Perguntas Frequentes

Routing

Routing para redes pequenas e médias

Redes pequenas e médias não requerem grandes necessidades de performance e escalabilidade, pelo que a melhor estratégia é utilizar protocolos IGP de complexidade baixa para facilitar o processo de configuração: RIP / IGRP e HELLO.

RIP é um protocolo IGP standard da IETF e o mais antigo protocolo de routing IP. É baseado na arquitetura distance-vector para partilha de informação entre os routers na rede. Nesta arquitetura, os routers enviam periodicamente as suas tabelas routing completas para todos os routers na rede, de modo a transmitirem a informação e permitirem a construção das tabelas de routing atualizadas. Tem um grande tempo de convergência devido à periodicidade destes envios. As sua métrica para decidir a melhor rota é o Hop Count, limitado a 15 Hops, relacionado com o problema de contar até ao infinito, onde dois routers apontam para si próprios a melhor rota. O seu melhor atributo é a simplicidade de configuração e funcionamento.

A iteração v2 veio trazer suporte para VLSM, assim como multicast e mais métricas.

O IGRP é um protocolo até há pouco tempo proprietário da CISCO. Desse modo, não tem uma presença extensa noutros sistemas. É também baseado em Distance-vector, com um tempo de convergência elevado, ainda que melhor que o RIP. Suporta várias métricas, e faz a decisão da melhor rota com base no delay e bandwidth da ligação. Suporta mais Hop Counts que o RIP.

A versão EIGRP veio trazer tempos de convergência muito mais rápidos (1s) e resolver parcialmente os problemas de polling associados com a arquitetura distance-vector, suportando updates parciais e enviando apenas rotas que tenham alterado ao invés da tabela toda. Suporta também VLSM.

O HELLO é um protocolo muito simples distance-vector que baseia a sua operação em enviar pacotes HELLO (sinalização). Escolhe a melhor rota com base no delay associado. Tem um grande problema de polling pois é preciso fazer broadcast de pacotes HELLO para todos os nós constantemente para ver o status da rede e descobrir novos nós, podendo utilizar muita largura de banda. É instável com muitas mudanças na rede, e por isso o tempo de convergência é também alto e instável.

Routing para redes médias e grandes

Para redes de grande dimensão, distance-vector não é adequado pois não escala bem, principalmente devido ao problemas de polling associados a transmitir a tabela toda, assim como os tempos de convergência muito elevados.

Desse modo, protocolos Link-state são mais adequados. É uma arquitetura onde todos os router calculam as melhores rotas com base no algoritmo SPF para todos os destinos possíveis. Com base nas suas descobertas locais, são criados pacotes LSP que são enviados para todos os elementos da rede. Os router usam depois esse pacotes para construir o modelo global da rede e consequentemente construir as suas tabelas de routing.

O OSPF é um protocolo standard IETF, baseado em link-state, suporta VLSM, tem um overhead baixo e tempos de convergência muito baixos (1s). Funciona sobre a tipologia de redes, que permite a separação da rede em várias sub-redes, minimizando as tabelas de routing, descentralizando o processamento e isolando possíveis falhas. Apesar de mais complexo, escala muito bem e está disponível para todos os sistemas. A melhor rota é calculada com base no custo associado, que é uma função da largura de banda da ligação.

IS-IS é muito similar, no entanto distingue-se por operar sobre a layer 2, ao contrário do OSPF que opera na layer 3. Suporta também redes, mas não obriga a que todas estejam ligadas ao backbone diretamente. É também um standard OSI.

EIGRP é também uma solução, pois apresenta também tempos de convergência na mesma ordem e implementa um sistema híbrido de distance-vector, suportando partial updates que minimizam o problema de pooling. Suporta também um grande número de hops. A sua principal vantagem é de ser mais simples a sua implementação, no entanto era proprietário, pelo que a sua disponibilidade não é garantida em todos os sistemas.

Por fim, é possível para uma tipologia global fazer uso de um protocolo EGP, que opera sobre AS. AS são sistemas geridos todos pela mesma entidade, unificados na sua política de routing interna. O BGP4 permite o routing entre estes AS, funcionando sobre a arquitetura de path-vector, onde é registado todo o percurso entre todos os AS existentes, assim como o próximo hop. As escolha de melhor rota tem várias políticas de decisão, no entanto enumeram-se o número de hops ou em caso de empate o AS mais pequeno. Apresenta tempos de convergência baixos e suporta agregação de rotas. É também um standard IETF.

Modelo OSI

O modelo de gestão OSI baseia-se no modelo FCAPS: Fault / Configuration / Accounting / Performance / Security.

Gestão de falhas:

- Identificar / Localizar a falha;
- Isolar a falha;
- Reconfigurar a rede para minimizar o impacto da falha;
- Reparar a falha.

Gestão de configurações:

- Manutenção das versões de software instaladas
- Manutenção das configurações
- Modificação das configurações
- Atualização de software e eventualmente hardware
- Agendar manutenção.

Gestão de contabilidade:

- Contabilizar tráfego nas fronteiras;
- Identificar excesso de tráfego por parte um conjunto de utilizadores, limitando o uso da rede;
- Identificar baixa eficiência no uso da rede, e otimizar;
- Permitem ser definidas tarifas de uso da rede;
- Permite obter as métricas para ações de cobrança.

Gestão de performance:

- Monitorização;
- Recolher informação estatística;
- Controlo para melhorar a performance da rede;
- Verificação do SLA.

Gestão da segurança:

- Proteção de informação;
- Acesso de controlos, nomeadamente hierárquicos
- Centralização vs Descentralização da gestão
- Registo de logs e consequente análise.

Traffic Flow

Análise de tráfego é o processo de caracterizar o fluxo de tráfegos numa rede: onde é que ocorrem e que níveis de performance é que não necessários para os garantir. Processo fundamental no design da rede.

Enumeram-se 3 tipos de fluxos:

- Individual: Tráfego gerado por uma sessão de uma aplicação, com requisitos garantidos;
- Composto: Combinação de requisitos de fluxos individuais que partilham a mesma ligação, caminho ou rede;
- Backbone: Combinação de requisitos de fluxos compostos quando a rede apresenta hierarquia.

Podem também se identificar pelo menos 4 modelos de fluxo:

- Peer-to-peer: Ambos os sistemas estão no mesmo nível hierárquico, não apresentando uma direcionalidade, sendo de facto o ponto de partida numa análise. EX: Teleconferência;
- Client-Server: Apresenta hierarquia e direcionalidade. Apesar do fluxo ser bidirecional, é geralmente assimétrico dado que os pedidos são mais pequenos que as respostas. VoIP é client-server no estabelecimento da chamada e Peer-to-peer durante a própria chamada;
- Client-Server Hierárquico: Quando o modelo fica mais hierárquico e mais complexo. Tem fluxos server-server e manager-server;

- Computação distribuída: Todos os computadores comunicam com todos.

Requisitos

Requisitos de utilizadores

São aqueles que são discutidos diretamente com os utilizadores. Enumeram-se:

- Delay: Disponibilidade e Interatividade;
- Fiabilidade: Fiabilidade, Qualidade, UI, Adaptabilidade e Segurança;
- Capacidade: Custo, users suportados e escalabilidade futura.

Requisitos de aplicações

São os requisitos das aplicações para garantir o seu bom funcionamento. Não garantir pode levar a perdas financeiras, de dados, ou até mesmo de vidas.

As aplicações podem ser:

- Mission-critical: Requerem altos níveis de previsão e garantias, com o sistema desenhado para garantir os padrões RMA.
- Rate critical: Requerem alta capacidade. Nas aplicações Best-effort não há garantias de capacidade ou até mesmo previsões.
- Real time: Requerem muito baixo delay. Também podem ser interativas, onde é mais importante a informação chegar correta do que rapidamente, ou mesmo até mesmo assíncronas, insensíveis ao delay.

Requisitos dos dispositivos

Depende obviamente do tipo de dispositivos. Estes podem ser ser dispositivos genéricos, como PCs ou telemóveis, servidores, ou dispositivos específicos.

O problema Last-mile consiste em instalar infraestrutura, redes ou serviços dentro de um campos ou edifício.

O problema Last-foot consiste em levar esse serviços e performance até aos utilizadores.

Muitas vezes os problemas são dos lado do dispositivos, nomeadamente drivers ou falta de capacidade de processamento, e não da rede.

A localização dos dispositivos é importante para determinar as relações entre eles, por exemplo, LAN. É o primeiro ponto na determinação dos fluxos de tráfego. É particularmente importante em serviços por exemplo, de cloud computing, por causa do delay e capacidade.

Requisitos da rede

São os principais requisitos e que estão sempre presentes no planeamento da rede. O primeiro ponto a ter em conta é a existência de infraestrutura de rede já presente. Tem que acomodar dependências:

- Escalabilidade;
- Localização;
- Performance;
- Serviço de suporte;
- Interoperabilidade;
- Obsolescência da rede existente.

Requisitos de gestão

- Métodos de monitorização;
- Protocolos e ferramentas;
- Características a monitorizar;
- In-band vs Out-band;
- Centralizado vs Descentralizado;
- Performance.

Requisitos financeiros

- Orçamento para a fase de design e instalação, como SW, HW e cabos;
- Orçamento para a fase de produção, como staff, partes suplentes e aluguer de serviços.

Requisitos de segurança

Inicialmente, tem que ser definida a tipologia de rede, nomeadamente a existência de uma DMZ, Firewall, ou ambas. Depois tem que se considerar o valor dos bens: SW, HW, Data, Know-how.

Falhas de segurança podem ser causadas por:

- OS desatualizados;
- Fraca encriptação
- Sistema comprometido
- DoS e Sniffing

Performance da rede

- Bandwidth;
- Throughput;
- Good-put;

- Delay;
- RMA;
- Considerar o SLA.

SNMP

Versões

O SNMP é um protocolo standard IETF de gestão de redes, cuja arquitetura é baseada em 4 entidades:

- Manager, uma entidade SNMP de gestão com uma ou mais aplicações de gestão de rede instaladas;
- Agente, uma entidade SNMP que permite o acesso à informação de gestão desse nó;
- SNMP, um protocolo que é usado pelos NMS e agentes para troca de informação;
- Informação de gestão, SBI & MIB.

O SNMP suporta 3 tipos de operações:

- GET, onde o manager recolhe informação de um objeto numa estação com um agente;
- SET, onde o manager muda o valor de um objeto numa estação com um agente;
- TRAP, onde o agente na estação envia para o manager sem qualquer pedido deste o valor de um objeto que foi modificado.

Um nó gerível pode ser um sistema (computador, PC, etc), um router, uma bridge ou switch, ou mesmo um dispositivo IoT. Estes nós são caracterizados por um conjunto de variáveis como por exemplo o Operating time, Contact, Name, Location, etc.

A framework contém também o SMI e a MIB. A MIB é um repositório conceptual que contém a informação / objetos geríveis de um sistema e as respetivas operações. Tem uma tipologia hierárquica para organização e facilitar o acesso e possível expansão da árvore OID.

A SMI define a estrutura e sintaxe destes objetos, i.e, se são inteiros ou strings, como é que se chamam e como é que se escrevem. Basicamente, é a sintaxe da MIB de modo a garantir que todos os sistemas sabem trabalhar com as informação.

As mensagens são trocadas baseadas em PDU (Protocol Data Units), sendo que existem:

- GetRequest, GetNextRequest;
- GetResponse;
- SetRequest;
- Trap, com um conjunto de sub-traps.

O SNMP apresenta um conjunto de problemas:

- Polling, quando há demasiado tráfego SNMP na rede;

- Não há garantia de entrega dos pacotes críticos, pois é suportada em UDP;
- Não suporta trocas de informação grandes;
- A MIB é limitada e não permite expansão.

O SNMPv2 veio trazer algumas soluções. Permite a comunicação entre managers, diminuindo o problema de polling ao descentralizar a gestão. Suporta TCP/IP para garantia de entrega de pacotes críticos (Traps) e error codes. Suporta também a transferência de muita informação com a PDU getBulk. E existiu uma expansão da OID tree, com mais informação, entre outros.

No entanto, em ambas a versões, a autenticação e controlo de acesso era feita com recurso a community strings, não encriptadas e desse modo, facilmente descobertas com recurso a packet sniffing. Desse modo, não é aconselhável usar o SNMPv2 e SNMP para fazer SET operations, apenas para ler informação.

O SNMPv3 foi o patch de segurança tão necessário para garantir a fiabilidade da framework. Mantém a mesma tipologia das 4 entidades no entanto garante agora algumas áreas novas na segurança:

- Autenticação, como identificação de origem e integridade de mensagem;
- Privacidade, como a encriptação para garantir a confidencialidade da informação;
- Autorização e controlo de acesso;
- Configuração e administração remota para os 3 aspetos mencionados.

Ameaças

As ameaças à operação do SNMP podem ser divididas em 3 graus de severidade:

- Principais, como *mascarade* que afeta a autenticação de origem, onde um sistema se faz passar por outro para ganhar privilégios, e modificação de informação, que afeta a integridade da informação, onde os pacotes são intercetados e modificado o seu conteúdo.
- Secundárias, como a modificação da ordem de chegada dos pacotes, ou repetições, e quebra de confidencialidade, onde a informação é descoberta por hackers.
- Outras, onde se inclúi DoS e análise do padrão de tráfego para descobrir informação relevante.

MIB Privada

MIB é uma especificação standard de monitorização que possibilita a gestão de uma rede. Ela especifica que elementos são geríveis e que tipo de parâmetros lhes estão associados. Existe uma OID-tree standard para todos os sistemas, que permite um conjunto de operações básicas de controlo e gestão para todos os sistemas. A MIB privada é um ramo da OID-tree que permite que empresas coloquem lá as suas especificações para os seus próprios sistemas, em adição aos standard. Por exemplo, a CISCO corresponde ao número 9, logo encontra-se em .4(private).9(cisco).x. Aqui podem ser encontrados mais objetos geríveis específicos daquele sistema. É no entanto necessário que esta informação/ extensão da árvore esteja disponível quer no agente, quer no manager.

MIB RMON

RMON (Remote Monitoring) é uma especificação que permite que vários NMS e sistemas trocam informação de gestão. Funciona sobre o conceito de probes, uma espécie de sub-managers, que fazem a gestão dos sistemas diretamente ao invés do NMS, e que depois comunicam a informação aos NMS.

Deste modo, devido à sua descentralização em relação aos NMS, funciona em modo-offline, que resolve o excesso de tráfego SNMP na rede. Como já não há esta limitação de tráfego, se houver performance disponível, deve ser feita uma gestão pro-ativa constante dos sistemas e serviços.

A informação só é enviada para o NMS numa base periódica ou quando há alguma problema, garantindo value-added-data nos NMS e libertando assim os seus recursos de monitorização, suportando mais sistemas.

Por fim, permite que existam múltiplos NMS, e garante a comunicação entre eles, permitindo a descentralização da monitorização.