Unidade III

5 ANÁLISE DAS RESTRIÇÕES E DOS OBJETIVOS TÉCNICOS

Recomendar o uso de tecnologias apropriadas para satisfazer o usuário é um dos pontos do projeto de redes, mas, para que essa recomendação seja possível, é necessário analisar os objetivos técnicos do cliente.

Durante este capítulo serão examinados os seguintes objetivos técnicos: escalabilidade, disponibilidade, desempenho, gerenciabilidade, segurança, usabilidade, *cost-effectiveness*, adaptabilidade; também serão verificados os *tradeoffs*, isto é, os fins conflitantes.

O objetivo primário da maioria dos projetos de rede é a escalabilidade, a qual se refere a quanto crescimento é suportado, pois adicionam-se usuários, aplicações, *sites* e conexões de rede a um ritmo muito veloz.

Pensando nesse crescimento, deve existir um planejamento para a expansão. Para isso, temos de descobrir qual é o crescimento planejado da rede nos próximos 3 anos após a implantação. Infelizmente são raros os clientes que possuem uma programação maior que esse período.

Para descobrir esse planejamento, é necessário realizar algumas perguntas ao cliente, tais como:

- Qual a nova quantidade de *sites* (locais) que serão adicionados?
- Qual será a abrangência da rede em cada novo *site*?
- Haverá usuários adicionais para acesso à rede?
- Quantos servidores e *hosts* deverão ser adicionados?

Pensando na escalabilidade é preciso fornecer mais dados a mais gente. Para Albert e Barabási (2002, p. 79-82), quanto mais conexões tem um modo, mais oportunidades tem de ter outras, formando um modelo de "redes sem escalas". Seguindo este conceito, fornecer mais dados a mais gente se enquadra neste padrão de rede. Ainda de acordo com os autores (2002, p. 66-71), o nome sem escala vem da representação matemática da rede, que segue uma curva denominada *power low*, conhecida também como lei de Pareto ou regra 80/20, que faz referência a uma proporção que ocorre com frequência em fenômenos de rede. Segundo tal teoria 80% do tráfego em uma rede fica no setor departamental e 20% sai do departamento, mas ela era válida no tempo em que redes serviam muito para compartilhar discos e impressos.

Hoje em dia acontece uma inversão desta regra, pois, com o número maior de acesso a servidores corporativos, incluindo intranet, páginas *web* e extranet, a qual permite a colaboração de parceiros, fornecedores e grandes clientes, o tráfego departamental pode cruzar um *backbone*, devido ao uso de um conjunto de servidores, normalmente mantidos por uma empresa ou universidade para executar tarefas que vão além da capacidade de uma só máquina corrente, tornando o uso centralizado. O resultado é a tecnologia da informação fornecer gradualmente mais dados a mais gente, para que se tomem melhores decisões de negócio de modo rápido. Caso isso aconteça a consequência são os seguintes objetivos técnicos:

- Na rede corporativa conectar redes departamentais.
- Obter maior tráfego entre as redes, após resolver os gargalos.
- Com uma *server farm* prover servidores centralizados.
- Incluir novos *sites* e dar suporte a funcionários que trabalham em casa e nas filiais.
- Adicionar novos *sites* para prestar suporte a grandes clientes, parceiros e fornecedores.

Toda escalabilidade possui restrições. Ao pensar nisso é preciso ter em mente que algumas tecnologias de rede não são inerentemente escaláveis, tais como redes com endereçamento plano, envolvendo *hubs* e *switches* simples, redes que suportam serviços baseados em *broadcast* etc.

Lembrete

A escalabilidade se refere a quanto crescimento um projeto de rede deve suportar.

Após entender e planejar a escalabilidade é necessário prever a disponibilidade. Ela normalmente refere-se ao percentual de tempo que a rede ficará disponível, sendo este com frequência um objetivo crucial ao cliente.

Para compreender melhor a disponibilidade, observe um cenário considerado ruim. Ele é composto de rede ativa 168 horas por semana, ou seja, 24 horas por dia, mas para de funcionar por 4 horas; logo a disponibilidade da rede seria de 97,62%.

Vale ressaltar que disponibilidade é diferente de confiabilidade, pois a segunda inclui dados de acurácia, taxas de erro, estabilidade etc. Já a recuperabilidade é um dos aspectos da disponibilidade, pois é uma habilidade de recuperar rapidamente o funcionamento em caso de falhas. Assim também a recuperação é um outro aspecto da disponibilidade, pois deve haver um planejamento em caso de desastres – por exemplo, onde ficarão as cópias dos *backups* dos dados e se poderá haver chaveamentos de acessos a eles.

Para especificar os requisitos da confiabilidade, tenhamos o seguinte como parâmetro:

Tabela 1 – Quantidade permitida de queda no período de tempo

Disponibilidade (% ativa)	Período/dia	Período/semana	Período/mês	Período/ano
99,99%	8,7 s	1,0 m	4,4 m	0,88 h
99,98%	17,3 s	2,0 m	8,75 m	1,75 h
99,95%	43,2 s	5,05 m	21,9 m	4,38 h
99,50%	7,2 m	50,5 m	3,7 h	43,8 h
95%	1,2 h	8,4 h	36,5 h	438 h

Fonte: Serpanos e Wolf (2011, p. 234).

Observando a tabela anterior, é possível entender os níveis da disponibilidade, sendo 99,99% o padrão atual e limite da tecnologia, pois até 99,9% é considerada uma disponibilidade baixa; consequentemente acima disso considera-se alta. Normalmente os sistemas operam em 99,95%, permitindo uma parada maior no mês com cerca de 5 minutos por semana, mas 95% é uma margem que deve ser utilizada apenas para testes.

O custo ou prejuízo da rede parada por muito tempo pode ser alto se houver aplicações de uso crítico no ambiente.

Após compreender a disponibilidade na rede e sua necessidade é preciso entender e explicar o seu desempenho, pois diversos clientes não conseguem especificar suas demandas com exatidão, normalmente exigindo apenas que a rede seja veloz.

Para entender a necessidade de desempenho, alguns aspectos devem ser levados em conta, tais como: a capacidade da rede de carregar tráfego em *bits* por segundo; um percentual da capacidade usada, na média; um valor da utilização em que a rede é considerada saturada; a quantidade de dados úteis transferidos sem erro por segundo; a soma de todo o tráfego oferecido à rede (em Bps) em um determinado momento; a quantidade de tráfego útil corretamente transmitido, relativo ao tráfego total; o nível de dados úteis transmitidos, descontados os *overheads*; a latência, se haverá variação de atraso; o tempo entre um pedido de serviço e a recepção de uma resposta, dependendo da situação.

Muitas aplicações do tipo interativas necessitam que haja um atraso, tendo como principais causas: tempo de transmissão, de propagação, de chaveamento de pacotes e em fila por utilização ou transmissão, podendo sofrer variações no atraso. Um dos recursos dessas variações é chamado de *jitter*, utilizado normalmente com áudio e vídeo; ele é causado por rajadas de tráfegos, que se minimizam com o *buffer* do receptor.

O atraso normalmente utilizado é de 1% a 2% no total, sendo diferente apenas quando especificado pelo cliente. Uma alternativa para variações de atrasos é o uso da tecnologia ATM, que emprega pequenas células de 53 *bytes* e oferece o serviço QoS (qualidade de serviço).

Considerando a importância da utilização dessas aplicações multimídia para os usuários, é necessário ter um curto tempo de resposta, no máximo de 100 ms, pois após esse período os usuários sentem a lentidão; já em páginas *web* ou arquivos alguns minutos são razoáveis.

A utilização máxima do atraso é de 70% para enlaces normais e de 40% a 45% para Ethernet, em que existe a perda de banda por colisões. Para outras aplicações, não há o porquê de se preocupar com os atrasos, apenas com a quantidade de dados úteis que são transferidos sem erro por segundo, saturando o enlace e diminuindo essa vazão para o aumento da carga oferecida.

Geralmente os clientes informam a vazão desejada para um dispositivo processar sem o descarte de pacotes via pps ou pacotes por segundo; em cenário ATM são cps ou células por segundo. Observemos o limite máximo desses pacotes pps:

Tabela 2 – Pps máximo para Ethernet 10 Mbps

Tamanho do quadro (*bytes*)	Limite
1.518	812
1.280	961
1.024	1.197
768	1.586
512	2.349
256	4.528
128	8.445
64	14.880

Fonte: Serpanos e Wolf (2011, p. 262).

Assim, se existir um roteador capaz de rotear 30 fluxos Ethernet a 10 Mbps e os pacotes forem de 64 *bytes*, ele operará a 446.400 pps, sendo o cálculo feito de 14.880 pps (30 fluxos).

No que se refere à aplicação, a vazão se torna melhor para o usuário, sendo medida em Kbps ou Mbps (*kylobytes* ou *megabytes* por segundos), o que é importante apenas em transferências de grande volume de informação, tais como *download* ou transferência de arquivos. Essa vazão de nível de aplicação normalmente é afetada por fatores como: taxas de erros fim a fim, capacidade de enlaces, tamanho dos quadros etc., além de pelo desempenho nos servidores e clientes - velocidade de acesso aos discos, desempenho dos *drivers*, memória e barramentos, velocidade da CPU, problemas com sistema operacional ou aplicação. Se houver problemas de vazão alguns *softwares* perfiladores de desempenho e análise dos protocolos podem investigá-los.

Para fazer com que os dados enviados e recebidos sejam iguais em ambos os lados, existe a acurácia. Quando ela está ausente é possível que haja problemas de conexões físicas (como cabos frouxos), falhas de dispositivos e até mesmo ruído, devido a máquinas ou rede elétrica.

A sobrecarga na transmissão da informação é descrita através da eficiência. Muitas vezes a ineficiência ocorre por colisões, cabeçalhos etc. Normalmente, uma forma de minimizar as sobrecargas por cabeçalhos é usar o maior quadro possível na tecnologia em atividade.

Um aspecto muito importante em um projeto de redes é a segurança, principalmente com conexões à extranet e internet. Seu objetivo básico em um projeto deve ser o de que problemas relacionados à segurança não afetem a empresa na condução de seus negócios. A primeira tarefa deste objetivo é planejar, levantando os requisitos e analisando os riscos, o que envolve muito o conflito de escolhas, conhecido como *tradeoff*, pois, quando o nível de segurança é maior, a facilidade de uso e a produtividade dos usuários são reduzidas ou perdidas.

Para analisar os riscos, é necessário investigar o que pode acontecer se não houver segurança implantada, questionando quais informações do cliente são sensíveis ou, se os dados fossem roubados ou modificados, qual seria o efeito.

Supondo que seja sugerido usar VPN (Virtual Private Network) para acessar uma rede corporativa pela internet, quais seriam os riscos por esta utilização? O provedor teria a tecnologia com funções adequadas?

Imagine um roubo de informação por *sniffing* de rede. Ele não teria grande sucesso em furtar os pacotes de rede se a VPN utilizasse a criptografia adequada, mas o maior perigo seria o de acessar ou modificar dados direto no servidor, seja uma página *web*, seja um arquivo de uso interno.

Muitos *hackers* usam maneiras de ataques como a utilização de recursos que não deveriam acessar, a inibição do uso de recursos por usuários válidos, o roubo e até mesmo a destruição de recursos, além de tirar proveito de falhas de segurança comuns em alguns sistemas operacionais.

Os aspectos mais comuns de preocupação das empresas são os problemas causados por erros humanos, como propagação de vírus, erros de usuários e adversidades causadas por usuários mal-intencionados.

Alguns requisitos de segurança devem existir, pois há recursos que têm de ser protegidos, como *hosts* dos equipamentos, inclusive de servidores, dispositivos como roteadores, *switches*, dados de sistemas ou aplicações, ou informações que possam prejudicar a imagem da empresa.

Recomenda-se: implantar requisitos típicos que permitam a pessoas externas acessar dados públicos via http, ftp etc., mas não os internos; identificar, autenticar e autorizar usuários de filiais, móveis ou que trabalham de casa; detectar e identificar intrusos e danos causados por eles; proteger as informações recebidas ou enviadas para locais remotos via VPN; salvaguardar os *hosts* e dispositivos de modo físico (utilizando portas de acesso, senhas etc.); utilizar métodos de proteção contra vírus; e principalmente treinar os usuários sobre a política de segurança da empresa e mostrar meios para que problemas de segurança possam ser evitados.

A gerenciabilidade pode ser dividida por áreas para todos os clientes que precisarem de gerência de configuração, falha, desempenho, segurança e contabilidade.

Todo e qualquer usuário necessita ter acesso aos serviços da rede. Facilidade para realizá-los é uma das características da usabilidade, pois ela busca melhorar os impactos da política de segurança quanto à facilidade do uso, da configuração da rede, do acesso remoto e da integração de um usuário móvel para outros pontos, como sede e filiais, ao contrário da gerenciabilidade, que visa melhorar os aspectos para gerentes da rede.

Para um projeto poder englobar o avanço da tecnologia e projetar o uso de novas tecnologias por um período, é necessário que ele possua adaptabilidade, visando que a rede se adapte a mudanças de tecnologias, protocolos, formas de negócio e legislação.

Para a empresa, o principal objetivo é implantar uma nova rede com o menor custo possível ou dentro de um orçamento estipulado. Esses custos podem ser para aquisição ou operação, sendo classificados não recorrentes ou recorrentes. Como em rede local a disponibilidade e a velocidade são altas e o objetivo é o menor custo, realizar a aquisição de equipamentos com custo baixo por porta, diminuir os gastos com cabeamento e obter placas de rede com baixo custo é uma prioridade para garantir um bom preço ao projeto total.

Em ambientes com rede corporativa, no geral, ter disponibilidade torna-se mais importante que o custo na maioria dos casos, mas o item essencial do custo é a contratação de *links* ou enlaces de comunicação. Essa parte deve ser mantida no menor valor possível, dentro das especificações. Dá para minimizar os custos de operação WAN. Para isso, é necessário usar um protocolo para roteamento com baixo tráfego na WAN, que empregue rotas mínimas para tarifação, além de precisar eliminar troncos paralelos, consolidando o tráfego de voz e dados.

O salário e os custos com treinamento para o pessoal de suporte e operação são o aspecto mais caro. As possibilidades para minimizá-los podem ser adquirir equipamentos com fácil configuração, gerenciamento e operação, utilizar um projeto simples de depurar, além de entender e manter o projeto todo documentado com boa organização.

Embora o baixo custo seja o principal objetivo das empresas, alguns aspectos técnicos entram em conflito, pois, se forem exigidos alta disponibilidade e alto desempenho, será necessário maior custo para o uso de tecnologias caras como ATM e aplicação de redundância. Assim como o custo, outros aspectos também apresentam conflitos, como a segurança, que diminui a facilidade de uso, a adaptabilidade, que se houver mudanças constantes pode diminuir a disponibilidade, e a alta vazão, que pode implicar alto atraso. Como lidar com esses conflitos?

O principal objetivo deve ganhar sempre, ou seja, ele serve como critério de desempate em caso de conflitos. Assim também devem ser priorizados outros fins técnicos, podendo ser estipulado com o cliente um percentual que cada categoria talvez possua no projeto, ou seja, se o cliente determinar que a importância da usabilidade é de 20% e da segurança 15%, caso haja divergência para a decisão que implique algum dos itens, a prioridade seria da usabilidade, por ter maior critério de escolha, portanto funcionando para todos os aspectos.

5.1 *Checklist* de objetivos técnicos

Para avaliar se está pronto para cumprir esta fase do projeto, algumas perguntas devem ser respondidas:

- Os planos da expansão do cliente foram documentados para os dois anos seguintes, com relação a servidores, *sites*, usuários, estações?
- O cliente informou os planos para migrar servidores dos departamentos para *server farm*?
- O cliente informou se possui planos para usar intranet ou extranet?
- Sobre % de *uptime*, há objetivos da disponibilidade?
- Documentei se existem desejos de utilização máxima nos segmentos compartilhados?
- Documentei objetivos para a vazão necessária para cada aplicação desejada?
- Documentei objetivos de vazão pps para dispositivos de interligação?
- Documentei objetivos de acurácia em termos de BER aceitáveis?
- Discuti com o cliente a importância de utilizar quadros grandes para maximizar a eficiência da rede?
- Identifiquei aplicações que precisam de tempos de resposta menores do que o normal, de 100 ms?
- Discuti os riscos e requisitos de segurança com o cliente?
- Levantei requisitos de gerenciabilidade, incluindo objetivos de gerência de configuração, falha, desempenho, segurança e contabilidade?
- Priorizei objetivos técnicos e de negócio com o cliente? Sei qual o mais importante dos objetivos?

6 CARACTERIZAÇÃO DA REDE EXISTENTE

Em projetos de expansão em uma rede existente devem ser examinados e caracterizados detalhadamente alguns aspectos, como topologia, estrutura física e identificação de gargalos, além de desempenho da rede para possíveis comparações futuras.

A fim de caracterizar a infraestrutura da rede, temos de elaborar um mapa, incluindo a localização dos segmentos e dispositivos de interconexão, sendo necessário descobrir quais os métodos utilizados para nomear os dispositivos e segmentos da rede, descobrindo também o tamanho da estrutura de cabeamento usado e os tipos de cabos, além de restrição de arquitetura e ambiente envolvido.

Para desenvolver um mapa da rede, existe a necessidade de entender os fluxos de tráfego. Esse processo inicia-se com a descoberta dos *hosts*, segmentos e dispositivos importantes na rede. Realizando a junção dessa informação com os dados de desempenho, é formado um bom conhecimento do nível de tráfego e concentração de usuários que a rede deve suportar.

Será utilizado como recurso para montar o mapa da rede o Microsoft Visio e algumas ferramentas que descobrem a topologia automaticamente, como Clicknet Professional e NetSuite Professional Audit, além de ferramentas ou métodos manuais para encontrar dispositivos da rede contendo detalhes sobre *host*, CPU, memória e placas de rede.

Um mapa da rede também deve ter a informação geográfica (países, estados, cidades, *campi*), as conexões WAN que existem entre países, estados, cidades, prédios, andares, chegando às vezes até salas ou cubículos, as conexões LAN e WAN entre prédios e entre *campi*, as tecnologias dos enlaces (Ethernet, Fast Ethernet, ATM, *frame relay*, Datasat etc.) e o nome do provedor de serviços de telecomunicações (enlaces WAN).

Ainda é necessário conter localização dos *switches* e roteadores, localização e alcance de qualquer VPN, localização de servidores principais e *server farms*, localização de *mainframes*, localização de estações de gerência, localização e alcance de VLANs. Além da topologia dos sistemas de *firewall* e *bastion host*, é preciso ter a localização dos contadores por área das *workstations* e a topologia lógica da rede (*collapsed backbone*, *server|core|distribution|access blocks*).

Observação

O cabeamento físico não indica quem pertence a qual VLAN. Faça o uso de cores para diferenciar VLANs.

Na próxima figura é possível observar um mapa de alto nível desenhado pelo Visio, porém ele não é muito detalhado.

Saiba mais

Para mais dados sobre o funcionamento do Visio, acesse suas vantagens e qualidades em:

MICROSOFT. *Visio*. [s.d.]. Disponível em: <https://products.office.com/pt-br/visio/visio-online>. Acesso em: 18 jul. 2018.

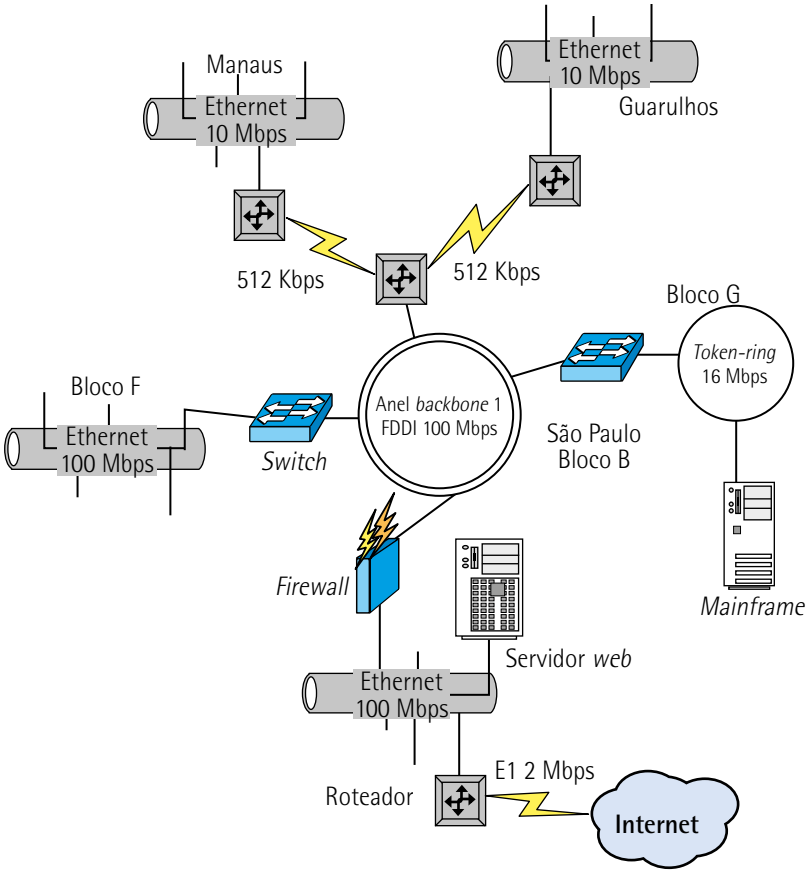

Figura 10 – Mapa da rede

Através do programa Microsoft Visio é possível realizar desenhos de diagramas. Ele possui fluxogramas, gráficos organizacionais etc., principalmente projetos e plantas, sendo este um produto complementar ao pacote Office. Essa será sua principal ferramenta para a elaboração de projetos e mapas de rede.

Após realizar o desenho do mapa é necessário caracterizar a estrutura lógica, iniciando pelo descobrimento dos esquemas de endereçamento e nomes de rede usados na empresa. Para isso devem-se documentar as estratégias existentes, como as denominações utilizadas em equipamentos (p. ex., rtr de roteadores ou códigos de aeroportos, como GRU) e os esquemas de endereçamento IP com as sumarizações de rotas, NAT etc. Esses esquemas poderão afetar a forma de escolher os protocolos de roteamento.

Observação

Frequentemente, todo o esquema de endereçamento deve ser refeito.

Caracterizar a estrutura física também é uma das necessidades. Portanto os cabeamentos e mídias devem ser caracterizados. Assim é preciso documentar o tipo de produto utilizado, se é UTP cat 5, cat 6, coaxial, fibra ótica etc., o comprimento desses cabos e se eles estão dentro do limite estipulado pelo tipo.

É necessário levantar a forma como esses cabos estão etiquetados, se existem outros meios de comunicação disponíveis entre os prédios, como tecnologias *wireless*, rádio, infravermelho etc. Nos ambientes internos precisa ser caracterizado se há salas de telecomunicações, armários, entre outros, além do tipo de cabeamento passado (vertical, horizontal ou de área de trabalho.)

Após fazer todo o levantamento e a caracterização da estrutura lógica e física, é essencial verificar as restrições sobre a arquitetura e os ambientes da rede, realizando as seguintes perguntas:

Sobre cabeamento externo (restrições ambientais) deve-se questionar:

- Ele deve passar por áreas que podem sofrer enchente?
- Ele deve passar perto de linhas de trem?
- Ele deve passar perto de estradas onde o tráfego pode deslocar cabos?
- Ele deve passar por áreas onde atividades de construção poderiam quebrar cabos?
- Ele deve passar por áreas que pertencem a terceiros?
- Há restrições de "visada" a serem observadas entre locais remotos?

Quanto ao cabeamento interno (restrições arquiteturais) há as restrições a seguir:

- Como está o ar condicionado para a nova rede?
- Como está a ventilação para a nova rede?
- Como está a energia para a nova rede?
- Como está a proteção contra interferência eletromagnética para a nova rede?
- Há espaço para canaletas de cabeamento, *patch panels*, *racks* de equipamentos?
- Há acesso fácil aos equipamentos para *troubleshooting*?

Mesmo com todos os levantamentos e caracterizações realizados, é extremamente importante verificar a saúde da rede existente, pois muitas vezes será fácil mostrar ao cliente a mudança de desempenho, seja para que ele veja a nova rede como algo melhor, seja em casos de redução de custo, em que a nova rede não perdeu o desempenho. Para isso devemos fazer uma *baseline* da *performance*.

Segundo o PMBoK (2013, p. 543), *baseline* ou linha-base é uma versão aprovada do orçamento referencial do projeto, que pode ser mudada por procedimentos formais do controle de mudança.

Portanto devemos considerá-la como um planejamento acordado e autorizado pelas partes interessadas, como a meta de progresso (evolução) para o projeto.

Entretanto, desenvolver uma *baseline* de desempenho não é algo simples, pois, nos casos em que a rede é muito ampla, onde os dados poderão ser adquiridos? Qual o melhor momento para obter a média ou o pico deles? Durante quanto tempo devem ser adquiridos? O cliente permitirá o acesso à rede para esses levantamentos? Quais os meios para adquirir esses dados?

Para montar a *baseline*, é fundamental realizar a análise da disponibilidade, da utilização, da acurácia, da eficiência, do atraso e do tempo de resposta da rede, além de verificar o *status* dos roteadores principais.

Para analisar a disponibilidade na rede, é necessário obter as métricas de *downtime* do cliente, identificar se essas estatísticas são realísticas para a nova rede, ter relatos de quando houve a última queda de conexão importante e qual foi a causa. Todas essas informações devem ser anotadas, seja para a rede como um todo, seja individualmente por seus segmentos.

Após analisar a disponibilidade de rede é preciso verificar sua utilização, entendendo se o uso dos enlaces é o principal responsável por causar lentidão.

Observação

Para analisar a utilização da rede, o melhor é usar médias de granularidade no intervalo de 10 minutos, por no máximo dois dias.

A fim de analisar a acurácia de rede, um Bert pode ser utilizado para realizar testes de taxas de erros, mas o melhor é medi-la em enlaces contratados, verificando os níveis de SLA que constam nos contratos. Em redes locais o melhor é fazer a medição dos erros de quadros.

Problemas de interferência elétrica e de cabeamento devem ser descobertos antes da implantação da nova rede.

A eficiência da rede pode ser checada através de analisadores dos protocolos, os quais são capazes de ver o tamanho dos quadros que nela circulam. Devem-se medir atraso e tempo de resposta na rede realizando um simples teste pelo utilitário *ping*, pois ele fornece o tempo de ida e volta entre os *hosts* escolhidos.

Os roteadores principais devem sempre ser verificados. Muitos deles permitem que estatísticas internas sejam analisadas. Siga as instruções do fabricante para checar as interfaces, os processos e os *buffers*.

6.1 *Checklist* para a saúde da rede

Para avaliar se a rede está saudável, algumas perguntas devem ser respondidas:

- Os documentos para a topologia da rede e infraestrutura física foram criados?
- Endereços de rede e nomes estão sendo atribuídos de forma estruturada e bem documentados?
- A instalação do cabeamento foi realizada de forma estruturada?
- O cabeamento para as estações não ultrapassa 100 m?
- A disponibilidade de rede é satisfatória aos objetivos deste cliente?
- A segurança de rede satisfaz os objetivos do cliente?
- Existe saturação em algum segmento Ethernet (40% no máx. por 10 minutos)?
- Algum outro segmento/enlace está saturado (70% no máx. por 10 minutos)?
- Nenhum dos segmentos tem mais de 1 erro de CRC por milhão de *bytes*?
- Dos segmentos Ethernet algum possui total de colisão com taxa maior de 3%?
- Nenhum segmento Ethernet possui colisões tardias?
- O tráfego do *broadcast* não passa de 20% do total?
- Foi otimizado o tamanho do quadro para cada tecnologia utilizada no enlace?
- Nenhum roteador está sendo utilizado em excesso (70% de utilização)?
- Nenhum roteador está descartando mais que 1% de pacotes?
- O período de resposta entre clientes e servidores (ida e volta) não ultrapassa 100 ms?

Após realizar a caracterização e os levantamentos necessários da rede é preciso fazer a caracterização do tráfego passado. Quatro itens serão abordados: o fluxo do tráfego, tanto no sentido de ida como no de volta, a carga para permitir estabelecer a capacidade dos enlaces, o comportamento do tráfego com relação a *broadcast* e eficiência, e o serviço de qualidade (QoS), permitindo assim selecionar soluções adequadas para o projeto físico e lógico da rede.

Para identificar o tráfego da rede, será preciso caracterizá-lo à rede existente e à rede nova de modo a reconhecer as fontes, direções e simetria do tráfego, analisando aplicações como as do tipo cliente-servidor, as quais geralmente são assimétricas, enviando poucos dados e recebendo muitos.

As principais fontes e servidores de fluxo na rede são inicialmente identificadas encontrando as comunidades de usuários e os locais de armazenamento maciço de dados. Comunidade é um grupo com usuários que fazem uso das mesmas aplicações, podendo ser em um ou vários departamentos. Recomenda-se que elas sejam documentadas.

Os grandes servidores de dados são tipicamente os locais onde as informações são armazenadas (*data stores* ou armazéns de dados), sendo em geral um servidor comum, *server farm*, *mainframe*, unidade de *backup* em fita ou biblioteca de vídeo. Recomenda-se que tudo seja documentado.

Para realizar a documentação de todo o fluxo de tráfego na rede existente, é preciso identificar e caracterizar os fluxos individuais de tráfego entre fontes e servidores, pois um fluxo individual entre entidades durante uma sessão comporta o tráfego de protocolo e de aplicação transmitido, possuindo os atributos de direção, simetria, *path*, número de *bytes* e pacotes e endereços de fonte e destino.

Saiba mais

Para informações a respeito da caracterização da rede da RFC 2063, acesse:

BROWNLEE, N.; MILLS, C.; RUTH, G. *Traffic flow measurement*: architecture. Auckland: IETF, 1997. Disponível em: <https://tools.ietf.org/html/rfc2063>. Acesso em: 5 jul. 2018.

Com o uso do analisador dos protocolos ou de uma estação de gerência de rede é possível identificar a quantidade de *bytes* de um fluxo, utilizando o programa *traceroute* (*tracert*). Com ele dá para realizar a coleta de informações por meio de um ponto central da rede durante dias, documentando o volume de dados a uma rota durante o ínterim.

Observação

Recomenda-se o uso de quatro fontes diferentes para realizar as medições no *tracert*.

Para a nova rede é impossível caracterizar o tráfego de novas aplicações. Usam-se técnicas indiretas para isso, sendo fundamental entender em termos de tráfego como as típicas aplicações se comportam. Existem modelos de fluxos que podem ser utilizados para ajudar nessa tarefa: terminal-hospedeiro, cliente-servidor, *peer-to-peer*, computação distribuída e servidor-servidor.

O modelo fluxo de tráfego terminal-hospedeiro possui fluxo assimétrico, no qual o terminal envia alguns *bytes* e o hospedeiro responde com muitos deles, assim como no *telnet*, que pode enviar apenas 1 *byte* por pacote do terminal para o hospedeiro, mas se esperar um pouco será capaz de mandar vários.

O fluxo cliente-servidor é o mais utilizado, possuindo dados nas duas direções, tornando-se bidirecional e assimétrico com pedidos pequenos e respostas maiores. Nesse modelo a direção servidor>cliente é a mais comum. Em muitos casos o fluxo torna-se unidirecional. A figura a seguir ilustra o seu funcionamento.

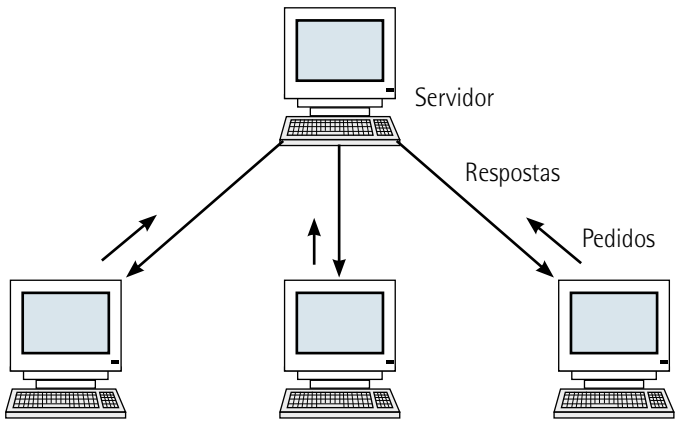

Figura 11 – Fluxo unidirecional

No modelo *peer-to-peer* os usuários e aplicações são basicamente equivalentes nos seus requisitos de comunicação, não possuindo uma direção exata.

Já a estrutura servidor-servidor é o fluxo de tráfego em que os servidores conversam entre si. Possuir simetria é a sua característica particular, como serviços de diretório, cache de dados, redundância e balanceamento da carga via *mirroring* de dados e realização de *backup*.

O modelo mais raro dos existentes é o fluxo de tráfego de computação distribuída, sendo bem especializado. Nele os fluxos dependem do acoplamento presente e da granularidade, podendo estar entre o *manager* e os nodos de computação ou entre estes. Caso haja granularidade grossa e acoplamento fraco, existirá o *cluster* de computação. Veja exemplo a seguir.

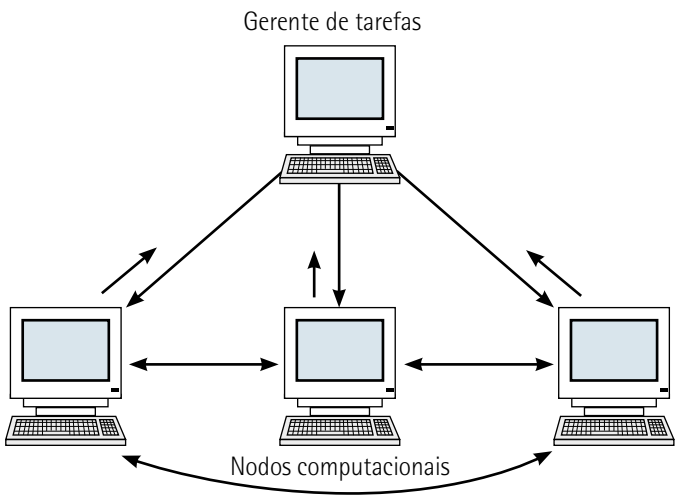

Figura 12 – Modelo de fluxo de tráfego para computação distribuída

Esse modelo é muito parecido com o cliente-servidor, porém os dados finais gerados pelos nodos podem ser maiores se comparados à informação inicial enviada pelo gerente, além de possuir fluxo assimétrico, apesar de inverso ao padrão cliente-servidor.

A figura na sequência ilustra o funcionamento do *cluster* de computação.

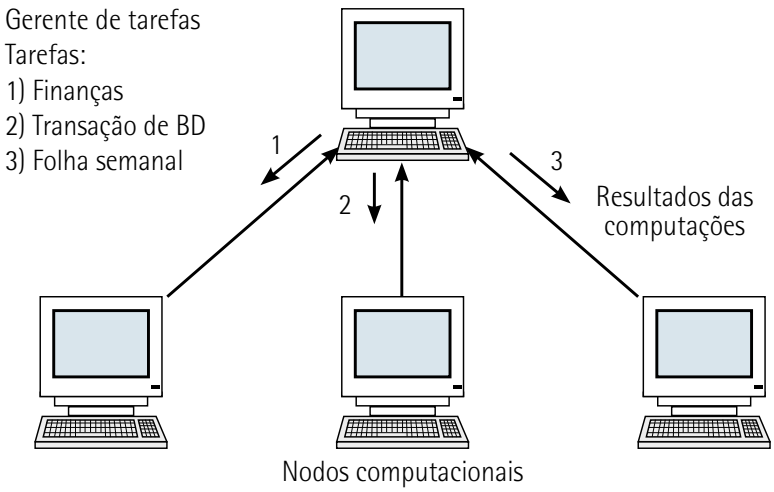

Figura 13 – *Cluster* de computação

Todavia, se o estado for inverso ao *cluster* de computação, com granularidade fina e acoplamento forte, será o sistema de processamento paralelo, com tarefas alocadas pelo gerente de tarefas e distribuídas aos nodos de computação. Logo, os nodos trocam informação devido a esse acoplamento forte. Esta estrutura possui grandes requisitos de desempenho em comparação às outras.

Planejar corretamente a capacidade dos enlaces e evitar o máximo possível de gargalos na rede é o motivo de realizar a caracterização de carga do tráfego, pois na teoria é relativamente simples, basta possuir um número de estações que geram o tráfego, o tempo médio entre quadros gerados e o tamanho médio dos quadros transmitidos, além de alguns parâmetros que ajudam a obter a carga, como a frequência das sessões de aplicações, o número das sessões simultâneas e o tempo médio de cada uma dessas sessões.

Infelizmente na prática nem tudo é tão simples quanto na teoria, pois estimar todos esses parâmetros demanda um enorme esforço e trabalho, muitas vezes tornando-se um problema, uma vez que requer conhecer as aplicações e fazer as estimativas. Existem ferramentas para modelagem das redes que têm base de conhecimento sobre certos tipos de aplicações. Elas podem ser utilizadas para que tornem possível a parametrização do modelo interno.

A seguir consta uma base do tamanho dos objetos trocados em uma sessão de trabalho.

Tabela 3 – Tamanho dos objetos em sessão

Tipo de objeto	Tamanho em *Kbytes*
Tela de terminal	4
Mensagem de *mail*	10
Página *web* (com alguns gráficos)	50
Planilha	100
Documento de processador de texto	200
Tela gráfica	500
Documento de apresentação	2.000
Imagem de alta qualidade (qualidade de impressão)	50.000
Objeto multimídia	100.000
Backup de base de dados	1.000.000

Fonte: Peterson e Davie (2013, p. 99).

O *overhead* dos protocolos deve-se a esses protocolos serem usados pelas aplicações. Vejamos a seguir o modelo que nos ajudará a fazer as estimativas.

Tabela 4 – Indicação de *overheads*

Protocolo	Detalhes do *overhead*	Total de *bytes*
Ethernet com LLC	Preâmbulo = 8 *bytes*; Cabeçalho = 14 *bytes*; LLC = 4 *bytes*; CRC = 4 bytes; *Interframe gap* = 12 *bytes*	42
HDLC	*Flags* = 2 *bytes*; Endereços = 2 *bytes*; Controle = 2 *bytes*; CRC = 4 *bytes*	10
IP	Cabeçalho sem opções	20
TCP	Cabeçalho sem opções	20
IPX	Cabeçalho	30

Fonte: Peterson e Davie (2013, p. 127).

Resumo

Nesta unidade vimos como analisar os objetivos e restrições técnicas do cliente, tornando possível a compreensão de que para fazer recomendações de tecnologias e ferramentas é necessário entender se elas podem ser aplicadas ao negócio do cliente. Observamos que a análise correta das restrições técnicas pode envolver a escalabilidade da rede, que resulta na disponibilidade, sendo disponibilidade diferente de confiabilidade, pois a confiabilidade inclui dados de acurácia, taxas de erro, estabilidade etc.

Entendemos que para analisar os riscos é necessário investigar o que pode acontecer se não houver segurança implantada, questionando quais dados do cliente são sensíveis e em caso de roubo ou modificação deles qual seria o efeito, a fim de sabermos como escolher o que deve ser feito. Vimos que se houver conflitos para a realização de algo o principal e mais importante objetivo deverá ganhar sempre, ou seja, ele servirá como critério de desempate.

Constatamos que, em projetos de expansão em uma rede existente, devem ser examinados e caracterizados detalhadamente alguns aspectos, como topologia, estrutura, identificação de falhas etc., pois para determinar a infraestrutura da rede deve-se elaborar um mapa dela, incluindo a localização dos segmentos e dispositivos de interligação, sendo preciso descobrir os métodos utilizados para nomear os dispositivos e segmentos da rede, entre outros.

Aprendemos que a caracterização deve conter mapas sobre a rede e que eles podem ser desenvolvidos pelo Microsoft Visio.

Exercícios

Questão 1. (FCC 2010) Em termos de roteamento é correto afirmar:

A) No roteamento dinâmico, todos os protocolos trabalham sempre avaliando os congestionamentos, os caminhos mais curtos e os caminhos mais rápidos.

B) O protocolo RIP escolhe o melhor caminho baseado na análise de desempenho de cada alternativa, por meio da verificação de existência de congestionamento.

C) No roteamento estático, o roteador é impedido de procurar a rota mais curta e também a rota mais rápida.

D) Procurar caminhos mais curtos é característica típica do protocolo OSPF.

E) A exemplo do RIP e OSPF, o protocolo BGP replica todas as suas tabelas de roteamento aos demais roteadores.

Resposta correta: alternativa C.

Análise das alternativas

A) Alternativa incorreta.

Justificativa: existem protocolos que não avaliam esses três requisitos. O RIP, por exemplo, só avalia a distância para decidir a rota.

B) Alternativa incorreta.

Justificativa: a afirmação é incorreta, pela mesma justificativa da alternativa A.

C) Alternativa correta.

Justificativa: a diferença primordial entre o roteamento dinâmico e o estático está na adaptabilidade. No roteamento estático as tabelas são predefinidas, ou seja, se um caminho mais curto for inserido, ele não será utilizado se não for cadastrado na tabela. Também o tráfego não é considerado. Portanto, se houver congestionamento num caminho preestabelecido, o roteador não vai buscar outro mais rápido, vai por ele mesmo. No roteamento dinâmico busca-se o melhor caminho, considerando o tráfego. As tabelas são atualizadas automaticamente e a maioria dos protocolos são de duas categorias: vetor de distância e *link state*.

D) Alternativa incorreta.

Justificativa: procurar caminhos mais curtos também é uma característica do RIP.

E) Alternativa incorreta.

Justificativa: o protocolo RIP replica todas as suas tabelas de roteamento. Os protocolos OSPF e BGP enviam atualizações e informações sobre os *links* para os demais roteadores.

Questão 2. (Cespe 2013) Acerca dos protocolos de roteamento de redes, assinale a opção correta.

A) Os protocolos da classe *link state* mantêm registros de todas as mudanças ocorridas nas redes, por meio de mensagens de *broadcast* periodicamente trocadas entre os roteadores de borda.

B) O RIP é um protocolo da classe *distance vector* que utiliza contagem de saltos para determinação da melhor rota para uma rede remota. Caso se encontre mais de um *link* para a mesma rede com o mesmo número de saltos para ambas, o referido protocolo executará, automaticamente, o *round-robin load balance*.

C) O RIP v2, diferentemente do RIP v1, não envia sua tabela completa de roteamento periodicamente. Ao contrário, ele envia somente os registros que foram alterados na última atualização por meio de *broadcast*.

D) Os protocolos da classe *distance vector* utilizam o conceito *hop*, pois, quanto maior o número de *hops* necessários para alcançar uma rede remota, mais bem classificada é a rota.

E) O OSPF é um tipo de protocolo híbrido, pois guarda características do *distance vector* e do *link state*.

Resolução desta questão na plataforma.