Unidade IV

7 PROJETO LÓGICO E PROJETO FÍSICO DA REDE

7.1 Projeto lógico da rede

Após identificar todas as necessidades e caracterizar a rede do cliente, será possível iniciar o projeto de topologia de rede realizando diversas tarefas, projetando a rede logicamente, e não fisicamente.

Existirá a necessidade de identificação dos pontos de interconexão, do tamanho da rede e de seu alcance, e dos tipos dos dispositivos para interconexão, tendo como principal objetivo projetar uma rede segura, redundante e escalável. Nesta etapa não é necessário especificar tecnologias, dispositivos e cabeamento.

Projete a hierarquia da rede, atualmente muito utilizada devido ao fato de a rede estar cada vez maior. Embora a estrutura chamada de *collapsed backbone* com o tipo de conexão estrela seja bastante usada, pois oferece facilidade de manutenção, o modelo hierárquico ajuda a desenvolver uma rede dividida, com cada parte focada em um objetivo diferente, ao contrário da estrela, em que toda a fiação vai das pontas a um lugar central.

A seguir é possível ver que a rede hierárquica trabalha com três camadas: de *core*, com *switches* e roteadores de alto desempenho e disponibilidade; de distribuição, com roteadores e *switches* que implementam políticas; de acesso, responsável por conectar os usuários com os *hubs* e *switches*.

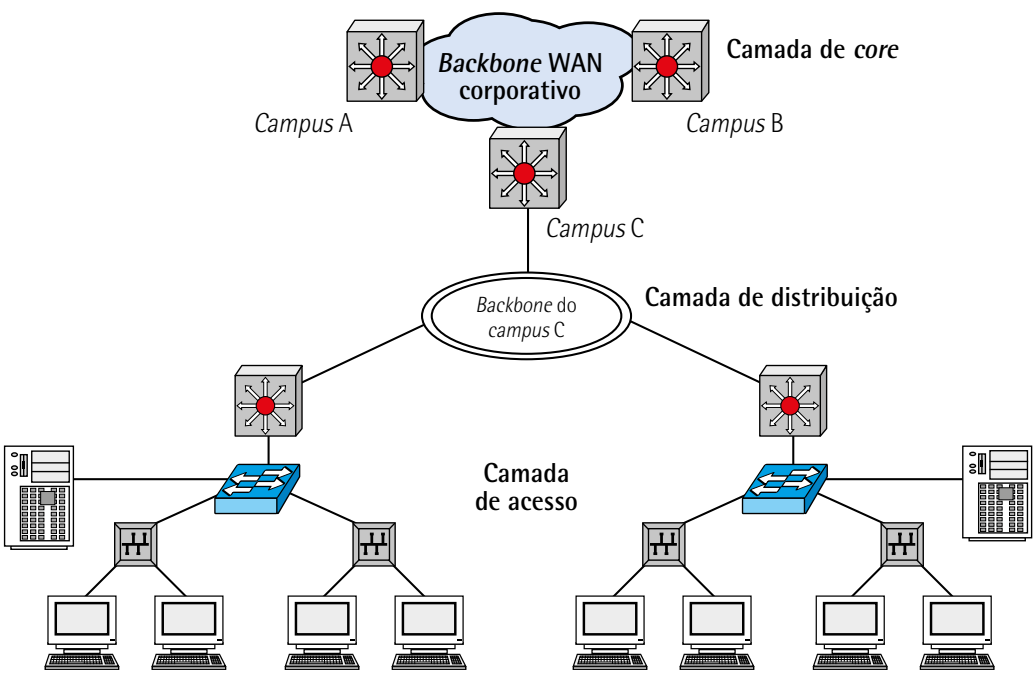

Figura 14 – Rede hierárquica

Ao analisar a topologia é possível entender que uma rede não estruturada cria várias adjacências entre os equipamentos, tornando-se ruim para propagar rotas, assim como uma rede achatada em camada 2, que devido ao *broadcast* não é escalável. Utilizar o modelo hierárquico minimiza os custos. Os equipamentos possuem funções determinadas devido a estarem separados em camadas, tornando a estrutura mais simples para testar, reparar e entender, podendo facilitar as mudanças, a replicação dos elementos e a sumarização de rotas via protocolos de roteamentos.

Utilizar redundância em uma hierarquia WAN traz maior escalabilidade, disponibilidade e baixo atraso, conforme demonstrado a seguir:

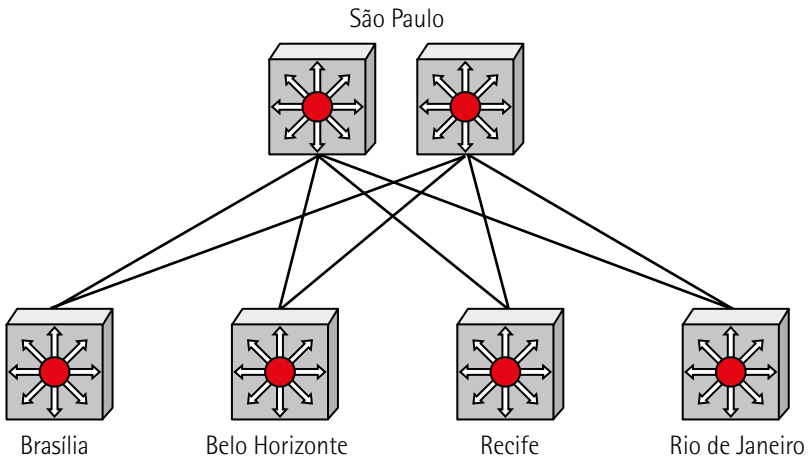

Figura 15 – Hierarquia WAN

Em uma estrutura LAN o problema básico é a perda de desempenho pelo uso de um domínio de *broadcast* grande. Implantando-se a hierarquia, os equipamentos serão usados em cada lugar de modo apropriado. Os domínios de *broadcast* podem ser delimitados se forem utilizados roteadores ou VLANs. Para maximizar a banda passante devem-se usar *switches* de alto desempenho.

Utilizar o modelo hierárquico de rede em 3 camadas permite juntar o tráfego dos três níveis diferentes, o que é mais escalável para grandes redes corporativas, sendo a camada de *core* o transporte rápido entre *sites*, ficando conectadas e aplicadas as políticas através da camada de distribuição, garantindo maior segurança, roteamento e agregação de tráfego. Contudo a camada de acesso para uma WAN são os roteadores de borda do *campus* de rede, e em uma LAN os que provêm acesso aos usuários finais.

A camada de *core* deve ser projetada para minimizar o atraso com componentes redundantes para interconexão. Devido a esta criticidade de interconexão é necessário ter um *backbone* de alta velocidade e dispositivos de alta vazão, além de evitar o uso de filtragem de pacotes.

A camada de distribuição controla a segurança por possuir muitos papéis, verificando o acesso ao recurso e o desempenho pelo tráfego que arruma o *core* e mesmo que possa ser feito na camada de acesso. Ela delimita domínios de *broadcast*.

A camada de acesso é responsável por prover aos usuários o acesso à rede nos segmentos locais, a qual geralmente faz o uso de *switches* ou *hubs*.

A fim de projetar a hierarquia em rede, controle o diâmetro da topologia inteira, para que o atraso seja pequeno, mas mantenha o controle rígido sobre a camada de acesso, pois nela os departamentos que possuem dependência implementam suas próprias redes, dificultando o funcionamento da rede como um todo, devendo-se assim evitar a adição de uma quarta camada, a qual se chama *chain*. *Chains* podem fazer sentido para conectar mais de um país em uma rede corporativa, porém causam atrasos e dependências maiores de tráfego. Também é necessário evitar a conexão entre dispositivos para a mesma camada, normalmente chamada de porta dos fundos, já que causam problemas inesperados de roteamento.

Veja a figura a seguir e entenda como funcionam *chains* e portas dos fundos.

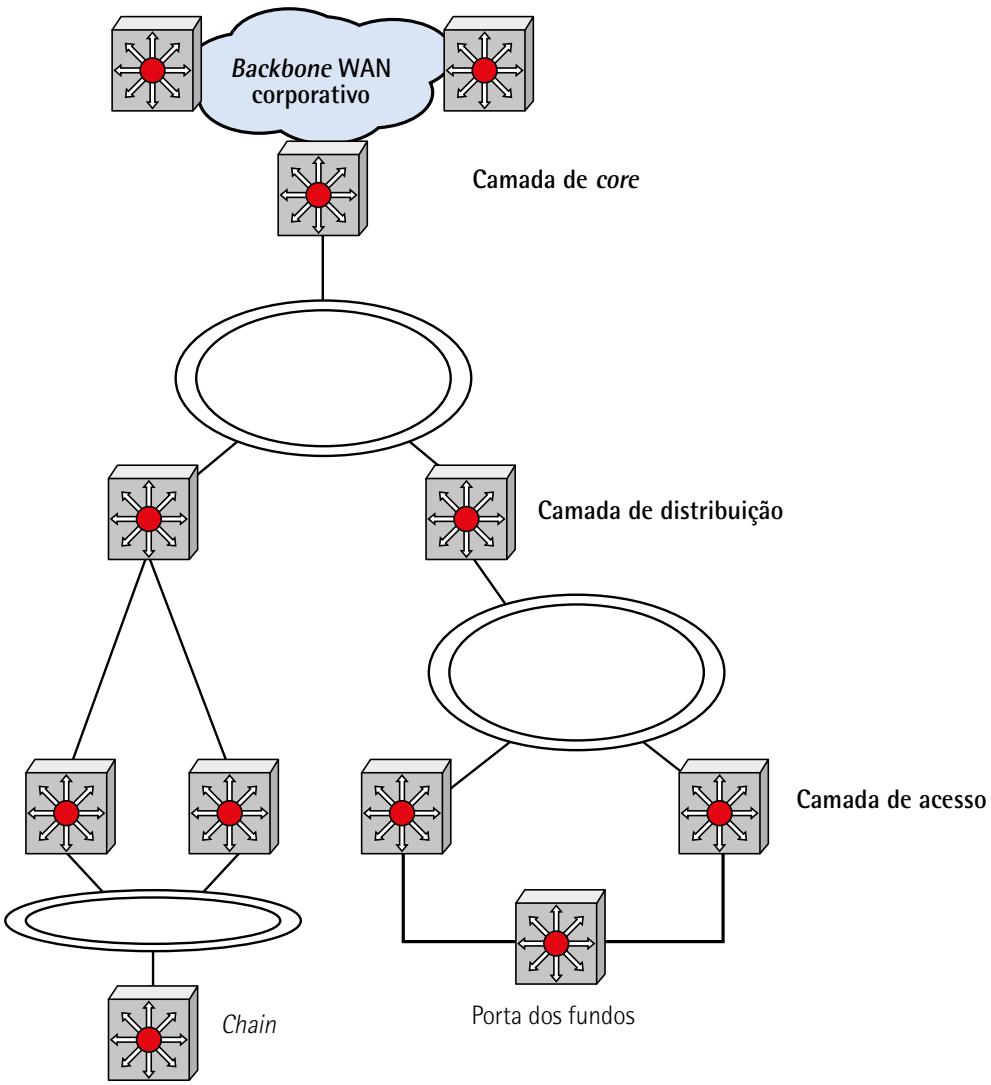

Figura 16 – Utilização de *chains* e porta dos fundos

Portanto, para facilitar um planejamento da capacidade, primeiro projete a camada de acesso, depois a de distribuição e por último a de *core*.

A redundância é a garantia de que, em caso de falha no item principal, o secundário estará disponível para utilização, assegurando a disponibilidade. Fazer topologias com redundância dos enlaces e dispositivos para interconexão em um projeto de rede torna a disponibilidade óbvia, eliminando pontos únicos de falhas.

Alternativamente, caso a redundância possua um custo muito elevado e não aprovado, para realizar o *backup* de enlaces deve-se observar a capacidade do enlace redundante, o qual geralmente possui menor desempenho que o primário. Quanto ao tempo que levará para o uso deste caminho alternativo, comumente ele muda se a troca dos *links* for manual ou se for utilizado *failover* automático. Recomenda-se o uso de *failover* automático para que os usuários não sofram interrupções de serviços.

Observação

O caminho alternativo deve ser testado sempre. Utilize-o para balanceamento de carga.

Existem considerações especiais quando o projeto é para a topologia de rede para *campus*. Devem ser mantidos pequenos domínios de *broadcast*, com segmentos redundantes na camada de distribuição, além do uso de redundância para os servidores importantes e de formas alternativas de uma estação encontrar o roteador para comunicação fora da rede de camada 2.

Um modo de configurar o domínio de *broadcast* pequeno é utilizar uma VLAN – a *virtual* LAN é configurável. Ela é criada em *switches*, fazendo com que, se eles estiverem em segmentos físicos diferentes, os usuários sejam agrupados em um domínio de *broadcast*. A função de roteamento é usada dentro dos *switches* para passar de uma VLAN a outra, tornando-se importante para empresas que não podem garantir a participação de usuários em um projeto caso não estejam localizados juntos.

Os usuários podem ser agrupados em VLANs de diversas formas, de acordo com o *switch* a ser usado, devendo ser realizadas nas portas desses *switches* por MAC *address* ou IP, até mesmo para *multicast*.

Lembrete

Cada VLAN é uma rede de camada 2 que precisamos passar para a camada 3 (rotear) a fim de cruzar as redes de camada 2.

É possível garantir a disponibilidade de uma LAN realizando a redundância por enlaces entre *switches* em que os laços são evitados através do protocolo *spanning tree* (IEEE 802.1d). Assim é fornecida redundância sem balanceamento de carga.

A redundância de servidores pode ser feita para diversos serviços, sendo mais comum em servidores DHCP e DNS, pois o servidor DNS é crítico para o mapeamento de nome das máquinas a endereços IP, e o DHCP geralmente é colocado na camada de distribuição, podendo ser alcançado por todos.

Para a topologia em uma rede corporativa, existem considerações especiais no projeto, como os segmentos redundantes de WAN e a utilização de VPN para barateá-la.

Realizar segmentos redundantes de WAN exige cuidados especiais para ter a diversidade de circuito. Caso os enlaces de redundância usem a mesma tecnologia, serão fornecidos pelo mesmo provedor, passando pelo mesmo lugar, podendo haver queda de um *link* e isso afetar outro, sendo necessário discutir essa questão com o provedor. Normalmente o uso de uma *mesh* parcial é suficiente.

A VPN permite que um cliente utilize a internet ou outra rede pública para ter acesso seguro à rede corporativa, sendo extremamente útil para criação de extranet, dando acesso a usuários móveis, quando o protocolo básico é o PPTP com técnica de tunelamento.

Em aspectos de topologia é necessário planejar a segurança física, verificando onde os equipamentos serão instalados, para prevenir acesso não autorizado, furto, vandalismo etc.

Com o intuito de alcançar requisitos de segurança utiliza-se um *firewall* responsável por estabelecer um limite entre duas ou mais redes, podendo este ser implementado de forma simples, via roteador com filtro de pacote, ou complexa, através de *software* específico, servindo para separar a rede da internet.

A topologia básica usa um roteador com filtro de pacote, servindo apenas para uma empresa com política de segurança simples. Ela pode ser vista a seguir.

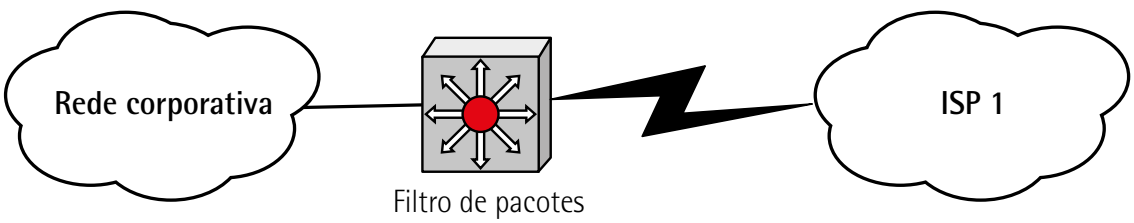

Figura 17 – Topologia básica com filtro de pacote

Privatizar o uso na rede corporativa tem sido uma forma muito comum que diversas empresas utilizam para melhorar a segurança, seja por meio de NAT, de proxy para serviços como ftp e *web* ou de máquinas em área DMZ, onde os *hosts* são bastante protegidos contra invasão e possuem *firewalls* especializados que fornecem ações especiais para implementação de políticas de segurança.

Neste padrão existem duas topologias, a serem utilizadas com um ou dois roteadores, conforme ilustrado na sequência.

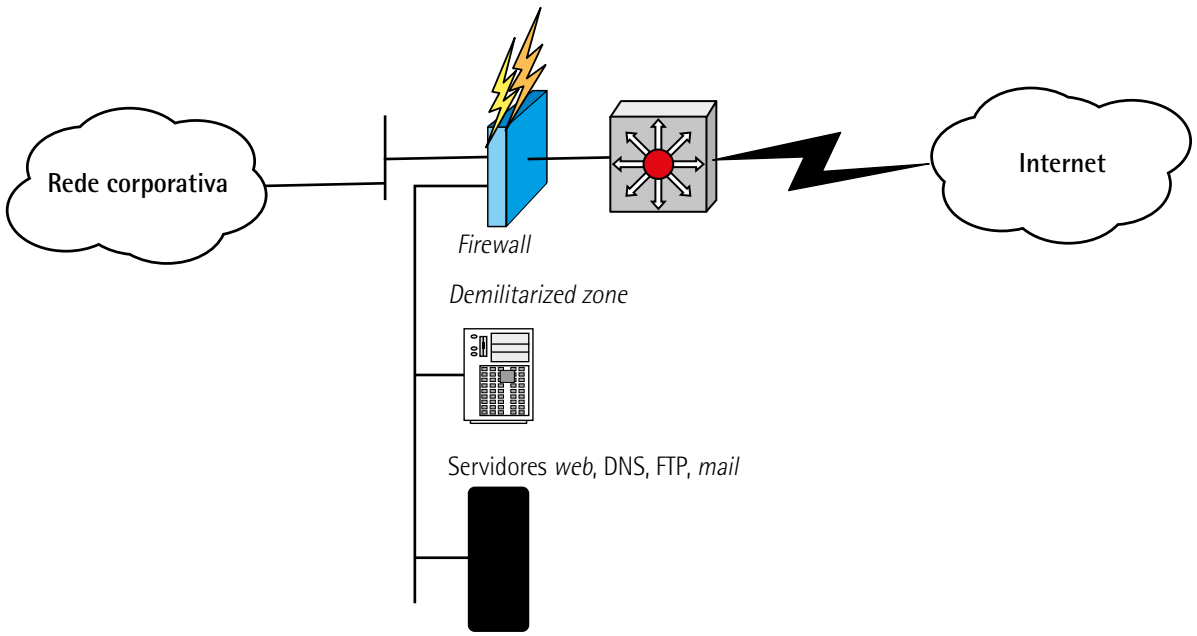

Figura 18 – Topologia com *firewall* dedicado e um roteador

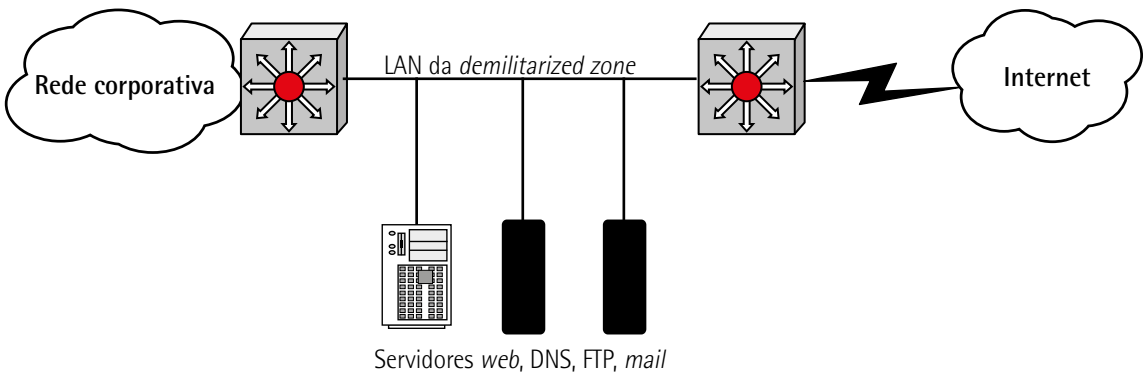

Figura 19 – Topologia com dois roteadores filtrando pacote

Com base no conteúdo desenvolvido neste capítulo dá para compreender o projeto da topologia da rede, sendo necessário iniciar o conhecimento sobre o esquema de endereçamento da camada de rede por endereços IP e nomes de recursos. O foco estará sobre o protocolo IP, que basicamente possui dificuldades de roteamento se não há um modelo estruturado e hierárquico ou se há esgotamento de endereço.

Antes de realizar a escolha de protocolos deve-se falar sobre o endereçamento, pois alguns protocolos de roteamento não suportam determinados esquemas de endereçamento, como o VLSM.

Para atribuir endereços de rede não existe um mecanismo dinâmico. Isso deve ser feito manualmente seguindo algumas regras simples, como projetar um modelo organizado para endereçamento antes de realizar a atribuição de endereço e deixar espaços para o crescimento do número de redes e hospedeiros, pois caso se ultrapasse o limite inicial será bastante trabalhoso efetuar a renumeração. A fim de melhorar a escalabilidade e a disponibilidade, devem ser atribuídos blocos de endereço de forma hierárquica, com instruções para aperfeiçoar a flexibilidade, minimizar o trabalho com configuração ou maximizar a segurança e a adaptabilidade.

Fazer o uso de um modelo estruturado para endereçamento de rede facilita a implementação de soluções otimizadas sobre tráfego de roteamento, a implantação de políticas de segurança em *firewall*, a gerência de endereços, a localização e o conserto de problemas e a operação da rede.

Realizar a administração de endereços com autoridade centralizada significa possuir o modelo global de endereço projetado por um departamento centralizado, com número de redes escolhido para a camada de *core* e blocos de endereços de sub-rede reservados para a camada de distribuição e acesso, com subdivisões estruturadas ou não. Estes blocos podem ser recebidos por entidades como Fapesp (no Brasil), ISP ou Iana. Caso haja a dependência dos endereços fornecidos pelo ISP, lembre-se de escolher um ISP que possua margem para manobrá-los, pois se tiver a necessidade de crescer uma mudança nele poderá envolver uma alteração geral de endereços. Atualmente utiliza-se com maior frequência o endereçamento privativo em redes corporativas, permitindo de modo alternativo crescer sem problemas com endereços.

A responsabilidade de escolher endereços e realizar a configuração dos dispositivos é muito importante. Portanto os profissionais que farão a administração de endereços devem ser selecionados com muito cuidado, pois se for alguém sem conhecimento da rede precisará manter o esquema de endereçamento simples, com o uso de DHCP para minimizar o trabalho.

O DHCP é uma das ferramentas desenvolvidas para simplificar a tarefa do administrador de rede e endereçar com IP as estações. Um servidor DHCP é responsável por entregar endereços IP a partir de um bloco de endereços reservados para isso, através do *broadcast*. Ele pede um endereço IP sem requerer qualquer configuração. O DHCP suporta os tipos de alocação de endereço: automático, com endereço permanente fornecido à estação; manual, com uma tabela de endereços fixos configurados manualmente; e dinâmico, no qual o endereço IP é dado à estação por *lease period* (período de tempo). O modo dinâmico é o método mais popular.

Fazer o uso de endereçamento privativo possui grandes vantagens, como a segurança, pois as máquinas não podem ligar-se diretamente na internet devido ao fato de os endereços privativos não serem roteados pela internet. Para que consigam acessá-la, precisam ter servidores com endereço público com NAT mapeando os endereços privados em públicos dinamicamente. Outra vantagem é a enorme margem de manobra para alocação de endereços, pois endereçamento privativo faz o uso de uma classe A inteira, tornando-se melhor do que a dependência dos poucos endereços fornecidos por um ISP.

A desvantagem de utilizar endereçamento privativo é que para a empresa de *outsourcing* de rede passa a ser mais difícil, pois ela necessita usar uma VPN ou instalar consoles de gerência, além de esquemas de *out-of-band*, que possuem custo muito mais elevado.

Por padrão os endereços IP são hierárquicos. A fim de diminuir a banda passante necessária para trocar tabelas de roteamento entre roteadores, eles foram divididos em parte rede e parte *host*, sendo que o roteamento utiliza apenas a parte de rede. Resumidamente isso foi realizado porque os roteadores não compreendem a topologia completa, pois não entendem os *hosts* das redes. Mesmo com esta hierarquia, ainda é necessário um pouco mais para atribuir endereços. Por isso existem vantagens em utilizar modelos como o fornecimento de melhor resolução de problemas, atualizações e gerenciabilidade, otimização de desempenho, melhor escalabilidade e estabilidade etc.

Para realizar um roteamento apenas, a parte de rede do endereço IP é usada, o que geralmente significa que ele está se baseando em classes, pois cada uma delas possui tamanho fixo de prefixo, sendo 8 *bits* para a classe A, 16 *bits* para a classe B e 24 *bits* para a classe C. O tamanho desses prefixos está junto às classes e não é transmitido nas trocas de rotas. Caso haja a necessidade de estender o prefixo, será preciso utilizar sub-redes, sendo esta uma solução local.

Esses roteamentos com classe automaticamente sumarizam as rotas para sub-redes; elas são anunciadas para as classes A, B e C para assim serem repassadas às sub-redes, permitindo o menor número de informação de roteamento.

A fim de minimizar o tráfego de roteamento dentro da rede, pode ser utilizado o CIDR, que permite fazer a sumarização de rotas de modo mais eficiente, usando prefixos menores e juntando rotas de várias classes, em vez de apenas A, B e C. A seguir veremos que o roteador pode anunciar que ele tem a faixa de IP 172.16.0.0/24 com 14 *bits* de prefixo.

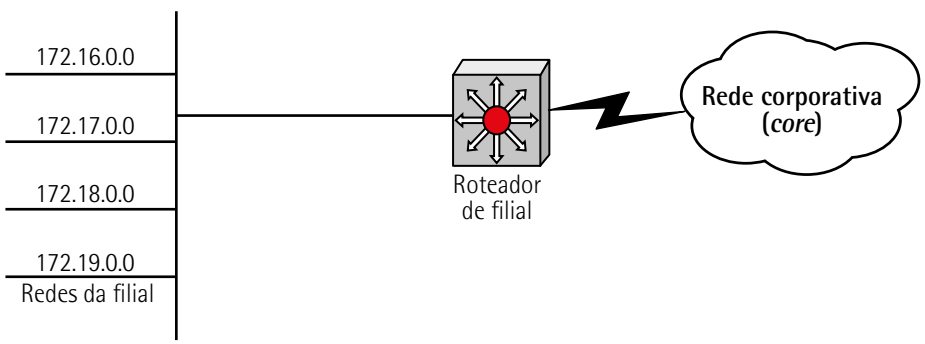

Figura 20 – Sumarização

Ao fazer o uso de roteamento com classes não é possível utilizar sub-redes não contíguas. Rede não contígua é a ação de uma rede principal separar outra principal, conforme ilustrado na sequência.

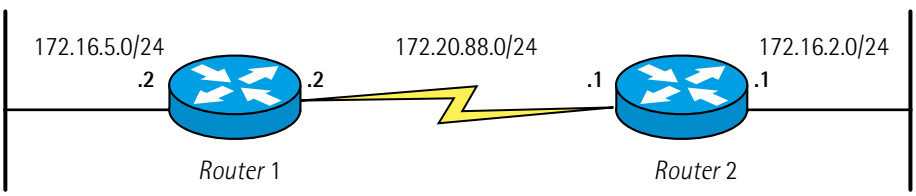

Figura 21 – Rede não contígua

A seguir observamos uma rede não contígua, que nos permite entender o uso de roteamento com classes. O roteador A anuncia que chega à rede 10.0.0.0, mas o roteador B ignora isso, pois ele também chega a ela, porém não consegue ir às sub-redes 10.108.16.0 e 10.108.31.0.

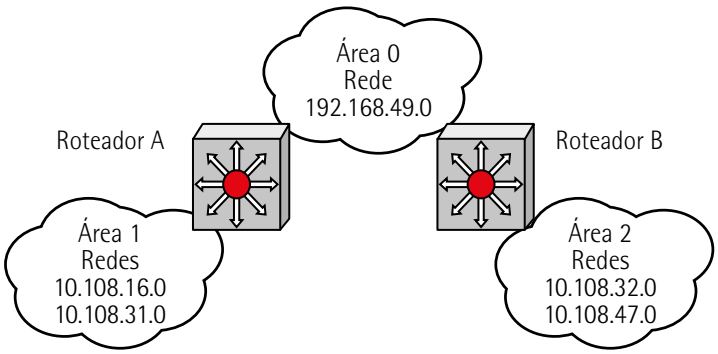

Figura 22 – Rede não contigua com sub-rede

Para preparar sub-redes não contíguas, é preciso usar roteamento sem classes.

O roteamento sem classe surgiu na década de 1990, quando a IETF introduziu um esquema com mais hierarquia no endereçamento devido ao crescente tamanho nas tabelas do roteamento de internet. Assim foi implantado o CIDR. Com o seu uso os endereços passaram a ser alocados em blocos, nos quais os roteadores agrupam para diminuir a quantidade da informação do roteamento na comunicação entre roteadores.

Segundo Hubbard *et al.* (1996), para a alocação de endereços um ISP recebe um bloco de endereços e os distribui entre os clientes conforme sua necessidade, sendo que o anúncio para a internet sai apenas de um bloco. Para utilizar roteamento sem classes, não é possível empregar os protocolos RIP v1 e IGRP, apenas RIP v2, Enhanced IGRP da Cisco, OSPF, BGP-4 e IS-IS.

Saiba mais

Para informações adicionais sobre a RFC 2050, acesse:

HUBBARD, K. *et al. RFC 2050*: best current practice: internet registry IP allocation guidelines. Virginia, 1996. Disponível em: <https://tools.ietf.org/html/rfc2050>. Acesso em: 18 jul. 2018.

Seguindo a estrutura da figura anterior, se em vez de usar o roteamento com classe for utilizado um roteamento sem classes, tanto o roteador A quanto o B anunciarão que podem chegar à rede 10.108.16.0/20. Ambos farão uso dessa informação por conseguirem analisar o prefixo e entender o que está acontecendo.

Com essa estrutura é possível inclusive dar suporte a hospedeiros móveis, que possuem endereço de IP fixo, mas podem ir de uma sub-rede a outra. A figura a seguir ilustra essa possibilidade.

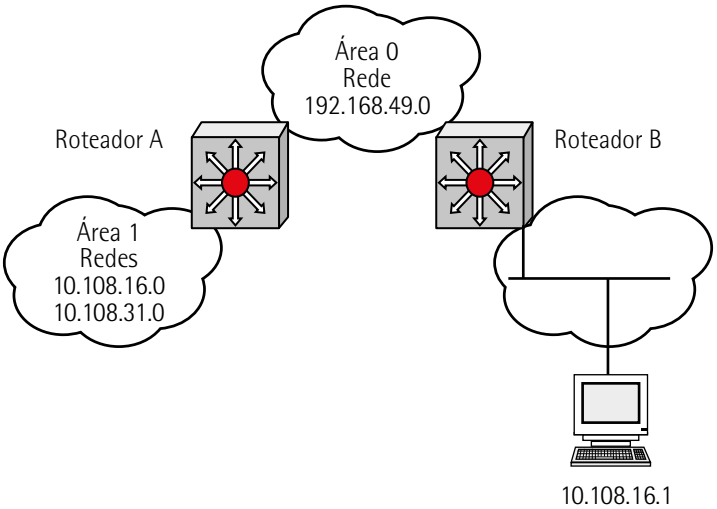

Figura 23 – *Host* móvel

Neste cenário o roteador A anuncia que pode chegar à rede 10.108.16.0/20; já o roteador B informa que pode ir à 10.108.32.0/20 e à 10.108.16.1/32, com prefixo de 32 *bits* para a rota do *host*. Desta forma os roteadores possuirão informações praticamente conflitantes: A informará ter acesso à 10.108.16.0/20 e B à 10.108.16.1/32. Felizmente a prioridade de rota é para o que possui maior prefixo.

Ao utilizar o roteamento sem classes a rede fica com a consequência de ter prefixos de tamanhos diferentes ou sub-redes de tamanhos distintos na mesma rede. Esse fato é chamado de VLSM (*variable-length subnet masking*), possuindo maior flexibilidade.

Após compreender como realizar o endereçamento deve-se conhecer e entender um modelo para atribuir nomes, pois recursos como roteadores, *switches*, *hosts*, impressoras etc. devem possuir nome.

A fim de melhorar a usabilidade, é preferível que os recursos sejam acessados por nome, e não por endereço. Com base nessa preferência precisa-se mapeá-los de modo dinâmico. Sendo assim algumas perguntas devem ser respondidas: como que recursos precisam de nomes? Nas estações de trabalho os nomes são fixos? Como é a estrutura para nomes? O tipo do recurso é identificado neste nome? Como os nomes são arquivados, gerenciados ou acessados? Quem atribui os nomes? Como mapear esses nomes aos endereços? A forma é estática ou dinâmica? Como um *host* encontra seu próprio nome? O endereço é atribuído de forma dinâmica? O nome muda se o endereço mudar? Quanta redundância é necessária nos servidores de nomes? A base de dados de nomes será distribuída entre vários servidores de banco de dados? Como este sistema para nomes afeta o tráfego na rede? A segurança da rede é impactada pelo sistema dos nomes?

A distribuição de autoridade para atribuir nomes, se aplicada com a solução centralizada, possuirá um problema onde for burocrática, tornando-se o ponto único de falha com mais tráfego na rede, ao contrário da descentralizada.

Ao atribuir nomes recomenda-se utilizar a designação do recurso no nome, como sw para *switches* ou rtr para roteadores; quando existem filiais é viável usar o nome do local com o do equipamento, como SW_SPO para um *switch* de São Paulo. Em casos de NetBIOS deve-se ter um cuidado extra com $: este símbolo esconde o nome e normalmente serve para fins administrativos.

NetBIOS é o protocolo usado em uma rede Microsoft e pode ser implementado sobre um único domínio de *broadcast* NetBEUI, TCP/IP e Novell, sendo este o mais comum atualmente.

Caso necessite empregar o NetBIOS com NetBEUI é importante saber que não pode ser uma rede grande, pois são utilizados muitos *broadcasts*. Ao usar o NetBIOS com TCP/IP, cadastro e mapeamento de nomes podem ser feitos via Wins (Windows Internet Name Service); esse servidor armazena a base de dados, permitindo o mapeamento de modo dinâmico e fornecendo o endereço à estação na resposta do DHCP.

Também pode ser utilizado o Wins com DNS (Domain Name Service). Desta forma uma estação consegue ter um NetBIOS e um nome DNS, não necessariamente iguais. Essa integração é permitida através do Windows-NT. Um ambiente IP serve-se do DNS para usar nomes.

Saiba mais

Veja mais informações sobre DNS em:

FURTADO, C. M. *Introdução ao DNS*: aprenda a instalar e configurar uma infraestrutura de DNS na prática. São Paulo: Novatec, 2016.

Nesta etapa passaremos a falar de: protocolos, endereçamento de rede, princípios básicos dos protocolos de *bridging*, roteamento e *switching*, uma vez que eles diferem quanto às características do tráfego, uso da CPU, memória e/ou banda passante, número máximo dos pares de roteadores suportados, capacidade para se adaptar de modo rápido às novas situações da rede e autenticar a atualização de rota pela segurança.

Após a escolha dos protocolos, será possível listar as características eficientes dos dispositivos selecionados.

Em qualquer tipo de projeto devem-se, de maneira geral, conhecer os objetivos do projeto, explorar diversas alternativas, entender e conhecer as consequências das decisões e criar um plano para contingência. De modo habitual, recomenda-se fazer as anotações com a utilização de tabelas, apontando pontos críticos e não críticos com classificação de prioridades.

Ao término de cada decisão, é possível verificar o que poderia dar errado, se a solução indicada já foi usada em outros clientes e se houve algum problema, como o cliente atual reagiria com a escolha e qual o plano de contingência caso a opção não seja aprovada.

Os protocolos *bridges* e *switches* são basicamente iguais, pois ambos pertencem à camada 2 e permitem o uso de portas de redes com tecnologias diferentes.

Observação

Neste ponto devemos estar familiarizados com os seguintes protocolos de *switching* e *bridging*: *Ethernet transparent switching* ou *bridging*, *spanning tree* e *transparent switching* ou *bridging* com *spanning tree*.

Em geral, ao utilizar o protocolo de *switching* para o transporte de informações entre VLANs, chama-se de *trunking protocol* quando os quadros são etiquetados com a informação da VLAN a que pertencem. Recomenda-se o uso de *switches* com suporte ao protocolo 802.1q devido ao padrão estabelecido pelo IEEE.

Ao ter de selecionar o protocolo do roteamento é necessário entender que ele faz com que o roteador veja formas de chegar a outras redes e trocar informações com outros roteadores. Por isso é mais difícil escolhê-lo do que um protocolo de *bridging|switching*. Neste caso também pode ser utilizada uma tabela de decisão.

Nos vários protocolos existentes seus algoritmos são apenas de dois tipos, *link state* e vetor de distância. No vetor de distância, é anunciado pelo roteador o espaço que há até o destino. Os protocolos que fazem uso desse tipo são: RTMP, AURP, Enhanced IGRP, BGP, IP Routing Information Protocol (RIP) versões 1 e 2, IGRP e IPX RIP. No *link state* é anunciado pelo roteador o estado das interfaces de rede que ele possui. Por ser uma tecnologia mais recente, tais protocolos convergem rápido e não geram muitos *loops* nas rotas durante a convergência, mas são mais complexos. Os protocolos que fazem parte deste tipo são: OSPF, IS-IS e NLSP.

Por serem mais velhos os protocolos de vetor de distância usam uma única métrica de *hops* (saltos). Alguns possuem um limite máximo, como o RIP, que tem apenas 15 *hops*. Os protocolos recentes podem utilizar banda passante, atraso e outras coisas, como métricas.

Existem protocolos hierárquicos e não hierárquicos de roteamento. Alguns são iguais em cada par de roteador. Outros possuem hierarquia, sendo agrupados em áreas de certos roteadores, podendo conectar duas delas e sumarizar as rotas anunciando menos informação de sua área.

O protocolo interior (IGRP, RIP e OSPF) foi desenvolvido para encontrar a melhor rota, fazendo uso de métricas em um sistema autônomo, como o de uma empresa. Já o protocolo para roteamento exterior (BGP) faz o roteamento entre sistemas autônomos; por esse motivo nem todos são anunciados, a fim de obedecer a algumas políticas de roteamento.

Existem restrições de escalabilidade em protocolos de roteamento. Muitos deles podem ser investigados quanto a esses impedimentos. Esta verificação deve ser realizada tendo como base as perguntas:

- As métricas possuem limites?
- Qual a velocidade de convergência do protocolo após as mudanças da rede?
- Para convergência em poucos segundos, OSPF pode ser um bom protocolo?
- Para atualizar uma rota, qual a quantidade de dados transmitida? Toda a tabela ou só as mudanças?
- No protocolo qual o consumo de banda passante?
- As atualizações das rotas são enviadas aos roteadores vizinhos ou a todos os roteadores em um sistema autônomo?
- Para processar as atualizações de rotas recebidas, quanto de CPU é necessário?
- É suportada a sumarização das rotas?

Após entender as restrições de escalabilidade dos protocolos para roteamento pode ser iniciado o estudo sobre o roteamento IP, quando na rede TCP/IP são mais utilizados protocolos como RIP, IGRP, Enhanced IGRP, OSPF e BGP.

O protocolo RIP, criado no início da década de 1980, foi o primeiro na internet. Ele ainda é usado por possuir simplicidade e disponibilidade em todos os equipamentos, sendo do tipo vetor de distância. Por ser antigo possui *broadcast* a cada 30 segundos para tabela de rotas e uma tabela de rotas grande, com 25 rotas por pacote.

O protocolo IGRP também foi desenvolvido nos anos 1980, mas pela Cisco, sendo ele muito usado porque os roteadores da marca estão entre os mais vendidos. O IGRP possui mais métricas que o RIP, não tem a limitação de 15 *hops*, permite balanceamento de carga e diminui a ocorrência de *loops* durante a convergência.

Em 1990, a Cisco desenvolveu o Enhanced IGRP para ser usado em grandes redes, com múltiplos protocolos de roteamento, comunicando-se com RIP, IS-IS, BGP e OSPF, tendo portanto uma convergência muito rápida e com garantia de que nela não ocorram *loops*.

O protocolo OSPF foi desenvolvido no fim dos anos 1980, pela IETF, com o intuito de substituir o RIP e ser para grandes redes. É do tipo *link state*. Possui vantagens como rápida convergência e suporte em todos os fabricantes de roteadores. Suporta redes não contíguas e VLSM, faz uso de *multicast* em vez de *broadcast*, autentica atualizações de rotas para melhor segurança e faz a propagação apenas de mudanças e não da tabela inteira.

De todos os protocolos para roteamento IP, o BGP é o único de roteamento exterior. Ele possui alto nível de complexibilidade e não deve ser utilizado em empresas pequenas.

Em redes muito pequenas é frequente o uso de rotas estáticas, mas ao iniciar o crescimento são utilizados RIP ou IGRP e OSPF. Em caso de redes maiores apenas é usado BGP entre sistemas autônomos. A seguir está o resumo de protocolos.

Quadro 3 – Dos protocolos de roteamento

	Tipo	Interior/ exterior	*Classful/ classless*	Métricas	Escalabilidade
RIP v1	Vetor de distância	Interior	*Classful*	Contador de *hop*	15 *hops*
RIP v 2	Vetor de distância	Interior	*Classless*	Contador de *hop*	15 *hops*
IGRP	Vetor de distância	Interior	*Classful*	Atraso, banda passante, carga e confiabilidade	255 *hops* (*default* 100)
Enhanced IGRP	Vetor de distância	Interior	*Classless*	Atraso, banda passante, carga e confiabilidade	Milhares de roteadores
OSPF	*Link state*	Interior	*Classless*	Custo (conforme fabricante)	Aprox. 100 áreas e aprox. 50 roteadores/área
BGP	*Path-vector*	Exterior	*Classless*	Diversos fatores configuráveis e valor de atributos do caminho	Milhares de roteadores
IS-IS	*Link state*	Interior	*Classless*	Atraso, valor de caminho configurado, erros e custo	Milhares de roteadores
RTMP	Vetor de distância	Interior	N/A	Contador de *hop*	15 *hops*
AURP	Vetor de distância	Ambos	N/A	Contador de *hop*	15 *hops* de cada lado
IPX RIP	Vetor de distância	Interior	N/A	Contador de *hop* e *ticks*	15 *hops*
NLSP	*Link state*	Interior	N/A	Banda passante e custo	127 *hops*

Adaptado de: Comer (2008, p. 454).

Quadro 4 – Convergência e consumo

	Tempo da convergência	Consumo dos recursos	Autenticação nas rotas?	Facilidade da configuração, projeto, *troubleshooting*
RIP v1	Quase grande	Memória: baixo CPU: baixo BW: alto	Não	Fácil
RIP v 2	Quase grande	Memória: baixo CPU: baixo BW: grande	Sim	Fácil

IGRP	Rápida (com *triggered updates* ou *poison reverse*)	Memória: baixo CPU: baixo BW: grande	Não	Fácil
Enhanced IGRP	Bem rápido	Memória: médio CPU: baixo BW: baixo	Sim	Médio
OSPF	Rápido	Memória: alto CPU: alto BW: baixo	Sim	Médio
BGP	Rápido	Memória: alto CPU: alto BW: baixo	Sim	Médio
IS-IS	Rápido	Memória: alto CPU: alto BW: baixo	Sim	Médio
RTMP	Quase grande	Memória: médio CPU: médio BW: grande	Não	Fácil
AURP	Rápido	Memória: baixo CPU: médio BW: baixo	Sim	Médio
IPX RIP	Rápido	Memória: médio CPU: médio BW: grande	Não	Fácil
NLSP	Rápido	Memória: alto CPU: alto BW: baixo	Sim	Médio

Fonte: Comer (2008, p. 473).

Até aqui foram descritos a topologia de rede, o esquema de endereçamento e nomes e a seleção dos protocolos de *bridging*, *switching* e roteamento. Após a compreensão desses tópicos é necessário entender como desenvolver estratégias de segurança e gerência para efetuar a conclusão do propósito.

O desenvolvimento de estratégias de segurança e gerência envolve aspectos importantes, embora sejam frequentemente esquecidos por diversos projetistas, em geral por se tratar de questões operacionais. É importante ressaltar que tais pontos não são apenas questões operacionais, pois afetam a escalabilidade e o desempenho.

Saiba mais

Obtenha informações adicionais sobre segurança de rede em:

FRASER, B. Y. *Site security handbook*. Pittsburgh: IETF, 1997. Disponível em: <https://tools.ietf.org/html/rfc2196>. Acesso em: 20 jul. 2018.

A segurança é sem dúvida o fator mais importante e tem ganhado ainda mais espaço nos projetos devido ao grande número de conexões com a internet, à formação de extranet e ao uso da rede corporativa por usuários móveis. Para implantar o projeto de segurança, devem-se identificar os recursos da rede, analisar os riscos, requisitos e *tradeoffs* de segurança, e desenvolver um plano para segurança, uma política de segurança, procedimentos para aplicar as políticas criadas e uma estratégia de implementação. Além de obter o compromisso de usuários, gerentes e equipe técnica, também é preciso treinar os profissionais, implementar a estratégia e os procedimentos de segurança, testar a segurança, caso oportuno rever as decisões e, por fim, manter a segurança realizando periodicamente auditorias independentes, com a análise de *logs*, respondendo a incidentes de segurança, atualizando-se quanto a alertas gerados, reforçando o treinamento de usuários e os testes da segurança.

Lembrete

Para a identificação dos recursos de rede e de riscos com relação à segurança, devem ser analisados os recursos de rede e os riscos associados ao acesso indevido, em hospedeiros, dispositivos ou dados transmitidos.

É possível revisar como identificar os recursos estudando a parte de segurança no capítulo de análise dos objetivos e restrições técnicas.

Em segurança existem *tradeoffs* como custos, usabilidade, desempenho, disponibilidade e gerenciabilidade. Para analisar esses *tradeoffs*, o custo da proteção contra uma ameaça necessita ser menor do que se recuperar da efetivação dela.

Para desenvolver um plano de segurança, é preciso que haja um documento de alto nível que possa especificar como ou o que a empresa fará para cumprir os requisitos de segurança. Este plano informa tempo, pessoas e demais recursos do desenvolvimento das políticas de segurança, além de como implementá-las. Ele faz referência à topologia de rede, especificando os serviços que serão providos e quem os proverá, quem poderá acessar os serviços, como o acesso será provido, quem administrará os serviços e como será o treinamento sobre aspectos de segurança.

Observação

O maior perigo da segurança está nas pessoas. Por isso todos devem ter compromisso com o plano de segurança.

Para desenvolver uma política de segurança, devem-se especificar formalmente as regras que as pessoas precisam seguir ao acessarem os recursos da empresa. Os usuários têm de possuir obrigações para manter a segurança. A referida política necessita conter componentes como: política de acesso, de autenticação, de aquisição de tecnologia de computadores e de responsabilidades. Veja mais a seguir:

- A política de acesso define os direitos de acesso, provendo regras sobre quem, quando e como pode utilizar conexões externas, sobre dispositivos na rede ou sobre adicionar novos *softwares* em máquinas ou dispositivos.

- A política de responsabilidade deve prover uma forma de fazer auditoria e reportar os problemas de segurança, definindo as responsabilidades da gerência da empresa, da equipe de operação e de usuários.

- A política de autenticação é definida pelo uso de senhas e regras para autenticação.

- Uma política de aquisição de tecnologia de computadores deve conter regras para aquisições, configurações e auditoria de sistemas de redes e computadores, mantendo a integridade da política de segurança.

Os procedimentos de segurança são desenvolvidos com o intuito de implementar a política de segurança. Eles definem os processos de configuração, auditoria, *login* e manutenção. Os usuários, administradores de rede e de segurança devem possuir procedimentos específicos, os quais precisam descrever como responder a um incidente de segurança, o que necessita ser feito ou com quem tem de ser realizado contato.

Lembrete

Os envolvidos devem sempre receber treinamento sobre todos os procedimentos.

Algumas soluções de segurança, como autenticação, autorização, auditoria, sigilo, *firewall* e filtros de pacotes, são técnicas que podem ser utilizadas como mecanismos de segurança.

O mecanismo de autenticação padrão utiliza *login* e senha, mas, para obter mais segurança, podem ser utilizados cartões de segurança para usuários remotos, ou seja, o indivíduo deve possuir duas coisas: a identificação e o cartão.

No mecanismo de autorização, o gerenciamento concede permissões facilitadas ao usar grupos de usuários, permissões essas baseadas em liberação de ingresso, geralmente por lista de controle de acesso.

O mecanismo de auditoria é o responsável pela coleta de dados sobre o uso de recursos, para descobrir se algo foi feito e quando foi feito. Geralmente entende-se por "algo" todas as tentativas de autenticação e autorização, nomes de *login*, *logouts*, mudanças de permissões, podendo incluir tentativas de penetração nos sistemas. Logo gerenciar os *logs* e revisar a política de segurança deve ser frequente.

Ter sigilo nas informações é um aspecto de segurança em qualquer segmento. Nas redes de computadores é necessário escolher a criptografia para camuflar os dados; caso não haja, são chamados de *clear text*. Geralmente utilizam-se técnicas básicas de criptografia, com chave simétrica, pública ou uma solução híbrida.

Saiba mais

Para informações adicionais sobre criptografia e segurança de redes, recomenda-se a leitura de:

STALLINGS, W. *Criptografia e segurança de redes*: princípios e práticas. 6. ed. São Paulo: Pearson, 2014.

Deve-se compreender que a filtragem de pacotes é um mecanismo de segurança, assim como o *firewall* é um filtro de pacote inteligente com definição de ações e interface gráfica.

Escolher uma solução de segurança engloba entender como utilizar os mecanismos citados, pois existem diversas soluções como: segurança da conexão com a internet, segurança de serviços da rede, segurança do acesso discado e segurança de serviços do usuário.

Utilizar a combinação de mecanismos como *firewalls*, segurança física, autenticação, autorização e *logs* de auditoria é um dos meios para conseguir segurança na conexão com a internet, sendo que apenas alguns serviços públicos podem ser utilizados sem autenticação ou autorização. A principal chave é a desativação de todos os serviços não necessários.

A segurança de acesso discado necessita da combinação de mecanismos como *firewalls*, segurança física, *logs* de auditoria, autenticação, autorização e criptografia. Os usuários remotos que utilizam o

PPP devem ser autenticados pelo protocolo Chap, pois o PAP é um sistema muito mais fraco, que envia a senha em modo *clear text*. Uma alternativa a esses protocolos é a utilização do Remote Authentication Dial-In User Service ou simplesmente Radius. Ele mantém um banco de dados centralizado, especificando o tipo do serviço permitido para usuários e senhas.

Em segurança de serviços de rede é mantida a regra-chave de desativação dos serviços não necessários. Em todos os acessos aos servidores e *switches* há a necessidade de senha, além da implementação em dois níveis de autorização com frequência. Geralmente, no primeiro nível, visualização de *status* do dispositivo e, no segundo, alteração de configuração. A fim de controlar o acesso a muitos roteadores, o Tacacs pode ser utilizado com o Radius.

Para obter a segurança de serviços do usuário partindo da necessidade da existência de uma política de senhas, as pessoas precisam aprender como escolher e quando trocar a senha, a fim de efetivar o uso dessa política, sempre deixando que suas máquinas façam *logout* automático.

7.2 Projeto físico da rede

No projeto físico da rede, é necessário selecionar os dispositivos e tecnologias. Em uma rede para *campus* devemos escolher o tipo de cabeamento que será usado, os protocolos de camadas física e de enlace, além dos dispositivos de ligação.

É importante saber que nesta fase do projeto não existe uma escolha certa, nem recomendada para qualquer circunstância. Este tópico englobará como criar o projeto físico da rede.

Em geral este planejamento do cabeamento tende a considerar que tais dispositivos deverão ser usados por vários anos em comparação a outras tecnologias.

Observação

Em vários casos, é necessário adaptar o projeto ao cabeamento existente.

Em cabeamento existem dois tipos de topologias:

- com cabeamento centralizado, com cabos em uma única área física;
- distribuído, com cabos em várias áreas físicas.

Em prédios pequenos, a arquitetura pode ser centralizada ou distribuída, pois todos os cabos não terão mais de 100 m. Já em prédios grandes deve ser implantada a arquitetura distribuída, pois cabos individuais geralmente ultrapassam os 100 m. A figura a seguir ilustra como fica a utilização das duas topologias.

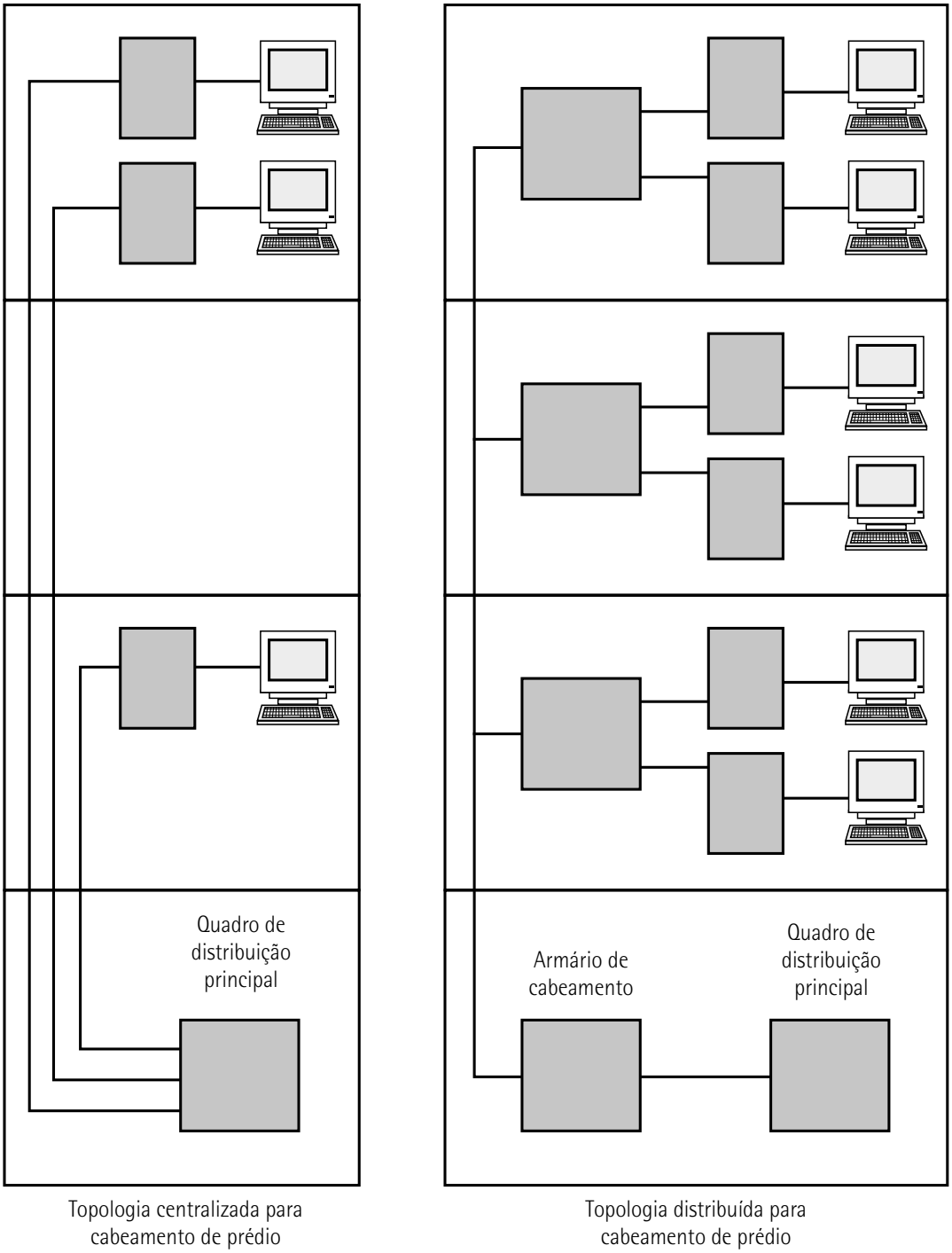

Figura 24 – Topologia distribuída e centralizada em prédios

A estrutura de cabeamento em *campus* possui muito mais perigos físicos, indo de escavações a enchentes, além de outras restrições, como cruzamento das áreas de outras empresas. Neste caso, utilizam-se tecnologias de comunicação sem fio. Por esse tipo de cenário se faz necessário ter muito cuidado quanto ao cabeamento de prédios, sendo mais complicada a realização do manuseio, mas, ainda assim, é melhor o uso de arquitetura distribuída, evitando um único ponto de falha. Veja na figura a seguir como as duas arquiteturas funcionariam em um *campus*.

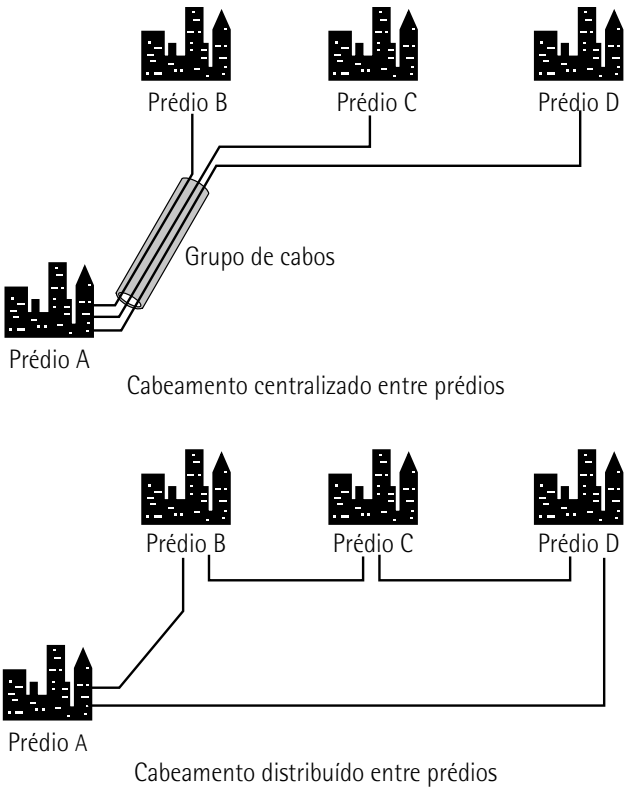

Figura 25 – Topologia distribuída e centralizada em *campus*

Os tipos de cabos que podem ser utilizados nas estruturas dos clientes são: metálicos STP e UTP e fibra ótica. O modelo de cobre possui blindagem STP e UTP sem blindagem; o UTP é o tipo mais comum nos prédios e tem diversas categorias: Cat 1; Cat 2, que não é recomendada para dados; Cat 3 (*grade voice*), tem até 16 MHz e pode ser utilizada em Ethernet 10BaseT; Cat 4, tem até 20 MHz e não é utilizada; Cat 5, de até 100 MHz, é a mais utilizada; Cat 6, tem ganhado muito espaço no mercado para a criação de redes *gibabit*.

A fibra ótica é usada para ligar prédios em cabeamento vertical, mas normalmente não é utilizada para estações, pois seu custo é muito caro. Ela possui dois tipos, monomodo de *laser* e multimodo de LED, com a vantagem de não estar sujeita a interferência eletromagnética e ruído e ainda ter alcance de 40 Gbps.

Saiba mais

Para informações adicionais sobre os tipos de cabos, leia os capítulos 3 e 4 do seguinte livro:

SHIMONSKI, R. J.; STEINER, R. T.; SHEEDY, S. M. *Cabeamento de rede*. Rio de Janeiro: LTC, 2010.

Entender sobre tecnologias LAN é essencial para escolher qual tipo utilizar em redes *campus*, pois conforme compreendido em outras disciplinas as tecnologias ATM e Ethernet são empregadas normalmente.

Selecionar os dispositivos da interconexão em uma rede *campus* é uma tarefa que neste ponto do projeto já deve estar em mente, bem como quais segmentos devem ser compartilhados ou chaveados e onde o roteamento será feito. A seguir serão exibidas as principais diferenças entre os equipamentos de interconexão.

Quadro 5 – Comparação dispositivos da interconexão

	Camadas OSI	Domínios *bandwidth*	Domínios *broadcast*	Local usado tipicamente	Características
Hub	1	Todas as portas compartilham um único domínio *bandwidth*	Todas as portas compartilham um único domínio *broadcast*	Conecta dispositivos individuais, pequenas LANs	Autoparticionamento de parar portas defeituosas
Ponte	1-2	Todas as portas compartilham diferentes domínios *bandwidth*	Todas as portas compartilham um único domínio *broadcast*	Conecta as redes entre si por SW	Filtragem dos pacotes configurada por usuário
Switch camada 2	1-2	Todas as portas compartilham diferentes domínios *bandwidth*	Todas as portas compartilham um único domínio *broadcast*	Conecta dispositivos individuais ou redes	Filtragem, portas ATM, *cut-through switching*, *multicast*
Switch camada 3	1-3	Todas as portas compartilham diferentes domínios *bandwidth*	Depende de uma estrutura das VLANs	Conecta dispositivos em redes ou individuais	Portas ATM, filtragem, *multicast*, *cut-through switching*, diversas formas para criar VLANs
Roteador	1-3	Todas as portas compartilham diferentes domínios *bandwidth*	Todas as portas compartilham diferentes domínios *broadcast*	Conecta redes	Enlaces WAN com alta velocidade, filtragem, enfileiramento especial, compressão, *multicast*, *load balancing* etc.

Fonte: Carissimi, Rochol e Granville (2009, p. 196).

As escolhas do dispositivo e fabricante são muito particulares, pois englobam diversos critérios.

Critérios gerais

- quantidade de portas;
- latência;
- velocidade do processamento;
- tecnologias LAN atendidas (ATM, Ethernet 10/100/1000 etc.);

- facilidade para configuração;
- custo;
- cabos suportados;
- gerenciabilidade (RMON e SNMP);
- MTBF/MTTR;
- qualidade e disponibilidade no suporte técnico;
- redundância de fontes de alimentação;
- documentação com qualidade e disponibilidade;
- reputação dos fabricantes.

Critérios adicionais dos *switches*

- vazão por segundo nos quadros e nas células quando ATM;
- *spanning tree* suportado;
- padronização dos protocolos usados;
- capacidade de VLANs, incluindo modos para defini-los com suporte aos protocolos *trunking*;
- suporte ao IGMP de *multicast* (para multimídia);
- autodetecção no modo *half* ou *full-duplex*.

Critérios adicionais de roteadores ou *switches* camada 3

- suporte aos protocolos da camada 3;
- suporte a *multicast* IP e RSVP;
- protocolos para roteamento;
- ação como BUS, LES, Lecs ou LES em ATM;
- funções *firewall*;
- suporte de compressão;
- *load balancing*;
- suporte para criptografia.

A seguir será demonstrado um caso de um cliente fictício chamado Universidade Paulista (UNIP), que possui 400 alunos e 30 professores (15 dos quais possuem salas fixas). Os cursos estão divididos nas áreas de Medicina, Ciências Sociais, Humanidades, Ciência da Terra, Ciência da Computação, Negócios, Matemática e Física, contando com 15 profissionais de apoio e, em tempo médio, 3 administradores de redes.

Foi identificado que, devido à deficiência da infraestrutura de computadores, novos alunos não podem se matricular. O orçamento estipulado está limitado à R$ 349.950,00 (trezentos e quarenta e nove mil, novecentos e cinquenta reais), sendo que este deve ser um projeto com baixo custo, sem administração e gerência de rede, tornando-se assim simples.

Os requisitos do negócio foram desenvolvidos com o intuito de permitir que os usuários conectem seus dispositivos móveis à rede do *campus*, tanto para navegar quanto para acessar os serviços da faculdade, prover laboratórios maiores, aumentar a matrícula de 500 para 600 em dois anos, atrair alunos que busquem faculdades com inovações e vantagens tecnológicas, reduzir as taxas de evasão de 25% para 10%, também em dois anos, além de manter (ou diminuir, se possível) o orçamento da rede em operação.

Os requisitos técnicos foram elaborados a fim de centralizar as conexões com a internet e bloquear o acesso departamental a ela, reduzir custos e facilitar a administração de serviços e servidores centralizando-os. Os servidores descentralizados não serão gerenciados e não haverá cálculo de tráfego durante o planejamento de rede, mas serão considerados. Outras exigências são: melhorar a velocidade de conexão de internet para suportar as aplicações existentes, prover segurança e proteção nas conexões, fornecer escalabilidade da rede para o uso das aplicações multimídia no futuro e padronizar a rede para utilizar TCP/IP.

Neste caso, se dispositivos com sistema operacional Macintosh se conectarem, deverão fazer uso desse protocolo ou de ferramentas que o reconheçam. Será necessário ainda que a rede possua servidores Windows com DHCP instalado, pois deverá haver portas adicionais nos *switches* para permitir que os alunos com *notebooks* se conectem à rede. É necessária uma disponibilidade de 99,90%. Será preciso que a rede possua alta disponibilidade, já que os usuários de Computação e Matemática não ficaram completamente convencidos com o projeto. Assim a alta disponibilidade evitará que eles busquem soluções próprias ou alternativas.

Existem diversas aplicações de rede em uso, como envio e recebimento de *e-mail*, acesso ao cadastro na biblioteca, navegação *web* para chegar às informações, participação em *chats*, jogos etc. e processamento de textos com impressão, além do armazenamento de dados em servidor de arquivos.

No centro de ciências e tecnologia existem aplicações que fazem a modelagem de padrões climáticos em conjunto com professores e alunos de outras instituições de ensino no estado. Existem ainda professores e alunos de Astronomia que constantemente baixam imagens gráficas do telescópio da universidade estadual com o objetivo de monitoração.

Além das aplicações mencionadas, existe um sistema acadêmico sendo executado em um ambiente Novell como aplicação de administração.

O Departamento de Artes possui a necessidade de uma aplicação nova para tornar possível a realização do *upload* de inúmeras imagens para impressão a *laser* em uma gráfica externa. O Departamento de Ciência da Computação tem um projeto de ensino EaD (a distância) em conjunto com a universidade estadual. Com essa nova aplicação, os alunos poderão receber as aulas ministradas por vídeo, o que permitirá que participem via *chat*.

A rede atual é composta de um único laboratório principal no andar térreo da biblioteca, no centro de computação e em outros espalhados. Inicialmente, isso ocorreu porque alunos e professores faziam mais uso de suas residências do que dos laboratórios. A figura a seguir ilustra esse cenário.

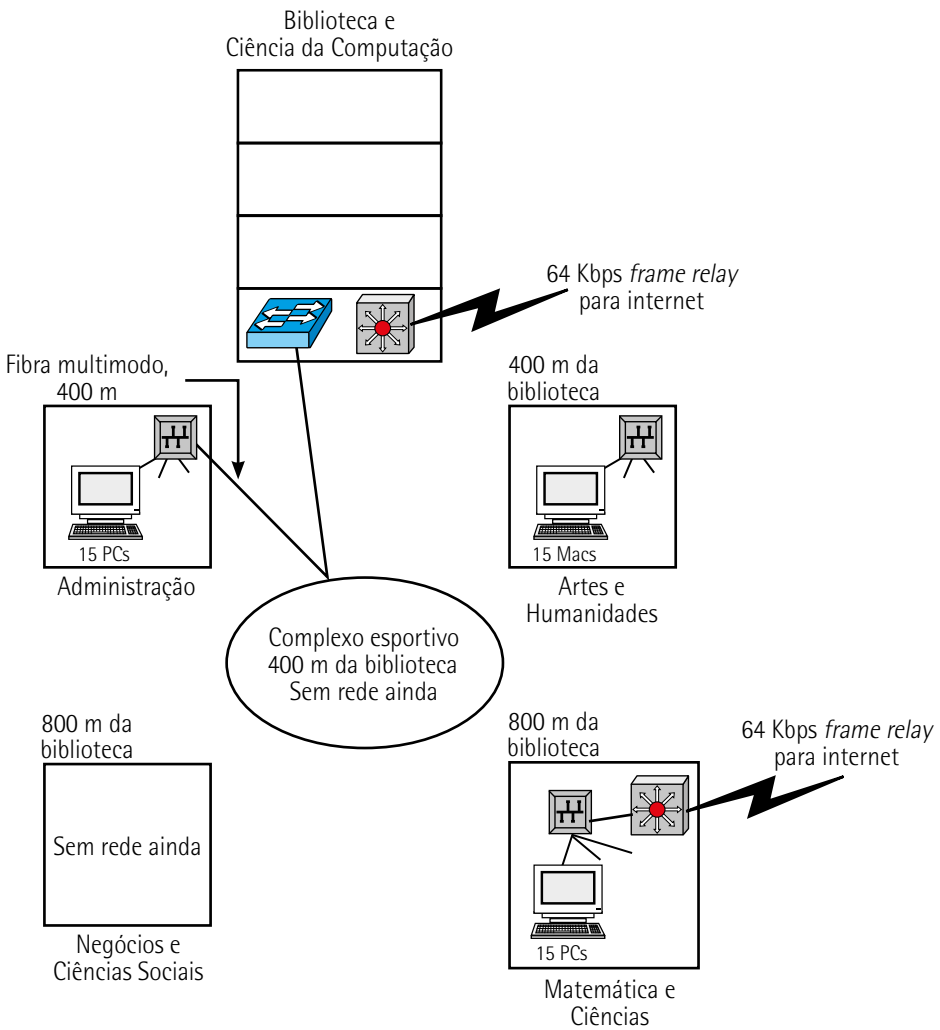

Figura 26 – Rede atual

Conforme já informado, o laboratório central da computação está na biblioteca. Nele existem 20 PCs e 15 Macs, além de um *switch* para conectar os *hubs*, servidores, impressoras e estações. A filtragem dos pacotes funciona através do roteador que não possui protocolo. Em cada andar há 5 PCs de acesso à

internet e acervo bibliotecário, sendo todas as LANs Ethernet com velocidade de 10 Mbps. Cada prédio possui cabeamento tipo Cat 5, embora alguns deles não façam o devido uso. Para compreender melhor, veja a topologia da biblioteca na figura a seguir.

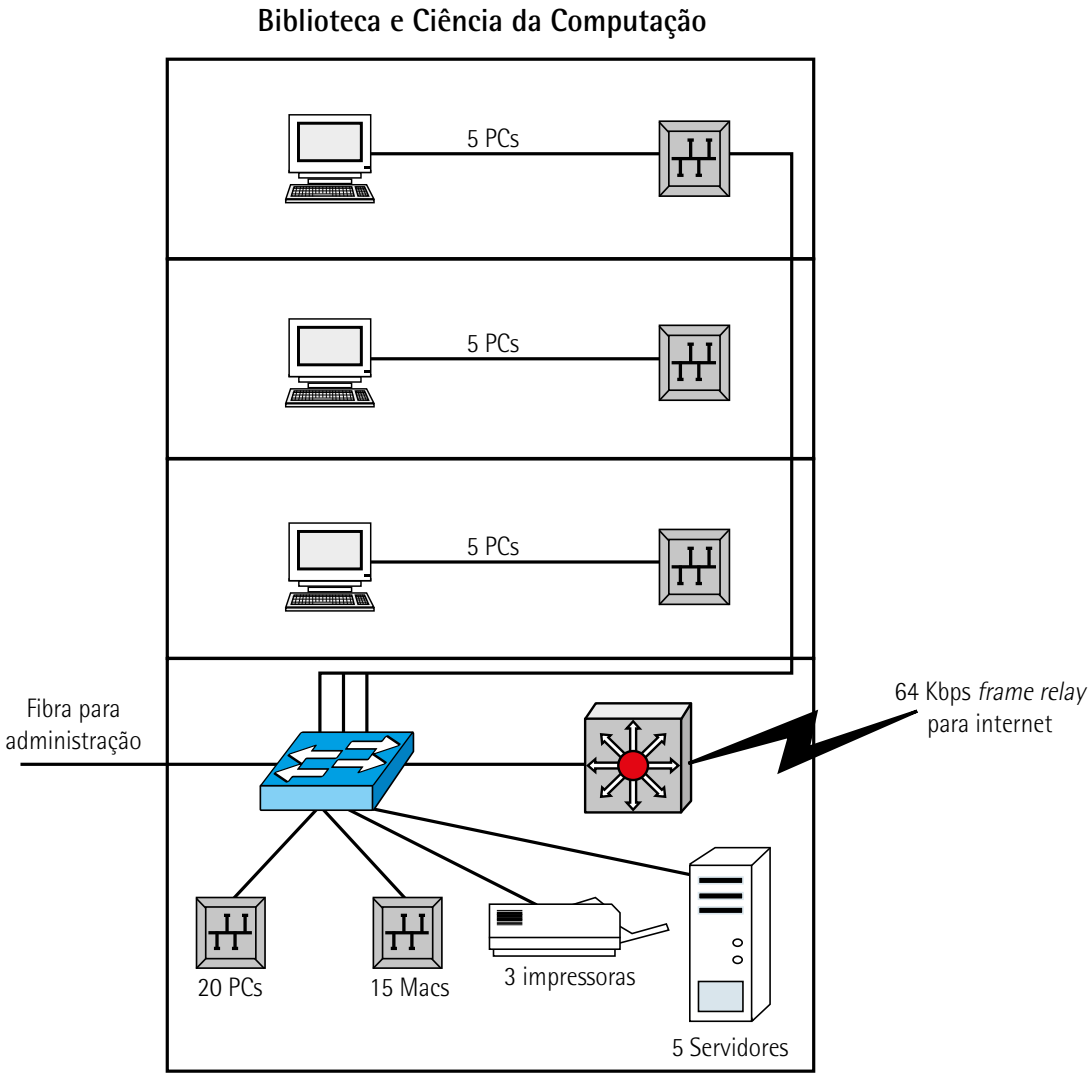

Figura 27 – Topologia da biblioteca

Os usuários da biblioteca fazem uso do *link frame relay* com 64 Kbps para através da internet chegar à universidade estadual. Para não esperarem o tempo proposto pela faculdade, os usuários de Matemática contrataram uma solução própria para conexão de internet, um *link frame relay* 64 Kbps até o ISP.

Estima-se que a comunidade de usuários cresça consideravelmente devido à implantação de novos computadores e pelo uso dos *notebooks* pessoais dos alunos. A seguir consta o resumo da comunidade no cenário atual.

Quadro 6 – Comunidade de usuários

Nome da comunidade dos usuários	Número dos usuários da comunidade	Localização da comunidade	Aplicações usadas na comunidade
Usuários de PCs do centro de computação	20, crescimento para 30	Térreo da biblioteca	*E-mail*, atividades escolares, acervo da biblioteca e navegação *web*
Usuários de Macs do centro de computação	15, crescimento para 20	Térreo da biblioteca	*E-mail*, atividades escolares, acervo da biblioteca e navegação *web*
Usuários da biblioteca	15	Andares 1 até 3 na biblioteca	*E-mail*, acervo da biblioteca e navegação *web*
Usuários de PCs em Negócios e Ciências Sociais	16 planejados	Prédio de Negócios e Ciências Sociais	*E-mail*, atividades escolares, acervo da biblioteca e navegação *web*
Usuários de Macs em Artes e Humanidades	15, crescimento para 24	Prédio de Artes e Humanidades	*E-mail*, *upload* de imagens, atividades escolares, acervo da biblioteca e navegação *web*
Usuários de PCs em Artes e Humanidades	24 planejados	Prédio de Artes e Humanidades	*E-mail*, upload de imagens, atividades escolares, acervo da biblioteca e navegação
Usuários de PCs em Matemática e Ciências	15, crescimento para 24	Prédio de Matemática e Ciências	*E-mail*, modelagem climática, atividades escolares, acervo da biblioteca, navegação *web*, monitoração do telescópio, piloto em EAD
Usuários de PCs em Administração	15, crescimento para 24	Prédio de Administração	Navegação *web*, *e-mail*, acervo da biblioteca e sistema acadêmico
Usuários externos	Desconhecido	Internet	Acesso para *site* da Nasa na *web*

Observamos o tamanho típico de objetos e *overhead* de protocolos. Além desses dois itens será necessário para levantar as características de tráfego das aplicações um analisador de protocolos, bem como fazer entrevistas com usuários.

Existem aplicações que não possuem sensibilidade com atraso, tais como *e-mail*, navegador *web*, sistema acadêmico, acervo da biblioteca e tarefas escolares. Estima-se que, com a criação de conta interna de *e-mails*, o tráfego pelo seu uso, principalmente pelo envio de anexos, seja reduzido de 80% para 60%, assim melhorando o tráfego desta aplicação.

Apesar da expectativa de redução do tráfego das aplicações existentes, as aplicações em expansão e as novas precisam ser consideradas. Na modelagem climática e na monitoração do telescópio existe um desgaste por conexão ruim com a internet. Após realizar uma pesquisa com os usuários sobre planos futuros e analisar os protocolos foi possível ver sobre o *upload* de gráficos onde não é

transferido mais de um arquivo por hora. Todos concordaram em esperar no máximo 10 minutos pela conclusão do *upload*.

Com a educação a distância fazendo uso do fluxo de vídeo direcionado apenas na recepção com a utilização dos protocolos RPT e RTSP, cada um dos fluxos consumirá no máximo 56 Kbps segundo a universidade estadual. Fora esse consumo, os alunos participarão da aula por *chat*, mas a faculdade limitará o número de usuários para assistir ao vídeo em, no máximo, 10 e eles estarão localizados no edifício de Matemática e Ciências. Futuramente será utilizado *multicast*. Nesta ocasião todos os alunos do *campus* terão acesso ao sistema.

A figura a seguir exibe o sumário das características de tráfego, bem como o fluxo de tráfegos durante o uso de pico.

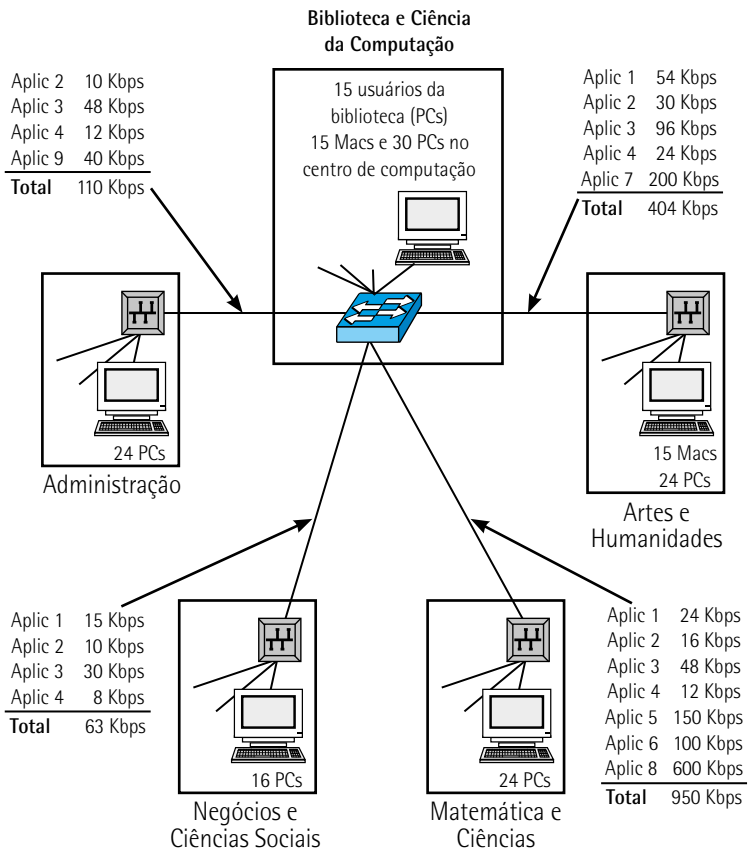

Figura 28 – Fluxo de tráfego de dados

Conforme ilustrado anteriormente, os fluxos no prédio da biblioteca estão em aplicação 1: 48 Kbps; 2: 36 Kbps; 3: 120 Kbps; 4: 30 Kbps, totalizando 234 Kbps. Para o uso da internet, os fluxos são na aplicação 2: 60 Kbps; 3: 370 Kbps; 5: 120 Kbps; 6: 100 Kbps; 7: 200 Kbps; 8: 600 Kbps, formando o total de 1.450 Kbps de consumo.

Neste cenário o projeto tem redundância de enlaces entre os prédios com a topologia lógica *mesh* hierárquica, conforme exibido a seguir.

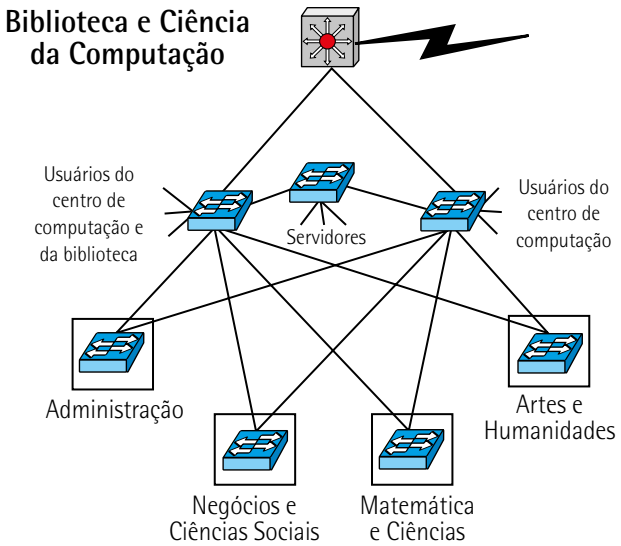

Figura 29 – Topologia lógica

Além do uso desta topologia outras decisões foram tomadas. Uma delas é que ainda serão aceitos *hubs*, mas nos casos de banda passante será utilizado *switch*, pois é melhor para escalabilidade e o custo foi aceito. Todos os dispositivos estarão na mesma sub-rede IP com o endereço que virá da universidade estadual, sendo que todos os dispositivos participarão de um único domínio de *broadcast*. O protocolo a ser executado nos *switches* será o *spanning tree*, mas os gerenciáveis utilizarão SNMP e RMON. O roteador funcionará como *firewall* simples para filtro de pacotes e não executará protocolos de roteamento.

A figura a seguir mostra que, com a topologia escolhida, será utilizada a tecnologia de camada 2 nos enlaces.

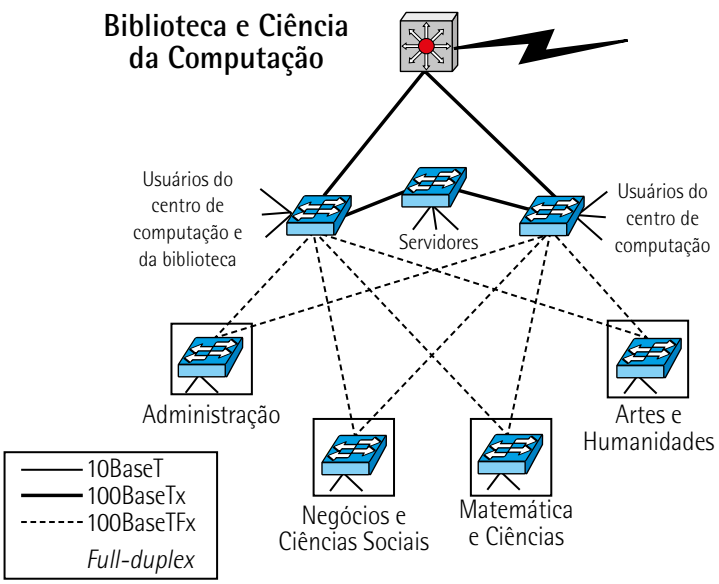

Figura 30 – Topologia física

Para esta topologia física, serão utilizados *switches* de 24 e 48 portas. A interligação dos prédios será com Ethernet de base Fx 100 *full-duplex*, pois permite enlaces de até 2.000 m. Dentro dos prédios serão utilizados *switches* Ethernet de 10 Mbps, exceto para os andares 1-3 da biblioteca, em que os 15 PCs utilizarão *hubs* de 10 Mbps, que já existem nos andares a fim de permitir a expansão no futuro para uso de aplicações multimídia. Todos os *switches* poderão ser expandidos para a implementação de VLANs e segmentação dos domínios de *broadcast*. Além disso eles suportam *multicast* IP com IGMP para facilitar o suporte às aplicações multimídia.

A segunda conexão, que está em Matemática, será desativada e passará a utilizar como enlace WAN uma LPCD E1 de 1 Mbps. Neste caso o roteador do centro de computação será substituído para dar suporte a duas portas 100BaseTx e a uma porta E1. A fim de garantir a disponibilidade, será adicionada uma fonte de energia redundante, pois este é o único ponto de falha.

A figura a seguir mostra que o cabeamento do *campus* será através da topologia estrela centralizada por fibra ótica do tipo multimodo entre os prédios.

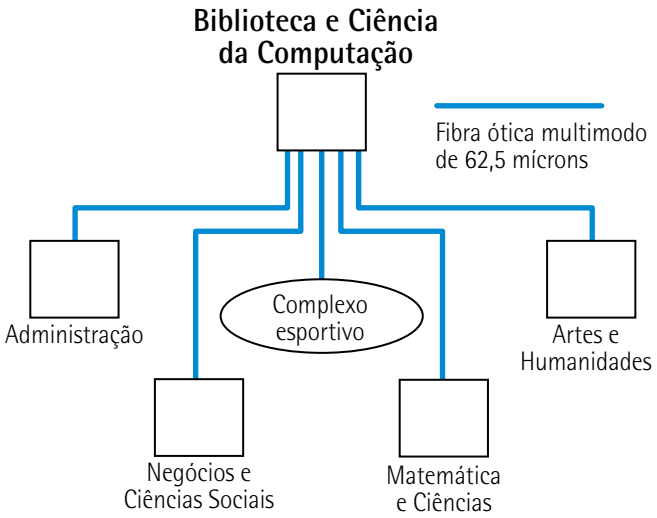

Figura 31 – Cabeamento

Desta forma, encerra-se o projeto para a rede *campus* da Universidade Paulista.

A partir deste ponto veremos como realizar a seleção de dispositivos e tecnologias para o uso de rede corporativas, nas quais será possível ver as tecnologias de acesso remoto com o protocolo Point-to-Point (PPP) com *digital subscriber line* (xDSL), e quais os dispositivos devem ser selecionados para o acesso remoto. Para tecnologia WAN, deverão ser selecionados sistemas para alocação de banda passante com redes ATM e linhas para comunicação privada de dados. Os dispositivos e provedores WAN serão selecionados com base em roteadores, *switches* e provedores de serviços.

Com base na localização de comunidades de usuários e aplicações em uso, as tecnologias a serem usadas para o acesso remoto à rede corporativa serão selecionadas conforme a necessidade, pois, caso os usuários remotos ou móveis necessitem de velocidades altas ou períodos longos, poderão ser utilizados conexão xDSL e *modems* para conexão DSL por meio do protocolo de enlace PPP.

O protocolo PPP é de ligações seriais ponto a ponto em enlace, sendo mais utilizado para conexões seriais remotas; através deste protocolo poderão se conectar à sede desde um usuário remoto até um escritório remoto com vários usuários. O PPP aceita diversos protocolos de camada de rede, como TCP/IP. Seus serviços mais básicos são: compressão de cabeçalho, detecção de erro, multiplexação dos protocolos da camada de rede, teste da qualidade do enlace, configuração do enlace, negociação de opções de enlace e autenticação via PAP ou CHAP.

Saiba mais

Para conhecer melhor sobre autenticação com modos PAP ou CHAP, leia os capítulos 5 e 6 do livro a seguir:

KUROSE, J. F.; ROSS K. W. *Redes de computadores e a internet*: uma abordagem *top-down*. 6. ed. São Paulo: Pearson, 2013.

O acesso remoto com xDSL, através do cabo telefônico normal, conecta a residência do usuário ou escritório à central com tráfego de alta velocidade. Todavia é necessário um *modem* especial em cada lado. Assim as velocidades dependerão da tecnologia DSL particular. DSL é chamado de xDSL devido a algumas tecnologias envolvidas, sendo elas Asymmetric DSL (ADSL), High-bit-rate DSL (HDSL), Very High-bit-rate DSL (VDSL), Single-line DSL (SDSL – também chamado de Symmetric DSL), Rate-adaptive DSL (RADSL), ISDN DSL (IDSL) e Consumer DSL (CDSL). Dessas tecnologias, as mais utilizadas são ADSL e HDSL.

A tecnologia ADSL possui capacidade assimétrica. Neste caso recebe muito mais do que envia. Suas velocidades são dependentes da qualidade da linha, numa distância com limite de até 18.000 pés. Há vários canais, inclusive para telefone, sendo que tudo funciona pelo mesmo cabo. Para compreender melhor, observe o seguinte.

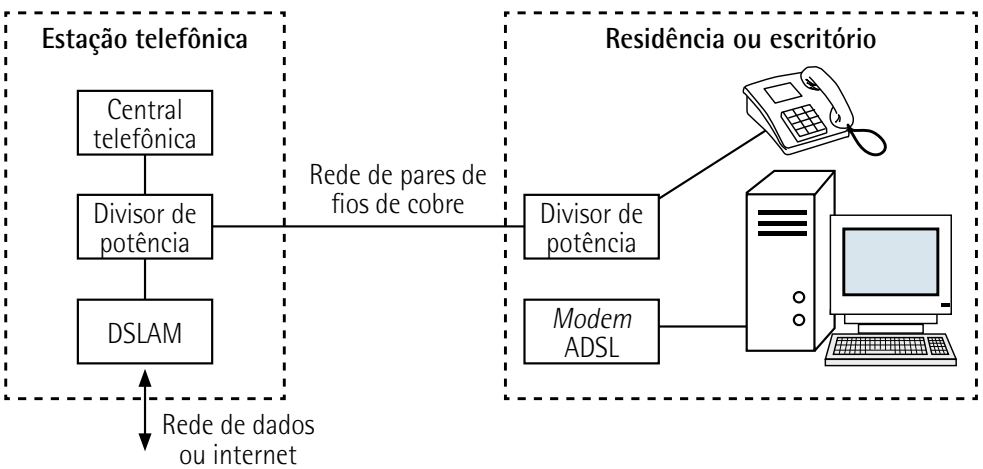

Figura 32 – Esquema da aplicação da tecnologia ADSL

A tecnologia HDSL possui capacidade simétrica de 2 Mbps, fazendo o uso de 3 pares, sendo ela uma alternativa bem mais econômica com relação ao enlace E1, com alcance de até 12.000 pés.

Para o recebimento do acesso remoto, será utilizado um RAS (Remote Access Server) como servidor de acesso. Ele possui alguns números de portas e tipos de portas, flexibilidade de configuração e módulos, suporte a NAT para *hosts* em redes remotas, suporte a DHCP e aplicações de multimídia, além de outros tipos de serviços, como: acesso remoto para terminais e estações, serviços de tradução de protocolo e serviço de roteamento assíncrono.

Acessar remotamente as estações possibilita que elas façam a conexão remota ao *site* central via PPP, Slip, ARA ou IPXWAN para Macs. Este acesso remoto para terminais é capaz de prover serviços como *telnet* e *rlogin* (Unix).

Os serviços para tradução dos protocolos servem para terminais que realizam o acesso via *host* remoto que aguardam um tipo de terminal diferente, assim como o serviço para roteamento assíncrono, que provê o roteamento na camada 3 para interligação de LANs por um enlace assíncrono.

Como tecnologia WAN para conexões a distância, existem poucas alternativas, como LPCDs, *frame relay* e ATM. Tecnologias *wireless* como satélite, rádio e celular não serão abordadas.

A LPCD (Linha Privada de Comunicação de Dados) é apenas um circuito dedicado fornecido por um provedor por um longo período, sendo este um enlace exclusivo para o tráfego do cliente que faz uso da topologia ponto a ponto com emprego frequente dos protocolos PPP ou HDLC. Entretanto, o uso dessa tecnologia não traz muitas vantagens, pois seu custo é alto, ela possui capacidade limitada e não tem flexibilidade de QoS, uma vez que não há compartilhamento de tráfego com outro cliente. Mesmo assim é uma tecnologia madura e estável.

As redes ATM são na maioria das vezes uma boa escolha para clientes que possuem grande aceleração de banda passante por demanda ou com requisitos fortes de QoS. Elas têm altas capacidades de velocidades, chegando a 9.952 Gbps com uso de fibra ótica e 34 Mbps via par metálico, sendo assim muito mais baratas que a LPCD.

Os dispositivos e provedores para a WAN devem ser selecionados com as críticas de que o *backbone* WAN faz uso de equipamentos com alto desempenho. Por esse motivo, selecione um roteador para a rede corporativa parecido com o da rede *campus*, mas com a observação de alguns itens, como alta disponibilidade, otimização de enlaces WAN avançada e alta vazão, pois neste caso de vazão a regra de 80/20 torna-se 20/80, o que gera bastante tráfego no *backbone*. Por fim, escolha um roteador com portas e tecnologias desejadas e vazão adequada.

A seleção de *switches* é importante, pois eles mudam a forma como os *backbones* corporativos são construídos, dando suporte a: ATM, *frame relay*, acesso remoto, voz, podendo ainda fazer a alocação dinâmica de banda passante a serviços como voz e dados, sendo uma boa opção para a fusão de rede de dados e voz para uma única rede corporativa.

Após realizar a seleção dos roteadores, outro fator importante é escolher o provedor de serviços WAN. Neste caso, devem ser levados em consideração: custos dos serviços, tipos de tecnologias oferecidas, tipos de serviços oferecidos, área geográfica de cobertura, SLA oferecido, se a equipe do nível de suporte possui certificação ISO 9002, disponibilidade de uma única central para todos os tipos de problemas e experiência em suporte comprovada, nível de segurança oferecido e desempenho da rede local do provedor e sua confiabilidade, sendo ainda necessário o contato com a equipe de engenharia do provedor para saber sobre a redundância da rede, os mecanismos de alocação de banda que garantem o QoS e a frequência da queda da rede.

A fim de facilitar o entendimento até esse ponto do projeto, será demonstrado um exemplo de rede corporativa de um cliente fictício chamado Buip (Brasil União Interativa de Papéis).

A Buip realiza a fabricação de produtos de papel, que vão de simples sulfite a caixas e papel-jornal. Sua sede fica em Belém, PA, porém possui 15 *sites* em todo o Brasil e conta com 1.500 colaboradores e clientes em todo o mundo. Após uma forte crise em meados de 1998 por dificuldade em encontrar matéria-prima (madeira), a empresa perdeu muito lucro com os clientes da Ásia, o que ocasionou um plano de recuperação com novos processos internos e o uso de papel reciclado.

Para que o plano de recuperação pudesse ser executado plenamente, identificou-se uma necessidade para realização de um programa de educação a distância, a fim de que todos os empregados pudessem aprender como utilizar melhor o papel reciclado, conservar melhor a matéria-prima e exercer um trabalho mais eficiente. Por ser algo crucial para a recuperação da empresa, a direção aprovou a instalação de salas para videoconferência em quase todos os *sites*. O objetivo da instituição é futuramente oferecer treinamento a outras empresas do ramo, tendo subsídios federais para treinar novamente os empregados.

Os principais propósitos do negócio são aumentar lucros através da implementação de uma WAN para apoiar o plano de recuperação com foco no uso de videoconferência, melhorar a eficiência das operações por meio do aperfeiçoamento no desempenho da WAN existente, conter os custos crescentes da operação da WAN atual e prover uma rede que permita aos empregados trocarem ideias mais facilmente sobre crescimento de eficiência e uso de materiais reciclados, além de fornecer uma nova fonte de faturamento através do sistema com videoconferência.

Os objetivos técnicos serão aumentar a capacidade e o oferecimento de QoS da rede atual para suportar o sistema de videoconferência, projetar uma rede com uso de tecnologias disponíveis através dos provedores de serviços WAN da região, uma rede com fornecimento do tempo de resposta máximo de 100 ms para aplicações interativas com disponibilidade de 99,98%, MTBF de 3.999 horas e MTTR de 1 hora, melhorar a gerenciabilidade de rede através da topologia mais simples possível, pois na atualidade há uma *mesh* complexa de circuitos de dados e voz, o que torna necessário projetar rede de escalabilidade para banda passante das aplicações futuras, podendo carregar voz no futuro.

Serão considerados aplicações da rede, sistemas de educação a distância, de modelagem financeira, de suporte à manufatura, de entrada e rastreamento de pedidos, de produção gráfica e outras aplicações.

O sistema de educação a distância fará uso de vídeo digital comprimido, de serviço bidirecional, com padrão H.320 para videoconferência. Em cada *site* serão instalados uma câmera digital e um conversor de sinal analógico para digital, e existirá um servidor de vídeo que disponibilizará os seus fluxos para acesso *on-line* e *off-line*.

O sistema da modelagem financeira faz uso de um banco de dados Oracle, localizado na matriz em máquinas Unix, que é acessado via TCP/IP pelos PCs dos analistas.

O sistema do suporte à manufatura roda em SNA terminal/*host*, sendo executado no *mainframe* da matriz em Belém. Este sistema permite que as ordens de fabricação sejam escalonadas e que haja seu acompanhamento (este é de missão crítica).

O sistema de entrada e/ou rastreamento de pedidos é utilizado pelos usuários de *marketing* e vendas. Sua execução é realizada em servidores Novell NetWare.

O sistema da produção gráfica é o único que é executado em Mac com servidores AppleShare. As outras aplicações usadas na rede são computadores que fazem uso de *e-mail*, agenda corporativa, navegação *web* e compartilhamento de impressora e arquivos.

A seguir exibiremos quais são as comunidades dos usuários e como elas estão distribuídas.

Quadro 7 – Comunidade de usuários

Nome da comunidade	Quantidade de usuários	Localização	Aplicações usadas
Sede	350	Belém	Todas
Manufatura e vendas de papel para escritórios	200	Manaus	Todas
Manufatura e vendas de caixas e papel-jornal	250	Recife	Todas
Manufatura e vendas de polpa e produtos químicos	150	Salvador	Todas
Outros pequenos escritórios de manufatura e vendas	25-75	Brasil inteiro	Todas

Na sequência veremos a representação do armazenamento dos dados e onde os servidores que os comportam estão localizados.

Quadro 8 – *Data stores*

Data store	Localização	Aplicações	Comunidades que usam
Mainframe	Belém	Sistema de suporte à manufatura	Todos os locais de manufatura
Servidores de arquivos Unix	Belém	Modelagem financeira	Departamentos financeiros de Belém, Manaus, Recife, Salvador
Servidores NetWare	Belém, Manaus, Recife, Salvador	Sistema de entrada e rastreamento de pedidos	Todos os *sites* de venda
Servidores AppleShare	Belém, Manaus, Recife, Salvador	Sistema de produção gráfica	Departamentos gráficos em Belém, Manaus, Recife, Salvador
Servidor de vídeo (novo)	Belém	Educação a distância	Todas

Atualmente a rede da empresa trabalha com LPCDs de 4 Kbps, que fazem a conexão dos 15 *sites* com a topologia *mesh* parcial. Nesta rede o tráfego de voz utiliza canais separados para o carregamento com 64 Kbps. O fornecimento de acesso à internet ocorre por um canal E1 em Belém. Ele se dá pelo mesmo provedor dos LPCDs.

Na matriz o roteador funciona como *firewall* para filtragem de pacotes. Ele possui conexão com o *mainframe* pelo CIP (Channel Interface Processor), local onde faz o encapsulamento do tráfego SNA via conexão TCP/IP na conexão WAN. Ainda o dispositivo de *core* da rede de dados tem enlaces de 64 Kbps via topologia *full-mesh*, sendo que em cada *site* o roteador conecta a WAN à LAN Ethernet local.

Para compreender melhor a estrutura, veja a figura a seguir.

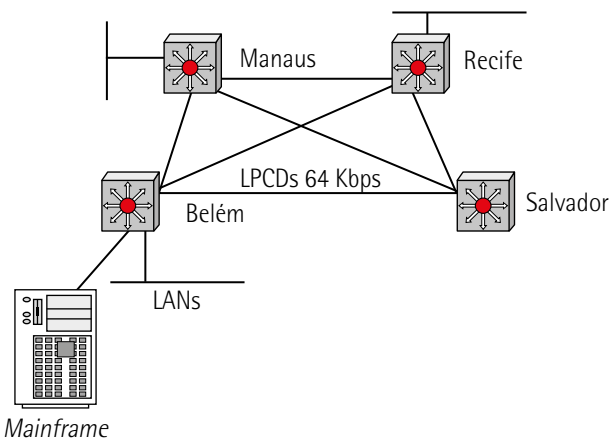

Figura 33 – *Full-mesh* atual

Esta rede possui como característica atual do tráfego de WAN um baixo desempenho, que tem piorado com o crescimento da empresa. Existem reclamações dos usuários sobre a lentidão da rede, sempre entre 10h e 11h da manhã. O grande problema de acordo com o sistema da manufatura seria a lentidão no tempo de resposta, que pode chegar a 3 minutos.

Com o intuito de medir a utilização dos enlaces de 64 Kbps foi empregado um analisador de protocolos WAN em cada *site* importante para a empresa. Por meio dele foi possível observar que em Belém os circuitos estão com o uso acima de 80% no período de medição em uma janela de 10 minutos. Na *full-mesh* os outros enlaces estão acima de 70%.

Durante a medição foi identificado que não há problemas sérios sendo causados por protocolos em particular. As aplicações estão usando janelas e quadros grandes. Assim o tráfego de *broadcast* é de aproximadamente 5%, o que aparenta normalidade. Já a taxa de erro está dentro do aceitável.

Os roteadores de *core* da rede são da Cisco e não apresentaram problemas de CPU nem de *buffers*, mas os *frames* nas interfaces estão com cerca de 5% descartados, devido ao grande fluxo de tráfego. Concluiu-se que o único problema da rede é a enorme demanda de tráfego para a capacidade instalada.

Os *sites* serão conectados à rede ATM por um *switch* específico para isso. Ele terá suporte a E1 e a E3 de 34 Mbps para um futuro crescimento. A fim de conectar ao roteador e ao equipamento de videoconferência em cada *site*, o *switch* possui duas portas de fibra a 155 Mbps. Além desses recursos, ele é capaz de tratar o tráfego de voz, mas no futuro as centrais PBX se conectarão ao *switch*. A partir daí a rede de voz será realizada por fora da operação, uma vez que dados e voz utilizarão a rede ATM, diminuindo os custos de operação e facilitando a gerência.

A figura a seguir ilustra como ficará a rede ao final da implantação.

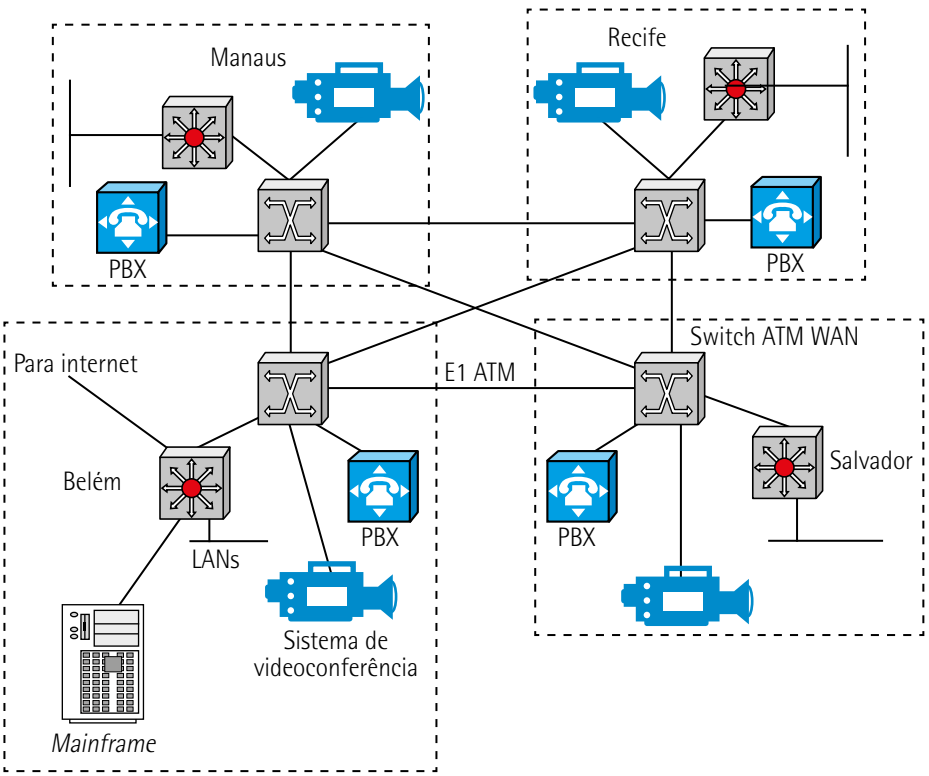

Figura 34 – Nova estrutura de rede

Após todo o desenvolvimento realizado neste curso, é possível compreender e criar um projeto físico e lógico para uma rede.

8 TESTES E DOCUMENTAÇÃO DO PROJETO

Em qualquer área de negócio, todo serviço realizado deve ser testado, pois os testes comprovam o funcionamento para quem o executou e para o cliente. Portanto testar o projeto da rede provará que se atingiram os objetivos técnicos e de negócio.

Em projetos existem diversas ferramentas prontas que servem para teste. Recomenda-se realizar alguns específicos na rede, desenvolvendo assim a construção de um modelo que possa calcular o desempenho.

De acordo com os objetivos dos testes é possível selecionar os procedimentos e ferramentas que serão utilizados. Vejamos os mais comuns:

- analisar e concluir se o projeto atende aos objetivos de maior importância para o negócio;
- validar a escolha de dispositivos e tecnologias LAN e WAN;
- confirmar se os serviços prometidos pelo fornecedor estão de acordo;
- identificar se há gargalos ou falta de conectividade;
- realizar testes de redundância na rede;
- verificar se há efeitos com as quedas dos enlaces no desempenho;
- escolher técnicas para otimização (RSVP, *multicast* etc.) a fim de satisfazer objetivos do desempenho;
- realizar uma análise *what-if* para saber se os efeitos das atualizações dos enlaces ou dispositivos afetam o desempenho;
- comprovar que este projeto é o correto, e não o do concorrente (se o cliente pedir a comparação);
- convencer os gerentes e interessados sobre a eficácia do projeto;
- constatar os riscos que dificultarão a implementação e planejar as contingências.

Alguns fabricantes, revistas especializadas ou laboratórios privados publicam testes comparativos. Eles geralmente verificam dispositivos comuns, mas os resultados podem ser utilizados apenas em redes similares àquelas que sofreram as avaliações, pois naquelas de maior complexibilidade devem ser feitas análises do sistema como um todo. Indica-se a realização de testes próprios.

A fim de elaborar um protótipo próprio, existem algumas tarefas que são necessárias para que se verifique e comprove o comportamento da rede.

Observação

Ao elaborar um protótipo deve-se ter em mente que ele necessita ser apenas funcional, e não a implantação completa da rede.

Para determinar o que será feito pelo modelo, deve-se pensar o quanto é necessário da rede para que ele possa demonstrar ao cliente que seu projeto atende com satisfação os requisitos. Os aspectos considerados importantes e que envolvem riscos, como as restrições técnicas ou de negócio, devem ser isolados e demonstrados. Recursos como: equipe técnica, tempo e dinheiro serão os responsáveis por definir o alcance do modelo. Ele pode ser implantado de várias maneiras, mas recomenda-se fazê-lo em um laboratório com uma rede para testes, pois é possível acertar falhas, verificar a capacidade de equipamentos novos e ajustar as configurações iniciais dos dispositivos. Há ainda como executá-lo em rede, integrado à produção, com testes dentro ou fora do horário de funcionamento.

Entretanto os testes finais devem explicitamente ocorrer no ambiente de produção no horário de funcionamento, mas neste caso a equipe de testes precisa se atentar a alguns itens importantes, como a necessidade de avisar a todos os usuários antecipadamente sobre os momentos em que ocorrerão os testes, apenas para que estejam cientes se o desempenho de rede diminuir, não para que parem de trabalhar, pois o ambiente precisa estar em produção para que a eficiência seja testada. Devem-se informar os administradores da rede para que não façam testes próprios no mesmo período. Os operadores de rede têm de ser informados para que não estranhem novos alertas inesperados em seu gerenciamento.

Os testes precisam ser realizados de forma gradativa. Todos eles devem ser monitorados para identificar se os objetivos foram alcançados e se houve impacto fora do previsto na rede.

Assim como na criação de todos os itens deste curso, será preciso elaborar um plano – neste caso o plano de testes de modelo do projeto, pois, após a decisão do escopo, ele deverá ser escrito.

O plano para testes deverá conter os objetivos dos exames, seus tipos, os critérios para aceitação, o cronograma de projeto dos testes, o *script* do teste e os recursos ou equipamentos obrigatórios para sua execução.

Para elaborar os objetivos de testes, deve-se compreender que tais fins fazem parte do passo mais sério e eles têm de ser específicos e concretos, além de possuir os requisitos de aceitação. Os métodos podem ser baseados tanto nos objetivos técnicos quanto nos de negócio que foram levantados para o projeto, uma vez que o cliente e o testador precisam estar de acordo com o significado dos critérios. Não pode haver dúvidas sobre um teste ter sido bom ou ruim. É preciso que ele seja fundamentado no comportamento da rede atual, utilizando itens-base como a redução do tráfego de *broadcast* para N%.

Temos de determinar quais tipos de testes serão realizados. Os básicos são: testes do desempenho, de estresse e de falhas.

Saiba mais

Obtenha informações sobre testes de redes ao ler da página 215 à 328 do seguinte livro:

MCNAB, C. *Avaliação de segurança de redes*. São Paulo: Novatec, 2017.

O teste do desempenho é responsável por caracterizar vazão, atraso e sua variação, tempo de eficiência e resposta da rede; o teste de estresse faz o aumento da carga para a deterioração do serviço; a caracterização da acurácia de rede e da disponibilidade é realizada pelo teste de falhas.

Além de realizar os testes, documentar os equipamentos da rede e todos os seus recursos é extremamente importante – por exemplo, mapa da rede, lista dos dispositivos, enlaces, outros equipamentos e ferramentas; ademais, aplicações específicas que melhoram a eficiência dos testes e recursos, como o auxílio dos usuários, parceiros, nomes ou endereços IP e tempo de laboratório.

Em cada teste realizado deve ser elaborado um *script*, listando todas as etapas da execução. A sua função é identificar como e quais ferramentas foram utilizadas para medição, além de verificar quais os valores de início, para assim parametrizar os testes, ou como eles podem ser alterados.

A seguir consta um cenário para execução de testes.

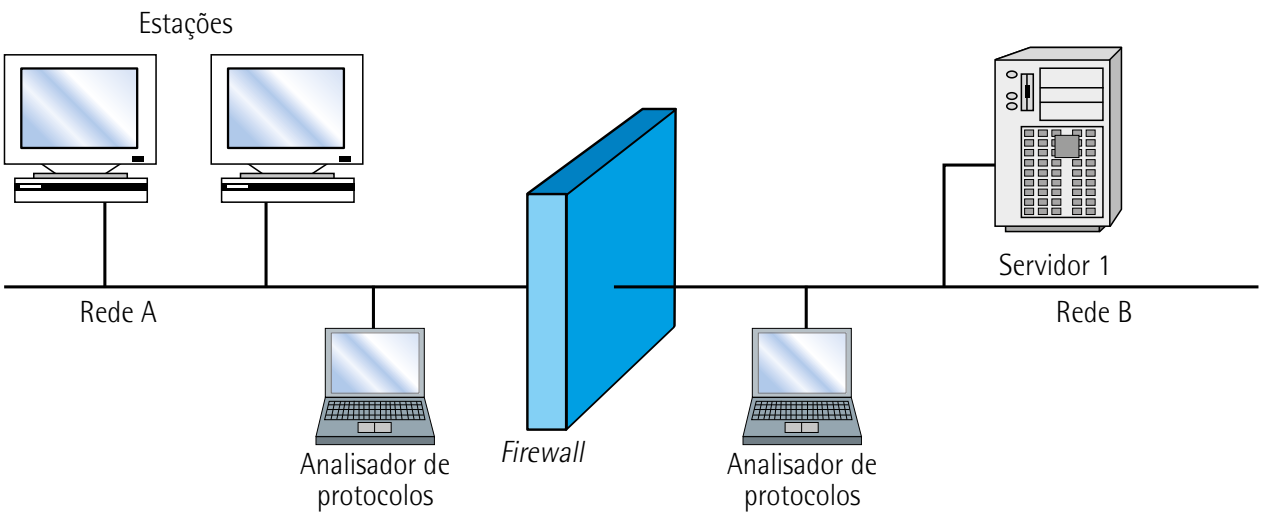

Figura 35 – Cenário de teste

O objetivo dos testes é avaliar se há capacidade para bloquear o tráfego realizado pelo *firewall* de uma aplicação denominada JAS. Ele se dará em duas condições: leve e meio pesado. O critério para aceitação dos testes será que o pedido do início de conexão/sincronização TCP (SYN) seja bloqueado no *firewall*; se alguma estação na rede A tentar acessar a JAS no servidor 1 pela rede B também será impedida e retornará com o *reset* TCP(RST).

Esse teste iniciará com a captura do tráfego da rede A através do analisador dos protocolos, que fará o mesmo com a rede B. Na sequência a aplicação JAS será utilizada pela rede A com o objetivo de acessar o servidor 1 da rede B. Após essas etapas, a captura realizada pelos analisadores de protocolos será interrompida para que eles possam exibir os dados coletados na rede A, de modo que torne possível verificar se foi capturado o pacote TCP(SYN), observando se o destino deste pacote está correto e se a porta utilizada foi a 58599, porta aplicação JAS, e, por fim, se o *firewall* está respondendo com o pacote TCP(RST).

Depois das verificações os resultados devem ser salvos com os arquivos do rastreamento dos analisadores no diretório determinado. Este processo precisa ser repetido com o aumento gradual da carga nos *firewalls* de 1 a 50 máquinas da rede A, tentando realizar acessos ao servidor.

Após o desenvolvimento do *script* é necessário também que haja um cronograma para testes, pois muitas vezes um projeto com testes complexos pode ultrapassar uma semana. Se houver um cronograma que indique a data de início e término das tarefas e quem são os responsáveis por elas, será muito mais prático de acompanhar e de demonstrar organização para o cliente.

Algumas tarefas comuns de cronogramas são: escrever os critérios para aceitação e os objetivos dos testes, analisar e revisar resultados, mostrar resultados ao cliente, arquivar corretamente os resultados, projetar uma topologia adequada para testes em um ambiente, determinar *softwares* e *hardwares* necessários para testes, escolher quais ferramentas utilizar nos testes, determinar e providenciar outros recursos essenciais, desenvolver *scripts* para testes, instalar o *hardware* e configurar o *software*, iniciar testes e, caso necessário, reduzir os dados dos resultados e gerar um pedido de compra de *hardwares*, *softwares* e ferramentas dos testes.

O segredo para implementação do plano dos testes é segui-lo fielmente.

Após todo esse desenvolvimento documental, é necessário saber quais ferramentas serão utilizadas para checar a rede. Estes tipos de testes podem ser realizados com basicamente três ferramentas: gerência de nível de serviço, gerência de monitoração de rede e ferramentas de simulação e testes.

Como ferramentas de gerência e monitoração utilizam-se Cisco Prime LAN Management Solution e HP OpenView. Ambos permitem a obtenção de diversas informações de tráfego, *logs* e erros em geral. Caso não dê para utilizar as ferramentas mencionadas é possível ainda, conforme o roteador, usar os comandos nativos naqueles que geram informações equivalentes, como *show buffers*, *show interfaces*, *show processes* etc., e, por fim, conforme demonstrado, os analisadores de protocolo também são uma opção.

Saiba mais

Obtenha dados adicionais sobre a ferramenta Cisco Prime na página a seguir:

CISCO. *Informações*. [s.d.]. Disponível em: <https://www.cisco.com/c/pt_br/support/cloud-systems-management/prime-lan-management-solution/products-licensing-information-listing.html?dtid=osscdc000341>. Acesso em: 18 jul. 2018.

As ferramentas para gerência de nível de serviço analisam o desempenho das aplicações em todo o seu ciclo de funcionamento fim a fim, englobando os requisitos de QoS. Por sua vez, as ferramentas que são especiais para teste e simulação podem ser úteis se o custo-benefício for melhor do que realizar os testes em uma rede real, mas de modo geral é muito difícil comparar a simulação com o ambiente existente.

Para melhorar a compreensão dos testes, será exibido a seguir o exemplo do cliente Klaus Corporation. Trata-se de uma empresa que projeta e confecciona circuitos especiais e integrados para equipamentos eletrônicos, possui uma rede *campus* de 4 prédios, sendo 3 próximos e o outro a 5 km de distância. Sua equipe de colaboradores está dividida em 4 setores (vendas, finanças, *marketing* e engenharia), totalizando 400 empregados.

O projeto para esta empresa tem como objetivo de testes determinar o desempenho e a carga da rede atual com foco no *backbone* de FDDI e estabelecer se poderá ocorrer algo com relação ao desempenho desta rede, além de verificar a possibilidade de aplicar uma nova entrada com base em Oracle se for executada por cerca de 10 a 20 colaboradores. Atualmente, não há monitoramento de *performance* na rede, apenas alertas gerados pelo OpenView.

Na rede estão em execução aplicações padrão de escritório, aplicações em CAD para projeção dos circuitos. Elas fazem pequenas edições no arquivo principal, salvo no servidor. Caso precisem ocorrer grandes alterações, serão realizadas no PC local e, em todo término de dia, efetua-se a sincronização dos arquivos através de um programa que roda em todas as estações, salvando os itens novos ou recém-modificados no servidor novamente. Tais arquivos não podem ultrapassar 20 Mb.

A seguir observaremos que a rede atual possui um *backbone* FDDI que faz a conexão entre os prédios A, B e C; apenas o prédio D está ligado por 2 enlaces paralelos E1 de 2 Mbps de fibra ótica, com um canal de *frame relay* de 64 Kbps e acesso às filiais domésticas, além de um de 128 Kbps com o objetivo de conectar às filiais da Europa. A comunicação com a internet sai pelo prédio 2 em um *link* de 64 Kbps. Nesta estrutura os servidores são conectados diretamente ao *backbone* FDDI, mas os PCs estão ligados a um segmento 10BaseT, enquanto as estações Sun a 100BaseTx.

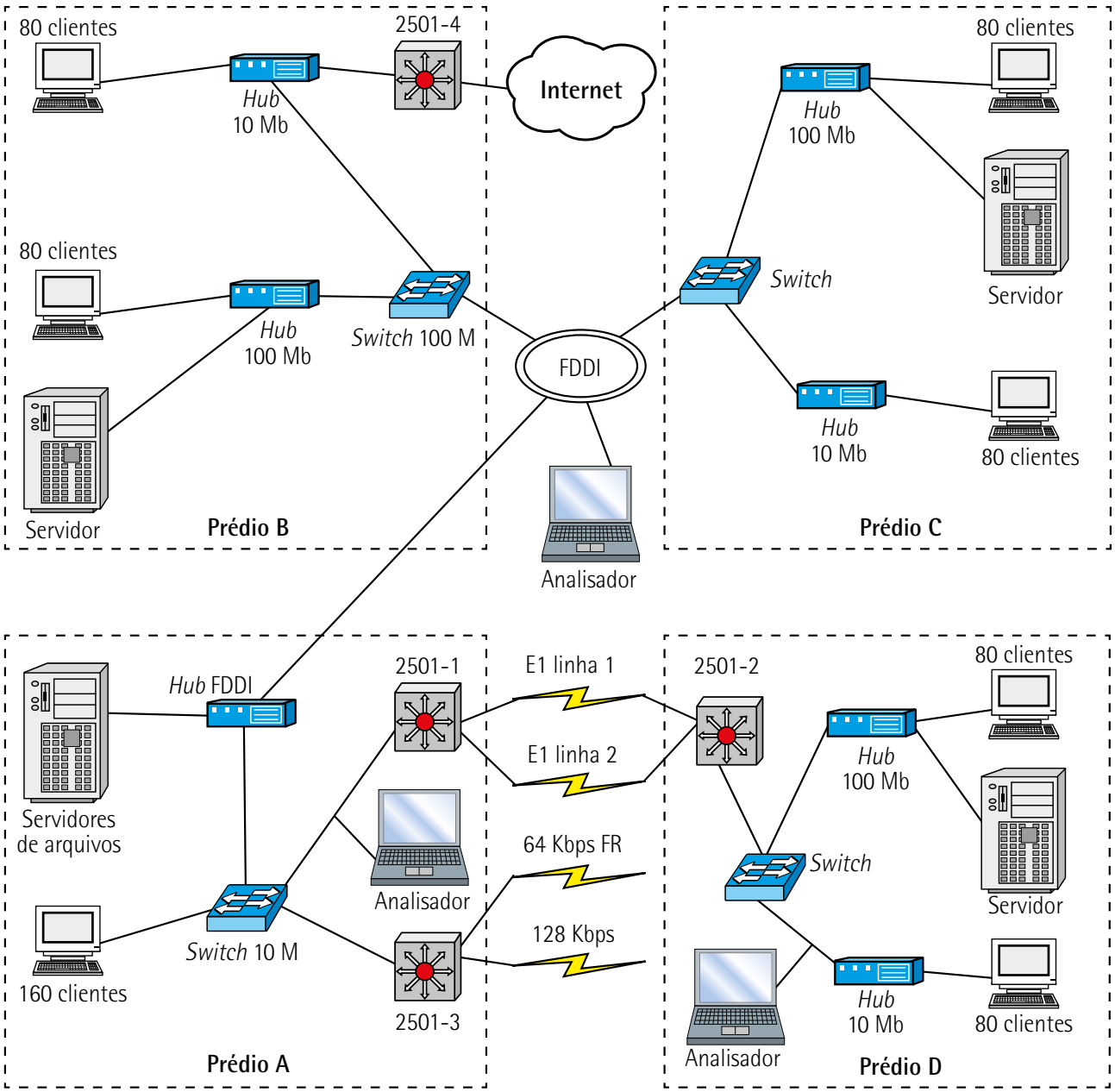

Figura 36 – Rede atual da Klaus Corporation

Neste cenário os testes utilizados ocorreram através de um plano escrito com os objetivos específicos de medição do desempenho atual a fim de prever a *performance* futura da rede com a nova aplicação. A ferramenta utilizada foi NetPredictor.

A seguir observaremos o modelo que foi utilizado na Klaus Corporation. Ele foi desenvolvido com base em medições obtidas anteriormente na rede existente com dados de 1 em 1 minuto, por 24 horas.

Tabela 5 – Modelo para distribuição da carga na Klaus Corporation

Prédio D			
Quantidade das máquinas clientes	160		
Média do arquivo acessado	2	Mb	
Média de atividade por pessoa	3	Mb/hora	
Total da carga iniciada	540	Mb/hora	
Segmento de carga de 10 Mbps e 100 Mbps	13%	83%	
Carga saindo do prédio local	9%		
Carga local da LAN com 10 Mbps	80,32	Mb/hora	
Carga local da LAN com 100 Mbps	501,28	Mb/hora	
Tráfego nos outros prédios	12	Mb/hora	
Tráfego prédio A	51%	25,4	Mb/hora
Tráfego prédio B	41%	20,49	Mb/hora
Tráfego prédio C	11%	5,10	Mb/hora
		Dados do modelo	
Utilização na LAN com 10 Mbps	1,00%	1,00%	
Utilização na LAN com 100 Mbps	1,13%		
Utilização no *backbone* FDDI com 100 Mbps	16%	16%	
Utilização nas linhas de E1	4,50%	4,30%	
Prédio B			
Quantidade das máquinas clientes	160		
Média do arquivo acessado	30	Mb	
Média de atividade por pessoa	50	Mb/hora	
Total da carga iniciada	6.909	Mb/hora	
Segmento de carga de 10 Mbps e 100 Mbps	13%	80%	
Carga local saindo do prédio	61%		
Carga saindo do prédio local	540	Mb/hora	
Carga local da LAN com 10 Mbps	5.733	Mb/hora	
Tráfego nos outros prédios	3.012	Mb/hora	
Tráfego prédio A	70%	3.230,33	Mb/hora
Tráfego prédio B	23%	812,5	Mb/hora
Tráfego prédio C	1%	1	Mb/hora
Utilização na LAN com 10 Mbps	21,92%		
Utilização na LAN com 100 Mbps	19,82%		
Prédio A			
Quantidade das máquinas clientes	160		
Média do arquivo acessado	11	Mb	
Média de atividade por pessoa	31	Mb/hora	

Total da carga iniciada	6.432	Mb/hora	
Segmento de carga de 10 Mbps e 100 Mbps de carga local saindo do prédio	30%	80%	
Carga saindo do prédio local	71%		
Carga local da LAN com 10 Mbps	664	Mb/hora	
Tráfego nos outros prédios	2.192	Mb/hora	
Tráfego prédio A	5.512	Mb/hora	
Tráfego prédio B	82%	4.848,90	Mb/hora
Tráfego prédio C	16%	712,5	Mb/hora
Quantidade das máquinas clientes	1%	2	Mb/hora
Utilização LAN em 10 Mbps	22,15%		
Utilização LAN em 100 Mbps	19,07%		
Prédio C			
Máquinas clientes	160		
Tamanho do arquivo acessado	2	Mb	
Atividade por pessoa	1	Mb/hora	
Carga total de início no prédio	234	Mb/hora	
Carga local de saída no prédio	72%		
Carga local da LAN em 10 Mbps	622	Mb/hora	
Tráfego dos outros prédios	2,58	Mb/hora	
Tráfego prédio A	73%	133,7	Mb/hora
Tráfego prédio B	53%	85,9	Mb/hora
Tráfego prédio C	7%	11,2	Mb/hora
Supor 2 LANs com 10 Mbps:			
Utilização de cada LAN com 10 Mbps	13,38%		

Adaptado de: Assunção *et al.* (2003, p. 12).

Posteriormente às conclusões da análise dos dados emitidos pelos analisadores informados é possível apresentar os resultados em gráficos gerados pelo NetPredictor.

Em alguns casos, a carga sobre os enlaces é pequena e possui apenas um pico, que tem duração de aproximadamente 4 horas noturnas, mas ele é justificado pela execução da sincronização de arquivos programada. A carga foi inferior a 10% por volta de 90% do dia, concluindo-se que também não há problemas nos enlaces.

O novo sistema a ser implantado pela empresa é responsável pela entrada de pedidos. Em uma medição realizada com o acesso de um único usuário foi possível fazer uma análise do tráfego usando um analisador de protocolos. Os resultados obtidos foram que para a entrada de um só pedido gerou-se um tráfego de 2 Mb. Deste valor 220 Kb destinaram-se à comunicação com a base de dados Oracle no prédio 1, via protocolo TCP/IP, e 1,7 Mb à comunicação entre o usuário e o servidor de arquivos para carregar a aplicação e os formulários de entrada de pedido na referida instalação.

Após análise realizada por 3 minutos com a carga de aproximadamente 90 Kbps, concluiu-se que o tráfego médio é de 40 Kbps, com o uso contínuo da aplicação já carregada. Este valor é estimado por usuário, devendo ser multiplicado pela quantidade de indivíduos.

Portanto, concluiu-se que a rede suportará o novo tráfego sem causar problemas, pois, se forem implantados 10 usuários no novo sistema, o consumo será de 400 Kbps, o que não sobrecarregará a LAN, e o consumo dos enlaces E1 passará de 4,3% de uso para aproximadamente 17%.

Como última etapa de projeto, é preciso realizar a documentação da rede e para isso, geralmente, existem duas situações: a primeira, quando possuir a necessidade de responder uma RFP (Request for Proposal), carta-consulta, licitação ou outro formulário; a segunda é sem RFP.

O modo de lidar com as duas condições é praticamente igual, havendo apenas algumas particularidades, pois em ambas o documento de projeto deve conter a explicação dos requisitos do cliente, como o seu projeto atenderá essas necessidades, a documentação da rede atual, os detalhes do projeto lógico e físico e o custo previsto para a nova rede.

Responder a uma RFP requer o atendimento de uma lista de requisitos básicos para um projeto e costuma ter a seguinte estrutura:

- objetivos de negócio para a rede;
- escopo do projeto;
- informação sobre a rede e as aplicações existentes;
- dados sobre novas aplicações;
- requisitos técnicos, incluindo escalabilidade, disponibilidade, desempenho, segurança, gerenciabilidade, usabilidade, adaptabilidade e custo-benefício;
- requisitos de prazos de garantia para produtos adquiridos;
- restrições arquiteturais e ambientais que podem afetar a implementação;
- condições de treinamento e suporte;
- cronograma inicial com *milestones* e artefatos a entregar (*deliverables*);
- termos e condições contratuais legais.

Observação

Em alguns casos, o RFP já possui formato da resposta e se acontecer ele deverá ser seguido.

Geralmente estão inclusos no formato de resposta uma topologia para a rede nova, informações sobre os protocolos, tecnologias e produtos que formam o projeto, um plano de implementação e de treinamento, dados sobre serviços de suporte, o preço e as formas de pagamento, a qualificação de quem está respondendo ao RFP, se existem recomendações de clientes para os quais projetos de redes já foram feitos, além dos termos e condições contratuais legais.

Vale ressaltar que essa resposta é apenas um esboço para que seja possível ganhar uma licitação ou RFP, ou seja, não se trata de um projeto completo.

Caso não haja uma RFP, ou se houve uma e ela foi aprovada, será necessário apresentar um documento de projeto completo da rede, que deve ser separado por seções, as quais comumente são: resumo executivo, objetivo do projeto, escopo do projeto, requisitos de *design* (de negócio e técnicos), estado da rede atual, projeto lógico, projeto físico, resultados de testes, plano de implementação, orçamento e apêndices.

Veja a seguir uma breve explicação das seções que compõem o documento.

Um resumo executivo possui todos os pontos importantes do projeto, mas de modo resumido, geralmente em uma única página. Trata-se de uma seção orientada a gerentes que têm ou terão o poder de decidir sobre a continuidade do trabalho. Por isso ele não deve conter aspectos técnicos. Se houver, precisarão estar sumariamente descritos, uma vez que o principal objetivo desta seção é focar os negócios, ou seja, vender vantagens da transação.

Ao descrever o objetivo do projeto é necessário mostrar como através dos principais propósitos a empresa ficará mais competitiva. Essa descrição deve ocorrer em um único parágrafo, deixando claro ao leitor o entendimento do negócio de seu cliente e como a nova rede afetará positivamente a instituição.

Na seção do escopo do projeto deve-se explicar qual o tamanho do trabalho, se ele é para uma rede nova ou existente, precisando mencionar os departamentos e esclarecer as coberturas, deixando claro o que está incluso ou não. Veja o exemplo a seguir: "O escopo do projeto é atualizar a WAN que interliga vendas principais e escritórios essenciais de *marketing* no país à sede. Essa nova rede WAN será acessada por colaboradores de diversas áreas, como: vendas, marketing e treinamento. É importante lembrar que não faz parte do escopo do projeto atualizar qualquer LAN usada por tais colaboradores e/ou as redes acessadas via satélite ou de uso *home office*".

Na sessão de requisitos de *design* de negócio e técnicos é necessário listar os objetivos em ordem de prioridade, destacando-se os críticos. Os fins relacionados a disponibilidade, desempenho, escalabilidade, segurança, gerenciabilidade, adaptabilidade, usabilidade, relação custo-benefício fazem parte dos objetivos técnicos, e portanto devem ser demonstrados com os *tradeoffs* selecionados pelo cliente. Para isso, recomenda-se o uso de uma tabela de priorização de metas, além da listagem de aplicações e seus atributos, comunidades de usuários e *data stores*.

Também é necessário escrever o estado da rede atual, mostrando VPNs, VLANs, *firewalls*, segmentos, endereçamento etc. Recomenda-se usar um mapa de alto nível apenas para demonstrar a estrutura e a base do desempenho da rede atual. Mapas com maiores detalhes devem ser inclusos no apêndice.

No projeto lógico da rede deve ser demonstrada a topologia lógica, com um modelo para endereçar segmentos e dispositivos, além de dar nome a eles, listar os protocolos de *switching* e roteamento e as recomendações para uso dos protocolos, e incluir um plano completo de segurança como apêndice. Entretanto, é preciso descrever para a gerência um resumo das políticas de segurança e as recomendações de produtos e mecanismos para ela, além de sugestões sobre produtos e arquitetura. Por fim, é necessário explicar o porquê das decisões tomadas e como elas se relacionam aos objetivos do cliente.

O projeto físico deve apenas conter tecnologias, dispositivos, informação de preços e escolha de provedor.

Com o intuito de comprovar a funcionalidade do projeto temos de mostrar que através dos testes praticados existem evidências demonstrando o funcionamento da rede. Geralmente torna-se mais fácil esclarecer se um modelo ou protótipo foi criado. Em caso afirmativo, devem-se incluir objetivos dos testes realizados, critérios de aceitação dos testes, ferramentas de testes usadas, *scripts* de testes, resultados e conclusões.

Ao fazer um plano de implementação, leve em consideração que não é possível detalhá-lo se não for o responsável pela implantação; caso seja, inclua recomendações sobre como implantá-lo. Um plano de implementação deve conter: um cronograma, um plano para informar usuários, gerentes e administradores do projeto, planos com fornecedores ou provedores de serviço para a instalação de enlaces, equipamentos ou serviços, um plano de treinamento para administradores de rede e usuários, um plano para medir a eficácia da nova rede depois de implantada, planos ou recomendações de *outsourcing* da implementação e/ou da gerência da rede, uma lista de riscos conhecidos que podem ocasionar atraso, um plano para a evolução da rede diante do surgimento de novos requisitos e aplicações, um plano de contingência, caso a implementação venha a falhar. A seguir consta um exemplo que pode ser usado.

Quadro 9 – Exemplo de cronograma

Data de término	Ponto de controle importante
01/fev	Projeto terminado e versão inicial do Documento de Projeto distribuída aos principais gerentes, administradores e usuários finais
15/fev	Recepção de comentários sobre o Documento de Projeto
15/fev	Documento de Projeto final distribuído
24/fev	Instalação de LPCDs entre todos os prédios pelo provedor WAN
28-29/fev	Administradores de rede treinados sobre o novo sistema
01/mar	Usuários finais treinados sobre o novo sistema
06/mar	Implementação-piloto terminada no prédio 1

20/mar	*Feedback* recebido dos administradores de rede e usuários finais sobre o piloto
27/mar	Implementação terminada nos prédios 2-5
10/abr	*Feedback* recebido dos administradores de rede e usuários finais sobre a implementação nos prédios 2-5
17/abr	Implementação terminada nos prédios remanescentes
Contínuo	Monitoração do novo sistema para verificar se satisfaz os requisitos

No orçamento é necessário documentar: aquisição de *hardware* e *software*, treinamento, contratos de suporte e manutenção, contratos de serviços, recursos humanos, taxas de consultoria e despesas de *outsourcing*. Um dos segredos para que os clientes não se assustem ou já pensem que o valor do orçamento ficou alto é descrever sequencialmente uma ROI (Análise de Retorno de Investimento). Veja a seguir como fazê-la.

O cliente UNIP está considerando gastar R$ 900.000,00 em um novo equipamento de comutação WAN, mas, se em vez de comprar objetos da rede fosse investido por 5 anos o mesmo valor, o retorno seria de 5%. Portanto, o investimento seria de R$ 945 mil. Além disso, há a depreciação do equipamento neste período.

Os equipamentos atualmente em uso já estão pagos e depreciados, porém precisamos comparar os custos entre operar a rede antiga e a nova e o novo equipamento. Serão usados 12 enlaces E1, em vez dos 20 da rede antiga. Cada um deles custa R$ 1.500,00 por mês (12 enlaces custam R$ 18 mil e 20 valem R$ 30 mil). Logo os custos recorrentes ficarão R$ 12 mil mais baratos por mês, e o preço de aquisição de R$ 945 milhões estará pago em 945.000/12.000 = 7 anos e 8 meses, maior que o tempo de depreciação.

A gestão entendeu que o processo não é viável. Portanto deve-se tentar de novo.

Para finalizar a documentação é necessário incluir os apêndices, informações suplementares como: mapas topológicos detalhados, configurações de dispositivos, detalhes de endereçamento IP, resultados de testes e outras informações julgadas relevantes.

Resumo

Nesta unidade, vimos que o projeto lógico da rede é necessário para identificar os pontos de interconexão, o tamanho da rede e seu alcance e os tipos de dispositivos de interconexão, tendo como principal objetivo projetar uma rede segura, redundante e escalável.

Observamos que uma rede pode ser hierárquica tanto para LAN quanto para WAN e que é possível utilizar roteamentos com classe, porém para um tipo de rede não contígua é preciso que ele seja sem classe, para permitir a conversação entre redes.

Analisamos os protocolos de rede e suas particularidades, como *bridging* e *switching*, que são basicamente iguais, pois ambos são de camada 2 e permitem o uso de portas de redes com tecnologias diferentes. Observamos que nos protocolos de roteamento há diversas distinções. Por exemplo, o RIP possui *broadcast* no intervalo de 30 segundos na tabela das rotas, com 25 rotas em cada pacote e limitação de 15 *hops*; já o IGRP tem mais métricas que o RIP, não possuindo a restrição de 15 *hops*, o que permite balanceamento da carga e diminui a ocorrência dos *loops* na convergência.

Vimos ainda que após a realização do projeto integral da rede e de todas as análises temos de fazer testes, o que pode se dar de diversas formas. Tudo deve ser estudado e anotado para posteriormente efetuar a documentação do projeto de rede, que é responsável por juntar todo o estudo do negócio e técnico para apresentação ao cliente.

Exercícios

Questão 1. (Cesgranrio 2013) As redes de computadores caracterizam-se pelo compartilhamento de recursos lógicos e físicos, por meio de sistemas de comunicação.

Entre os recursos físicos de uma rede, **não** se incluem os:

A) *Modems*.

B) Repetidores.

C) *Softwares*.

D) Transceptores.

E) *Switches*.

Resposta correta: alternativa C.

Análise das alternativas

A) Alternativa incorreta.

Justificativa: *modems* são recursos físicos de uma rede.

B) Alternativa incorreta.

Justificativa: repetidores são recursos físicos de uma rede.

C) Alternativa correta.

Justificativa: *softwares* são recursos lógicos de uma rede.

D) Alternativa incorreta.

Justificativa: transceptores são recursos físicos de uma rede.

E) Alternativa incorreta.

Justificativa: *switches* são recursos físicos de uma rede.

Questão 2. (Fepese 2010, adaptada) Com relação à autenticação de usuários nas redes de computadores, assinale a alternativa correta:

A) A credencial é uma evidência fornecida por um usuário ao requisitar acesso lógico a um recurso da rede. Para que um usuário prove a sua identidade, ele deve sempre mostrar o conhecimento de um segredo (senha) e apresentar credencias biométricas.

B) As senhas são um meio comum de validar a identidade de um usuário para acessar uma aplicação ou serviço. Um usuário deve usar a mesma senha para acessar diferentes aplicações e serviços para que possa provar a sua identidade.

C) As técnicas biométricas são classificadas como baseadas em características fisiológicas – por exemplo, o padrão de íris e a impressão digital – e como baseadas em características comportamentais – por exemplo, o padrão de voz e a dinâmica de assinatura.

D) As áreas de segurança devem ser protegidas por controles físicos de entrada apropriados. Combinar autenticação baseada em senha com autenticação baseada em cartões magnéticos com PIN é a única forma segura de implantar controles físicos.

E) Em uma rede de computadores, todos os usuários devem ser aconselhados a selecionar senhas de qualidade, com um tamanho mínimo de seis caracteres e máximo de oito caracteres, totalmente numéricas e que sejam trocadas regularmente, pelo menos uma vez por mês.

Resolução desta questão na plataforma.

FIGURAS E ILUSTRAÇÕES

Figura 1

PMI. *Um guia do conhecimento em gerenciamento de projetos*: guia PMBoK. 5. ed. Pensilvânia: PMI, 2013. p. 89.

Figura 2

PMI. *Um guia do conhecimento em gerenciamento de projetos*: guia PMBoK. 5. ed. Pensilvânia: PMI, 2013. p. 95.

Figura 3

PMI. *Um guia do conhecimento em gerenciamento de projetos*: guia PMBoK. 5. ed. Pensilvânia: PMI, 2013. p. 112.

Figura 4

PMI. *Um guia do conhecimento em gerenciamento de projetos*: guia PMBoK. 5. ed. Pensilvânia: PMI, 2013. p. 260. Adaptada.

Figura 5

PMI. *Um guia do conhecimento em gerenciamento de projetos*: guia PMBoK. 5. ed. Pensilvânia: PMI, 2013. p. 294.

Figura 6

DOROW, E. *Itil e o ciclo de vida*: estratégia do serviço. 2010. p. 69.

Figura 7

DOROW, E. *Itil e o ciclo de vida*: estratégia do serviço. 2010. p. 69. Adaptada.

Figura 8

DOROW, E. *Itil e o ciclo de vida*: estratégia do serviço. 2010. p. 80. Adaptada.

Figura 9

DOROW, E. *Itil e o ciclo de vida*: estratégia do serviço. 2010. p. 113. Adaptada.

Figura 10

PETERSON, L. L.; DAVIE, B. S. *Redes de computadores*: uma abordagem de sistemas. São Paulo: Elsevier, 2013. p. 78. Adaptada.

Figura 11

FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. Porto Alegre: AMGH, 2009. p. 507. Adaptada.

Figura 12

FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. Porto Alegre: AMGH, 2009. p. 518. Adaptada.

Figura 13

FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. Porto Alegre: AMGH, 2009. p. 529. Adaptada.

Figura 14

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 23.

Figura 15

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 26. Adaptada.

Figura 16

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 30. Adaptada.

Figura 17

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 37. Adaptada.

Figura 18

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 44. Adaptada.

Figura 19

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 46. Adaptada.

Figura 20

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 47. Adaptada.

Figura 21

13724-55A.GIF. Disponível em: <https://www.cisco.com/c/dam/en/us/support/docs/ip/interior-gateway-routing-protocol-igrp/13724-55a.gif>. Acesso em: 5 jul. 2018.

Figura 22

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 48. Adaptada.

Figura 23

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 49. Adaptada.

Figura 24

CHAKI, N.; MEGHANATHAN, N.; NAGAMALAI, D. *Computer Networks & Communications (NetCom)*. New York: Springer New York, 2013. p. 56. Adaptada.

Figura 25

CHAKI, N.; MEGHANATHAN, N.; NAGAMALAI, D. *Computer Networks & Communications (NetCom)*. New York: Springer New York, 2013. p. 70. Adaptada.

Figura 26

CHAKI, N.; MEGHANATHAN, N.; NAGAMALAI, D. *Computer Networks & Communications (NetCom)*. New York: Springer New York, 2013. p. 90. Adaptada.

Figura 27

CHAKI, N.; MEGHANATHAN, N.; NAGAMALAI, D. *Computer Networks & Communications (NetCom)*. New York: Springer New York, 2013. p. 98. Adaptada.

Figura 28

CHAKI, N.; MEGHANATHAN, N.; NAGAMALAI, D. *Computer Networks & Communications (NetCom)*. New York: Springer New York, 2013. p. 112. Adaptada.

Figura 29

CHAKI, N.; MEGHANATHAN, N.; NAGAMALAI, D. *Computer Networks & Communications (NetCom)*. New York: Springer New York, 2013. p. 119. Adaptada.

Figura 30

CHAKI, N.; MEGHANATHAN, N.; NAGAMALAI, D. *Computer Networks & Communications (NetCom)*. New York: Springer New York, 2013. p. 121. Adaptada.

Figura 31

TORRES, G. *Redes de computadores*. Rio de Janeiro: Novaterra, 2015. p. 114. Adaptada.

Figura 32

FIGURA2_TUTORIALENLACEADSL.GIF. Disponível em: <http://www.teleco.com.br/imagens/tutoriais/figura2_tutorialenlaceadsl.gif>. Acesso em: 5 jul. 2018.

Figura 33

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 77. Adaptada.

Figura 34

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 90. Adaptada.

Figura 36

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013. p. 113. Adaptada.

REFERÊNCIAS

Textuais

ALBERT, R.; BARABÁSI, A. Statistical mechanics of complex networks. *Reviews of Modern Physics*, Indiana, v. 74, 2002. Disponível em: <http://barabasi.com/f/103.pdf>. Acesso em: 18 jun. 2018.

ASSUNÇÃO, M. D.; WESTPHALL, C. B.; KOCH, F. L. Arquitetura de *grids* de agentes aplicada à gerência de redes de computadores e telecomunicações. *In*: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 21., 2003, Santa Catarina. *Anais*... Santa Catarina: UFSC, 2003. p. 789-804. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbrc/2003/050.pdf>. Acesso em: 18 jun. 2018.

BELIZÁRIO, L. C. V. *Tecnologia ADSL*. São Paulo: [s.n.], 2001.

BON, J. V. *Foundations of IT Service Management, based on Itil, ITSM Library*. Gelderland: Van Haren Publishing, 2006.

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.

BUNGART, J. W. *Redes de computadores*: fundamentos e protocolos. São Paulo: Senai, 2017.

CARISSIMI, A. S.; ROCHOL, J.; GRANVILLE, L. Z. *Redes de computadores*. Porto Alegre: Bookman, 2009.

CESTARI FILHO, F. *Itil v3*: fundamentos. Rio de Janeiro: RNP/ESR, 2011.

CHAKI, N.; MEGHANATHAN, N.; NAGAMALAI, D. *Computer Networks & Communications (NetCom)*. New York: Springer New York, 2013.

CISCO. *Informações*. [s.d.]. Disponível em: <https://www.cisco.com/c/pt_br/support/cloud-systems-management/prime-lan-management-solution/products-licensing-information-listing.html?dtid=osscdc000341>. Acesso em: 18 jul. 2018.

COMER, D. *Internetworking with TCP/IP*. 5. ed. New Jersey: Prentice-Hall, 2008.

COX III, J. F.; SCHLEIR JR., J. G. *Handbook da teoria das restrições*. Porto Alegre: Bookman, 2013.

DIÓGENES, Y. *Certificação Cisco*: CCNA 4.0: guia de certificação para o exame 640-801. Rio de Janeiro: Axcel Books do Brasil, 2004.

DOROW, E. *Itil e o ciclo de vida*: estratégia do serviço. 2010.

ENOMOTO, C. *Uma linguagem para especificação de fluxo de execução em aplicações paralelas*. 2005. Dissertação (Mestrado em Engenharia Elétrica) - Universidade Estadual de Campinas (Unicamp), Campinas, 2005. Disponível em: <http://www.repositorio.unicamp.br/bitstream/REPOSIP/261813/1/Enomoto_Cristina_M.pdf>. Acesso em: 18 jun. 2018.

FAZZANARO, P. L. *Projetos de redes de computadores*: utilizando o Microsoft Visio 2010. Leme: Clube dos Autores, 2013.

FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. Porto Alegre: AMGH, 2009.

FRASER, B. Y. *Site security handbook*. Pittsburgh: IETF, 1997. Disponível em: <https://tools.ietf.org/html/rfc2196>. Acesso em: 20 jul. 2018.

FURTADO, C. M. *Introdução ao DNS*: aprenda a instalar e configurar uma infraestrutura de DNS na prática. São Paulo: Novatec, 2016.

GALLO, M. A.; HANCOCK, W. M. *Comunicação entre computadores e tecnologias de rede*. São Paulo: Thomson Learning, 2003.

GREENE, J.; STELLMAN, A. *Use a cabeça*! PMP: o guia amigo do seu cérebro. Rio de Janeiro: Alta Books, 2010.

HELDMAN, K. *Gerência de projetos*: guia para o exame oficial do PMI. 5. ed. Rio de Janeiro: Campus, 2009.

HUBBARD, K. *et al*. *RFC 2050*: best current practice: internet registry IP allocation guidelines. Virginia, 1996. Disponível em: <https://tools.ietf.org/html/rfc2050>. Acesso em: 18 jul. 2018.

KUROSE, J. F.; ROSS K. W. *Redes de computadores e a internet*: uma abordagem *top-down*. 6. ed. São Paulo: Pearson, 2013.

MAGALHÃES, I. V.; PINHEIRO, W. B. *Gerenciamento de serviços de TI na prática*: uma abordagem com base na Itil. São Paulo: Novatec, 2007.

MANSFIELD JR., K. C.; ANTONAKOS, J. L. *Computer networking for LANs to WANs*: hardware, software and security. Massachusetts: Cengage Learning, 2009.

MCNAB, C. *Avaliação de segurança de redes*. São Paulo: Novatec, 2017.

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

O'BRIEN, J. A. *Sistemas de informação e as decisões gerenciais na era da internet*. São Paulo: Saraiva, 2001.

PETERSON, L. L.; DAVIE, B. S. *Redes de computadores*: uma abordagem de sistemas. São Paulo: Elsevier, 2013.

PMI. *Um guia do conhecimento em gerenciamento de projetos*: guia PMBoK. 4. ed. Pensilvânia: PMI, 2008.

___. *Um guia do conhecimento em gerenciamento de projetos*: guia PMBoK. 5. ed. Pensilvânia: PMI, 2013.

SERPANOS, D.; WOLF, T. *Architecture of network systems*. Massachusetts: Elsevier, 2011.

SHIMONSKI, R. J.; STEINER, R. T.; SHEEDY, S. M. *Cabeamento de rede*. Rio de Janeiro: LTC, 2010.

SILVA, E. L.; MENEZES, E. M. *Metodologia da pesquisa e elaboração de dissertação*. 4. ed. Florianópolis: Universidade Federal de Santa Catarina (UFSC), 2005.

STALLINGS, W. *Criptografia e segurança de redes*: princípios e práticas. 6. ed. São Paulo: Pearson, 2014.

TORRES, G. *Redes de computadores*. Rio de Janeiro: Novaterra, 2015.

Exercícios

Unidade I – Questão 1: CESGRANRIO. *Profissional Júnior 2013*: Tecnologia da Informação – Análise de sistemas. Questão 57. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/31851/cesgranrio-2013-liquigas-profissional-junior-analise-de-sistemas-tecnologia-da-informacao-prova.pdf>. Acesso em: 16 jul. 2018.

Unidade I – Questão 2: INSTITUTO BRASILEIRO DE FORMAÇÃO E CAPACITAÇÃO (IBFC). *Concurso público para provimento de cargo de perito criminal de 3ª classe 2013*. Questão 100. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/32617/ibfc-2013-pc-rj-perito-criminal-engenharia-da-computacao-prova.pdf>. Acesso em: 16 jul. 2018.

Unidade II – Questão 1: EMPRESA DE SELEÇÃO PÚBLICA E PRIVADA (ESPP). *Banparaná 2012*: Engenheiro Agrônomo. Questão 21. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/29255/espp-2012-banpara-engenheiro-agronomo-prova.pdf>. Acesso em: 16 jul. 2018.

Unidade II – Questão 2: COORDENADORIA DE CONCURSOS (CCV). *Concurso Público Universidade Federal do Ceará 2016*: Técnico de Laboratório/Informática. Questão 28. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/55932/ccv-ufc-2016-ufc-tecnico-de-laboratorio-informatica-prova.pdf>. Acesso em: 16 jul. 2018.

Unidade III – Questão 1: FUNDAÇÃO CARLOS CHAGAS (FCC). *Assembleia Legislativa do Estado de São Paulo 2010*: Agente Técnico Legislativo – Análise de Infraestrutura de Redes. Questão 44. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/1772/fcc-2010-al-sp-agente-tecnico-legislativo-especializado-analise-de-infraestrutura-de-redes-prova.pdf>. Acesso em: 16 jul. 2018.

Unidade III – Questão 2: CENTRO DE SELEÇÃO E DE PROMOÇÃO DE EVENTOS (CESPE). *Tribunal Regional Eleitoral do Mato Grosso do Sul 2013*: Analista Judiciário – Análise de Sistemas. Questão 33. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/29273/cespe-2013-tre-ms-analista-judiciario-analise-de-sistemas-prova.pdf>. Acesso em: 16 jul. 2018.

Unidade IV – Questão 1: CESGRANRIO. *Banco da Amazônia 2013*: Técnico Bancário. Questão 30. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/31929/cesgranrio-2013-banco-da-amazonia-tecnico-bancario-1-prova.pdf>. Acesso em: 16 jul. 2018.

Unidade IV – Questão 2: FEPESE. *Secretaria de Estado da Fazenda 2010*: Auditor Fiscal da Receita Estadual – Parte III – Tecnologia da Informação. Questão 57. Disponível em: <https://www.qconcursos.com/arquivos/prova/arquivo_prova/10762/fepese-2010-sefaz-sc-auditor-fiscal-da-receita-estadual-parte-iii-tecnologia-da-informacao-prova.pdf>. Acesso em: 16 jul. 2018.

Interativa

Informações:
www.sepi.unip.br ou 0800 010 9000