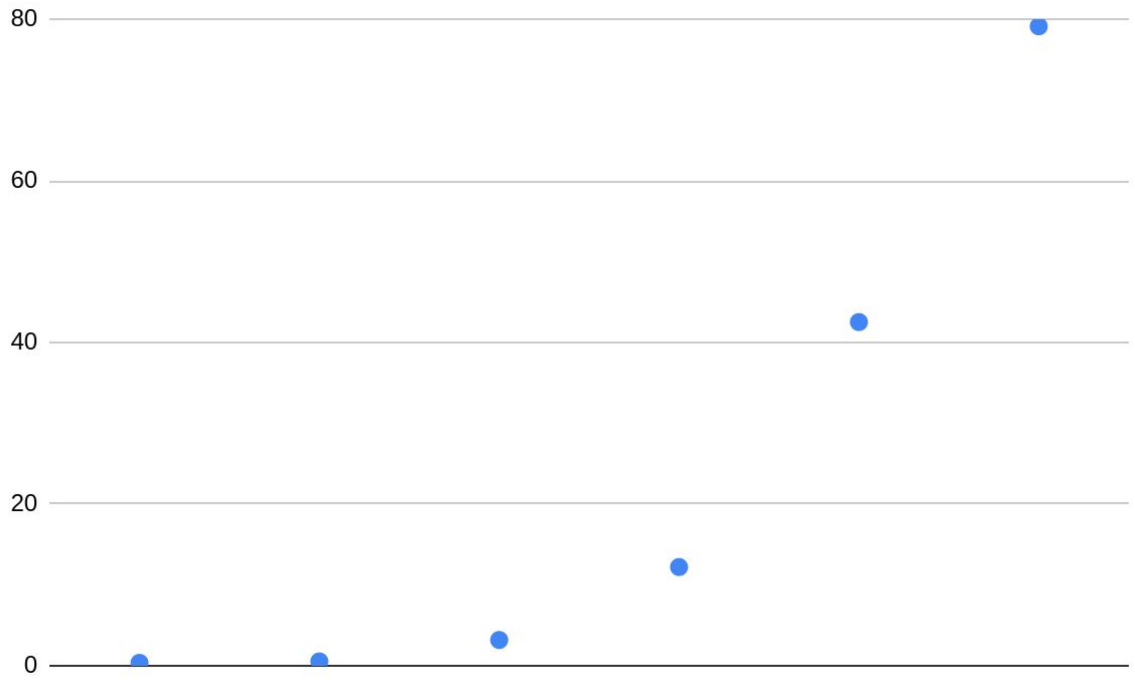

Figura 3 - Diferença de tempo entre cada datagrama enviado do roteador 0 ao roteador 1

O NS-3 envia datagramas com que encapsulam segmentos UDP para enviar as mensagens de requisição e resposta do protocolo RIP, cujo cabeçalho segue a RFC2453 e é representado pelo NS-3 da seguinte forma:

SendTo: ns3::RipHeader (command 1 | prefix 0.0.0.0/0 Metric 16 Tag 0 Next Hop 0.0.0.0)
SendTo: ns3::RipHeader (command 1 | prefix 0.0.0.0/0 Metric 16 Tag 0 Next Hop 0.0.0.0)
SendTo: ns3::RipHeader (command 1 | prefix 0.0.0.0/0 Metric 16 Tag 0 Next Hop 0.0.0.0)
Received ns3::RipHeader (command 1 | prefix 0.0.0.0/0 Metric 16 Tag 0 Next Hop 0.0.0.0) from 192.169.0.1:520
SendTo: ns3::RipHeader (command 2 | prefix 192.169.0.0/24 Metric 16 Tag 0 Next Hop 0.0.0.0 | prefix 192.1.0.0/24 Metric 1 Tag 0 Next Hop 0.0.0.0 | prefix 192.169.1.0/24 Metric 1 Tag 0 Next Hop 0.0.0.0)
Received ns3::RipHeader (command 1 | prefix 0.0.0.0/0 Metric 16 Tag 0 Next Hop 0.0.0.0) from 192.2.0.0:520

O log acima é um recorte das várias mensagens enviadas, mais exatamente, são os cabeçalhos dos primeiros datagramas enviados e recebidos. Das informações, algo que deve ser destacado é que estão sendo enviados datagramas para identificar o endereço dos vizinhos diretos, tais mensagens RIP são recebidas por padrão na porta 520 do endereço IP.

Outro log que descreve a formação dos datagramas pela análise dos cabeçalhos segue a seguinte estrutura:

ns3::PppHeader (Point-to-Point Protocol: IP (0x0021)) ns3::Ipv4Header (tos 0x0 DSCP Default ECN Not-ECT ttl 1 id 0 protocol 17 offset (bytes) 0 flags [none] length: 52 192.169.0.1 > 224.0.0.9)

ns3::UdpHeader (length: 32 520 > 520) ns3::RipHeader (command 1 | prefix 0.0.0.0/0 Metric 16 Tag 0 Next Hop 0.0.0.0)

Além das informações de comprimento do segmento UDP encapsulado e do cabeçalho da mensagem RIP, são dados alguns detalhes do protocolo IP. Destaca-se o ttl (time to live) igual à 1, significando que a duração de confiança na mensagem é de um salto a partir da origem,. Além disso, há a informação do campo ECN (Explicit Congestion Notification), que é uma extensão ao protocolo IP (RFC 3168) para notificar os pontos do enlace se há congestionamento de pacotes que visa reduzir a perda no envio de pacotes não é habilitado (Not-ECT, ou Not ECN-Capable Transport, representado pelos bits 00 quando enviado o cabeçalho). Ainda no cabeçalho IPv4 há o campo DSCP, informando a capacidade de transmitir serviços escaláveis e diferentes pelo protocolo IP (RFC 2474) por padrão.

Um último detalhe sobre o funcionamento do RIP pode ser identificado pelo fragmento de log abaixo (primeiras linhas):

Processing RT m_local=192.170.5.0; m_mask=255.255.255.0; m_broadcast=192.170.5.255; m_scope=2; m_secondary=0 1
Processing RT m_local=192.2.0.0; m_mask=255.255.255.0; m_broadcast=192.2.0.255; m_scope=2; m_secondary=0 1
Processing RT m_local=192.170.3.0; m_mask=255.255.255.0; m_broadcast=192.170.3.255; m_scope=2; m_secondary=0 1

Processing RT refere-se ao processamento da Tabela de Roteamento (Routing Table ou simplesmente RT). Desse log entende-se mais de como as mensagens RIP propagadas, isto porque para cada endereço IP de conhecimento é realizado um broadcast nessa sub rede, identificando novos roteadores e transmitindo as informações de custo aos destinos conhecidos.

AODV (Ad hoc On-Demand Distance Vector)

Uma rede ad hoc é usada principalmente em contextos wireless (sem fio), porque não precisa de uma rede de roteadores pré-existentes uma vez que todos os nós instalados com protocolo AODV atuam da mesma forma que roteadores, propagando dados que precisam chegar a outros nós. Tais redes sem fio ad hoc são configuradas dinâmica e automaticamente o que permite que os nós envolvidos se locomovam, perfeito para uma rede móvel sem fio.

O protocolo AODV utiliza quatro mensagens para realizar a comunicação entre nós: RREQ, RREP, RERR e HELLO. São usadas, respectivamente, para requisitar uma rota, responder à requisição de rota, apontar um erro de rota, geralmente causado pela exclusão de um nó e a última serve para notificar os vizinhos de que o nó ainda está online. Além disso, o protocolo AODV utiliza números de sequências atrelados a cada rota existente, eles são armazenados em nós no final de uma rota, servem para auxiliar nós procurando rotas e impede a formação de loops durante o roteamento.

Este protocolo trabalha encontrando caminhos entre nós para fazer a comunicação entre eles à medida que for necessário, então quando um nó precisar descobrir um caminho até outro nó é necessário que o nó inicial mande uma mensagem RREQ em broadcast para todos seus vizinhos. Seus vizinhos, por sua vez, devem retornar uma mensagem de RREP em Unicast, fazendo o caminho reverso de volta até o nó inicial, caso conheçam um caminho para o nó destino. Caso contrário eles devem propagar a mensagem de RREQ para seus vizinhos assim como foi feito com eles até que o nó destino seja encontrado. A mensagem de RERR é enviada por um nó quando uma rota desativada (Flag DOWN) expira, indicando que aquela rota não está mais ativa.

O protocolo AODV começa somente com as interfaces do próprio nó. Para que ele de fato conecte dois nós, encontrando uma rota entre eles, é necessário antes que eles queiram se comunicar, portanto enviamos 10 pacotes de 1024 bytes do roteador 0 até o roteador 7. Nas tabelas abaixo é possível verificar o resultado ao longo do tempo.

Tabela 5 - Tabela de Roteamento AODV do roteador 0 no segundo 0

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372036.85	1
192.168.2.255	192.168.2.255	192.168.2.0	UP	9223372036.85	1
192.168.3.255	192.168.3.255	192.168.3.0	UP	9223372036.85	1
192.168.5.255	192.168.5.255	192.168.5.0	UP	9223372036.85	1
192.168.7.255	192.168.7.255	192.168.7.0	UP	9223372036.85	1

Tabela 6 - Tabela de Roteamento AODV do roteador 7 no segundo 0

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372036.85	1

192.170.0.255	192.170.0.255	192.170.0.1	UP	9223372036.85	1
192.170.1.255	192.170.1.255	192.170.1.0	UP	9223372036.85	1
192.170.4.255	192.170.4.255	192.170.4.0	UP	9223372036.85	1

-3:00:00.000000 IP 192.168.5.0.654 > 192.168.5.255.654: aodv rreq 24 hops 0 id 0x00000001 dst 192.170.0.1 seq 0 src 192.168.5.0 seq 1
-3:00:00.010400 IP 192.168.5.1.654 > 192.168.5.255.654: aodv rrep 20 prefix 0 hops 0 dst 192.168.5.1 dseq 0 src 192.168.5.1 2000 ms

No primeiro momento, somente as interfaces dos nós estão em suas respectivas tabelas de roteamento. A Flag se refere a conectividade da entrada na tabela, UP significa que a conexão é recente enquanto DOWN significa que já passou um tempo desde a última comunicação com aquele IP. Através dos logs gerados pelos arquivos .pcap é possível notar que o roteador 0 enviou a mensagem RREQ pela sua interface 192.168.5.255 e obteve uma resposta RREP logo em seguida do roteador 3 (IP 192.168.5.1) indicando que este sabia o caminho até o roteador 7.

O campo exibido como Expire auxilia a Flag, pois é usado para alterar a Flag das entradas na tabela de acordo com o tempo em que foram atualizadas. Quando uma nova conexão é feita/descoberta ela é inserida na tabela de roteamento com Flag UP e Expire que varia de acordo com a distância e o tempo de descoberta entre os nós em questão. O Expire decresce e chega a 0 caso não haja comunicação com o IP da entrada na tabela dentro do tempo estabelecido no próprio campo, quando isso acontece a Flag muda para DOWN e então Expire começa a contar regressivamente a partir de 15. Se a rota continuar inativa depois que Expire chegue em 0 novamente, então aquela entrada na tabela de roteamento será removida, ou seja, aquela rota será esquecida. Esses 15 segundos de “tolerância” servem para evitar que a rota seja desfeita muito rapidamente e também para auxiliar outros nós que talvez queiram chegar até aquele destino.

Tabela 7 - Tabela de Roteamento AODV do roteador 0 no segundo 1

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372035.85	1
192.168.2.1	192.168.2.1	192.168.2.0	UP	2.11	1
192.168.2.255	192.168.2.255	192.168.2.0	UP	9223372035.85	1
192.168.3.1	192.168.3.1	192.168.3.0	UP	2.07	1
192.168.3.255	192.168.3.255	192.168.3.0	UP	9223372035.85	1
192.168.5.1	192.168.5.1	192.168.5.0	UP	2.01	1
192.168.5.255	192.168.5.255	192.168.5.0	UP	9223372035.85	1
192.168.7.255	192.168.7.255	192.168.7.0	UP	9223372035.85	1

192.170.0.1	192.168.5.1	192.168.5.0	UP	2.06	5

Tabela 8 - Tabela de Roteamento AODV do roteador 7 no segundo 1

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372035.85	1
192.168.2.0	192.170.0.0	192.170.0.1	UP	4.88	6
192.168.3.0	192.170.0.0	192.170.0.1	UP	4.96	6
192.168.5.0	192.170.0.0	192.170.0.1	UP	4.95	5
192.170.0.0	192.170.0.0	192.170.0.1	UP	2.10	1
192.170.0.255	192.170.0.255	192.170.0.1	UP	9223372035.85	1
192.170.1.1	192.170.1.1	192.170.1.0	UP	2.05	1
192.170.1.255	192.170.1.255	192.170.1.0	UP	9223372035.85	1
192.170.4.255	192.170.4.255	192.170.4.0	UP	9223372035.85	1

-3:00:00.680327 IP 192.168.5.0.49153 > 192.170.0.1.discard: UDP, length 1024
-2:-59:-59.000000 IP 192.168.5.0.49153 > 192.170.0.1.discard: UDP, length 1024

No segundo seguinte, todos os vizinhos dos roteadores 0 e 7 já receberam a mensagem HELLO e foram adicionados a tabela de roteamento, ambos roteadores já encontraram um caminho para se alcançarem, que envolve outros 5 roteadores como exibido pelo campo Hops, e portanto seus IPs foram adicionados a suas tabelas de roteamento. Flag UP indicando que a conexão está ativa, pois existem datagramas sendo enviados, e Expire acima de 0. Portanto a comunicação entre os roteadores 0 e 7 já iniciou, como o log acima confirma.

Tabela 9 - Tabela de Roteamento AODV do roteador 0 no segundo 6

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372030.85	1
192.168.2.1	192.168.2.1	192.168.2.0	UP	1.66	1
192.168.2.255	192.168.2.255	192.168.2.0	UP	9223372030.85	1
192.168.3.1	192.168.3.1	192.168.3.0	UP	1.67	1
192.168.3.255	192.168.3.255	192.168.3.0	UP	9223372030.85	1
192.168.5.1	192.168.5.1	192.168.5.0	UP	2.00	1

192.168.5.255	192.168.5.255	192.168.5.0	UP	9223372030.85	1
192.168.7.255	192.168.7.255	192.168.7.0	UP	9223372030.85	1
192.170.0.1	192.168.5.1	192.168.5.0	UP	2.00	5

Tabela 10 - Tabela de Roteamento AODV do roteador 7 no segundo 6

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372030.85	1
192.168.2.0	192.170.0.0	192.170.0.1	DOWN	15.00	6
192.168.3.0	192.170.0.0	192.170.0.1	DOWN	15.00	6
192.168.5.0	192.170.0.0	192.170.0.1	DOWN	15.00	5
192.170.0.0	192.170.0.0	192.170.0.1	UP	1.10	1
192.170.0.255	192.170.0.255	192.170.0.1	UP	9223372030.85	1
192.170.1.1	192.170.1.1	192.170.1.0	UP	1.05	1
192.170.1.255	192.170.1.255	192.170.1.0	UP	9223372030.85	1
192.170.4.255	192.170.4.255	192.170.4.0	UP	9223372030.85	1

-2:-59:-51.000000 IP 192.168.5.0.49153 > 192.170.0.1.discard: UDP, length 1024

É importante dizer que a entrada da tabela do roteador 0, referente ao roteador 7 (IP 192.170.0.1), permaneceu com o valor Expire quase inalterado desde o segundo 1 até o 6 devido ao contínuo uso dessa rota, uma vez que o último dos 10 datagramas foi enviado somente com 9 segundos de simulação. A partir daí, o Expire passou a decair com o passar da simulação e próximo dos 12 segundos o Expire dessa rota chegou a 0 portanto a rota foi marcada como DOWN. Então o Expire começou um timer de 15 segundos, como não houve comunicação alguma entre esses roteadores durante esse período a entrada na tabela foi removida próxima ao segundo 28.

Ainda no segundo 6, a entrada na tabela do roteador 7 sobre os IPs 192.168 atingiu Expire 0 e portanto sua Flag foi atualizada para DOWN pois a rota, partindo do roteador 7, não estava em uso. Expire foi estabelecido como 15 por padrão. Próximo do segundo 21, Expire chegou em 0 novamente e então essas entradas foram retiradas da tabela pois realmente o roteador 7 não havia enviado nenhum datagrama nesta rota.

Aos 30 segundos de simulação todos os datagramas já haviam sido enviados, a rota entre os roteadores 0 e 7 usada nessa comunicação já não existia mais e assim ficaram suas respectivas tabelas de roteamento.

Tabela 11 - Tabela de Roteamento AODV do roteador 0 no segundo 30

Destination	Gateway	Interface	Flag	Expire	Hops

127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372006.85	1
192.168.2.1	192.168.2.1	192.168.2.0	UP	1.66	1
192.168.2.255	192.168.2.255	192.168.2.0	UP	9223372006.85	1
192.168.3.1	192.168.3.1	192.168.3.0	UP	1.66	1
192.168.3.255	192.168.3.255	192.168.3.0	UP	9223372006.85	1
192.168.5.1	192.168.5.1	192.168.5.0	UP	1.67	1
192.168.5.255	192.168.5.255	192.168.5.0	UP	9223372006.85	1
192.168.7.255	192.168.7.255	192.168.7.0	UP	9223372006.85	1

Tabela 12 - Tabela de Roteamento AODV do roteador 7 no segundo 30

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372006.85	1
192.170.0.0	192.170.0.0	192.170.0.1	UP	1.10	1
192.170.0.255	192.170.0.255	192.170.0.1	UP	9223372006.85	1
192.170.1.1	192.170.1.1	192.170.1.0	UP	1.05	1
192.170.1.255	192.170.1.255	192.170.1.0	UP	9223372006.85	1
192.170.4.255	192.170.4.255	192.170.4.0	UP	9223372006.85	1

Cenário 1: Custo do enlace

Mesma rede exibida no tópico 2 porém o custo de alguns enlaces foi aumentado. Pretendemos verificar como os protocolos se adaptam a essa alteração e como isso se reflete nas tabelas de roteamento.

RIP

Um dos princípios para a construção da tabela de roteamento pelo RIP é a métrica estabelecida em um enlace, chamado de custo. O custo no enlace de um computador a outro é considerado por padrão pelo NS-3 como sendo 1, podendo ser alteradas essas métricas. Abaixo seguem algumas das entradas das tabelas de roteamento do roteador 0 e do roteador 4 considerando custo 1 para todos os enlaces.

Tabela 13 - Parte da Tabela de Roteamento do roteador 0 no segundo 40

Destination	Gateway	Metric	Iface
192.170.4.0	192.168.5.1	6	3
192.168.1.0	192.168.2.1	2	1
192.169.0.0	192.168.5.1	3	3
192.170.2.0	192.168.5.1	5	3
192.2.0.0	192.168.5.1	4	3
192.169.2.0	192.168.5.1	4	3
192.1.0.0	192.168.5.1	2	3
192.168.6.0	192.168.3.1	2	2
192.168.0.0	192.168.3.1	2	2

Tabela 14 - Parte da Tabela de Roteamento do roteador 4 no segundo 40

Destination	Gateway	Metric	Iface
192.170.4.0	192.169.0.1	4	1
192.168.1.0	192.1.0.0	2	2
192.169.0.0	0.0.0.0	1	1
192.170.2.0	192.169.0.1	3	1
192.2.0.0	192.169.0.1	2	1
192.169.2.0	192.169.0.1	2	1
192.1.0.0	0.0.0.0	1	2
192.168.6.0	192.1.0.0	3	2

192.168.0.0	192.1.0.0	3	2

Note que um datagrama que sai do roteador 0 com destino ao endereço da subrede 192.170.4/24 consegue chegar no destino com, no mínimo, 6 saltos no Sistema Autônomo. Esse é o menor custo encontrado pelo algoritmo de vetores de distância. Roteadores de meio de caminho equilibram essa quantidade de saltos, como é o caso do roteador 4.

Dependendo da importância do enlace, um aumento em seu custo pode ser crucial para o desempenho do roteamento, como é visto na tabela abaixo, quando aumenta-se o custo em 8 para os pacotes que saem do roteador 4 em direção ao 5.

Tabela 15 - Parte da Tabela de Roteamento do roteador 0 no segundo 40 com aumento de custo igual à 8 no enlace entre os roteadores 4 e 5.

Destination	**Gateway**	**Metric**	**Iface**
192.170.4.0	192.168.5.1	13	3
192.168.1.0	192.168.2.1	2	1
192.169.0.0	192.168.5.1	3	3
192.170.2.0	192.168.5.1	12	3
192.2.0.0	192.168.5.1	11	3
192.169.2.0	192.168.5.1	11	3
192.1.0.0	192.168.5.1	2	3
192.168.6.0	192.168.3.1	2	2
192.168.0.0	192.168.3.1	2	2

Quem se lembrar da topologia da rede irá notar que para o roteador 0 se comunicar com o roteador 7 (que tem ligação direta à sub rede 192.170.4/24) é necessário passar pelo enlace entre os roteadores 4 e 5. Visto que aumentamos o custo desse enlace crítico, não há maneira da tabela de roteamento encontrar um caminho de custo menor que 13 à esse destino, pois é o único possível nessa rede.

Contudo, quando existem alternativas a um enlace, o protocolo vai escolher aquele com menor soma no custo dos enlaces. No exemplo abaixo aumentou-se o custo para 3 tanto nos enlaces entre os roteadores 0 e 2 quanto no enlace entre os roteadores 0 e 3. Assim, o único caminho para outro roteador direto ao 0 com custo 1 é o pelo endereço 192.168.2.0, chegando ao roteador 1.

Tabela 16 - Parte da Tabela de Roteamento do roteador 0 no segundo 40 com aumento de custo igual à 3 nos enlaces entre os roteadores 0 e 2 e nos enlaces entre os roteadores 0 e 3.

Destination	Gateway	Metric	Iface
192.170.4.0	192.168.2.1	7	1
192.168.1.0	192.168.2.1	7	1
192.169.0.0	192.168.2.1	4	1
192.170.2.0	192.168.2.1	6	1
192.2.0.0	192.168.2.1	5	1
192.169.2.0	192.168.2.1	5	1
192.1.0.0	192.168.2.1	3	1
192.168.6.0	192.168.2.1	3	1
192.168.0.0	192.168.2.1	3	1

A comparação entre essa última tabela e a tabela apresentada sem alteração no custo dos enlaces manifesta a utilização do canal entre os roteadores 0 e 1 (interface de rede 1 do roteador, com gateway endereçando para 192.168.2.1) para toda a comunicação entre roteadores da rede, pois ainda que seja necessário mais de um salto entre roteadores, esse salto tem custo 1, sendo mais viável para qualquer comunicação entre roteadores do que ir direto à um roteador com um salto igual à 3.

Por fim, a tabela de roteamento do RIP armazena apenas caminhos à roteadores cujo custo seja menor ou igual à 15, como é evidenciado pela tabela de exemplo abaixo.

Tabela 17 - Parte da Tabela de Roteamento do roteador 0 no segundo 40 com aumento de custo igual à 13 no enlace entre os roteadores 4 e 5

Destination	Gateway	Metric	Iface
192.170.4.0	Não há registro		
192.168.1.0	192.168.2.1	2	1
192.169.0.0	192.168.5.1	3	3
192.170.2.0	Não há registro		
192.2.0.0	Não há registro		
192.169.2.0	Não há registro		
192.1.0.0	192.168.5.1	2	3
192.168.6.0	192.168.3.1	2	2
192.168.0.0	192.168.3.1	2	2

A tabela de roteamento gerada para o roteador 4 considerando esse último cenário não contém as entradas que estão presentes na tabela de exemplo acima, contudo, foram evidenciados aqui para mostrar que, quando à um caminho com custo maior que 15 para um determinado destino não será registrado na tabela de roteamento pelo protocolo RIP.

AODV

O protocolo AODV padrão, utilizado nesse EP, escolhe qual rota tomar primariamente baseando-se no número de saltos necessários para chegar até o nó destino, independentemente de custos, métricas ou estabilidade dessas conexões. Concomitantemente, caso haja duas rotas já existentes para o nó destino com o mesmo número de saltos necessários, o critério de desempate seria então o número de sequência das rotas, tomando a rota com o maior número de sequência, o que indica que esta rota é mais recente.

Existe um artigo, “EM-AODV: Metric Based Enhancement to AODV Routing Protocol” publicado em 2006 no IEEE Xplore, que sugere a adoção de um sistema de métrica ao protocolo AODV, o que garantiria mais estabilidade nas conexões wireless realizadas.

O helper da classe do protocolo AODV da ferramenta NS-3 não permite alterar a métrica dos enlaces entre nós com tal protocolo. Levando isso em consideração, é impraticável alterar custos de links entre roteadores com o protocolo AODV, não somente por causa do NS-3, mas também porque este protocolo somente cria rotas quando necessário e somente as mantém enquanto estiverem ativas. Então não faz sentido adicionar pesos nos enlaces uma vez que, independentemente do possível custo de um link, se o menor caminho até o nó destino envolvê-lo, esta será a rota adotada.

Conclusão

O protocolo RIP se ajustou de forma louvável às alterações realizadas nos enlaces de sua topologia, conseguindo alternar, quando possível, o caminho adotado em suas tabelas de roteamento para obter a rota mais “barata” até o destino.

Já o protocolo AODV não altera suas rotas baseando-se em custos de enlaces mas sim de acordo com a distância de saltos total, portanto suas tabelas de roteamento não seriam afetadas pelas mudanças previstas neste cenário.

Cenário 2: Queda de link

Mesma rede dos cenários anteriores porém o link entre o roteador 0 e o roteador 1 deve cair aos 25 segundos de simulação. Pretendemos verificar as mudanças nas tabelas de roteamento dos roteadores quando um link é eliminado durante a simulação.

RIP

Sempre existe a possibilidade de um endpoint, por algum motivo, perder a conexão com o resto da rede. Isso é um potencial problema para os outros roteadores da rede, pois poderiam estar considerando esse enlace caído nas suas tabelas de roteamento, consequentemente, havendo uma inconsistência na rede que aumentará a perda de pacotes por tempo indeterminado. Para evitar esse problema o protocolo de roteamento RIP utiliza nessa simulação a técnica de retorno envenenado no seu algoritmo de vetores de distâncias. Ao reconhecer um caminho inacessível, o roteador propaga essa informação, informando que o custo de tal enlace é infinito (maior que 15), não sendo, portanto, utilizado para cálculo do menor caminho à um enlace. Contudo, isso sozinho não vai mudar o custo para um endereço na tabela de roteamento dos roteadores no caminho, sendo necessário a reversão envenenada para impedir um loop infinito. Essa técnica estabelece, basicamente, que enquanto o custo de um enlace depender de outro nó da rede, esse custo será propagado como infinito (logo, não será utilizado nas tabelas de roteamento, envenenando o caminho). Com isso o roteador pode identificar se há algum problema no enlace e propagá-lo, assim como evitar receber anúncios com custos de enlaces sem uma garantia mínima de integridade.

As tabelas abaixo demonstram como uma queda no link aos 25 segundos entre os roteadores 0 e 1 é refletida nas tabelas de roteamento considerando apenas os destinos afetados, isto é, os que consideram na tabela de roteamento a interface que conecta os dois pontos da rede, no caso, a interface de rede 1 para ambos roteadores:

Tabela 18 - Roteador 0 no segundo 25

Destination	**Gateway**	**Metric**	**Iface**
192.168.8.0	192.168.2.1	2	1
192.168.1.0	192.168.2.1	2	1
192.168.2.0	0.0.0.0	1	1

Tabela 19 - Roteador 1 no segundo 25

Destination	**Gateway**	**Metric**	**Iface**
192.168.7.0	192.168.2.0	2	1
192.168.5.0	192.168.2.0	2	1
192.168.3.0	192.168.2.0	1	1
192.168.2.0	0.0.0.0	1	1

Após 1 milisegundo da queda do link (segundo 25) até cerca de 20 segundos depois a simulação não mantém nenhum caminho até os destinos que antes utilizavam esse link que caiu.

Tabela 20 - Roteador 0 no segundo 50

Destination	Gateway	Metric	Iface
192.168.8.0	192.168.5.1	3	3
192.168.1.0	192.168.5.1	2	3

Tabela 21 - Roteador 1 no segundo 50

Destination	Gateway	Metric	Iface
192.168.7.0	192.168.1.1	3	3
192.168.5.0	192.168.1.1	2	3
192.168.3.0	192.168.4.1	2	2

Pela análise das tabelas depreende-se que a queda do sinal é perceptível rapidamente pelo RIP (em 1ms já havia notado o problema), contudo teve um tempo relevante para reformulação de sua tabela, dependendo da recepção dos anúncios RIP de roteadores vizinhos para identificar a nova melhor rota ao seu destino inacessível por alguns segundos. A utilização do retorno envenenado ainda assim é importante, pois impede que as informações de acesso ao enlace indisponível sejam propagadas.

AODV

Para que este protocolo de fato conecte dois nós, encontrando uma rota entre eles, é necessário antes que eles queiram se comunicar, portanto enviamos 10 pacotes de 1024 bytes do roteador 0 até o roteador 1 a partir do segundo 20, para verificarmos as mudanças quando o enlace entre eles cair.

Tabela 22 - Roteador 0 no segundo 20

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372016.85	1
192.168.2.1	192.168.2.1	192.168.2.0	UP	1.10	1
192.168.2.255	192.168.2.255	192.168.2.0	UP	9223372016.85	1
192.168.3.1	192.168.3.1	192.168.3.0	UP	1.07	1
192.168.3.255	192.168.3.255	192.168.3.0	UP	9223372016.85	1
192.168.5.1	192.168.5.1	192.168.5.0	UP	1.02	1

192.168.5.255	192.168.5.255	192.168.5.0	UP	9223372016.85	1
192.168.7.255	192.168.7.255	192.168.7.0	UP	9223372016.85	1

Tabela 23 - Roteador 1 no segundo 20

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372016.85	1
192.168.1.1	192.168.1.1	192.168.1.0	UP	1.10	1
192.168.1.255	192.168.1.255	192.168.1.0	UP	9223372016.85	1
192.168.2.0	192.168.2.0	192.168.2.1	UP	1.09	1
192.168.2.255	192.168.2.255	192.168.2.1	UP	9223372016.85	1
192.168.4.1	192.168.4.1	192.168.4.0	UP	1.08	1
192.168.4.255	192.168.4.255	192.168.4.0	UP	9223372016.85	1
192.168.8.255	192.168.8.255	192.168.8.0	UP	9223372016.85	1

-2:-59:-40.000000 IP 192.168.2.0.49153 > 192.168.2.1.discard: UDP, length 1024

No segundo 20, o roteador 0 começou a enviar os datagramas para o roteador 1, como o log acima afirma, e todos seus vizinhos aparecem em suas respectivas tabelas de roteamento.

Tabela 24 - Roteador 0 no segundo 25 (pós queda do link)

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372011.85	1
192.168.2.1	102.102.102.102	102.102.102.102	IN_SEARCH	5.60	1
192.168.2.255	192.168.2.255	192.168.2.0	UP	9223372016.85	1
192.168.3.1	192.168.3.1	192.168.3.0	UP	1.07	1
192.168.5.1	192.168.5.1	192.168.5.0	UP	1.02	1
192.168.5.255	192.168.5.255	192.168.5.0	UP	9223372011.85	1
192.168.7.255	192.168.7.255	192.168.7.0	UP	9223372011.85	1

Tabela 25 - Roteador 1 no segundo 25 (pós queda do link)

Destination	Gateway	Interface	Flag	Expire	Hops

127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372011.85	1
192.168.1.1	192.168.1.1	192.168.1.0	UP	1.01	1
192.168.1.255	192.168.1.255	192.168.1.0	UP	9223372011.85	1
192.168.4.1	192.168.4.1	192.168.4.0	UP	1.07	1
192.168.4.255	192.168.4.255	192.168.4.0	UP	9223372011.85	1
192.168.8.255	192.168.8.255	192.168.8.0	UP	9223372011.85	1

-2:-59:-36.000000 IP 192.168.2.0.49153 > 192.168.2.1.discard: UDP, length 1024

Após a queda do link entre os roteadores 0 e 1 (192.168.2.0 -> 192.168.2.1) no segundo 25, a tabela do roteador 0, que não tinha acabado de enviar todos os datagramas, portanto mantinha a rota ativa, continuou buscando pelo IP 192.168.2.1 referente ao nó 1 pois esse é o endereço dos datagramas a serem enviados, enquanto que a tabela do roteador 1 foi atualizada praticamente de forma instantânea ao remover todos as entradas relacionadas com IPs 192.168.2.. Isso se deve ao fato de que quando a conexão foi interrompida, o roteador 1 não recebeu resposta para a mensagem HELLO enviada ao roteador 0 indicando que algo aconteceu com este roteador, portanto suas entradas foram retiradas de sua tabela.

Tabela 26 - Roteador 1 no segundo 26

Destination	**Gateway**	**Interface**	**Flag**	**Expire**	**Hops**
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372010.85	1
192.168.1.1	192.168.1.1	192.168.1.0	UP	2.66	1
192.168.1.255	192.168.1.255	192.168.1.0	UP	9223372010.85	1
192.168.3.0	192.168.4.1	192.168.4.0	UP	5.10	2
192.168.4.1	192.168.4.1	192.168.4.0	UP	2.67	1
192.168.4.255	192.168.4.255	192.168.4.0	UP	9223372010.85	1
192.168.5.0	192.168.1.1	192.168.1.0	UP	5.10	2
192.168.8.255	192.168.8.255	192.168.8.0	UP	9223372010.85	1

No segundo seguinte à queda do enlace, a tabela do roteador 0 permaneceu do mesmo jeito, com a Flag IN_SEARCH ativa enquanto ainda restava tempo no Expire. Depois que o tempo de Expire acabou, por volta do segundo 36, a entrada da tabela foi diretamente removida, sem antes definir a Flag como DOWN e resetar o Expire.

Já o roteador 1, numa tentativa de retomar a conexão perdida, encontrou e atualizou sua tabela com duas novas entradas referentes ao próprio roteador 0 (192.168.3.0 e

192.168.5.0). Porém, como não houve nenhuma comunicação além dessa primeira conexão, já que o roteador 1 não tinha nenhum datagrama para enviar, assim que o tempo de Expire se esgotou a Flag foi alterada para Down e após mais 15 segundos a entrada da tabela seria removida se o tempo da simulação não tivesse acabado.

No final das contas, o roteador 0, responsável por enviar os datagramas, não conseguiu restabelecer conexão com o roteador 1 através de outros enlaces. Porém, o roteador 1 conseguiu estabelecer novas conexões com o roteador 0, mostrando que também é capaz de superar quedas de links.

Conclusão

Ambos os protocolos conseguem lidar bem e detectar rapidamente quedas de enlace entre nós. A tabela RIP é atualizada com uma certa lentidão, talvez seja o preço de encontrar o menor caminho possível, enquanto a tabela de roteamento AODV retira quaisquer rotas inválidas num piscar de olhos porém também leva um certo tempo (bem menos do que o RIP) até conseguir traçar uma nova entrada.

Cenário 3: Broadcast

Neste cenário substituímos a rede P2P por uma rede broadcast seguindo a mesma topologia e pretendemos analisar as consequências sobre os roteadores.

RIP

Visto que os anúncios RIP são feitos para destinos vizinhos com certa frequência e que devem ter um feedback rápido, canais broadcast parecem ser interessantes para tal. A necessidade de entrega de mensagens constante, contudo, acaba causando um delay maior na entrega de cada mensagem RIP na sequência quando comparado aos canais dedicados e, portanto, afetando o tempo de recebimento e envio, como pode ser visto nos fragmentos de tabelas de roteamento do roteador 0 abaixo (primeiras 4 entradas da tabela de roteamento):

Tabela 27 - Roteador 0 no segundo 5 (broadcast)

Destination	Gateway	Metric	Iface
192.169.2.0	192.168.5.1	4	3
192.2.0.0	192.168.5.1	4	3
192.170.0.0	192.168.5.1	5	3
192.170.2.0	192.168.5.1	5	3

Tabela 28 - Roteador 0 no segundo 20 (broadcast)

Destination	Gateway	Metric	Iface
192.170.4.0	192.168.5.1	6	3
192.170.1.0	192.168.5.1	6	3
192.170.3.0	192.168.5.1	6	3
192.169.2.0	192.168.5.1	4	3

Ainda que o CSMA tenha vantagens em detecção e controle de colisões, a reestruturação do canal causou um aumento no custo de alguns enlaces e uma certa demora para encontrar destinatários quando comparado à conexão ponto a ponto. Ao voltar à tabela 1, já haviam sido identificados 17 destinos possíveis no Sistema Autônomo pelo roteador 0 em 5 segundos, assim como na rede broadcast. Os custos foram os mesmos também. Aos 20 segundos, as tabelas de roteamento por P2P estavam iguais às de broadcast. Assim, a eficiência do canal CSMA para realizar a comunicação em broadcast nessa rede permitiu a mesma eficácia que uma comunicação ponto a ponto.

AODV

Os nós imbuídos com protocolo AODV constantemente enviam mensagens HELLO para seus nós vizinhos, logo, em uma rede broadcast, a velocidade de obtenção de resultados na tabela deve ser afetada.

Tabela 29 - Tabela de Roteamento AODV (broadcast) do roteador 0 no segundo 1

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372035.85	1
192.168.2.1	192.168.2.1	192.168.2.0	UP	2.09	1
192.168.2.255	192.168.2.255	192.168.2.0	UP	9223372035.85	1
192.168.3.1	192.168.3.1	192.168.3.0	UP	2.06	1
192.168.3.255	192.168.3.255	192.168.3.0	UP	9223372035.85	1
192.168.5.1	192.168.5.1	192.168.5.0	UP	2.07	1
192.168.5.255	192.168.5.255	192.168.5.0	UP	9223372035.85	1
192.168.7.255	192.168.7.255	192.168.7.0	UP	9223372035.85	1
192.170.0.1	192.168.5.1	192.168.5.0	UP	2.05	5

Porém, comparando a tabela acima com a tabela 7 (Tabela de Roteamento AODV do roteador 0 no segundo 1) nota-se poucas diferenças, em ambas as redes no segundo 1 de simulação já haviam encontrado uma rota para comunicação, apenas algumas variações esperadas no campo Expire já que ele depende da comunicação na rota.

Tabela 30 - Tabela de Roteamento AODV (broadcast) do roteador 0 no segundo 30

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223372006.85	1
192.168.2.1	192.168.2.1	192.168.2.0	UP	1.67	1
192.168.2.255	192.168.2.255	192.168.2.0	UP	9223372006.85	1
192.168.3.1	192.168.3.1	192.168.3.0	UP	1.66	1
192.168.3.255	192.168.3.255	192.168.3.0	UP	9223372006.85	1
192.168.5.1	192.168.5.1	192.168.5.0	UP	1.66	1
192.168.5.255	192.168.5.255	192.168.5.0	UP	9223372006.85	1
192.168.7.255	192.168.7.255	192.168.7.0	UP	9223372006.85	1

Após 30 segundos de simulação na rede broadcast o resultado obtido é incrivelmente semelhante à implementação na rede P2P. A rede csma não trouxe vantagens, porém também não trouxe desvantagens para o protocolo AODV.

Conclusão

Podemos concluir que para uma rede com uma quantidade pequena de nós praticamente não existe diferença de uso entre as redes P2P e broadcast já que em ambos os protocolos não sofreram alterações significativas no tempo de montagem de suas tabelas de roteamento.

Cenário 4: Protocolos diferentes em dois Sistemas Autônomos

Para este cenário a rede exibida no tópico 2 foi dividida da seguinte maneira: os roteadores de 0 até 5 foram atrelados ao protocolo RIP enquanto os roteadores de 6 até 8 ficaram com o protocolo AODV. Tentamos enviar 10 datagramas do roteador 6 (AODV) para o roteador 5 (RIP). Pretendemos analisar como essa mudança influenciará as tabelas de roteamento e a comunicação entre os roteadores.

Como os roteadores atuam com protocolos diferentes, uma mensagem originária de outro protocolo que chega a um roteador de borda do AS não reconhece o que deve ser feito com a mensagem e, consequentemente, não trata a mensagem como o protocolo esperado para a mensagem deveria atuar. Vale lembrar que não é possível estabelecer dois protocolos de roteamento em um roteador.

Contudo, roteadores que se comunicavam com o mesmo protocolo dentro de um AS conseguem definir suas tabelas de roteamento conforme o esperado, evidenciado pelas tabelas abaixo:

Tabela 31 - Roteador 5 (RIP) no segundo 60

Destination	Gateway	Metric	Iface
192.169.1.0	192.169.0.0	2	1
192.1.0.0	192.169.0.0	2	1
192.168.8.0	192.169.0.0	4	1
192.168.6.0	192.169.0.0	4	1
192.168.4.0	192.169.0.0	4	1
192.168.7.0	192.169.0.0	4	1
192.168.3.0	192.169.0.0	4	1
192.168.2.0	192.169.0.0	4	1
192.168.5.0	192.169.0.0	3	1
192.168.0.0	192.169.0.0	3	1
192.168.1.0	192.169.0.0	3	1
192.169.0.0	0.0.0.0	1	1
192.2.0.0	0.0.0.0	1	2
192.169.2.0	0.0.0.0	1	3

Tabela 32 - Roteador 6 (AODV) no segundo 60

Destination	Gateway	Interface	Flag	Expire	Hops
127.0.0.1	127.0.0.1	127.0.0.1	UP	9223371976.85	1
192.2.0.255	192.2.0.255	192.2.0.1	UP	9223371976.85	1
192.170.0.1	192.170.0.1	192.170.0.0	UP	1.75	1
192.170.0.255	192.170.0.255	192.170.0.0	UP	9223371976.85	1
192.170.2.1	192.170.2.1	192.170.2.0	UP	1.75	1
192.170.2.255	192.170.2.255	192.170.2.0	UP	9223371976.85	1
192.170.5.255	192.170.5.255	192.170.5.0	UP	9223371976.85	1

Sobre as mensagens enviadas à roteadores com outros protocolos, o log abaixo indica os cabeçalhos das requisições que um roteador com protocolo RIP (no caso o roteador 5) realizou para se comunicar com uma rede que utiliza o protocolo AODV, sendo descartada essa mensagem.

-3:00:00.482961 IP 192.2.0.0.route > 224.0.0.9.route: RIPv2, Request, length: 24
-2:-59:-24.064621 IP 192.2.0.0.route > 224.0.0.9.route: RIPv2, Response, length: 44
-2:-59:-22.125647 IP 192.2.0.0.route > 224.0.0.9.route: RIPv2, Response, length: 224

Os roteadores seguem o fluxo de seu protocolo de roteamento, independente de receber ou não as respostas de suas mensagens:

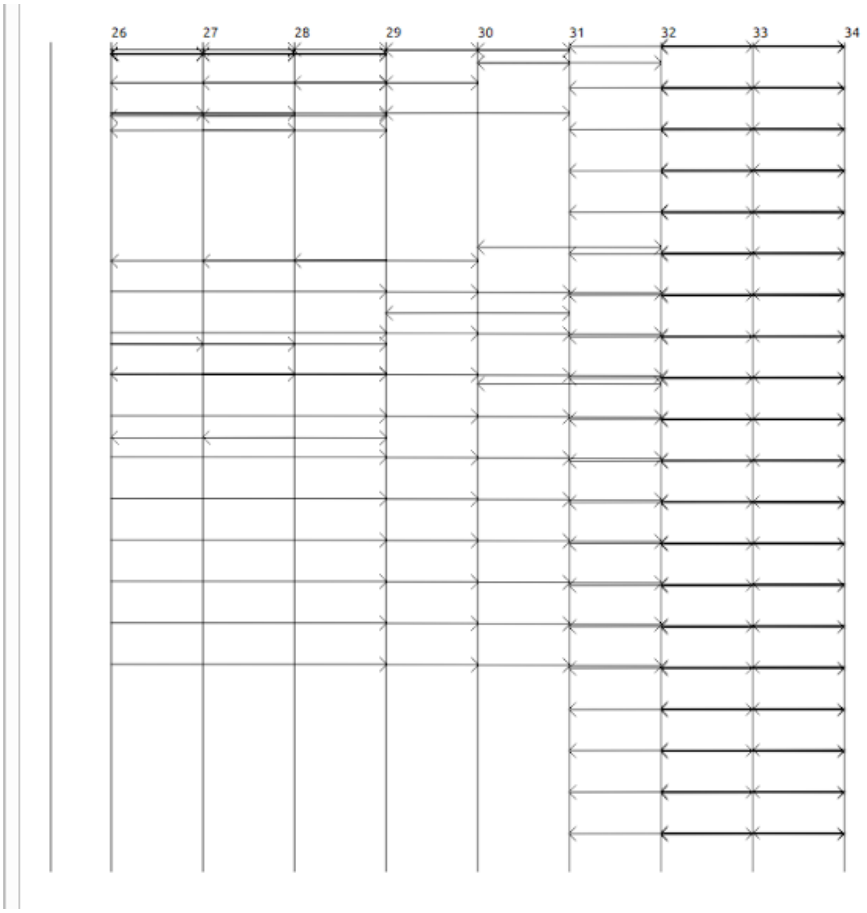

Figura 4 - Comunicação entre os roteadores da rede. O ó 26 é o roteador 0, indo até o roteador 8 representado pelo nó 34

A figura acima mostra o constante tráfego de datagramas na rede comunicação via AODV, e os anúncios RIP em intervalos de aproximadamente 30 segundos para identificar mudanças nos custos dos enlaces, demonstrando a continuidade do roteamento independente do desconhecimento da outra rede.

Conclusão

Devido a diferentes protocolos de roteamento, os roteadores 5 e 6 não conseguem trocar informações entre si causando, portanto, uma lacuna na tabela de roteamento dos roteadores o que impede que um datagrama enviado por um host de roteador RIP chegue até outro host dentro de uma AS que utiliza protocolo AODV. Protocolos inter-AS são importantes para suprir esse problema, sendo que conseguem gerenciar as mensagens vindas de outros sistemas autônomos de uma maneira eficiente, ao invés de deixar a responsabilidade pelo gerenciamento de um enlace unicamente.

Considerações finais

Cada protocolo possui contextos em que se dão melhor. Dentre circunstâncias móveis, onde a posição de hosts está sempre mudando, o fato do RIP ficar constantemente recalculando o melhor caminho faz com que não seja a melhor opção comparado ao AODV que ganha velocidade a custo de ser relativamente mais instável. Felizmente, quando se trata de falhas e quebras de links, AODV consegue se recuperar rapidamente com sua manutenção de rotas em relação ao protocolo RIP, que também acaba sendo um pouco lento nesse quesito. Em relação a broadcast, ambos protocolos tiveram desempenho semelhante na construção de tabelas de roteamento comparado à topologia construída com canais ponto a ponto. Pelos testes, vemos que os dois protocolos não são compatíveis um com ou outro, o que pode forçar desenvolvedores de redes a escolher logo no começo qual deles irá seguir pelo resto do projeto.

Conclui-se que AODV é um protocolo de bom desempenho, pelo seu feedback das mudanças na rede rapidamente, conseguindo suportar instabilidades no sinal (por isso é voltado à redes sem fio). O protocolo RIP preza por uma verificação periódica quando não há mudanças nos estados do link de seus vizinhos, visando manter uma tabela de roteamento confiável, mas sem sobrecarregar a rede de anúncios RIP. Cada protocolo tem um foco diferente que deve ser considerado na construção da rede, não havendo um com desempenho melhor que o outro.

6 - Observações

Nos apoiamos sobre os exemplos fornecidos pela ferramenta ns-3 principalmente para estudo sobre a própria ferramenta e em todas as referências citadas abaixo para inclusão dos protocolos de roteamento sobre a topologia.

As simulações levam podem variar de duração de acordo com o computador e a versão do NS-3 utilizado.

7- Referências

KUROSE, J. F.; ROSS, K. W (2014). **Redes de Computadores e a Internet, Uma abordagem top-down**". 6ª edição.

KUROSE, J. F.; ROSS, K. W (2000). **Routing in the Internet**. Disponível em: <http://www2.ic.uff.br/~michael/kr1999/4-network/4_05-routinet.htm>. Acesso em: 23/12/2020.

MALKING, G. (1998). **RFC 2453: RIP Version 2**. Disponível em: <https://datatracker.ietf.org/doc/rfc2453>. Acesso em: 23/12/2020.

MALKIN, G; MINNEAR R (1997). **RFC 2080: RIPng for IPv6**. Disponível em: <https://tools.ietf.org/html/rfc2080>. Acesso em: 23/12/2020.

MUSUVATHI, M (2002). **Description of the AODV Protocol.** Disponível em: <https://www.usenix.org/legacy/publications/library/proceedings/osdi02/tech/full_papers/musuvathi/musuvathi_html/node12.html>. Acesso em: 23/12/2020.

NETAPP, Inc (2010). **Routing table flags**. Disponível em: <https://library.netapp.com/ecmdocs/ECMM1278401/html/nag/GUID-07F1F043-7AB7-4749-8F8D-727929233E62.html>. Acesso em: 23/12/2020.

NICHOLS, K. et al. (1998). **RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers**. Disponível em: <https://tools.ietf.org/html/rfc2474>. Acesso em: 23/12/2020.

NSAM (2020). **Building Topologies**. Disponível em: <https://www.nsnam.org/doxygen/dynamic-global-routing_8cc_source.html>. Acesso em: 23/12/2020.

NSAM (2020). **dynamic-global-routing.cc**. Disponível em: <https://www.nsnam.org/docs/tutorial/html/building-topologies.html>. Acesso em: 23/12/2020.

NSAM (2020). **ns3::Ipv4AddressHelper Class Reference**. Disponível em: <https://www.nsnam.org/doxygen/classns3_1_1_ipv4_address_helper.html>. Acesso em: 23/12/2020.

NSAM (2020). **ns3::UdpClientHelper Class Reference.**. Disponível em: <https://www.nsnam.org/doxygen/dynamic-global-routing_8cc_source.html>. Acesso em: 23/12/2020.

NSAM (2016). **rip-simple-network.cc**. Disponível em: <https://www.nsnam.org/doxygen/rip-simple-network_8cc_source.html>. Acesso em: 23/12/2020.

NSAM (2009). **Unicast-routing**. Disponível em: <https://www.nsnam.org/docs/release/3.6/manual/manual_95.html#Unicast-routing>. Acesso em: 23/12/2020.

PERKINS, C., BELDING-ROYER, E., DAS. S. (2003). **RFC 3561: Ad hoc On-Demand Distance Vector (AODV) Routing**. Disponível em: <https://www.ietf.org/rfc/rfc3561.txt>. Acesso em: 23/12/2020.

RAMAKRISHNAN, K., FLOYD, S., BLACK, D (2001). **RFC 3168: The Addition of Explicit Congestion Notification (ECN) to IP**. Disponível em: <https://tools.ietf.org/html/rfc3168>. Acesso em: 23/12/2020.

ROCHA, C. G. da (2012). **RIP – Routing Information Protocol**. Instituto Federal de Educação, Ciência e Tecnologia, Rio Grande do Norte, [s.d.]. Disponível em:

<http://diatinf.ifrn.edu.br/prof/lib/exe/fetch.php?media=user:1379492:roteamento_internet:3-rip.pdf>. Acesso em: 23/12/2020.

Thanthry, N., Kaki, S. R., Pendse, **R.EM-AODV: Metric based enhancement to AODV routing protocol**. Proceedings of the IEEE 64th Vehicular Technology Conference (VTC '06 Fall)September 2006259425982-s2.0-3454884334110.1109/VTCF.2006.534

WIJEKOON, J. et al (2015). **Introducing a Distance Vector Routing Protocol for ns-3 Simulator.** SIMUTOOLS 2015, August 24-26, Athens, Greece. Disponível em: <https://eudl.eu/pdf/10.4108/eai.24-8-2015.2260345>. Acesso em: 23/12/2020.