

ENCAMINHAMENTO

Algoritmos:

– **Inundação:** cada pacote é enviado para todos os nós da rede, exceto para o nó de origem. Os nós vizinhos repassam o pacote para seus próprios vizinhos, e assim por diante, até que todos os nós da rede tenham recebido o pacote. É um método simples, porém ineficiente, pois cria um tráfego desnecessário na rede.

-**Ponto forte:** Simplicidade de implementação.

-**Ponto fraco:** Causa tráfego desnecessário na rede.

– **Link State:** cada nó da rede coleta informações sobre a topologia completa da rede e calcula o menor caminho para todos os outros nós usando essas informações. Cada nó compartilha seu estado de link com os outros nós, e todos os nós usam essas informações para calcular suas próprias tabelas de roteamento. Esse algoritmo é mais complexo do que a inundação, mas geralmente resulta em um roteamento mais eficiente.

-**Ponto forte:** Permite encontrar caminhos mais eficientes na rede.

-**Ponto fraco:** Requer mais processamento e recursos de memória devido à coleta e troca de informações completas da topologia da rede.

– **Bellman-Ford:** Cada nó mantém uma tabela de distâncias que registra o custo para alcançar cada destino possível na rede. Os nós trocam suas tabelas com os nós vizinhos e, em cada iteração, atualizam suas tabelas de acordo com as informações recebidas. O algoritmo continua iterando até que todas as tabelas de roteamento estejam estáveis. O Bellman-Ford lida com redes nas quais os custos das arestas podem variar e permite que os nós encontrem o caminho mais curto para um destino, mesmo em redes complexas.

Ponto forte: Lida com custos variáveis de arestas e permite encontrar caminhos mais curtos em redes complexas.

Ponto fraco: Pode levar a convergência lenta em grandes redes ou em cenários com múltiplos caminhos de mesmo custo.

– **Shortest Path Routing:** encontra o caminho mais curto entre um nó de origem e um nó de destino em uma rede utilizando informações sobre os custos das conexões entre os nós para determinar a rota com menor custo.

Ponto forte: Encontra o caminho mais curto entre um nó de origem e um nó de destino.

Ponto fraco: Pode não ser eficiente em redes com topologias dinâmicas, onde os custos das arestas podem mudar frequentemente.

– O encaminhamento por **inundação** é mais eficiente do que o shortest path routing quando há grandes taxas de perda de pacotes e variação de latência, a inundação aumenta a chance de o pacote passar por pelo menos um caminho que o leve ao destino.

PROTOCOLOS

– **DHCP** - Fornece dinamicamente endereços IP a computadores que se ligam à rede, e também fornece parâmetros de configuração (proposed IP address, mask, default router address, DNS server, etc).

– **ICMP** é um protocolo utilizado para relatar erros e mensagens de controle em redes IP. Quando ocorre um erro no tratamento de um pacote IP, a definição do protocolo IP admite que um computador ou um computador possam pura e simplesmente descartar o pacote. Exemplos: – TTL demasiado curto – Incapacidade de encaminhar o pacote por ausência de entrada na tabela de encaminhamento – Sistema desconhecido na sub-net de destino (não há resposta ao ARP) – Porta desconhecida ou inativa no destino final.

– **ARP:** mapeia endereços IP em endereços MAC em uma rede local (cada nó tem uma tabela IP-MAC). Quando um dispositivo precisa enviar um pacote para um endereço IP específico na rede, ele envia uma solicitação ARP para descobrir o endereço MAC correspondente. Essa solicitação é enviada em broadcast para todos os dispositivos na rede. O dispositivo com o endereço IP solicitado responde com seu endereço MAC. Se o endereço não estiver na tabela, faz a pergunta em broadcast “quem tem o endereço IP (x)” e consoante a resposta, dá update na tabela IP - MAC). O protocolo ARP é necessário para que os dispositivos em uma rede local possam se comunicar usando endereços MAC

– **NAT:** Um dispositivo NAT possui um endereço IP público atribuído pela Internet. Quando um dispositivo na rede local (com endereço IP privado) envia um pacote para a Internet, o dispositivo NAT substitui o endereço IP privado pelo seu próprio endereço IP público. O dispositivo NAT mantém uma tabela de tradução, que mapeia os endereços IP privados internos para os endereços IP públicos externos correspondentes. Quando um pacote de resposta é recebido, o dispositivo NAT consulta a tabela de tradução para identificar o dispositivo interno ao qual a resposta deve ser encaminhada. Os utilizadores internos vão todos aparecer na Internet como tendo sempre um só endereço IP origem, que partilham. Os endereços internos são privados, isto é, desconhecidos no exterior. Os computadores da rede local não podem ser endereçados do exterior — bom para proteção, mau para certas aplicações. Contudo, continua a permitir as ligações de aplicações **P2P** por **PORT FORWARDING**.

– **TCP:** O TCP estabelece uma conexão confiável entre dispositivos por meio de um handshake de três vias. Ele divide os dados em segmentos numerados, controla o fluxo para evitar congestionamentos, detecta e recupera erros por meio de verificações de soma e retransmissão se necessário. O TCP reordena os segmentos corretamente no destino e encerra a conexão de forma ordenada por meio de um handshake de quatro vias. Os computadores da rede local não podem ser endereçados do exterior — bom para proteção, mau para certas aplicações.

Ideias Base de ARP e DHCP:

•Broadcasting: “quando tiver dúvidas pergunte a todos” - o broadcasting substitui uma diretoria – Enviar por broadcast para todos os computadores da rede local – ... mas só quando não se sabe já o que se pretende.

•Caching: “guarde o que aprendeu por algum tempo” – Guardar o que se aprendeu para não repetir o processo – Lembrar o endereço e informação sobre os outros computadores (IP address + ARP cache).

•Soft state: ... “mas mais tarde ou mais cedo esquecer o passado (... e perguntar de novo) pois a informação pudesse ir desatualizando com o tempo” – Associar um time-to-live (TTL) à informação cached – ... refrescar ou suprimir a informação – fundamental “para se adaptar” a modificações inesperadas

– **TTL:** time to live. Ajuda a diminuir a saturação, mas não é um algoritmo de segurança da sua prevenção.

– 2 formas de obter o endereço ip de um host através do seu mac address: tabela de endereçamento do protocolo **ARP** ou O servidor DHCP mantém um registro dos endereços IP atribuídos aos dispositivos, juntamente com seus endereços MAC correspondentes.

- Geralmente, as entradas na tabela **DHCP** têm um TTL menor do que as entradas na tabela **ARP**, pois o DHCP é projetado para atribuir endereços IP de forma dinâmica e em períodos limitados, enquanto o mapeamento ARP é mais estático e pode ser mantido por períodos mais longos.(mas não necessariamente).
- O **TTL** (Time-to-Live) da tabela **ARP** (Address Resolution Protocol) é especialmente útil em situações em que os mapeamentos de endereços IP e MAC podem mudar com o tempo ou quando há mudanças na rede.
- (explique como, através do nat, é possível que a porta 8000 no host 192.168.1.2 fique disponível para toda a internet através do url <https://172.217.17.14:443/>) - - - Através do NAT, é possível disponibilizar a porta 8000 do host 192.168.1.2 para a internet. Isso é feito configurando um redirecionamento de porta no roteador ou dispositivo NAT, direcionando todas as solicitações recebidas na porta 443 do endereço IP público (172.217.17.14) para a porta 8000 do host interno. Isso permite que o host seja acessado pela internet através do URL <https://172.217.17.14:443>.
- **A ceninha da Google:** O protocolo NAT encaminhará o pacote a ser enviado para o gateway 192.168.3.254, através da interface eth5, que depois vai ser encaminhado para os servidores do Google pela internet. A resposta ao pedido seguirá o caminho inverso, chegando ao mesmo gateway e interface e sendo reencaminhado pelo NAT de novo ao dispositivo de origem do pedido.
- O principal sintoma de Redes Saturadas é a perda de pacotes. É normal ocorrer reenvio de pacotes e ACKs duplicados triplos.
- Hierarquia dos endereços **IP** é fundamental para escalabilidade de encaminhamento na Internet, fornecendo uma estrutura organizada que ajuda a otimizar o roteamento, gerenciamento e utilização dos endereços IP na Internet, além de ajudar a lidar com a escassez de endereços IPv4 disponíveis Coisas boas: reduz tamanho de tabelas | não obriga toda a gente a conhecer todos os outros | reduz o número de mudanças necessárias ao sistema quando algo muda ou quando metes o dedo no cu.
- Não ter gateway registrada significa que o encaminhamento é direto.
- **SLOW START:** Solução do TCP para evitar saturação .Arrancar devagar (slow start) – Inicialmente $\text{congWnd} = 1 \text{ MSS}$ – Logo, inicialmente o ritmo é $1 \text{ MSS} / \text{RTT}$ – por exemplo: $8000 \text{ bits} / 20 \text{ ms} = 400 \text{ Kbps}$ • Por cada ACK recebido aumentar congWnd de 1 MSS – A subida do ritmo de emissão passa a ser exponencial • Isto é, slow start is in fact fast start • Ao invés de slow-start, esta solução deveria chamar-se antes Multiplicative Increase Start.

