Metodologia de Projeto de Rede

1. A Metodologia de Projeto de Redes de Computadores

2. Identificação das Necessidades e Objetivos do Cliente

    2.1 Análise dos objetivos e restrições de negócio
    2.2 Análise dos objetivos e restrições técnicos
    2.3 Caracterização da rede existente
    2.4 Caracterização do tráfego de rede

3. Projeto Lógico da Rede

    3.1 Projeto da topologia da rede
    3.2 Projeto do esquema de endereçamento e naming
    3.3 Seleção de protocolos de bridging, switching e roteamento
    3.4 Desenvolvimento de estratégias de segurança e gerência

4. Projeto Físico da Rede

    4.1 Seleção de tecnologias e dispositivos para redes de campus
    4.2 Seleção de tecnologias e dispositivos para redes corporativas

5. Testes e Documentação do Projeto de Rede

    5.1 Testes do projeto de rede
    5.2 Documentação do projeto de rede

1. A Metodologia de Projeto de Redes de Computadores

Introdução

- Empresas estão dependendo cada vez mais de redes
  - Para reduzir o tempo de desenvolvimento e colocação no mercado de produtos, empregados precisam de acesso imediato a mais informação
    - Informação corporativa e departamental
  - Para vender e distribuir produtos em escala mundial, empresas montam:
    - Alianças globais
    - Corporações virtuais
  - Para melhorar a comunicação, novas aplicações surgem
    - E-commerce
    - Videoconferência
    - Telefonia na Internet
  - Empresas estão fundindo suas redes de voz e dados
- Queremos aprender a projetar redes de computadores para satisfazer as necessidades de tais empresas de alcance mundial

Breve descrição da metodologia

- Sem metodologia, o projeto final não tem a mínima chance de satisfazer os requisitos do cliente
  - Funcionalidade
  - Capacidade
  - Desempenho
  - Disponibilidade
  - Escalabilidade
  - Preço
  - Segurança
  - Gerenciabilidade
- A metodologia é estruturada, no sentido de incluir o projeto lógico da rede antes de abordar o projeto físico e abordar requisitos antes de tudo
- A metodologia é iterativa
  - Mais detalhes entram progressivamente no projeto, à medida que se conhece melhor a situação
- Os grandes passos são descritos a seguir

Identificação das Necessidades e Objetivos do Cliente

- Levantamento de requisitos, incluindo
  - Objetivos e restrições do negócio
  - Objetivos e restrições técnicos
- Caracterização da rede existente
- Caracterização do tráfego projetado para a rede
  - Incluindo fluxo, carga e requisitos de QoS (Quality of Service)

Projeto Lógico da Rede

- Desenvolvimento da topologia da rede
  - Pode ser achatada ou hierárquica, dependendo do tamanho
- Desenvolvimento de esquemas de endereçamento e naming
- Seleção de protocolos de bridging, switching e roteamento
- Desenvolvimento de aspectos de segurança e gerência

Projeto Físico da Rede

- Seleção de tecnologias e dispositivos para redes de campus
  - Tecnologias Ethernet, Fast Ethernet, ATM
  - Dispositivos: hubs, switches, roteadores, cabeamento
- Seleção de tecnologias e dispositivos para redes corporativas
  - Tecnologias: Frame relay, ATM, ISDN, DSL, linhas discadas
  - Dispositivos: roteadores, switches, servidores de acesso remoto (RAS)

Testes, Otimização e Documentação do Projeto de Rede

- Escrever e implementar um plano de testes
- Implementar uma rede piloto
- Otimizar o projeto da rede
  - Uso de traffic shaping
  - Uso de mecanismos especiais de enfileiramento em roteadores
  - Uso de mecanismos especiais de switching
- Documentar o projeto da rede

2. Identificação das Necessidades e Objetivos do Cliente

- Análise dos objetivos e restrições de negócio
- Análise dos objetivos e restrições técnicos
- Caracterização da rede existente
- Caracterização do tráfego de rede

Análise dos Objetivos e Restrições de Negócio

Análise de objetivos de negócio

- Analisar os objetivos de negócio é absolutamente crucial ao sucesso do projeto
  - O projeto final da rede não é analisado em termos de sua beleza ou elegância técnica mas em termos de benefícios para o negócio
- Embora seja tentador para o técnico não se meter em assuntos não técnicos, não se pode pular essa fase
- Segue uma lista do que deve ser descoberto junto ao cliente

1. Conhecendo o negócio do cliente

- Antes de discutir objetivos de negócio com o cliente, é bom entender o negócio
  - O cliente participa de que indústria ou área de serviços?
  - Qual é o mercado do cliente?
  - Quem são os fornecedores e parceiros do cliente?
  - Que produtos e serviços o cliente produz?
  - Que produtos e serviços o cliente utiliza?
  - Quais são as vantagens competitivas do cliente?
- Seu projeto poderá ajudar a melhorar a posição competitiva do cliente

2. Conhecendo a estrutura organizacional do cliente

- Nas primeiras reuniões com o cliente, descubra a estrutura organizacional
  - Quais são os departamentos?
  - Quais são as linhas de negócio?
  - Quais são os parceiros?
  - Onde estão as filiais?
- Seu projeto de rede refletirá provavelmente a estrutura corporativa
  - Identifique os maiores grupos de usuários pois isso afetará o fluxo de tráfego na rede
- Descubra quem são os responsáveis técnicos e financeiros pelo projeto da nova rede
  - Quem tem poder de aceitar ou rejeitar sua proposta de projeto?

3. Identificando o objetivo maior da rede

- Obtenha, em uma única frase, o objetivo maior da nova rede, do ponto de vista do negócio
  - Por que o cliente quer uma nova rede?
  - Para que a rede será usada?
  - Como a rede deve ajudar o cliente no seu negócio?
- Algumas possibilidades de objetivo de negócio para a rede são:
  - Aumentar faturamento e lucro
  - Melhorar a comunicação corporativa
  - Diminuir o time-to-market (ciclo de vida do produto), aumentando a produtividade dos empregados
  - Construir parcerias com outras empresas
  - Expandir a operação a empresa para mercados globais
  - Mudar o modelo de negócio para se basear numa rede de alcance mundial
  - Modernizar tecnologias obsoletas
    - Cuidado! Isso quase nunca é um objetivo de negócio!
    - A tecnologia não muda em função da tecnologia, mas do negócio
  - Reduzir custos de telecomunicações e de rede, incluindo overheads de manter redes separadas para voz, dados e vídeo
  - Fornecer mais informação a mais gente para que tomem decisões melhores de negócio, mais rapidamente
  - Melhorar a segurança e confiabilidade de aplicações e dados de missão crítica
  - Melhorar o suporte ao cliente (do cliente)
  - Oferecer novos serviços ao cliente (do cliente)

4. Identificando os critérios de sucesso

- Quais são os critérios de sucesso do projeto de rede, do ponto de vista do cliente?
- À luz de quê o cliente vai dizer que a nova rede é bem sucedida?
  - Diminuir os custos operacionais
  - Aumentar o faturamento
  - Construir parcerias
- A resposta pode ser diferente para pessoas diferentes:
  - Diretoria
  - Gerentes operacionais

- Usuários finais
- Engenheiros de suporte à rede

- Lembre de formar alianças e comprometimentos internos para melhorar as chances de sucesso do projeto

5. Identificando as consequências do fracasso

- O que ocorre se o projeto da rede for um fracasso (não for feito, não tiver desempenho adequado, ...)
- Qual é a visibilidade do projeto da rede à alta direção da empresa
- Quais são os efeitos de uma má operação da rede nos aspectos operacionais do negócio?

6. Identificando o escopo da nova rede

- Está-se contruindo uma nova rede ou ampliando uma rede existente?
- Qual é o tipo de rede sendo projetada?
  - Segmento: Uma rede única usando uma tecnologia particular e única de camada 2
  - LAN: Um conjunto de segmentos interconectados com pontes ou switches, normalmente usando uma única tecnologia de camada 2
    - Pode envolver alguns protocolos de camada 3 também
  - Rede de prédio: Múltiplas LANs dentro de um único prédio (grande), normalmente conectadas a um backbone no prédio
  - Rede de campus: Rede abrangendo múltiplos prédios, numa área geográfica limitada, normalemente conectados a um backbone de campus
  - Acesso remoto: Uso de linhas discadas
  - WAN: Rede geograficamente abrangente incluindo conexões ponto-a-ponto, Frame relay, ATM e outras tecnologias de longo alcance
  - Rede corporativa: Grande rede abrangente envolvendo múltiplos campi, serviços de acesso remoto (dial-in ou dial-out) e uma ou mais WANs

7. Identificando as aplicações do cliente que utilizarão a rede

- Decobrir aplicações atuais e futuras
- Uma tabela como mostrada abaixo pode ser preenchida:

Nome da aplicação	Tipo de aplicação	Aplicação nova? (sim/não)	Criticalidade	Comentários

- Nome da aplicação: dada pelo usuário
- Tipo de aplicação
  - Aplicações do usuário
    - Correio eletrônico
    - Transferência de arquivos
    - Compartilhamento de arquivos
    - Acesso a bancos de dados
    - Groupware
    - Desktop publishing
    - Web browsing
    - Disseminação de informação com tecnologia Push
    - Jogos em rede
    - Whiteboard eletrônico
    - Login remoto
    - Calendário
    - Diretório on-line (ex. catálogo telefônico)
    - Imagens médicas
    - Educação à distância
    - Videoconferência
    - Telefonia na Internet ou na rede corporativa
    - Fax na Internet ou na rede corporativa
    - Terminais ponto-de-venda (loja de varejo)
    - Entrada de pedidos de compra
    - Comércio eletrônico
    - Relatórios gerenciais
    - Modelagem financeira
    - Rastreamento de vendas
    - Gerência de recursos humanos
    - Computer-aided design (CAD)
    - Computer-aided manufacturing (CAM)
    - Controle de estoque e despacho
    - Controle de processos e chão de fábrica

        - Telemetria
    - Aplicações de sistema
        - Autenticação e autorização de usuários
        - Mapeamento de nomes de hospedeiros
        - Boot remoto
        - Download remoto de configuração
        - Serviços de diretório (naming service)
        - Backup via rede
        - Gerência de rede
        - Distribuição de software
- Criticalidade: usar um número, por enquanto. Mais tarde, pode-se levantar o downtime aceitável
    - 1. Extremamente crítico
    - 2. Mais ou menos crítico
    - 3. Não crítico
- Comentários: qualquer informação relevante. Exemplos:
    - Quando a aplicação deixará de ser usada
    - Quando a aplicação será implantada
    - Planos de uso regional de certas aplicações
    - etc.

Análise de restrições de negócio

- Restrições podem seriamente afetar o projeto de uma rede
- Alguns aspectos são descritos a seguir

Politicagem e políticas (Politics and Policies)

- Não entender certos aspectos políticos da situação do cliente podem comprometer o projeto da rede
    - Fracassos não são devidos exclusivamente a problemas técnicos!
- Escute o que acontece nas reuniões para identificar os seguinte aspectos políticos:
    - Agendas escondidas
    - Guerras de poder
    - Opiniões tendenciosas
    - "Comprometimentos" com certos fornecedores de tecnologia
    - Relações entre grupos
    - Fracassos passados envolvendo um projeto de rede
    - Quais são os gerentes mais comprometidos a favor e contra o projeto?
    - O que esses gerentes têm a ganhar ou perder com o sucesso ou fracasso do projeto
    - Quem deseja ardentemente que o projeto fracasse?
    - Que postos de trabalho serão removidos devido à nova rede?
    - Qual é a tolerância a risco na empresa?
        - Isso afeta se o projeto deve ser conservador ou se pode inovar com tecnologias de ponta
- Se informe sobre as políticas internas da empresa:
    - Há compromissos com certos protocolos, padrões, fornecedores?
    - Há um entendimento claro sobre o uso de soluções abertas ou proprietárias?
    - Há certas plataformas "aprovadas" na empresa?
    - Há tecnologias já escolhidas e que devem ser incorporadas ao projeto?
    - Há poder decentralizado (em departamentos, p. ex.) sobre a compra de soluções?
- Não ignore detalhes de politicagem ou de políticas!

Aspectos técnicos de recursos humanos

- Se informe sobre as habilidades dos técnicos da empresa
    - Certas empresas não estão prontas para certos tipos de redes complexas

Restrições orçamentárias

- Se informe sobre o orçamento disponível, incluindo:
    - Aquisição de equipamentos
    - Aquisição de licenças de software
    - Contratos de manutenção
    - Contratos de suporte
    - Contratação de novos empregados
        - Identifique a necessidade de novas contratações durante o projeto
    - Treinamento de empregados
        - Identifique a necessidade de treinamento durante o projeto
    - Consultoria
    - Despesas de outsourcing
- Às vezes, você poderá ajudar gerentes a elaborarem uma análise ROI (Return On Investment)
    - Pode ser necessário para aprovar a implantação do projeto

- Como a rede vai se pagar e em quanto tempo?
    - Pode incluir reduções de custo, melhoras de produtividade, expansão em outros mercados, aumentos de faturamento, etc.

Cronograma

- De forma geral, você não controla o cronograma mas deve se adequar a ele
- Descubra os major milestones do projeto como um todo
- Opine se achar o cronograma inviável

Checklist de Objetivos de Negócio

- Você está pronto se poder responder positivamente às seguintes perguntas:
    - Pesquisei a área de negócio e os competidores do meu cliente
    - Entendo a estrutura corporativa do cliente
    - Elaborei uma lista dos objetivos de negócio do cliente, incluindo uma breve descrição do objetivo maior da rede sendo projetada
    - O cliente identificou operações de missão crítica
    - Entendo os critérios de sucesso do cliente e as consequências do fracasso
    - Entendo o escopo do projeto de rede
    - Identifiquei as aplicações de rede do cliente
    - O cliente explicou políticas sobre fornecedores, protocolos e plataformas aprovados
    - O cliente explicou políticas sobre o uso de sistemas abetos versus soluções proprietárias
    - O cliente explicou políticas sobre a distribuição de responsabilidades para o projeto e implantação da rede
    - Conheço o orçamento do projeto
    - Conheço o cronograma do projeto, incluindo major milestones e data final e acredito que seja factível
    - Conheço as habilidades dos técnicos da empresa
    - Discuti as necessidades de treinamento de empregados com o cliente
    - Tenho conhecimento dos aspectos políticos (politicagem) da empresa que poderão afetar o projeto da rede e o sucesso do projeto como um todo

Análise dos Objetivos e Restrições Técnicos

- Analisar os objetivos técnicos do cliente é importante para poder recomendar tecnologias apropriadas para satisfazer o usuário
- Os objetivos técnicos que examineremos são:
    - Escalabilidade
    - Disponibilidade
    - Desempenho
    - Segurança
    - Gerenciabilidade
    - Usabilidade
    - Adaptabilidade
    - *Cost-effectiveness*
- Também deveremos ver os tradeoffs entre esses objetivos conflitantes

Escalabilidade

- Escalabilidade refere-se a quanto crescimento um projeto de rede deve suportar
- É um objetivo primário de quase todo projeto de rede
    - Adicionam-se usuários, aplicações, sites e conexões de rede a um ritmo veloz

Planejando para a expansão

- Descubra qual é o crescimento planejado para a rede no próximo ano e nos próximos 2 anos
    - Raramente o cliente sabe mais do que isso
- Faça as seguintes perguntas:
    - Quantos novos sites serão adicionados?
    - Qual será a abrangência da rede em cada novo site?
    - Quantos usuários adicionais acessarão a rede?
    - Quantos hosts (incluindo servidores) serão adicionados?

Fornecendo mais dados a mais gente

- A regra 80/20 diz que 80% do tráfego de uma rede fica na rede departamental, 20% sai do departamento
- Essa regra era válida no tempo em que redes serviam principalmente para compartilhamento de discos e impressoras
- Hoje, a regra está se invertendo, com muito mais acesso a:
    - Servidores corporativos, incluindo a Intranet
    - Web
    - Extranet (permitindo colaboração com parceiros, fornecedores, grandes clientes)
- Mesmo o tráfego departamental pode cruzar o backbone, devido ao uso de Server Farms
    - Devido à centralização, Server Farms simplificam o suporte dado aos servidores
- Como resultado, o papel da Tecnologia de Informação é cada vez mais:

    - "Fornecer mais informação a mais gente, para que tomem melhor decisões de negócio mais rapidamente"
- Os seguintes objetivos técnicos são o resultado:
    - Conectar redes departamentais na rede corporativa
    - Resolver gargalos surgindo como resultado do maior tráfego entre redes
    - Prover servidores centralizados numa server farm
    - Juntar a rede SNA (mainframes IBM) à rede IP corporativa
    - Adicionar novos sites para dar suporte a filiais e a funcionários que trabalham em casa
    - Adicionar novos sites para dar suporte a parceiros, fornecedores, grandes clientes

Restrições da escalabilidade

- Ao pensar sobre escalabilidade, lembre que certas tecnologias de rede não são inerentemente escaláveis
    - Exemplo: redes com endereçamento achatado (redes de camada 2 envolvendo hubs, pontes e switches simples)
    - Exemplo: redes que suportam serviços baseados em broadcast
        - Falaremos mais sobre tráfego de broadcast adiante

Disponibilidade

- Disponibilidade refere-se ao percentual de tempo que a rede está disponível
- É frequentemente um objetivo crucial do cliente
- Exemplo: Se uma rede deve ficar 24 horas no ar e pára 3 horas numa semana de 168 horas, a disponibilidade é de 98,21%
    - Isso é um valor normalmente considerado muito ruim
- Disponibilidade é diferente de confiabilidade
    - Confiabilidade inclui acurácia, taxas de erro, estabilidade, etc.
- A recuperabilidade (habilidade de recuperar rapidamente após uma falha) é um dos aspectos da disponibilidade
- Outro aspecto da disponibilidade é a recuperação após um desastre
    - Onde ter cópias de backup dos dados?
    - Como chavear processos para acessar o backup?

Especificação de requisitos de confiabilidade

DISPONIBILIDADE (% UPTIME)	QUANTIDADE DE DOWNTIME PERMITIDO NO PERÍODO DE TEMPO			
	ANUALMENTE	MENSALMENTE	SEMANALMENTE	DIARIAMENTE
95%	438 H	36,5 H	8,4 H	1,2 H
99,5%	43,8 H	3,7 H	50,5 M	7,2 M
99,95%	4,38 H	21,9 M	5,05 M	43,2 S
99,98%	1,75 H	8,75 M	2,0 M	17,3 S
99,99%	0,88 H	4,4 M	1,0 M	8,7 S

- 95% só serve para testes ou protótipos
- A maioria dos sistemas opera por volta de 99,95%
    - 5 minutos de downtime por semana permitem alguns transientes ou uma parada um pouco maior por mês
- 99,98% são desejáveis para muitos sistemas de missão crítica
- 99,99% é o limite da tecnologia atualmente (há não ser que tenha muita grana!)
- Até 99,9%, a disponibilidade é baixa, acima disso, é considerada alta (requer cuidados especiais)

O custo do tempo parado

- Para ter uma idéia da situação, descubra quanto dinheiro a empresa perde por hora de downtime

MTBF e MTTR

- Para aplicações com alto custo de downtime, pode-se mais útil especificar a disponibilidade com dois números em vez de um só:
    - Mean Time Between Failures (MTBF)
        - Também chamado de Mean Time Between Service Outage (MTBSO), já que uma rede é um serviço e não um componente
    - Mean Time To Repair (MTTR)
- Disponibilidade = MTBF/(MTBF+MTTR)
- Exemplo: MTBF de 4000 horas e MTTR de 1 hora (um valor típico) => 99,98%
- Um MTTR muito baixo indica que providências especiais deverão ser tomadas
    - Exemplos: peças de reposição, técnico residente, etc.

Desempenho

- Muitos clientes não sabem especificar seus requisitos de desempenho com precisão
    - "Quero que a rede seja rápida!"
- Neste caso, você terá que fazer algumas suposições
    - Mostraremos como fazer isso aqui

Definições de desempenho

- Capacidade (bandwidth): a capacidade de uma rede carregar tráfego em bits por segundo
- Utilização: percentual da capacidade usada, na média

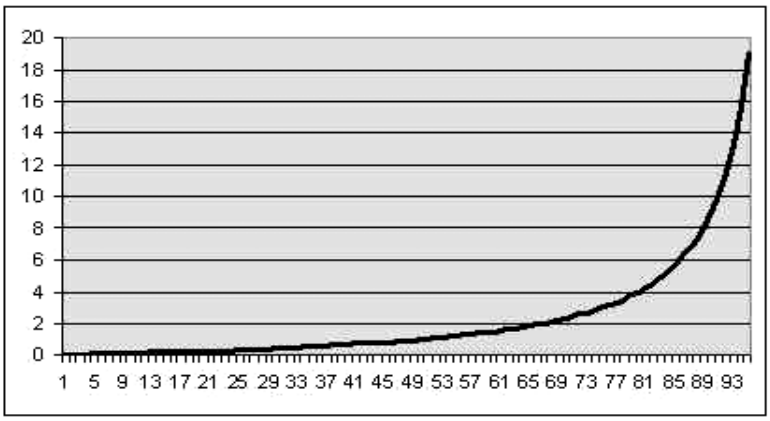
- Utilização máxima: valor da utilização em que a rede é considerada saturada
- Vazão: Quantidade de dados úteis transferidos sem erro por segundo
- Carga oferecida: A soma de todo o tráfego oferecido à rede (em bps) num determinado momento
- Acurácia: Quantidade de tráfego útil corretemente transmitido, relativo ao tráfego total
- Eficiência: Quantidade de dados úteis transmitidos, descontados os overheads
- Atraso (latência): Tempo médio entre o momento em que um quadro está pronto para ser transmitido e sua recepção em algum destino
- Variação de atraso: Quantidade de variação no atraso médio
- Tempo de resposta: Tempo entre um pedido de serviço e a recepção de uma resposta
- Dependendo da situação, uma ou outra (ou várias) dessas medidas se torna importante

Atraso e variabilidade no atraso

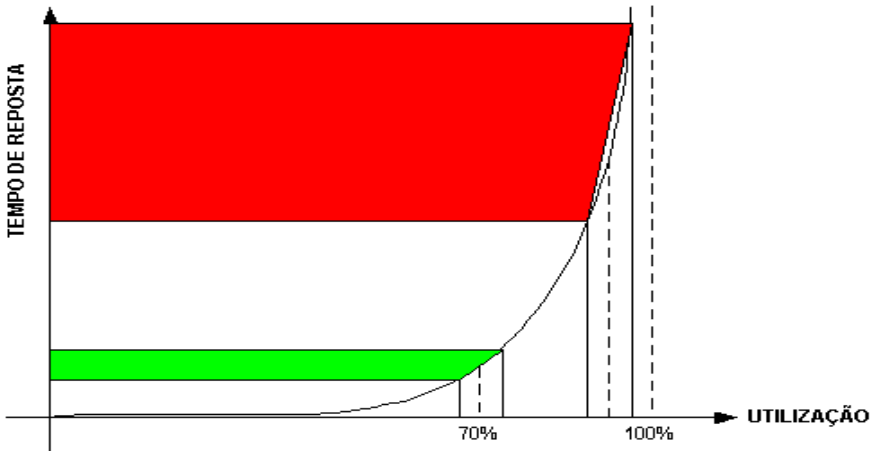
- Aplicações interativas precisam de atraso pequeno
    - Exemplo: Telnet (com o problema adicional do eco remoto de caracteres)

As causas do atraso

- Tempo de propagação
    - Propagação de sinais a 2/3 da velocidade da luz
    - Aproximadamente 4 microsegundos por kilometro
    - Muito importante em enlaces longos (intercontinentais, por exemplo)
    - Muito importante em enlaces de satélite
        - 36000 kilometros de altura
        - 270 ms para subir e descer
        - 540 ms para ter echo de um caractere com Telnet
- Tempo de transmissão
    - Para um pacote de P bits e um canal de C bps, o tempo de transmissão é de P/C segundos
    - Exemplo: P = 1024 bytes, enlace E1 de 2 Mbps, tempo de transmissão = 4 ms
- Tempo de chaveamento de pacotes
    - 10 a 50 microsegundos por pacote numa switch
    - Mais alto para roteadores
- Tempo em fila
    - Tamanho da fila = utilização/(1-utilização)
    - Utilização = (Número médio de pacotes por segundo * Tamanho médio do pacote)/C



    - Tempo em fila = Tamanho da fila * P/C
    - O joelho da curva:



    - Essas equações são fundamentais para calcular a capacidade de enlaces necessária para cumprir os requisitos de atraso

- Exemplo:
    - 5 usuários oferecem tráfego a uma taxa média de 10 pacotes/segundo, cada
    - Os pacotes têm tamanho médio de 1000 bytes
    - Qual é a capacidade do enlace usado para transmitir o tráfego de forma a não exceder um atraso total de 40 ms?

Variação no atraso

- Aplicações multimídia precisam de atraso pequeno e pequena variação no atraso
    - O audio se torna inaudível e o vídeo difícil de ver
- A variação no atraso se chama jitter
    - Jitter causado pelas rajadas de tráfego
    - Pode ser minimizado com bufferização no receptor, mas ao custo de aumentar o atraso
- Se o cliente não puder especificar a variação de atraso, use um máximo de 1% a 2% do atraso total
- ATM é uma boa tecnologia para ter pequena variação de atraso
    - Devido ao uso de células pequenas (53 bytes)
    - Devido ao oferecimento de Qualidade de Serviço (QoS)

Tempo de resposta

- É o mais importante para usuários humanos
- Para aplicações interativas, o limite básico é 100 ms
    - Tempos maiores que 100 ms são sentidos pelos usuários
- Para transferências maiores (página Web, por exemplo), usuários podem esperar uns 10 ou 20 segundos

Utilização máxima

- Pela figura de atraso acima, podemos observar que o joelho da curva representa a utilização máxima aguentável
- Em torno de 70% para enlaces normais
- Em torno de 40% a 45% para Ethernet, onde há perda de banda com colisões

Vazão

- Outras aplicações não se preocupam com atraso, mas precisam de vazão
    - Transferência de grandes arquivos, por exemplo
- Vazão = Quantidade de dados úteis transferidos sem erro por segundo
- Com a saturação do enlace, a vazão até diminuir mesmo com um aumento de carga oferecida

Vazão de dispositivos de interconexão

- Alguns clientes especificam a vazão desejada em termos de pacotes por segundo (PPS) que um dispositivo deve processar sem descartar pacotes
    - Para ATM, são células por segundo (CPS)
- Alguns dispositivos rápidos podem encaminhar pacotes no limite teórico máximo
    - Diz-se que eles operam em wire speed
- O limite máximo = Banda passante total / tamanho do pacote (incluindo cabeçalhos, preambles, ...)

Tamanho do quadro (bytes)	PPS máximo para Ethernet 10 Mbps
64	14.880
128	8.445
256	4.528
512	2.349
768	1.586
1024	1.197
1280	961
1518	812

- Exemplo
    - Um roteador Cisco Catalyst 5000 pode rotear 30 fluxos Ethernet de 10 Mbps
    - Se os pacotes forem de 64 bytes, o roteador estará operando a 14.880 * 30 = 446.400 PPS

Vazão em nível de aplicação

- É a vazão mais interessante para o usuário
- Medida em kilobytes/seg ou megabytes/seg
- Vazão em nível de aplicação só é importante para transferências razoavelmente grandes de informação
- Os fatores que afetam a vazão em nível de aplicação
    - Capacidade dos enlaces
    - Taxas de erros fim-a-fim
    - Funções de protocolos (handshaking, janelas de controle de fluxo, reconhecimentos)
    - Parâmetros de protocolos (tamanho de quadros, valores de timeouts)
    - A taxa de chaveamento de dispositivos (em PPS ou CPS)
    - Pacotes ou células descartados em dispositivos
    - Fatores de desempenho nos servidores e clientes:
        - Velocidade de acesso a disco
        - Buffers de I/O (cache de disco)

        - Desempenho dos drivers de dispositivos
        - Desempenho de barramentos
        - Velocidade de CPU
        - Desempenho de memória real
        - Hit ratio de memória virtual
        - Ineficiências de sistemas operacionais
        - Ineficiências de aplicações
- Analizadores de protocolos e perfiladores de desempenho de software podem ser usados para investigar problemas

Acurácia

- O objetivo da acurácia é de fazer com que os dados recebidos no destino sejam iguais ao dados enviados pela fonte
- Causas de falta de acurácia:
    - Transientes de energia
    - Problemas de descasamento de impedância
    - Problemas de conexões físicas (cabos frouxos, ...)
    - Dispositivos com falhas
    - Ruido causado por máquinas elétrica (motores, ...)
- Em enlaces WAN, a acurácia é especificada como Bit Error Rate (BER)
    - Enlaces analógicos têm BER típica de 1 bit em 10^5
    - Enlaces digitais de cobre têm BER típica de 1 bit em 10^6
    - Enlaces digitais de fibra ótica têm BER típica de 1 bit em 10^{11}
- Em LANs, espera-se não mais do que 1 quadro com erro a cada megabyte de informação
- Para enlaces Ethernet, a taxa de colisão deve ser, no máximo, 3% dos quadros, se a rede estiver saturada e muito menos do que 1% se não estiver saturada
    - Nenhuma colisão tardia deve ocorrer
        - Indica hub ou placa de rede (NIC) com problemas
        - As colisões devem ocorrer no preâmbulo ou nos primeiros 64 bytes (runt packet)

Eficiência

- A eficiência descreve o efeito de overhead na transmissão de informação
- Exemplo: Ethernet não é eficiente quando o enlace está saturado
- Causas de ineficiência:
    - Colisões
    - Passagem de ficha
    - Indicações de erro
    - Re-roteamentos
    - Reconhecimentos
    - Cabeçalhos
- Uma forma de minimizar ineficiências devidas a cabeçalhos é de usar o maior quadro possível na tecnologia sendo empregada
    - Há um limite no tamanho do quadro para diminuir erros de quadros, já que um quadro muito grande tem mais probabilidade de sofrer danos na transmissão, perdendo assim todo o quadro
- Observe os tamanhos máximos de quadros para várias tecnologias abaixo

Tecnologia	**Quadro máximo**
Ethernet 10 Mbps e Fast Ethernet 100 Mbps	1518 bytes (incluindo cabeçalho e CRC)
Token Ring 4 Mbps	4500 bytes
Token Ring 16 Mbps	18000 bytes
FDDI	4500 bytes
ATM com AAL5	65535 bytes (payload AAL5)
ISDN Basic Rate Interface (BRI) e Primary Rate Interface (PRI) usando Point-to-Point Protocol (PPP)	1500 bytes
E1	Não especificado, mas 4500 bytes geralmente usado

Segurança

- Aspecto muito importante do projeto de uma rede, especialmente com conexões à Internet e Extranet
- Objetivo básico: Problemas de segurança não devem afetar a habilidade da empresa conduzir negócios
- Primeira tarefa: planejamento
    - Análise de riscos
    - Levantamento de requisitos
- A segurança sempre envolve tradeoffs
    - Ao aumentar a segurança, perde-se facilidade de uso e produtividade dos funcionários

Análise de riscos

- Para implementar a segurança de um site, deve-se investigar os riscos de não implementar a segurança
    - Os dados do cliente são muito sensíveis?
    - Qual é o efeito do roubo de dados?

    - Qual é o efeito da mudança de dados?
- Se uma Virtual Private Network (VPN) for usada para acessar a rede corporativa usando a Internet, quais são os riscos envolvidos com o uso de um serviço VPN oferecido por um provedor? O provedor tem tecnologia VPN com funcionalidade adequada?
- Observe que o roubo de informação através de packet sniffing (roubando pacotes na rede) não é grande quando cripotografia adequada é usada (VPN, Secure Sockets Layer - SSL)
- Os perigos maiores são de acessar/mudar dados diretamente nos servidores
    - Páginas Web, por exemplo
- Hackers podem atacar um site das seguintes maneiras gerais:
    - Usando recursos que não deveriam poder acessar
    - Inibir o uso de recursos por usuários válidos (denial of service)
    - Alterar, roubar ou destruir recursos
    - Aproveitar-se de buracos de segurança bem conhecidos em sistemas operacionais e aplicações
- As empresas se preocupam principalmente com os seguintes três aspectos da segurança:
    - Virus
    - Problemas causados por erros de usuários
    - Problemas causados por usuários internos maliciosos

Requisitos de segurança

- Os "recursos" que devem ser protegidos são:
    - Hosts, incluindo servidores
    - Dispositivos de interconexão (switches, roteadores, ...)
    - Dados de sistemas ou de aplicações
    - A imagem da empresa
- Requisitos típicos podem incluir atingir os seguintes objetivos:
    - Permitir que pessoas externas acessem dados públicos (via http, ftp, ...), mas não dados internos
    - Identificar, autenticar e autorizar usuários de filiais, usuários móveis e empregados que trabalham em casa
    - Detectar "penetras" e identificar os danos causados pela intrusão
    - Autenticar atualizações de tableas de roteamento recebidas de roteadores internos e externos
    - Proteger dados recebidos de ou transmitidos para sites remotos via VPN
    - Proteger hosts e dispositivos fisicamente
    - Proteger hosts e dispositivos logicamente através de senhas e direitos de uso
    - Proteger aplicações e dados contra virus
    - Treinar usuários sobre a política de segurança da empresa e sobre formas de evitar problemas de segurança

Gerenciabilidade

- Seu cliente pode ter planos específicos de gerência que afetarão a escolha de equipamentos
    - Exemplo: uso de SNMP para gerenciar a rede
- A gerência pode ser dividida em 5 áreas:
    - Configuração: todos os clientes precisam desse tipo de gerência
    - Falha: todos os clientes precisam desse tipo de gerência
    - Desempenho: a maioria dos clientes precisa desse tipo de gerência
    - Segurança: a maioria dos clientes precisa desse tipo de gerência
    - Contabilidade: alguns clientes precisa desse tipo de gerência
- Aspectos de gerência não serão cobertos nessa disciplina, pois formam um aspecto crucial do propeto de uma rede e são cobertos em outra disciplina

Usabilidade

- Usabilidade diz respeito à facilidade com a qual usuários acessam os serviços via rede
- Enquanto a gerenciabilidade melhora a vida do gerente de rede, a usabilidade foca o usuário final
- Melhorar a usabilidade significa avaliar:
    - Os impactos da política de segurança na facilidade de uso
    - A facilidade com a qual a rede é configurada (usando DHCP, por exemplo)
    - A facilidade com a qual a rede corporativa é usada remotamente (usando VPN, por exemplo)
    - A facilidade com a qual um usuário móvel pode se integrar à rede em vários pontos (sede, filiais, ...)

Adaptabilidade

- A adaptabilidade descreve como o projeto de rede pode se adaptar a:
    - Mudanças de tecnologia
    - Mudanças de protocolos
    - Mudanças de formas de negócio
    - Mudanças de legislação
- Um dos aspectos mais importantes da adaptabilidade é a facilidade com a qual Moves-Adds-Changes (MAC) podem ser feitos na rede (usando VLANs, por exemplo)

Cost-effectiveness

- O objetivo principal aqui é de oferecer os serviços de rede com a qualidade desejada ao menor custo

    - Ou de maximizar a qualidade dos serviços para um determinado custo
- Os custos podem ser não recorrentes (custos de aquisição) ou recorrentes (custos de operação)
- Para redes locais, a velocidade e a disponibilidade já são altas e o objetivo principal é de minimizar custos
    - Aquisição de equipamentos com baixo custo por porta
    - Minimização dos custos de cabeamento
    - Aquisição de placas de rede de baixo custo
- Para a rede corporativa como um todo, a disponibilidade é frequentemente mais importante que o custo
- Mas a parte mais importante do custo, aluguel de enlaces de comunicação, deve ser mantida baixa
    - Para minimizar os custos de operação de uma WAN, os seguintes objetivos técnicos podem ser incluídos:
        - Usar um protocolo de roteamento que minimize tráfego na WAN
        - Usar um protocolo de roteamento que use rotas de tarifação mínima
        - Consolidar tráfego de voz e dados para eliminar troncos paralelos para cada tipo de tráfego
        - Usar tecnologias que compartilhem enlaces (comutação de pacotes em vez de comutação de circuitos)
        - Melhorar a eficiência de enlaces WAN usando compressão, supressão de silêncio, etc.
- O segundo aspecto mais caro da operação de uma WAN diz respeito ao pessoal de suporte e operação da rede (salários, treinamento)
    - Para minimizar tais custos:
        - Aquisição de equipamentos fáceis de configurar, operar, manter e gerenciar
        - Usar um projeto de rede simples de entender e depurar
        - Manter uma boa documentação do projeto de rede

Tradeoffs no projeto de redes

- Alguns objetivos técnicos entram em conflitos com outros
- Exemplos:
    - Custo versus a maioria dos outros objetivos
        - Alta disponibilidade implica em redundância (maior custo)
        - Alto desempenho requer alta capacidade de enlaces ou outras tecnologias caras (ATM)
    - Segurança diminui facilidade de uso
    - Adaptabilidade a constantes mudanças pode diminuir a disponibilidade
    - Alta vazão pode implicar em alto atraso
- Como lidar com esses tradeoffs?
    - Identificar o objetivo único mais importante que deve ganhar dos outros
        - Serve para desempatar decisões
    - Priorizar os outros objetivos técnicos
        - Pode ser feito pedindo ao cliente para dizer o percentual aproximado a ser gasto para cada objetivo
        - Exemplo:

Escalabilidade	20%
Disponibilidade	30%
Desempenho	15%
Segurança	5%
Gerenciabilidade	5%
Usabilidade	5%
Adaptabilidade	5%
Cost-effectiveness	15%
Total	**100%**

Checklist para objetivos técnicos

- Documentei os planos de expansão do cliente para os próximos dois anos, em termos de sites, usuários, servidores, estações
- O cliente me informou sobre planos para migrar servidores departamentais para um server farm
- O cliente me informou sobre planos para integrar mainframes SNA com a rede corporativa IP
- O cliente me informou sobre planos para implantar uma intranet ou extranet
- Documentei os objetivos de disponibilidade em termos de % de up time ou em termos de MTBF e MTTR
- Documentei os desejos sobre utilização máxima em segmentos compartilhados
- Documentei objetivos para a vazão desejada ou necessária para cada aplicação
- Documentei objetivos de vazão PPS para dispositivos de interconexão
- Documentei objetivos de acurácia em termos de BER aceitáveis
- Discuti com o cliente a importância de utilizar quadros grandes para maximizar a eficiência da rede
- Identifiquei aplicações que precisam de tempos de resposta menores do que o normal de 100 ms
- Discuti os riscos e requisitos de segurança com o cliente
- Levantei requisitos de gerenciabilidade, incluindo objetivos de gerência de configuração, falha, desempenho, segurança e contabilidade

- Junto com o cliente, priorizei os objetivos de negócio e técnicos. Sei qual é o objetivo mais importante
- Atualizei a tabela de aplicações (abaixo) para incluir objetivos técnicos

Nome da aplicação	Tipo de aplicação	Nova aplicação (sim/não)	Criticalidade	Custo de downtime	MTBF aceitável

MTTR aceitável	Vazão desejada	Atraso máximo	Variação máxima de atraso	Comentários

Caracterização da Rede Existente

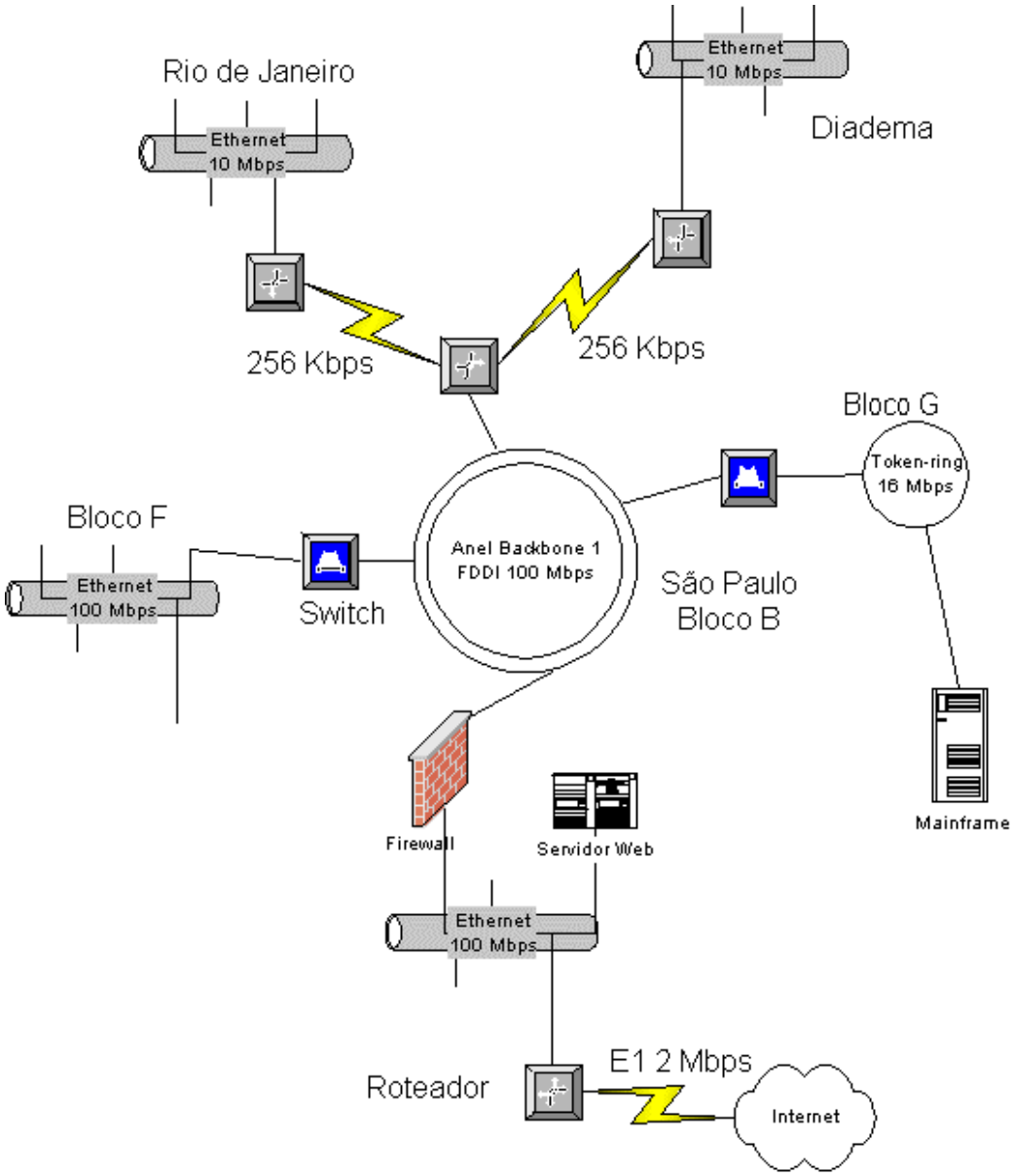
- Quando há uma rede existente que está sendo expandida, ela deve ser examinada e caracterizada detalhadamente
- A caracterização inclui:
  - A topologia
  - A estrutura física
  - O desempenho da rede
    - Deseja-se identificar gargalos existentes e adquirir um baseline de desempenho para efeitos comparativos futuros

Caracterização da infraestrutura da rede

- Precisamos montar uma mapa de rede, incluindo a localização dos segmentos e dispositivos de interconexão
- Descobrem-se os métodos usados para dar nomes aos segmentos e dispositivos
- São descobertos os tipos e tamanhos de estruturas de cabeamento usados
- Restrições arquiteturais e ambientais são descobertas

Desenvolvimento de um mapa de rede

- Para começar a entender os fluxos de tráfego, inicia-se com a descoberta de
  - Hosts importantes
  - Segmentos importantes
  - Dispositivos de interconexão importantes
- Ao juntar essa informação com dados de desempenho, você vai adquirir um bom conhecimento das áreas de concentração dos usuários e o nível de tráfego que a rede deve suportar
- Ferramentas que podem ser usadas para montar o mapa de rede
  - Visio Professional
    - Pode obter dados de um BD ou planilha
  - Ferramentas que descobrem topologias automaticamente
    - ClickNet Professional
    - NetSuite Professional Audit
  - Ajudam a descobrir dispositivos, hosts (com CPU, memória, interfaces de rede, ...)
- O que incluir no mapa de rede?
  - Informação geográfica (países, estados, cidades, campi)
  - Conexões WAN entre países, estados e cidades
  - Prédios, andares, chegando às vezes até salas ou cubículos
  - Conexões LAN e WAN entre prédios e entre campi
  - Tecnologias dos enlaces (Ethernet, Fast Ethernet, ATM, Frame Relay, Datasat, ...)
  - Nome do provedor de serviços de telecomunicações (enlaces WAN)
  - Localização de roteadores e switches, mas normalmente não chegando até hubs
  - Localização e alcance de qualquer VPN
  - Localização de servidores principais e server farms
  - Localização de mainframes
  - Localização de estações de gerência
  - Localização e alcance de VLANs
    - Use cores para diferenciar VLANS, já que o cabeamento físico não indica quem pertence a qual VLAN
  - Topologia de sistemas de firewalls e bastion hosts
  - Localização de sistemas de dial-in ou dial-out
  - Localização das workstations (contadores por área são suficientes)
  - Topologia lógica da rede (collapsed backbone, server/core/distribution/access blocks)
- Exemplo de um mapa de alto nível (com muitos detalhes ausentes)



Caracterização dos esquemas de endereçamento e de naming

- Para caracterizar a estrutura lógica, inicia-se pelo descobrimento de esquemas de endereçamento e naming usados na empresa
    - Documente essas estratégias
        - Exemplo: uso de códigos de aeroportos - CPV, REC, GRU
        - Exemplo: sufixos para roteadores (rtr, ...)
- Documente o esquema de endereçamento IP usado, incluindo estratégias de subnetting, supernetting (sumarização de rotas), Network Address Translation (NAT), endereçamento privativo (10.0.0.0), etc.
    - Esses esquemas poderão afetar a forma de escolher protocolos de roteamento, por exemplo
    - Frequentemente, todo o esquema de endereçamento deve ser refeito

Caracterização do cabeamento e mídias

- Documente o tipo de cabeamento usado (UTP cat-3, UTP cat-5, UTP cat-5 extended, STP, cabo coaxial, fibra multimodo, fibra monomodo, ...)
- Tente levantar o comprimento dos cabos
    - Muitas tecnologias de camada 2 têm limites de comprimento de cabos
    - Normalmente, 100 metros é o limite
- Levante a forma com a qual os cabos são etiquetados
- Levante os cabos (ou outras tecnologias) disponíveis entre prédios (tipos, número de pares)
    - Incluir tecnologias wireless (radio, laser, infra-vermelho, microondas)
- Dentro dos prédios, levante os wiring closets, salas de telecomunicações, etc.
- Levante todos os tipos de cabeamento disponíveis:
    - Cabeamento vertical (entre andares)
    - Cabeamento horizontal (para chegar aos conectores nas paredes das salas)
    - Cabeamento de área de trabalho (para chegar dos conectores de parede até as estações
- Preencha a tabela abaixo

Nome do prédio:						
Localização de wiring closets:						
Localização de salas de telecomunicação (acesso externo)						
Topologia lógica de cabeamento (estruturado, estrela, barramento, anel, mesh, árvore, ...)						
Cabeamento vertical						
	Coaxial	Fibra	STP	UTP cat-3	UTP cat-5	Outro
Shaft vertical 1						
Shaft vertical 2						
Shaft vertical 3						
Cabeamento horizontal						
	Coaxial	Fibra	STP	UTP cat-3	UTP cat-5	Outro
Andar 1						
Andar 2						
Cabeamento de área de trabalho						
	Coaxial	Fibra	STP	UTP cat-3	UTP cat-5	Outro
Andar 1						
Andar 2						

Verificação de restrições arquiteturais e ambientais

- Cabeamento externo (restrições ambientais)
  - O cabeamento deve passar por áreas que podem sofrer enchente?
  - O cabeamento deve passar perto de linhas de trem?
  - O cabeamento deve passar perto de estradas onde o tráfego pode deslocar cabos?
  - O cabeamento deve passar por áreas onde atividades de construção poderiam quebrar cabos?
  - O cabeamento deve passar por áreas que pertencem a terceiros?
  - Há restrições de "visada" a serem observadas entre locais remotos?
- Cabeamento interno (restrições arquiteturais)
  - Como está o ar condicionado para a nova rede?
  - Como está a ventilação para a nova rede?
  - Como está a energia para a nova rede?
  - Como está a proteção contra interferência eletromagnética para a nova rede?
  - Há espaço para canaletas de cabeamento, patch panels, racks de equipamentos?
  - Há acesso fácil aos equipamentos para troubleshooting?

Verificação da saúde da rede existente

- É extremamente útil poder comparar o desempenho da nova rede com a rede existente
  - Será mais fácil mostrar ao cliente como o desempenho melhorou na nova rede
  - Se desempenho não for um objetivo mas baixo custo for, você vai poder mostrar como o desempenho não sofreu na nova rede
- Para tanto, adquire-se um baseline de desempenho

O desafio de desenvolver um baseline de desempenho

- Não é fácil obter um baseline de desempenho:
  - Onde adquirir dados? (a rede pode ser muito grande)
    - Escolher segmentos representativos e extrapole conclusões
  - Em que momentos adquirir dados (média, pico)?
    - Depende do tipo de desempenho que você quer melhorar (média, pico)
  - Durante quanto tempo adquirir dados (horas? dias? semanas?)
    - O cliente pode não deixar que você acesse a rede
    - Você pode não ter muito tempo disponível
    - A aquisição não pode ser momentânea: deve representar uma média
  - Como adquirir dados?
    - Falaremos de ferramentas adiante

Análise da disponibilidade da rede

- Obtenha estatísticas de downtime (MTBF, MTTR) do próprio cliente (pessoal de suporte)
- Dadas as estatísticas, os objetivos de MTBF e MTTR do cliente para a nova rede são realísticos?
- Quando foi a última queda importante? Quais foram as causas?
- Documente os resultados usando a tabela abaixo:

	MTBF	MTTR	Data e duração da última queda importante	Causa da última queda importante
Rede como um todo				
Segmento 1				
Segmento 2				
Segmento 3				
Segmento 4				

Análise da utilização da rede

- A utilização dos enlaces é o que normalmente mais afeta a lentidão de uma rede
- Cuidado com a granularidade
    - Médias por hora podem não evidenciar problemas de saturação
    - Melhor usar médias a cada 10 minutos
    - Mais granularidade do que isso é indesejável pois mostra muitos "transientes" (detalhes demais)
- Adquira estatísticas durante uns dois dias
    - Dias típicos ou dias de pico, dependendo dos objetivos
- É interessante (porém mais tedioso) adquirir informação para cada protocolo utilizado na rede (tabela abaixo)

	Utilização relativa ao tráfego total	Utilização relativa à capacidade do enlace	Taxa de broadcast/multicast
IP			
IPX			
AppleTalk			
DECNet			
Banyan			
NetBIOS			
SNA			
Outros			

Análise da acurácia da rede

- Um BERT (BER tester) pode ser usado para testar a taxa de erros da rede
- Medir a BER é melhor para enlaces contratados
    - As promessas aparecem nos contratos (Service Level Agreements - SLAs)
- Em redes locais, é melhor medir erros de quadros
- Meça o número de frames por hora recebidos com erro durante alguns dias
- Um limiar típico é de 1 quadro em erro a cada Megabyte de dados
- Concentre os esforços onde pode haver problemas de interferência elétrica
- Problemas de cabeamento podem ser descobertos também antes que a nova rede seja implantada

Análise da eficiência da rede

- Use um analisador de protocolos para ver o tamanho dos quadros que circulam na rede
- Normalmente, haverá muitos quadros pequenos (quadros de controle) e muitos quadros grandes (quadros completos)

Análise do atraso e tempo de resposta

- Meça o atraso entre dispositivos e hosts importantes da rede
- O utilitário ping fornece o tempo de ida-e-volta (round trip time - RTT)

Verificação do status dos roteadores principais

- Roteadores possuem comandos que permitem verificar algumas estatísticas internas
    - SNMP também pode ser usado
- Exemplos (Cisco):
    - show interfaces
        - Para ver taxas de entrada e saída, pacotes descartados, tamanho das filas, quantas vezes a interface foi resetada, etc.
        - Lembre que contadores são cumulativos e não taxas
            - Faça várias medições e calcule as taxas
    - show processes
        - Para ver utilização de CPU, utilização por processos (roteamento, gerência de buffers, ...)
    - show buffers
        - Para ver tamanho de buffers, tentativas mal sucedidas de obter buffers de vários tamanhos, etc.

Ferramentas para caracterizar a rede existente

- Se a rede está sendo gerenciada, muita informação estará disponível através da estação de gerência

Analisadores de protocolos

- Captura tráfego de rede, decodifica os pacotes e provê estatísticas
- Um dos melhores é o Sniffer Network Analyzer da Network Associates
- Outro é EtherPeek da AG Group

Ferramentas de monitoração remota

- Probes RMON ajudam a adquirir uma quantidade fantástica de estatísticas de rede
- Os resultados são obtidos através de SNMP
- Pode-se ver, entre outras coisas:
    - Erros de CRC
    - Colisões em segmentos Ethernet
    - Errors em segmentos Token Ring
    - Tamanhos de quadros
    - Taxa de tráfego em cada interface
    - Taxa de broascast

- Quem conversa com quem
- etc.

Checklist de saúde da rede

- A rede existente está saudável se:
  - A topologia de rede e a infraestrutura física estão bem documentadas
  - Endereços de rede e nomes são atribuídos de forma estruturada e estão bem documentados
  - O cabeamento da rede foi instalado de forma estruturada e está bem etiquetado
  - O cabeamento entre os wiring closets e as estações não ultrapassa 100 metros
  - A disponibilidade da rede satisfaz os objetivos do cliente
  - A segurança da rede satisfaz os objetivos do cliente
  - Nenhum segmento Ethernet está saturado (40% max ao longo de 10 minutos)
  - Nenhum outro segmento ou enlace está saturado (70% max ao longo de 10 minutos)
  - Nenhum segmento tem mais do que 1 erro de CRC a cada milhão de bytes
  - Nenhum segmento Ethernet tem taxa total de colisão maior que 3%
  - Nenhum segmento Ethernet tem colisões tardias
  - Em redes Token Ring, menos de 0,1% dos quadros são pacotes de erro
  - O tráfego de broadcast não ultrapassa 20% do tráfego total
  - O tamanho máximo do quadro foi otimizado para cada tecnologia utilizada no enlace
  - Nenhum roteador está sobreutilizado (70% de utilização)
  - Nenhum roteador está descartando mais do que 1% dos pacotes
  - O tempo de resposta entre clientes e servidores (ida-e-volta) não ultrapassa 100 ms

Caracterização do Tráfego de Rede

- Queremos caracterizar quatro coisas nesse capítulo:
  - O fluxo de tráfego (de onde vem, para onde vai)
  - A carga de tráfego (para poder estabelecer capacidade de enlaces)
  - O comportamento do tráfego (considerações de broadcast, eficiência)
  - Considerações de qualidade de serviço (QoS)
- Com esta informação, poderemos escolher soluções adequadas no projeto lógico e no projeto físico da rede

Caracterização do fluxo de tráfego

- Identificações de fontes e sorvedouros de tráfego
- Identificação de direções e simetria
  - Exemplo: Uma aplicação cliente-servidor é tipicamente assimétrica, com o cliente enviando pouco e o servidor respondendo com muito
- Falaremos tanto da caracterização de tráfego na rede existente quanto da caracterização do tráfego das aplicações da rede nova

Identificação de fontes e sorvedouros principais

- Identificamos primeiro comunidades de usuários e locais de armazenamento maciço de dados
- Uma comunidade é um conjunto de usuários que utiliza as mesmas aplicações
  - Pode corresponder a um departamento ou conjunto de departamentos
  - Pode também cruzar fronteiras de departamentos
    - Exemplo: quando se formam times virtuais temporários numa empresa que utiliza "gerência em matriz" (alocação de times por projeto)
    - Neste caso, a divisão de comunidades é estritamente por utilização de aplicação e não por departamento
- Documentamos comunidades de usuários usando a tabela abaixo

Nome da comunidade de usuários	Tamanho da comunidade (número de usuários)	Localização da comunidade	Aplicações usadas pela comunidade

- Precisamos identificar também grandes sorvedouros de dados, que são tipicamente onde dados são armazenados (data stores ou armazens de dados)
  - Servidor, server farm, mainframe, unidade de backup em fita, biblioteca de vídeo
  - Observe que tais sorvedouros poderão também ser importantes fontes de informação
- Documentamos os data stores usando a tabela abaixo

Data store	Localização	Aplicações	Comunidades que usam o data store

Documentação do fluxo de tráfego na rede existente

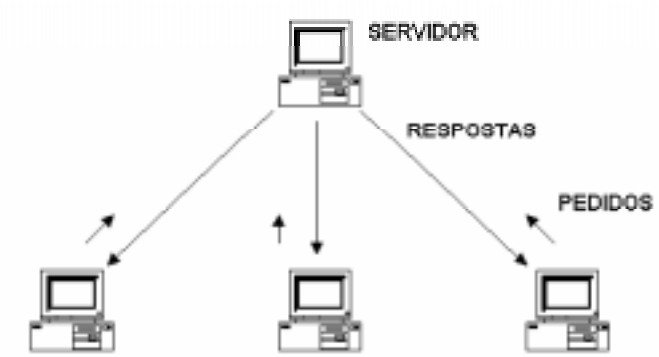
- Queremos identificar e caracterizar fluxos individuais de tráfego entre fontes e sorvedouros

- A RFC2063 (Traffic Flow measurement: Architecture) contém informação útil sobre este tópico
- Um fluxo individual comporta o tráfego de protocolo e de aplicação transmitido entre entidades durante uma única sessão
- Os atributos de um fluxo:
    - Direção
    - Simetria
    - Caminho (path)
    - Número de pacotes
    - Número de bytes
    - Endereços fonte e destino
- Pode -se identificar a quantidade de bytes de um fluxo usando um analizador de protocolos ou informação de uma estação de gerência de rede
- Coletando informação a partir de um ponto central da rede durante alguns dias, pode-se preencher a tabela abaixo
    - Um programa como traceroute (tracert) ou as próprias tabelas de roteamento podem ser usadas para descobrir as rotas

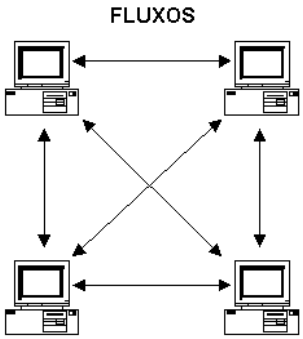
	Destino 1		Destino 2		Destino 3		Destino 4	
	Mbytes/seg	Rota	Mbytes/seg	Rota	Mbytes/seg	Rota	Mbytes/seg	Rota
Fonte 1								
Fonte 2								
Fonte 3								
Fonte 4								

Caracterização dos tipos de tráfego para a nova rede

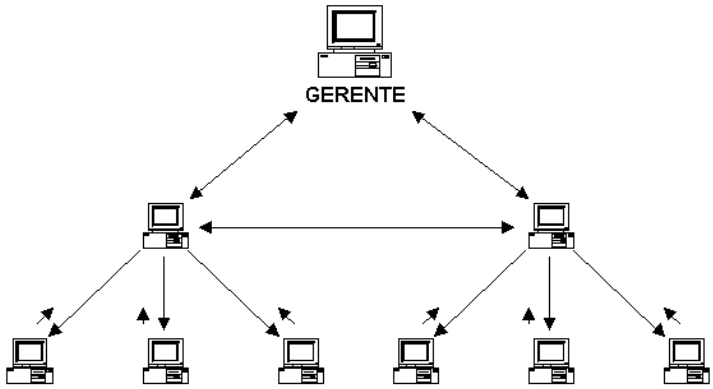
- Para novas aplicações, não podemos medir o tráfego na rede
- Temos que usar técnicas indiretas para caracterizar o tráfego
- Fundamental: precisamos entender como aplicações típicas se comportam (em termos de tráfego)
- Para ajudar na tarefa, usam-se Modelos de Fluxos bem conhecidos
    - Modelo termina-hospedeiro
    - Modelo cliente-servidor
    - Modelo peer-to-peer (par-a-par)
    - Modelo servidor-servidor
    - Modelo de computação distribuída
- Modelo de fluxo de tráfego terminal-hospedeiro
    - Fluxo assimétrico
    - O terminal manda alguns bytes e o hospedeiro responde com muitos bytes
    - Exemplo: telnet
    - Telnet pode mandar 1 byte por pacote do terminal para o hospedeiro
        - Mas também pode esperar um pouco e mandar muitos bytes
        - Para aplicações com linha de comando, pode-de ligar o eco local e mandar os bytes apenas ao digitar <ENTRA>
        - Para aplicações full-screen, não se pode esperar até o fim da linha
            - Uso de timeout para mandar vários caracteres de uma vez
            - A resposta desenha a tela
                - 1920 caracteres + caracteres de atributos + caracteres de posicionamento de cursor
                - Pode ser menos bytes com aplicações que desenham diferenças de tela
                - É assim para aplicações que usam o pacote libcurses no UNIX
                - É para saber como manipular a tela do terminal que se usa o comando "set term vt100"
- Modelo de fluxo de tráfego cliente-servidor
    - É o modelo mais aplicável hoje
    - É bidirecional e assimétrico
        - Tem dados nas duas direções (pedidos e respostas)
    - Pedidos pequenos e respostas maiores
    - Direção servidor ==> clientes é mais usada
        - Para muitas aplicações, pode-se considerar o fluxo unidirecional
    - O servidor é uma fonte de dados
    - Exemplo: a web moderna



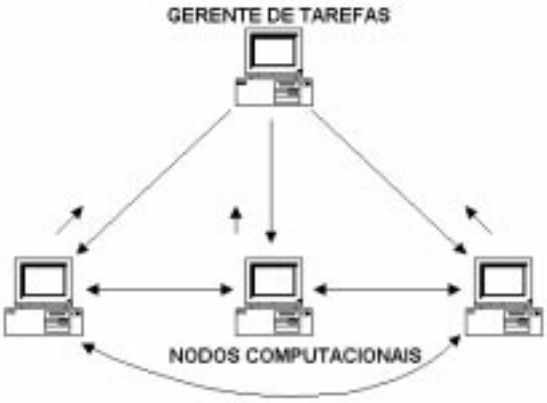
- Modelo de fluxo de tráfego peer-to-peer
  - Usuários e aplicações são mais ou menos equivalentes nos seus requisitos de comunicação
  - Não tem direcionalidade óbvia
  - Exemplo: teleconferência onde todos os usuários participam e podem ser fontes e/ou sorvedouros
  - Exemplo: Internet antiga ondes todos faziam FTP e mail a partir de computadores centralizados (usando terminais burros e não PCs)



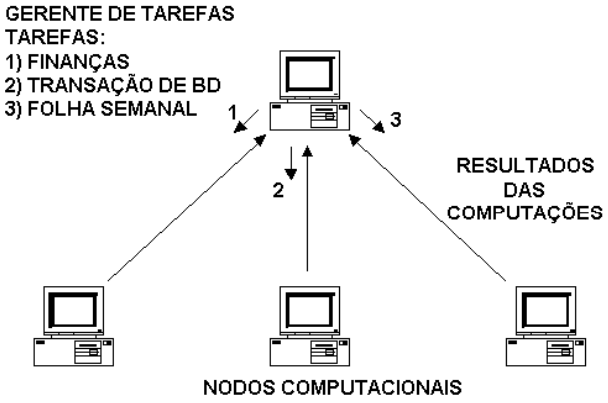
- Modelo de fluxo de tráfego servidor-servidor
  - Quando servidores conversam entre si
  - A simetria depende da aplicação particular
  - Exemplos:
    - Serviços de diretório
    - Cache de dados
    - Mirroring de dados para obter redundância e balanceamento de carga
    - Backup de dados
  - Exemplo final: computação cooperativa onde um trabalho é feito por várias máquinas comandadas por um hospedeiro gerente (ver figura)



- Modelo de fluxo de tráfego de computação distribuída
  - É o modelo mais especializado (e mais raro)



- Fluxos podem estar entre o manager e os nodos de computação ou entre os nodos de computação
  - Depende do acoplamento presente e da granularidade
- Com granularidade grossa e acoplamento fraco, temos um cluster de computação
  - Gerente aloca tarefas aos nodos
  - Comunicação entre gerente e nodos
  - Parece um modelo cliente-servidor
    - Porém os dados gerados no fim pelos nodos podem ser muito grandes comparados com a informação de inicialização enviada pelo gerente
    - Fluxo assimétrico mas no sentido contrário ao modelo cliente-servidor
  - Ver figura abaixo



- Com granularidade fina e acoplamento forte, temos um sistema de processamento paralelo
  - Tarefas são alocadas pelo gerente de tarefas aos nodos de computação
    os nodos trocam informação devido ao acoplamento forte
  - Entre todos os modelos, este tem os requisitos mais fortes de desempenho
  - O timing de transferência de informação é crítico porque as tarefas esperam pelos dados de outros nodos
  - Entre os nodos, não tem direcionalidade especial
  - Não tem fontes ou sorvedouros claros

Documentação do fluxo de tráfego na rede nova

- Para documentar os fluxos para aplicações existentes e novas, escolha o tipo de modelo, e identifique fontes e sorvedouros
- Use a tabela abaixo
  - Falaremos de requisitos QoS adiante
  - Os comentários pode dizer se a aplicação é full-screen, se é fortemente acoplada, etc.

Nome da aplicação	Modelo de fluxo	Protocolos usados pela aplicação	Comunidades de usuários que usam a aplicação	Data stores (Servidores, hospedeiros, ...)	Demanda aproximada de banda passante para a aplicação	Requisitos de QoS

Caracterização da carga de tráfego

- Queremos caracterizar a carga de tráfego para o correto planejamento de capacidade dos enlaces
- É muito difícil ter uma idéia precisa da carga de tráfego, mas queremos tentar evitar gargalos na rede final

Cálculo da carga teórica de tráfego

- Na teoria, as coisas são relativamente simples
- Para calcular a carga, precisamos saber:
  - O número de estações que geram tráfego
  - O tempo médio entre quadros gerados

    - O tamanho médio dos quadros transmitidos
- Alguns parâmetros adicionais que podem ajudar a levantar a carga:
    - A frequência de sessões de aplicações
    - O tempo médio de cada sessão
    - O número de sessões simultâneas
- O problema é justamente estimar todos esses parâmetros!
- Tem que conhecer as aplicações e fazer estimativas
- Pode-se usar ferramentas de modelagem de redes que possuem conhecimento embutido de certos tipos de aplicações e permitem parametrizar o modelo interno
- A tabela abaixo pode ajudar a ter uma noção do tamanho de objetos trocados numa sessão de trabalho

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

- Mostraremos um exemplo real de estimativas de tráfego adiante

Incluindo o overhead de protocolos

- Deve-se adicionar o overhead devido a protocolos usados pelas aplicações
    - A tabela abaixo ajudará a fazer as estimativas

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

Estimativas de carga de tráfego de protocolos de roteamento

- Protocolos de roteamento adicionam overhead de tráfego
- Calcular o overhead é especialmente importante para estimar o tráfego adicional num enlace WAN lento
- Os protocolos de roteamento ainda não foram escolhidos mas a tabela abaixo fornece uma idéia do overhead

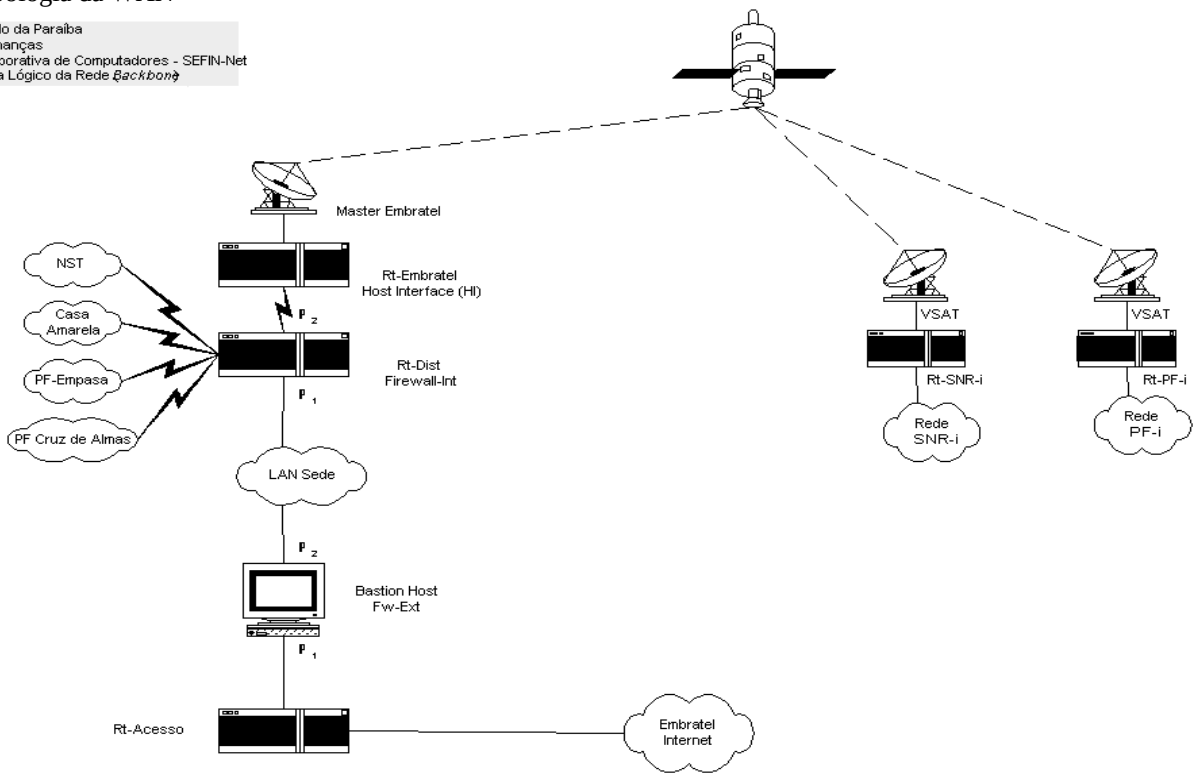
Protocolo de roteamento	**Tempo default de atualização (seg)**	**Tamanho da entrada da tabela**	**Rotas por pacote**	**Overhead da atualização (bytes)**	**Tamanho de um pacote cheio**
IP RIP	30	20	25	32	532
IP IGRP	90	14	104	32	1488
AppleTalk RTMP	10	6	97	17	599
IPX SAP (não é protocolo de roteamento)	60	64	7 serviços	32	480
IPX RIP	60	8	50	32	432
DecNet Phase IV	40	4	368	18	1490
Vines VTRP	90	8	104	30	862
XNS (Xerox)	30	20	25	40	540

Um exemplo

- Rede SEFIN conectando a sede, Superintendências Regionais, Coletorias e Postos Fiscais
- Só importa o levantamento de tráfego na WAN para caracterizar os enlaces WAN
    - A LAN é de 100 Mbps na sede e não há tráfego pesado
    - A LAN é de 10 Mbps nas SNRs e PFs e não há tráfego pesado

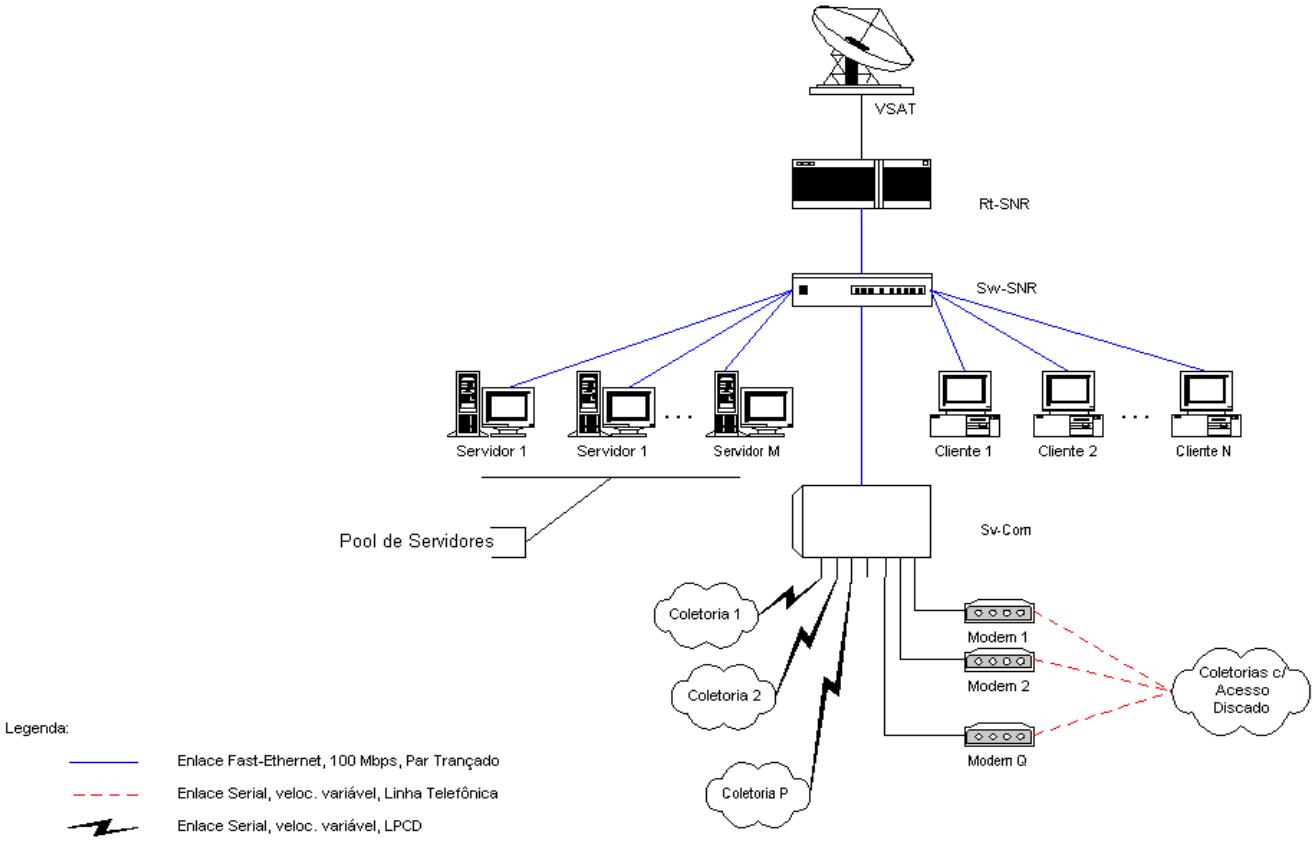
- Topologia da WAN

Governo do Estado da Paraíba
Secretaria das Finanças
Projeto: Rede Corporativa de Computadores - SEFIN-Net
Figura 1: Esquema Lógico da Rede *Backbone*



- Topologia de uma SNR

Governo do Estado da Paraíba
Secretaria das FInanças
Projeto: Rede Corporativa de Computadores - SEFIN-Net
Figura 3: Organização da Rede (Superintendência com Acesso Dedicado e Discado!)



- A planilha de tráfego está aqui
- Reproduzimos algumas planilhas abaixo
- Parâmetros usados

Parâmetros		
Parâmetro	Valor	Observação
Número de SNRs	9	Superintendências regionais
Número de PFs	19	Postos fiscais
Bytes numa tela	3000	Tela geral de consulta
Overhead telnet	20%	
Overhead replicação	100%	
Overhead Cliente/Servidor	100%	Pequenas transações significam overhead maior
Overhead de FTP	20%	
Espera por 1 tela telnet	2	Tempo que usuário deve esperar por uma tela
Compactação dados	70%	
Bits por byte	8	
Utilização máxima	0,4	Utilização máxima de um canal para ter fila média
Fila média	0,5	Fila aceitável
Overhead HTML	20%	
Página HTML	50000	Número de bytes numa página HTML com tags e imagens incluídos
Carga página HTML	5	Tempo que usuário deve esperar por uma página
Página HTML de legislação	10000	Número de bytes numa página HTML de legislação, com tags e imagens incluídos

- Fluxos individuais
  - Observe como a capacidade do enlace é calculada levando em consideração atraso razoável e vazão

Aplicação	**Tipo de Acesso**	**Número de sessões simultâneas**	**Número de "consultas" por hora na sessão**	**Número de Interações numa "consulta"**	**Descrição dos dados de uma interação**	**Tamanho em bytes de uma interação**	**Overhead de protocolo**	**Tamanho da interação com overhead**	**Tráfego total em bytes/hora**	**Tamanho em bytes da interação com limite de tempo**	**Limite de tempo da interação (segundos)**	**Tráfego total em bps**	**Capacidade total em bps necessária para atender ao limite de tempo**
Cadastro de contribuinte													
Replicação PF	Bulk	1	1	1	Replicação de 15 novas entradas	7500	100%	15000	15000	15000	60	33	3000
Replicação SNR	Bulk	1	1	1	Replicação de 15 novas entradas	7500	100%	15000	15000	15000	60	33	3000
Acesso Web interna de fora	HTTP	10	1	3	Página HTML	20000	20%	24000	720000	24000	5	1600	57600
Acesso central	telnet	2	1	4	Tela de consulta	3000	20%	3600	28800	3600	2	64	21600

(SNR pequena)													
Acesso central (Patos/Sousa)	telnet	10	1	4	Tela de consulta	3000	20%	3600	144000	3600	2	320	21600
Acesso central (JP/CG)	telnet	30	1	4	Tela de consulta	3000	20%	3600	432000	3600	2	960	21600
Acesso central (PF)	telnet	1	1	4	Tela de consulta	3000	20%	3600	14400	3600	2	32	21600
Sistema de fronteiras (Entrada de mercadoria)													
Replicação Cruz de Almas para sede	Bulk	1	5	110	Replicação de 1 entrada	1000	100%	2000	1100000	220000	300	2444	8800
Replicação outros PF para sede	Bulk	1	5	70	Replicação de 1 entrada	1000	100%	2000	700000	140000	300	1556	5600
Sistema de fronteiras (Saída de mercadoria)													
Replicação Cruz de Almas para sede	Bulk	1	5	5,5	Replicação de 1 entrada	1000	100%	2000	55000	11000	300	122	440
Replicação outros PF para sede	Bulk	1	5	3,5	Replicação de 1 entrada	1000	100%	2000	35000	7000	300	78	280
Sistema de fronteiras (Trânsito de mercadoria)													
Entrada de dados (Cruz de Almas)	C/S	1	193	1	Gravação de 1 registro	300	100%	600	115500	600	0,5	257	14400
Entrada de dados (Outros PF)	C/S	1	123	1	Gravação de 1 registro	300	100%	600	73500	600	0,5	163	14400
Legislação													
Consulta a legislação interna por SNR JP e CG	HTTP	1	10	1	Página HTML	10000	20%	12000	120000	12000	5	267	28800
Consulta a legislação interna por SNR pequena	HTTP	1	3	1	Página HTML	10000	20%	12000	36000	12000	5	80	28800
Consulta a legislação por PF	HTTP	1	1	1	Página HTML	10000	20%	12000	12000	12000	5	27	28800
Sistema de ficha financeira													
Acesso a dados de arrecadação na sede (SNR pequena)	telnet	1	1	7	Tela de consulta	3000	20%	3600	25200	3600	2	56	21600
Acesso a dados de	telnet	4	1	7	Tela de consulta	3000	20%	3600	100800	3600	2	224	21600

arrecadação na sede (Patos/Sousa)													
Acesso a dados de arrecadação na sede (JP/CG)	telnet	10	1	7	Tela de consulta	3000	20%	3600	252000	3600	2	560	21600
GIM													
Envio resultados JP para a sede	Bulk	1	1	1	Dados compactados	100000	0%	100000	100000	100000	300	222	4000
Envio resultados CG para a sede	Bulk	1	1	1	Dados compactados	66667	0%	66667	66667	66667	300	148	2667
Envio resultados Guarabira para a sede	Bulk	1	1	1	Dados compactados	15000	0%	15000	15000	15000	300	33	600
Envio resultados outras SNR para a sede	Bulk	1	1	1	Dados compactados	8333	0%	8333	8333	8333	300	19	333
Recepção GIM Internet	Bulk	1667	1	1	Dados compactados	171	20%	205	342000	205	10	760	246
Recepção GIM Intranet JP	Bulk	833	1	1	Dados compactados	171	20%	205	171000	205	10	380	246
Recepção GIM Intranet CG	Bulk	667	1	1	Dados compactados	171	20%	205	136800	205	10	304	246
Recepção GIM Intranet SNR pequena	Bulk	333	1	1	Dados compactados	171	20%	205	68400	205	10	152	246
Conta corrente													
Consultas	telnet	2	1	4	Tela de consulta	3000	20%	3600	28800	3600	2	64	21600
Relatório pequeno da consulta	telnet Bulk	2	1	1	Relatório	12000	20%	14400	28800	14400	10	64	17280
Entrada de dados para "Verso do DAR" (JP)	Bulk	1	1	1	Dados digitados localmente	240000	20%	288000	288000	288000	300	640	11520
Entrada de dados para "Verso do DAR" (CG)	Bulk	1	1	1	Dados digitados localmente	150000	20%	180000	180000	180000	300	400	7200
Entrada de dados para "Verso do	Bulk	1	1	1	Dados digitados localmente	60000	20%	72000	72000	72000	300	160	2880

DAR" (Outras SNR)													
Pré-disponibilização de NFs													
Envio para os postos	Bulk	1	1	1	as NF	600000	20%	720000	720000	720000	3600	1600	2400
Recepção na sede	Bulk Internet	1	1	1	as NF	600000	20%	720000	720000	720000	300	1600	28800
Sistema de fiscalização de estabelecimentos													
Consulta ao Contas correntes (JP e CG)	telnet	5	3	9	Tela de consulta	3000	20%	3600	486000	3600	2	1080	21600
Consulta ao Contas correntes (SNR menores)	telnet	1	3	9	Tela de consulta	3000	20%	3600	97200	3600	2	216	21600
Consulta ao Sistema de fronteiras	telnet								540000			1200	
Consulta ao GIM	tenet								540000			1200	
Relatórios das SNR JP e CG	Bulk	2	1	1	Relatório	264000	20%	316800	633600	316800	300	1408	12672
Relatórios das SNR menores	Bulk	1	1	1	Relatório	264000	20%	316800	316800	316800	300	704	12672
Navegação Internet													
Sede	HTTP e FTP	5	60	1	Página HTML	50000	0%	50000	15000000	100000	5	33333	240000
JP/CG	HTTP e FTP	2	60	1	Página HTML	50000	0%	50000	6000000	50000	5	13333	120000
SNR pequena	HTTP e FTP	1	60	1	Página HTML	50000	0%	50000	3000000	50000	5	6667	120000

- Fluxos consolidados

Fluxos Consolidados						
Enlace	**Fluxo**	**Tráfego em bytes/hora**	**Multiplicador (que ocorrerão durante 1 hora)**	**Total tráfego em bytes/hora**	**Tráfego total em bps**	**Capacidade total em bps necessária para atender ao limite de tempo**
Enlace Sede outbound						
	Replicação Cadastro para PF	15000	19	285000	633	3000
	Replicação Cadastro para SNR	15000	9	135000	300	3000
	Acesso Cadastro SNR pequena	28800	5	144000	320	21600
	Acesso Cadastro SNR Sousa e Patos	144000	2	288000	640	21600
	Acesso Cadastro SNR JP e CG	432000	2	864000	1920	21600
	Acesso a ficha financeira SNR pequena	25200	5	126000	280	21600
	Acesso a ficha financeira Patos e Sousa	100800	2	201600	448	21600
	Acesso a ficha financeira CG e JP	252000	2	504000	1120	21600
	Acesso Cadastro PF	14400	10	144000	320	21600
	Acesso CC SNR	28800	9	259200	576	21600
	Pequeno relatório de consulta CC SNR	28800	9	259200	576	17280
	Envio de NF	720000	9	6480000	14400	21600
	Consulta CC por JP e CG	486000	2	972000	2160	21600
	Consulta CC por SNR menores	97200	7	680400	1512	21600
	Navegação SNR CG e JP	6000000	2	12000000	26667	120000
	Navegação SNR pequenas	3000000	7	21000000	46667	120000
	Consulta a legislação interna por SNR JP e CG	120000	2	240000	533	28800
	Consulta a legislação interna por SNR pequena	36000	7	252000	560	28800
	Consulta a legislação por PF	12000	19	228000	507	28800
	Relatório Fiscalização JP e CG	633600	2	1267200	2816	12672
	Relatório Fiscalização SNR menores	316800	7	2217600	4928	12672
Total					107883	120000
Enlace Sede inbound						
	Replicação Fronteiras (Entrada) Cruz de Almas	1100000	1	1100000	2444	8800
	Replicação Fronteiras (Entrada) outros PF	700000	18	12600000	28000	5600
	Replicação Fronteiras (Saída) Cruz de Almas	55000	1	55000	122	440
	Replicação Fronteiras (Saída) outros PF	35000	18	630000	1400	280
	Entrada de dados (Trânsito - Cruz de Almas)	115500	1	115500	257	14400
	Entrada de dados (Trânsito - outros PF)	73500	1	73500	163	14400
	Envio resultados GIM JP para a sede	100000	1	100000	222	4000
	Envio resultados GIM CG para a sede	66667	1	66667	148	2667
	Envio resultados GIM Guarabira para a sede	15000	1	15000	33	600
	Envio resultados GIM outras SNR para a sede	8333	1	8333	19	333
	Entrega eletrônica GIM JP	171000	1	171000	380	246
	Entrega eletrônica GIM CG	136800	1	136800	304	246
	Entrega eletrônica GIM SNR pequena	68400	7	478800	1064	246
	Verso do DAR SNR JP	288000	1	288000	640	11520
	Verso do DAR SNR CG	180000	1	180000	400	7200
	Verso do DAR SNR outras SNR	72000	1	72000	160	2880
Total					35757	14400
Enlace SNR JP inbound						
	Replicação Cadastro para SNR	15000	1	15000	33	3000
	Acesso Cadastro SNR JP e CG	432000	1	432000	960	21600
	Acesso a ficha financeira CG e JP	252000	1	252000	560	21600
	Acesso CC SNR	28800	1	28800	64	21600
	Pequeno relatório de consulta CC SNR	28800	1	28800	64	17280
	Consulta CC por JP e CG	486000	1	486000	1080	21600
	Navegação SNR CG e JP	6000000	1	6000000	13333	120000
	Consulta a legislação interna por SNR JP e CG	120000	1	120000	267	28800
	Relatório Fiscalização JP e CG	633600	1	633600	1408	12672
Total					17769	120000
Enlace SNR JP outbound						
	Envio resultados GIM JP para a sede	100000	1	100000	222	4000
	Entrega eletrônica GIM JP	171000	1	171000	380	246
	Verso do DAR SNR JP	288000	1	288000	640	11520
Total					1242	11520
Enlace SNR Guarabira inbound						

	Consulta CC por SNR menores	97200	1	97200	216	21600
	Relatório Fiscalização SNR menores	316800	1	316800	704	12672
	Replicação Cadastro para SNR	15000	1	15000	33	3000
	Acesso CC SNR	28800	1	28800	64	21600
	Pequeno relatório de consulta CC SNR	28800	1	28800	64	17280
	Acesso Cadastro SNR pequena	28800	1	28800	64	21600
	Navegação SNR pequenas	3000000	1	3000000	6667	120000
	Consulta a legislação interna por SNR pequena	36000	1	36000	80	28800
	Acesso a ficha financeira SNR pequena	25200	1	25200	56	21600
Total					7948	120000
Enlace SNR Guarabira outbound						
	Envio resultados GIM Guarabira para a sede	15000	1	15000	33	600
	Entrega eletrônica GIM SNR pequena	68400	1	68400	152	246
	Verso do DAR SNR outras SNR	72000	1	72000	160	2880
Total					345	2880
Enlace SNR CG inbound						
	Replicação Cadastro para SNR	15000	1	15000	33	3000
	Acesso Cadastro SNR JP e CG	432000	1	432000	960	21600
	Acesso a ficha financeira CG e JP	252000	1	252000	560	21600
	Acesso CC SNR	28800	1	28800	64	21600
	Pequeno relatório de consulta CC SNR	28800	1	28800	64	17280
	Consulta CC por JP e CG	486000	1	486000	1080	21600
	Navegação SNR CG e JP	6000000	1	6000000	13333	120000
	Consulta a legislação interna por SNR JP e CG	120000	1	120000	267	28800
	Relatório Fiscalização JP e CG	633600	1	633600	1408	12672
Total					17769	120000
Enlace SNR CG outbound						
	Envio resultados GIM CG para a sede	66667	1	66667	148	2667
	Entrega eletrônica GIM CG	136800	1	136800	304	246
	Verso do DAR SNR CG	180000	1	180000	400	7200
Total					852	7200
Enlace SNR Cuité inbound						
	Replicação Cadastro para SNR	15000	1	15000	33	3000
	Acesso Cadastro SNR pequena	28800	1	28800	64	21600
	Acesso a ficha financeira SNR pequena	25200	1	25200	56	21600
	Acesso CC SNR	28800	1	28800	64	21600
	Pequeno relatório de consulta CC SNR	28800	1	28800	64	17280
	Consulta CC por SNR menores	97200	1	97200	216	21600
	Navegação SNR pequenas	3000000	1	3000000	6667	120000
	Consulta a legislação interna por SNR pequena	36000	1	36000	80	28800
	Relatório Fiscalização SNR menores	316800	1	316800	704	12672
Total					7948	120000
Enlace SNR Cuité outbound						
	Envio resultados GIM outras SNR para a sede	8333	1	8333	19	333
	Entrega eletrônica GIM SNR pequena	68400	1	68400	152	246
	Verso do DAR SNR outras SNR	72000	1	72000	160	2880
Total					331	2880
Enlace SNR Patos inbound						
	Replicação Cadastro para SNR	15000	1	15000	33	3000
	Acesso Cadastro SNR Sousa e Patos	144000	1	144000	320	21600
	Acesso a ficha financeira Patos e Sousa	100800	1	100800	224	21600
	Acesso CC SNR	28800	1	28800	64	21600
	Pequeno relatório de consulta CC SNR	28800	1	28800	64	17280
	Consulta CC por SNR menores	97200	1	97200	216	21600
	Relatório Fiscalização SNR menores	316800	1	316800	704	12672
	Navegação SNR pequenas	3000000	1	3000000	6667	120000
	Consulta a legislação interna por SNR pequena	36000	1	36000	80	28800
	Acesso Cadastro SNR pequena	28800	1	28800	64	21600
Total					8436	120000
Enlace SNR Patos outbound						
	Envio resultados GIM outras SNR para a sede	8333	1	8333	19	333
	Entrega eletrônica GIM SNR pequena	68400	1	68400	152	246
	Verso do DAR SNR outras SNR	72000	1	72000	160	2880
Total					331	2880
Enlace SNR Itaporanga/Catolé do Rocha/Monteiro/Sousa inbound						
	Replicação Cadastro para SNR	15000	1	15000	33	3000
	Acesso CC SNR	28800	1	28800	64	21600
	Pequeno relatório de consulta CC SNR	28800	1	28800	64	17280
	Consulta CC por SNR menores	97200	1	97200	216	21600

	Relatório Fiscalização SNR menores	316800	1	316800	704	12672
	Acesso a ficha financeira SNR pequena	25200	1	25200	56	21600
	Navegação SNR pequenas	3000000	1	3000000	6667	120000
	Consulta a legislação interna por SNR pequena	36000	1	36000	80	28800
	Acesso Cadastro SNR pequena	28800	1	28800	64	21600
Total					7948	120000
Enlace SNR Itaporanga/Catolé do Rocha/Monteiro/Sousa outbound						
	Envio resultados GIM outras SNR para a sede	8333	1	8333	19	333
	Entrega eletrônica GIM SNR pequena	68400	1	68400	152	246
	Verso do DAR SNR outras SNR	72000	1	72000	160	2880
Total					331	2880
Enlace PF Cruz de Almas inbound						
	Replicação Cadastro para PF	15000	1	15000	33	3000
	Acesso Cadastro PF	14400	2	28800	64	21600
	Consulta a legislação por PF	12000	1	12000	27	28800
	Envio de NF	720000	1	720000	1600	21600
Total					1724	28800
Enlace PF Cruz de Almas outbound						
	Replicação Fronteiras (Entrada) Cruz de Almas	1100000	1	1100000	2444	8800
	Replicação Fronteiras (Saída) Cruz de Almas	55000	1	55000	122	440
	Entrada de dados (Trânsito - Cruz de Almas)	115500	1	115500	257	14400
Total					2823	14400
Enlace PF outros PF inbound						
	Replicação Cadastro para PF	15000	1	15000	33	3000
	Acesso Cadastro PF	14400	2	28800	64	21600
	Consulta a legislação por PF	12000	1	12000	27	28800
	Envio de NF	720000	1	720000	1600	21600
Total					1724	28800
Enlace PF outros PF outbound						
	Replicação Fronteiras (Entrada) outros PF	700000	1	700000	1556	5600
	Replicação Fronteiras (Saída) outros PF	35000	1	35000	78	280
	Entrada de dados (Trânsito - outros PF)	73500	1	73500	163	14400
Total					1797	14400
Enlace para Network Access Provider (NAP) inbound						
	Entrega de NF	720000	1	720000	1600	28800
	Entrega GIM	342000	1	342000	760	246
	Navegação sede	15000000	1	15000000	33333	240000
	Navegação SNR CG e JP	6000000	2	12000000	26667	120000
	Navegação SNR pequenas	3000000	7	21000000	46667	120000
Total					62360	240000
Enlace para Network Access Provider (NAP) outbound						
	Acesso a cadastro de contribuintes	720000	1	720000	1600	57600
Total					1600	57600

- Resumo
  - Observe a assimetria dos fluxos
  - A maioria das tecnologias de rede é simétrica, mas algumas (ADSL, p.ex.) são assimétricas

Resumo das Capacidades dos Enlaces				
Enlace	**Tráfego total em bps**	**Capacidade em bps necessária para atender ao limite de tempo**	**Capacidade ajustada para não ter fila > 0,5**	**Capacidade Final**
Sede outbound	107883	120000	269707	**269707**
Sede inbound	35757	14400	89392	**89392**
SNR JP inbound	17769	120000	44423	**120000**
SNR JP outbound	1242	11520	3106	**11520**
SNR Guarabira inbound	7948	120000	19870	**120000**
SNR Guarabira outbound	345	2880	863	**2880**
SNR CG inbound	17769	120000	44423	**120000**
SNR CG outbound	852	7200	2130	**7200**
SNR Cuité inbound	7948	120000	19870	**120000**
SNR Cuité outbound	331	2880	826	**2880**
SNR Patos inbound	8436	120000	21090	**120000**
SNR Patos outbound	331	2880	826	**2880**
SNR Itaporanga/Catolé do Rocha/Monteiro/Sousa inbound	7948	120000	19870	**120000**

SNR Itaporanga/Catolé do Rocha/Monteiro/Sousa outbound	331	2880	826	**2880**
PF Cruz de Almas inbound	1724	28800	4310	**28800**
PF Cruz de Almas outbound	2823	14400	7058	**14400**
Outros PF inbound	1724	28800	4310	**28800**
Outros PF outbound	1797	14400	4492	**14400**
Network Access Provider (NAP) inbound	62360	240000	155900	**240000**
Network Access Provider (NAP) outbound	1600	57600	4000	**57600**

Caracterização do comportamento do tráfego

- Para caracterizar tráfego, não basta entender os fluxos normais das aplicações
- É necessário entender o comportamento das aplicações com respeito a atividade de broadcast

Comportamento broadcast e multicast

- Um quadro de broadcast vai para todas as estações do domínio de broadcast
  - Endereço MAC FF:FF:FF:FF:FF:FF
- Um quadro multicast (mais raro) vai para todas as estações que participam de um grupo de broadcast
- Dispositivos de interconexão de camada 2 (pontes e switches) propagam broadcast em todas as portas
- Isso leva a problemas de escalabilidade
  - Broadcast demais deixa as CPUs com muito overhead de processamento
  - 100 quadros de broadcast por segundo afeta o desempenho de um Pentium
  - Broadcast deve ser limitado a 20% do tráfego total
- Broadcast é necessário
  - Muitos serviços de redes locais precisam de broascast
    - DHCP, ARP, SAP, NETBIOS, RIP, IGRP, ...
- Domínios de broadcast são delimitados por:
  - Roteadores (eles não propagam broadcast)
  - LANs virtuais (VLANs) em switches de camada 3
- A tabela abaixo pode ser útil para determinar quantas estações colocar num único domínio de broadcast

Protocolo	**Número máximo de estações**
IP	500 (ou 200, se tiver aplicações multimídia)
NetWare	300
AppleTalk	200
NETBIOS	200
Misturado	200

Caracterização de requisitos de Qualidade de Serviço

- Além da carga de tráfego, precisamos saber se algumas aplicações possuem restrições quanto à inflexibilidade da vazão ou do atraso
- Caracterizamos portanto o QoS (Quality of Service) dos fluxos das aplicações
- Podemos usar dois modelos para caracterizar QoS
  - Categorias de serviço ATM
  - Modelo do Integrated Services Working Group da IETF

Especificação de QoS ATM

- Você pode caracterizar os requisitos de QoS usando as categorias ATM
  - CBR - Constant Bit Rate
    - Emula um fio
    - Sem controle de erro ou controle de fluxo
    - Para voz (telefone) e fluxos de áudio de alta qualidade e fluxos de vídeo
  - RT-VBR (Real-Time Variable Bit Rate)
    - Para vídeo comprimido interativo (vídeoconferência)
    - Compressão MPEG manda quadro completo seguido de quadros diferenciais
      - Mudança drástica de taxa de transmissão (VBR)
      - Fortes restrições no atraso e na variabilidade do atraso (RT)
  - NRT-VBR (Non Real-Time Variable Bit Rate)
    - Sem restrições de atraso e variabilidade de atraso
    - Exemplo: Email multimídia será visto off-line (não em tempo real)
  - ABR - Available Bit Rate
    - Tráfego em rajadas mas com banda passante mais ou menos conhecida
    - Exemplo: quero 5 mbps no mínimo mas usarei 10 mbps de vez em quando. Quero garantia dos 5 mbps mas aceito se não receber 10 mbps garantidamente
    - Usa feedback para pedir à fonte diminuir o ritmo se houver congestão
  - UBR - Unspecified Bit Rate
    - Sem promessas, sem feedback sobre congestão

- Apropriado para IP (que não garante nada) e para aplicações como ftp, email, ...
- Parâmetros podem ser usados para especificar os requisitos

Parâmetro	Acrônimo	Significado
Como o usuário quer transmitir		
Peak cell rate	PCR	Taxa máxima com a qual células serão transmitidas
Sustained cell rate	SCR	Taxa média de células a longo prazo
Minimum cell rate	MCR	Taxa mínima aceitável de submissão de células
Como o usuário deve transmitir		
Cell delay variation tolerance	CDVT	Jitter máximo aceitável entre células *submetidas*
Características negociadas da rede (medidas no destino)		
Cell loss ratio	CLR	Fração de células perdidas ou entregues tarde demais
Cell transfer delay	CTD	Latência (máxima e média)
Cell delay variation	CDV	A variância de tempos de entrega de células
Características não negociadas da rede		
Cell error rate	CER	Fração de células entregues com error
Severely-errored cell block ratio	SECBR	Fração de blocos com error ("garbled")
Cell misinsertion rate	CMR	Fração de células entregues no destino errado

Especificação de QoS do Integrated Services Working Group

- Garantias baseadas no protocolo RSVP (Reservation Protocol)
  - Ver RFCs 2205, 2208 até 2216
- RSVP é um protocolo de setup usado por um hospedeiro para requisitar um tipo de serviço
- RSVP também é usado entre roteadores para reservar recursos na rota do tráfego
- RSVP usa mecanismos de controle de tráfego
  - Packet Classifier (determina a classe QoS de cada pacote)
  - Admission Control Function (determina se um nodo tem recursos suficientes para suprir o QoS)
  - Packet Scheduler (para ordenar os pacotes para transmissão para satisfazer o QoS)
- Hospedeiros entregam
  - Uma Especificação de Tráfego (TSpec) que caracteriza o tráfego que o hospedeiro obedecerá
  - Uma Especificação de Pedido de Serviço (RSpec) que caracteriza o QoS desejado
- Há dois tipos principais de serviço:
  - Controlled Load para tráfego que precisa receber da rede o que normalmente receberia numa rede sem tráfego (mas continua best-effort)
    - Alto percentual de tráfego entregue
    - Atraso quase sempre igual ao atraso sem carga na rede
  - Guaranteed Service para obter garantias de atraso (mas não de jitter)

Checklist para o tráfego de rede

- Identifiquei as fontes importantes de tráfego e os sorvedouros importantes e documentei o fluxo de tráfego entre eles
- Categorizei o fluxo de cada aplicação usando os modelos termina-hospedeiro, cliente-servidor, peer-to-peer, servidor-servidor, computação distribuída
- Estimei os requisitos de banda passante para cada aplicação
- Estimei os requisitos de banda passante para os protocolos de roteamento
- Caracterizei as taxas aceitáveis de broadcast
- Determinei os requisitos de Qualidade de Serviço (QoS) para cada aplicação

3. Projeto Lógico da Rede

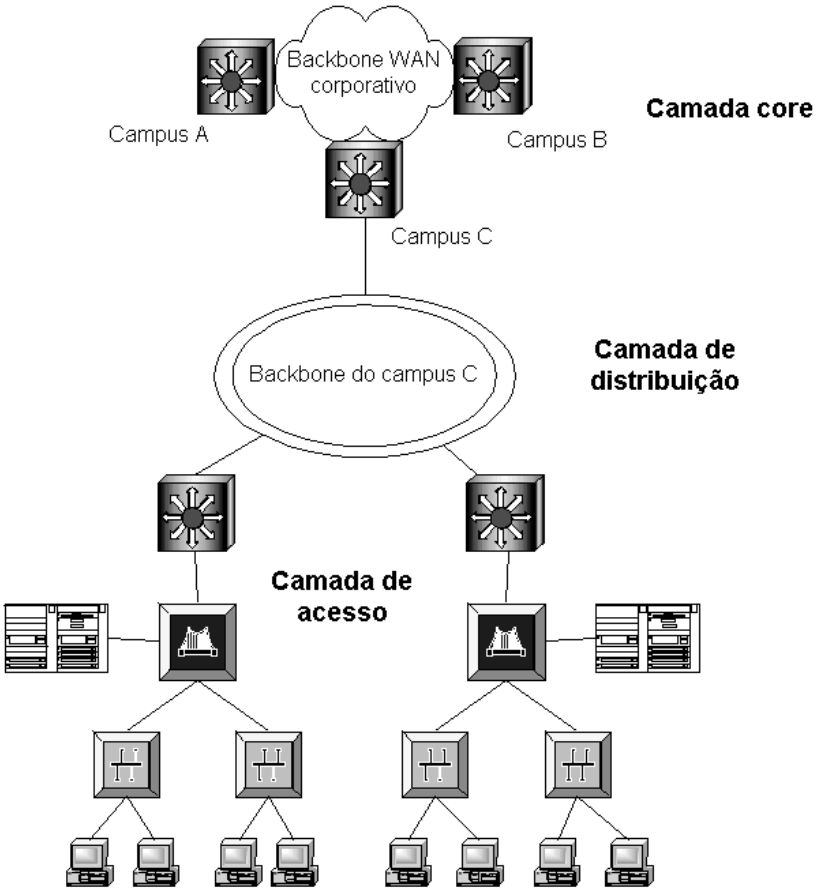
- Projeto da topologia da rede
- Projeto do esquema de endereçamento e naming
- Seleção de protocolos de bridging, switching e roteamento
- Desenvolvimento de estratégias de segurança e gerência

Projeto da Topologia da Rede

- Uma topologia é um mapa de uma rede que indica segmentos de rede (redes de camada 2), pontos de interconexão e comunidades de usuários
- Queremos projetar a rede logicamente e não fisicamente
  - Identificam-se redes, pontos de interconexão, o tamanho e alcance de redes e o tipo de dispositivos de interconexão
  - Não lidamos (ainda) com tecnologias específicas, dispositivos específicos, nem considerações de cabeamento
- Nosso objetivo é projetar uma rede segura, redundante e escalável

Projeto hierárquico de uma rede

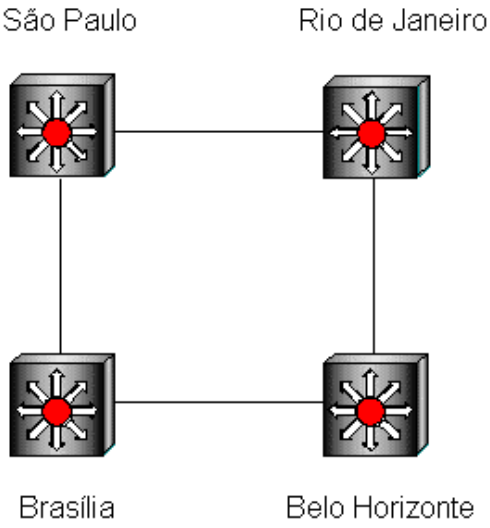
- Antigamente, usava-se muito uma rede com estrutura chamada Collapsed Backbone
  - Toda a fiação vai das pontas para um lugar central (conexão estrela)
  - O número de fios não era problemático quando as pontas usavam "shared bandwidth" com cabo coaxial em vez de hubs ou switches
  - Oferece facilidade de manutenção
  - Ainda é bastante usado
- Hoje, com rede maiores, usa-se cada vez mais uma estrutura hierárquica
- Um modelo hierárquico ajuda a desenvolver uma rede em pedaços, cada pedaço focado num objetivo diferente
- Um exemplo de uma rede hierárquica aparece abaixo
- As 3 camadas mostradas:
  - Camada core: roteadores e switches de alto desempenho e disponibilidade
  - Camada de distribuição: roteadores e switches que implementam políticas
  - Camada de acesso: conecta usuários com hubs e switches



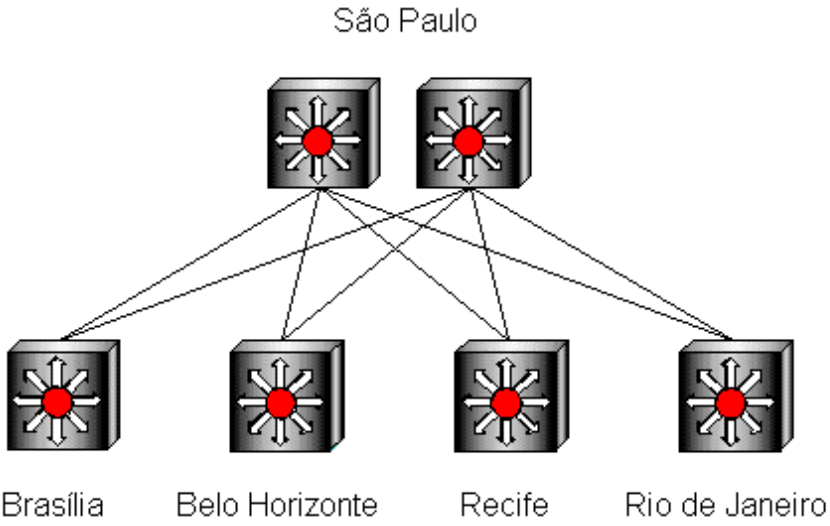
Por que usar um modelo hierárquico?

- Uma rede não estruturada (espaguete) cria muitas adjacências entre equipamentos
  - Ruim para propagação de rotas
- Uma rede achatada (camada 2) não é escalável devido ao broadcast
- Minimiza custos, já que os equipamentos de cada camada serão especializados para uma determinada função

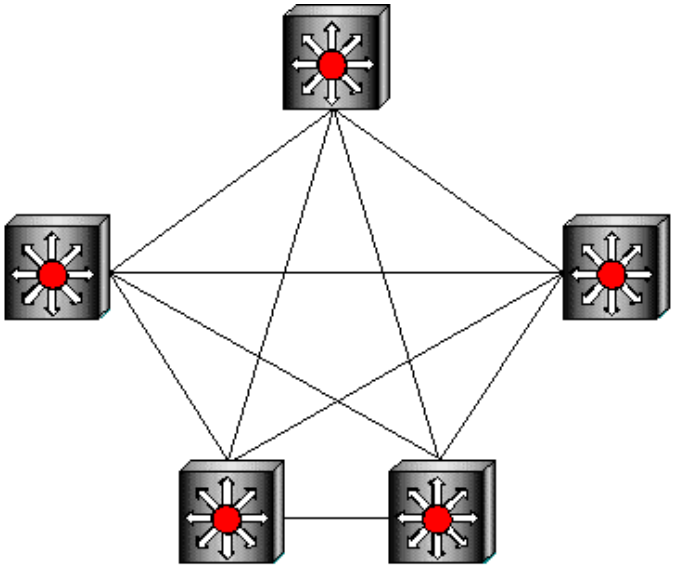
    - Exemplo: Usa switches rápidos no core block, sem features adicionais
- Mais simples de entender, testar e consertar
- Facilita mudanças, já que as interconexões são mais simples
- A replicação de elementos de torna mais simples
- Permite usar protocolos de roteamento com "sumarização de rotas"
- Comparação de estrutura hierárquica com achatada para a WAN
    - Pode-se usar um loop de roteadores
        - OK para redes pequenas
        - Para redes grandes, o tráfego cruza muitos hops (atraso mais alto)
        - Qualquer quebra é fatal



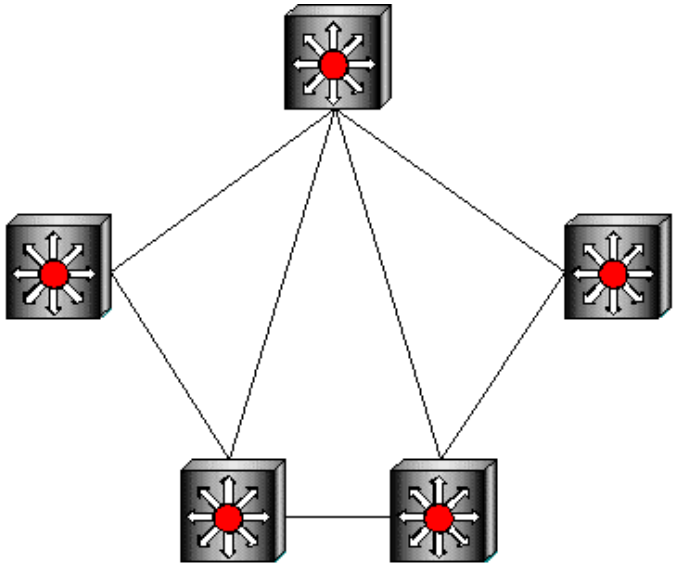
    - Roteadores redundantes numa hierarquia dão:
        - Mais escalabilidade
        - Mais disponibilidade
        - Atraso mais baixo



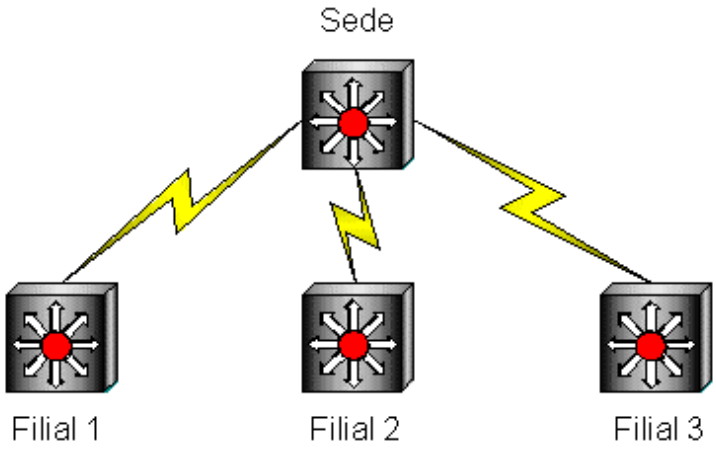
- Comparação de estrutura hierárquica com achatada para a LAN
    - O problema básico é que um domínio de broadcast grande reduz significativamente o desempenho
    - Com uma rede hierárquica, os equipamentos apropriados são usados em cada lugar
        - Roteadores (ou VLANs e switches de camada 3) são usados para delimitar domínios de broadcast
        - Switches de alto desempenho são usados para maximizar banda passante
        - Hubs são usados onde o acesso barato é necessário
- Topologias de full-mesh e mesh hierárquica
    - A full-mesh oferece excelente atraso e disponibilidade mas é muito cara
    - Uma alternativa mais barata é uma mesh parcial
    - Um tipo de mesh parcial é a mesh hierárquica, que tem escalabilidade mas limita as adjacências de roteadores
        - Para pequenas e médias empresas, usa-se muito a topologia hub-and-spoke



Topologia Full Mesh



Topologia Mesh Parcial



Topologia Hub-and-Spoke

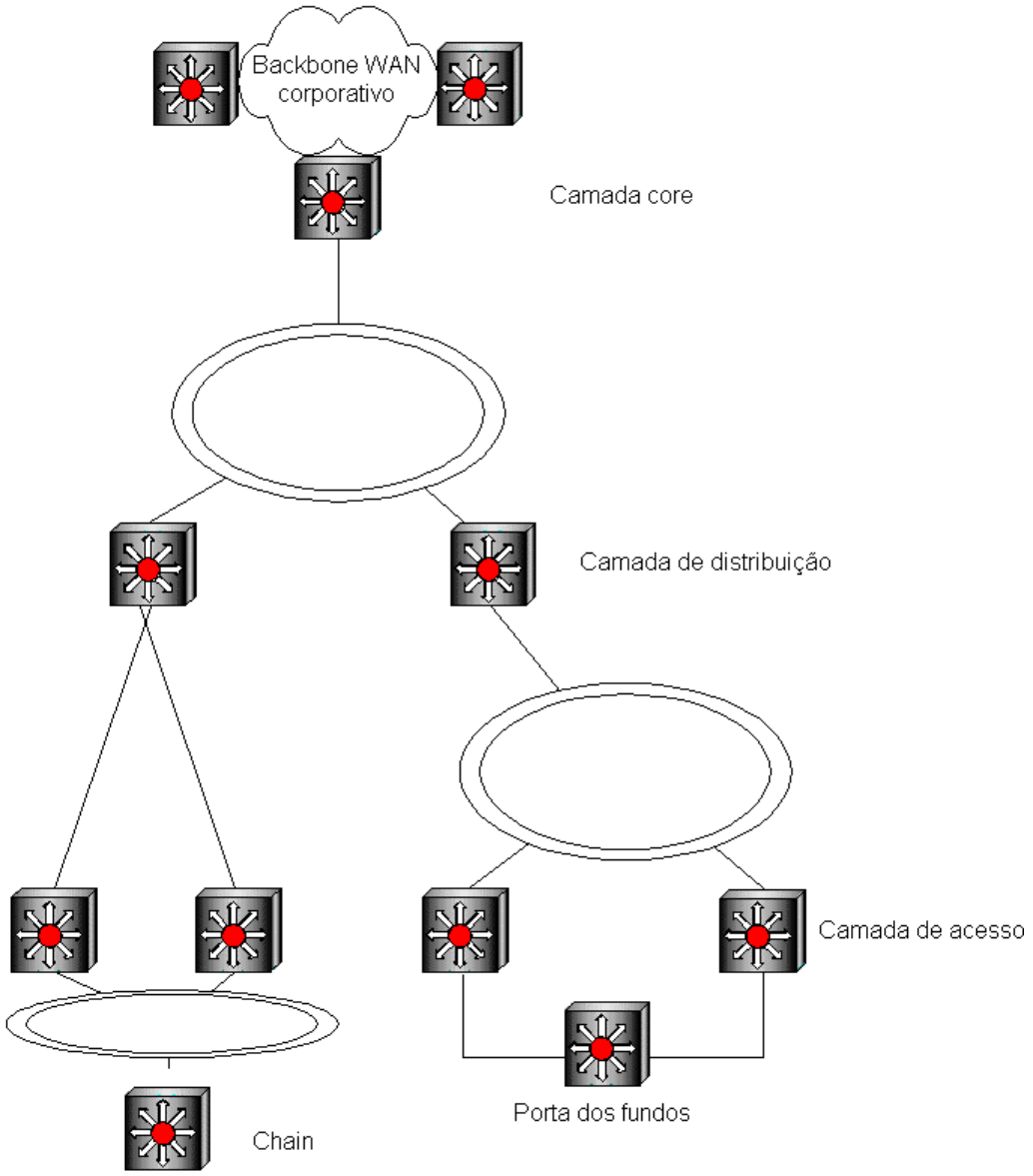
O modelo hierárquico clássico em 3 camadas

- Permite a agregação (junção) de tráfego em três níveis diferentes
- É um modelo mais escalável para grandes redes corporativas
- Cada camada tem um papel específico
    - Camada core: provê transporte rápido entre sites
    - Camada de distribuição: conecta as folhas ao core e implementa políticas
        - Segurança
        - Roteamento

        - Agregação de tráfego
    - Camada de acesso
        - Numa WAN, são os roteadores na borda do campus network
        - Numa LAN, provê acesso aos usuários finais
- A camada core
    - Backbone de alta velocidade
    - A camada deve ser projetada para minimizar o atraso
    - Dispositivos de alta vazão devem ser escolhidos, sacrificando outros features (filtros de pacotes, etc.)
    - Deve possuir componentes redundantes devida à sua criticalidade para a interconexão
    - O diâmetro deve ser pequeno (para ter baixo atraso)
        - LANs se conectam ao core sem aumentar o diâmetro
    - A conexão à Internet é feita na camada core
- A camada de distribuição
    - Tem muito papeis
        - Controla o acesso aos recursos (segurança)
        - Controla o tráfego que cruza o core (desempenho)
        - Delimita domínios de broadcast
            - Isso pode ser feito na camada de acesso também
        - Com VLANs, a camada de distribuição roteia entre VLANs
        - Interfaceia entre protocolos de roteamento que consomem muita banda passante na camada de acesso e protocolos de roteamento otimizados na camada core
            - Exemplo: sumariza rotas da camada de acesso e as distribui para o core
            - Exemplo: Para o core, a camada de distribuição é a rota default para a camada de acesso
        - Pode fazer tradução de endereços, se a camada de acesso usar endereçamento privativo
            - Embora o core também possa usar endereçamento privativo
- A camada de acesso
    - Provê acesso à rede para usuários nos segmentos locais
        - Frequentemente usa apenas hubs e switches

Guia para o projeto hierárquico de uma rede

- Controle o diâmetro da topologia inteira, para ter atraso pequeno
- Mantenha controle rígido na camada de acesso
    - É aqui que departamentos com alguma independência implementam suas próprias redes e dificultam a operação da rede inteira
    - Em particular, deve-se evitar:
        - Chains (adicionando uma quarta camada abaixo da camada de acesso)
            - Causam atrasos maiores e dependências maiores de tráfego
            - Chains podem fazer sentido para conectar mais um pais numa rede corporativa
        - Portas-dos-fundos (conexões entre dispositivos para mesma camada)
            - Causam problemas inesperados de roteamento



- Projete a camada de acesso primeiro, depois a camada de distribuição, depois o core
    - Facilita o planejamento de capacidade

Topologias redundantes no projeto de uma rede

- A disponibilidade é obtida com a redundância de enlaces e dispositivos de interconexão
- O objetivo é eliminar pontos únicos de falha, duplicando qualquer recurso cuja falha desabilitaria aplicações de missão crítica
- Pode duplicar enlaces, roteadores importantes, uma fonte de alimentação
    - Em passos anteriores, você deve ter identificado aplicações, sistemas, dispositivos e enlaces críticos
- Para dispositivos muito importantes, pode-se considerar o uso de componentes "hot-swappable"
- A redundância pode ser implementada tanto na WAN quanto na LAN
- Há obviamente um tradeoff com o custo da solução

Caminhos alternativos

- Para backupear enlaces primários
- Três aspectos são importantes
    - Qual deve ser a capacidade do enlace redundante?
        - É frequentemente menor que o enlace primário, oferecendo menos desempenho
        - Pode ser uma linha discada, por exemplo
    - Em quanto tempo a rede passa a usar o caminho alternativo
        - Se precisar de reconfiguração manual, os usuários vão sofrer uma interrupção de serviço
        - Failover automático pode ser mais indicado
        - Lembre que protocolos de roteamento descobrem rotas alternativas e switches também (através do protocolo de spanning tree)
    - O caminho alternativo deve ser testado!
        - Não espere que uma catástrofe para descobrir que o caminho alternativo nunca foi testado de não funciona!

        - Usar o caminho alternativa para balanceamento de carga evita isso

Considerações especiais para o projeto de uma topologia de rede de campus

- Os pontos principais a observar são:
    - Manter domínios de broadcast pequenos
    - Incluir segmentos redundantes na camada de distribuição
    - Usar redundância para servidores importantes
    - Incluir formas alternativas de uma estação achar um roteador para se comunicar fora da rede de camada 2

LANs virtuais

- Uma LAN virtual (VLAN) nada mais é do que um domínio de broadcast configurável
- VLANs são criadas em uma ou mais switches
- Usuários de uma mesma comunidade são agrupados num domínio de broadcast independentemente da cabeação física
    - Isto é, mesmo que estejam em segmentos físicos diferentes
- Esta flexibilidade é importante em empresas que crescem rapidamente e que não podem garantir que quem participa de um mesmo projeto esteja localizado junto
- Uma função de roteamento (noemalmente localizada dentro dos switches) é usada para passar de uma VLAN para outra
    - Lembre que cada VLAN é uma "rede de camada 2" e que precisamos passar para a camada 3 (rotear) para cruzar redes de camada 2
- Há várias formas de agrupar os usuários em VLANs, dependendo das switches usadas
    - Baseadas em portas do switches
    - Baseadas em endereços MAC
    - Baseadas em subnet IP
    - Baseadas em protocolos (IP, NETBEUI, IPX, ...)
    - VLAN para multicast
        - VLAN criada dinamicamente pela escuta de pacotes IGMP (Internet Group Management Protocol)
    - VLANs baseadas em políticas gerais (com base em qualquer informação que aparece num quadro)
    - Baseadas no nome dos usuários
        - Com ajuda de um servidor de autenticação

Segmentos redundantes de LAN

- Enlaces redundantes entre switches sõ desejáveis para aumentar a disponibilidade
- Laços são evitados usando o protocolo Spanning Tree (IEEE 802.1d)
- Isso fornece redundância mas não balanceamento de carga
    - O protocolo Spanning Tree corta enlaces redundantes (até que sejam necessários)

Redundância de servidores

- Servidor DHCP
    - Se usar DHCP, o servidor DHCP se torna crítico e pode ser duplicado
    - Em redes pequenas, o servidor DHCP é colocado na camada de distribuição onde pode ser alcançado por todos
    - Em redes grandes, vários servidores DHCP são colocados na camada de acesso, cada um servindo a uma fração da população
        - Evita sobrecarga de um único servidor
    - DHCP funciona com broadcast
        - Somos obrigados a colocar um servidor DHCP para cada domínio de broadcast?
            - Não, se utilizar uma função do roteador de encaminhar broadcast DHCP para o servidor de broadcast (cujo endereço foi configurado no servidor)
- Servidor DNS
    - P servidor DNS é crítico para mapear nomes de máquinas a endereços IP
    - Por isso, é frequentemente duplicado

Redundância estação-roteador

- Para obter comunicação fora da rede de camada 2 imediata, uma estação precisa conhecer um roteador
- Como implementar redundância aqui?
- O problema básico é que o IP do roteador que a estação conhece é frequentemente configurado manualmente ("parafusado") em cada estação
- Há algumas alternativas
- Alternativa 1: Proxy ARP
    - A estação não precisa conhecer roteadore nenhum
    - Para se comunicar com *qualquer* máquina (mesmo remota), a estação usa ARP
        - O roteador responde com seu próprio endereço MAC
    - Proxy ARP é pouco usado porque nunca foi padronizado
- Alternativa 2: DHCP
    - DHCP pode infromar mais coisas do que apenas o endereço IP da estação
    - Pode informar o roteador a usar (ou até mais de um roteador)

    - Alternativa muito usada
- Alternativa 3: Hot Standby Router Protocol (HSRP) da Cisco
    - É uma alternativa proprietária, mas a IETF está padronizando algo semelhante chamado Virtual Router Redundancy Protocol (VRRP)
    - HSRP cria um roteador fantasma (que não existe de verdade) e vários roteadores reais, um dos quais está ativo, os outros em standby
    - Os roteadores reais conversam entre si para saber qual é o roteador ativo
    - O roteadore fantasma tem um endereço MAC e os roteadores reais podem aceitar quadros de um bloco de endereços MAC, incluindo o endereço MAC do fantasma
    - O roteador fantasma (que nunca quebra!) é o roteador default das estações
    - Quando uma estação usa ARP para descobrir o MAC do fantasma, o roteador ativa, responde (com o MAC do fantasma)
    - Mas quem realmente atende a este endereço MAC é o roteador ativo
    - Se o roteador ativo mudar, nada muda para a estação (continua conversando com o roteador fantasma)

Considerações especiais para o projeto de uma topologia de rede corporativa

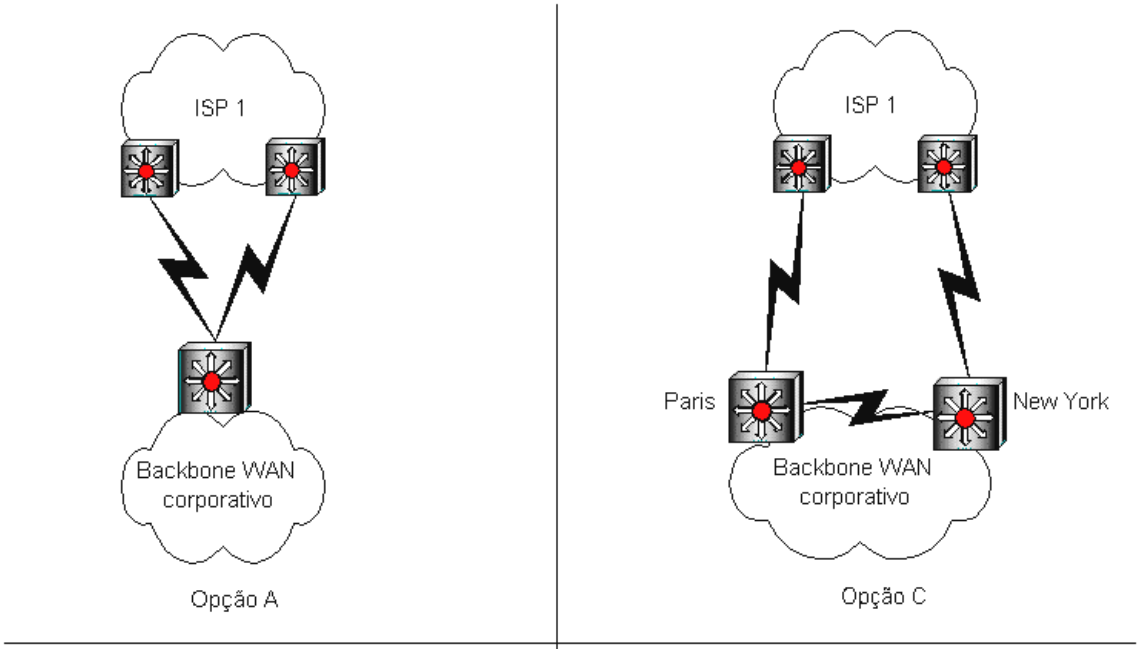
- Considerações especiais sobre:
    - Segmentos redundantes de WAN
    - Conexões múltiplas à Internet
    - Redes Privativas Virtuais (VPN) para montar redes corporativas baratas

Segmentos redundantes de WAN

- Uso de uma mesh parcial é normalmente suficiente
- Cuidados especiais para ter diversidade de circuito
    - Se os enlaces redundantes usam a mesma tecnologia, são fornecidos pelo mesmo provedor, passam pelo mesmo lugar, qual a probabilidade da queda de um implicar na queda de outro?
    - Discutir essa questão com o provedor é importante

Conexões múltiplas à Internet

- Há 4 alternativas básicas para ter acesso múltiplo à Internet



- Opção A
  - Vantagens
    - Backup na WAN
    - Baixo custo
    - Trabalhar com um ISP pode ser mais fácil do que trabalhar com ISPs múltiplos
  - Desvantagens
    - Não há redundância de ISPs
    - Roteador é um ponto único de falha
    - Supõe que o ISP tem dois pontos de acesso perto da empresa
- Opção B
  - Vantagens
    - Backup na WAN
    - Baixo custo
    - Redundância de ISPs
  - Desvantagens
    - Roteador é um ponto único de falha
    - Pode ser difícil trabalhar com políticas e procedimentos de dois ISPs diferentes
- Opção C
  - Vantagens
    - Backup na WAN
    - Bom para uma empresa geograficamente dispersa
    - Custo médio

        - Trabalhar com um ISP pode ser mais fácil do que trabalhar com ISPs múltiplos
    - Desvantagens
        - Não há redundância de ISPs
- Opção D
    - Vantagens
        - Backup na WAN
        - Bom para uma empresa geograficamente dispersa
        - Redundância de ISPs
    - Desvantagens
        - Alto custo
        - Pode ser difícil trabalhar com políticas e procedimentos de dois ISPs diferentes
- As opções C e D merecem mais atenção
    - O desempenho pode frequentemente ser melhor se o tráfego ficar na rede corporativa mais tempo antes de entrar na Internet
    - Exemplo: pode-se querer que sites europeus da empresa acessem a Internet pelo roteador de Paris mas acessem sites norte-americanos da empresa pelo roteador de New York
        - A configuração de rotas default nas estações (para acessar a Internet) pode ser feita para implementar essa política
    - Exemplo mais complexo: Queremos que sites europeus da empresa acessem sites norte-americanos da Internet pelo roteador de New York (idem para o roteador de Paris sendo usado para acessar a Internet européia pelos sites norte-americanos da empresa)
        - Fazer isso é mais complexo, pois os roteadores da empresa deverão receber rotas do ISP
    - Exemplo mais complexo ainda: tráfego que vem da Internet para sites norte-americanos da empresa devem entrar na empresa por New York (idem para Paris)
        - Neste caso, a empresa deverá anunciar rotas para a Internet
        - Observe que, para evitar que a empresa se torne um *transit network*, apenas rotas da própria empresa devem ser anunciados!

Redes privativas virtuais

- Redes privativas virtuais (VPN) permitem que um cliente utilize uma rede pública (a Internet, por exemplo) para acessar a rede corporativa de forma segura
    - Toda a informação é criptografada
- Muito útil para montar uma extranet (abrir a intranet para parceiros, clientes, fornecedores, ...)
- Muito útil para dar acesso a usuários móveis da empresa
- Solução muito usada quando a empresa é pequena e tem restrições de orçamento para montar a rede corporativa
- A técnica básica é o tunelamento
- O protocolo básico é Layer 2 Tunneling Protocol (L2TP)

Topologias de rede para a segurança

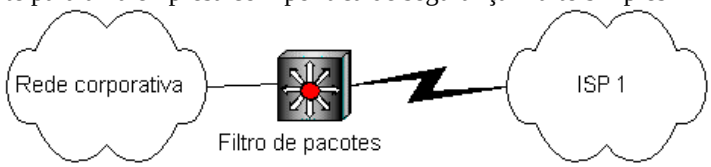
- Falaremos mais de segurança adiante
- Por enquanto, queremos ver os aspectos topológicos da questão

Planejamento da segurança física

- Verificar onde os equipamentos serão instalados
- Prevenção contra acesso não autorizado, roubo físico, vandalismo, etc.

Topologias de firewalls para alcançar requisitos de segurança

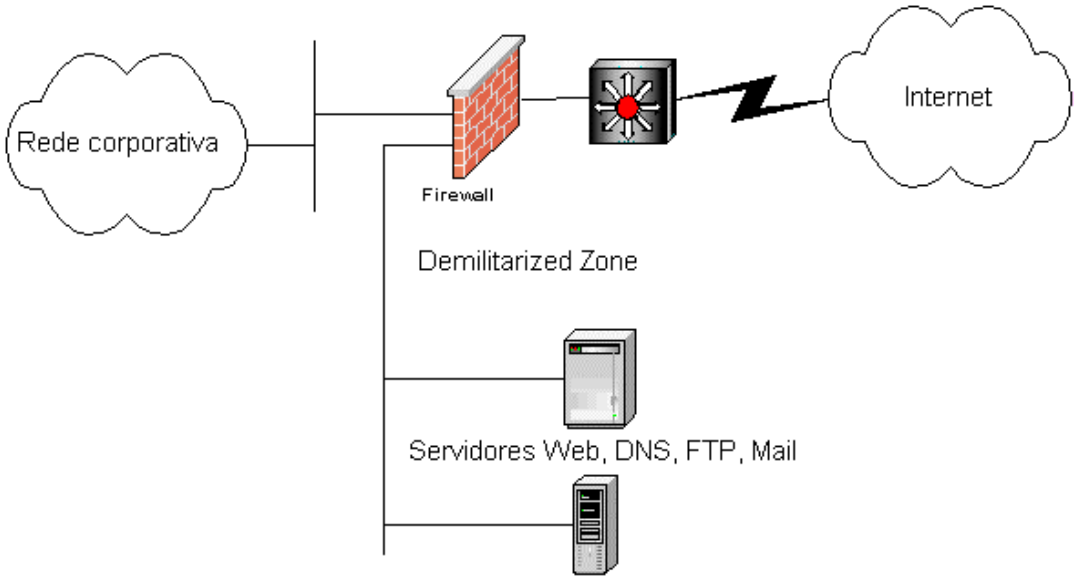
- Um firewall é um sistema que estabelece um limite entre duas ou mais redes
- Pode ser implementado de várias formas
    - Simples: um roteador com filtro de pacote
    - Mais complexo: software especializado executando numa máquina UNIX ou Windows NT
- Serve para separar a rede corporativa da Internet
- A topologia mais básica usa um roteador com filtro de pacote
    - Só é suficiente para uma empresa com política de segurança muito simples



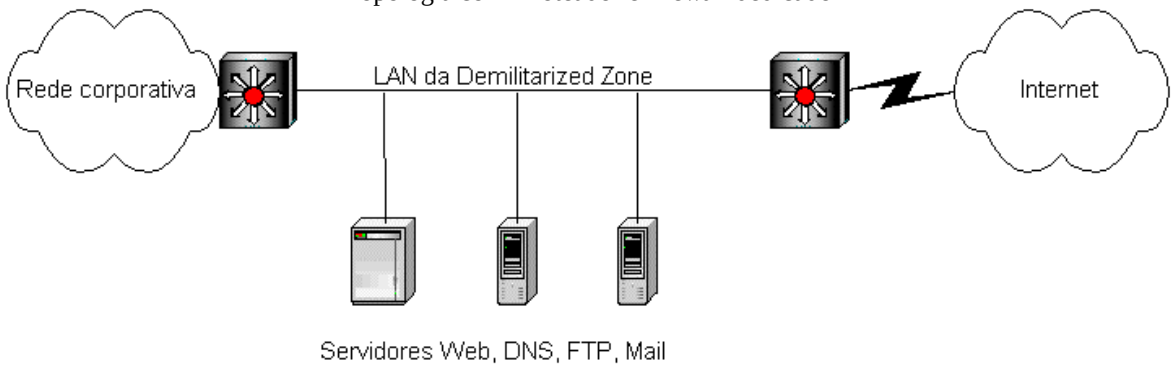
- A tabela de filtragem de pacotes poderia ser como segue
    - A primeira regra que casa com cada pacote examinado é aplicada

Ação	Host local	Porta	Host remoto	Porta remota
Nega	*	*	mau.ladrao.com	*
Permite	mailserver	25	*	*
Permite	*	*	*	25
Nega	*	*	*	*

- Para melhorar as coisas, pode-se usar endereçamento privativa na rede corporativa
  - Uso de Network Address Translation (NAT) implementada no roteador para acessar a Internet
  - Uso de um proxy para certos serviços (web, ftp, ...)
- Para empresas que precisam publicar informação na Internet (Web, DNS, FTP, ...), pode-se ter algumas máquinas na Internet, numa área chamada Demilitarized Zone (DMZ)
  - Os hosts têm que ser muito bem protegidos contra invasões (*Bastion Hosts*)
  - Um firewall especializado pode ser incluído
    - Fornece uma boa GUI e ações especiais para implementar a política de segurança
  - Há duas topologias básicas
    - Com um roteador
    - Com dois roteadores



Topologia com 1 roteador e firewall dedicado



Topologia com 2 roteadores filtrando pacotes

Projeto do Esquema de Endereçamento e Naming

- Trataremos da atribuição de endereços de camada de rede (endereços IP) e de nomes de recursos
- Enfoque no protocolo IP
  - Algum tratamento de NetBIOS (rede Microsoft)
- Por que não é simples atribuir endereços IP?
  - Basicamente, tem a ver com dificuldades de roteamento, se um modelo estruturado e hierárquico não for seguido
  - Outro problema tem a ver com o esgotamento de espaços de endereçamento
  - Também há outras implicações tais como segurança, desempenho
- Antes de começar, você deve lembrar a estrutura organizacional do cliente
  - Isso ajuda a planejar a atribuição de endereços e nomes
- O mapa topológico também ajuda, pois indica onde há hierarquia na rede e consequentes limites de endereçamento
- Precisamos tratar do assunto de endereçamento antes de escolher protocolos de roteamento pois alguns protocolos não suportam determinados esquemas de endereçamento
  - Exemplo: nem todo protocolo de roteamento suporta roteamento sem classes, variable length subnet masking (VLSM), etc.
- Supõe-se que o leitor conheça o mecanismo básico de endereços IP
  - Hierarquia com dois componentes: rede e hospedeiro
  - Um endereço IP por interface de rede

- Classes A, B, C
- Máscara de sub-rede para aumentar a parte rede e permitir mais flexibilidade ao definir mais redes menores de camada 2

Regras para atribuir endereços de rede

- Não há mecanismo dinâmico para atribuir endereços de rede (isto é, a parte rede do endereço IP)
  - Tem que ser feito manualmente
- Algumas regras simples seguem:
  - Projete um modelo estruturado (organizado) para endereçamento antes de atribuir qualquer endereço
  - Deixe espaço para crescimento no número de redes camada e e no número de hospedeiros
    - Se estourar os campos de endereçamento, uma renumeração futura pode ser muito trabalhosa
  - Atribua blocos de endereços de forma hierárquica para melhorar a escalabilidade e disponibilidade
    - Falaremos adiante sobre mecanismos para aumentar a hierarquia de endereçamento IP que é pobre, por default (só dois níveis)
  - Atribua blocos de endereços baseados em redes físicas (de camada 2) e não baseados em grupos de pessoas para permitir que pessoas ou grupos mudem de rede
  - Se o nível de conhecimento de redes em filiais for alto, é possível delegar a autoridade para atribuir endereços a redes locais, subredes, servidores e estações
  - Para maximizar a flexibilidade e minimizar o trabalho de configuração, use endereçamento dinâmico para estações
    - Usando DHCP, por exemplo
  - Para maximizar a segurança e a adaptabilidade, use endereçamento privativo
    - Network address translation (NAT) ou o uso de proxies permitirá que usuários saiam da rede corporativa

Uso de um modelo estruturado para endereçamento de rede

- Estruturado significa hierárquico e planejado
- Exemplo: usar um endereço de rede para a rede corporativa e usar subnetting (máscaras de subrede) é um esquema hierárquico
- Um modelo estruturado facilita:
  - A gerência de endereços
  - O troubleshooting (localização e conserto de problemas, principalmente de roteamento)
  - O entendimento de mapas de redes
  - A operação da rede
  - A implementação de soluções otimizadas, em termos de tráfego de roteamento
  - A implementação de políticas de segurança (filtragem de pacotes em firewalls)

Administração de endereços com autoridade centralizada

- O modelo global de endereçamento para a rede corporativa deve ser projetado por um departamento centralizado (departamento de rede corporativa, departamento de tecnologia de informação, ...)
- Número de redes são escolhidos para a camada core
- Blocos de endereços de subrede são reservados para as camadas de distribuição e de acesso
- Mais subdivisões dos blocos poderão ocorrer de forma centralizada ou não
- Blocos de endereços podem ser recebidos do ISP ou do IANA ou de alguma outra entidade no país (FAPESP, no Brasil)
  - Se depender de endereços fornecidos pelo ISP, escolha um ISP que tenha margem de manobra nos endereços para você crescer
    - Mudar de ISP depois pode envolver uma mudança geral de endereços
- Uma alternativa preferida, hoje em dia, é de usar endereçamento privativo na rede corporativa
  - Permite crescer sem problemas
  - Falaremos de endereçamento privativo adiante

Distribuição de autoridade para a administração de endereços

- As pessoas que terão responsabilidade de escolher endereços e configurar dispositivos devem ser escolhidas com cuidado
- Se forem pessoas sem muito conhecimento de rede, mantenha o esquema de endereçamento simples
- O uso de endereçamento dinâmico (DHCP) ajuda muito a minimizar o trabalho
- É preferível não delegar autoridade se os administradores de redes nas filiais forem inexperientes

Endereçamento dinâmico para estações

- Embora IP não tenha sido inventado com suporte a endereçamento dinâmico (escolha dinâmica de endereços IP), várias soluções apareceram para simplificar as tarefas do administrador de rede
  - BOOTP
  - DHCP
- DHCP (Dynamic Host Configuration Protocol)
  - Um servidor DHCP entrega endereços IP a partir de um bloco de endereços reservados para este fim
  - A estação pede uma endereço IP ao fazer boot, usando broadcast

- A estação não requer configuração de endereço IP
- DHCP suporta três tipos de alocação de endereços
    - Automática: um endereço permanente é dado à estação
    - Manual: uma tabela de endereços permanentes é configurada manualmente e o servidor DHCP entrega os endereços (pouco usado)
    - Dinâmica: um endereço IP é dado à estação por um período de tempo (lease period)
        - Este é o método mais popular
        - Conveniente também quando há mais hosts do que endereços disponíveis mas os hosts não estão sempre no ar
- No sentido de evitar ter um servidor DHCP em cada domínio de broadcast, um roteador pode ser configurado para repassar os broadcasts DHCP (DHCP discover message) para um servidor DHCP do outro lado do roteador
- A resposta do servidor DHCP fornece o endereço e, opcionalmente, outra informação de configuração
    - Exemplo: Rotedor default, que também não precisa ser configurado na estação!

Uso de endereçamento privativo

- Endereços privativos são blocos de endereços reservados que podem ser reutilizados em qualquer empresa e não são roteados pela Internet
    - Porque a Internet exige endereços únicos para qualquer computador conectado
- De que adianta isso se os computadores não podem se conectar à Internet?
    - Primeiro, os servidores da empresa que precisam ser acessados pela Internet recebem endereços públicos, além de privativos
    - Segundo, o Network Address Translation pode mapear endereços privativos em públicos dinamicamente, se desejado
    - Terceiro, servidores proxy (que têm endereços públicos e privativos) podem ser usados para acessar certos serviços da Internet (HTTP, FTP, ...)
- Endereços privativos reservados (RFC 1918)
    - Uma classe A: 10.0.0.0
    - 16 classes B: 172.16.0.0 até 172.31.0.0
    - 256 classes C: 192.168.0.0 até 192.168.255.0
- As grandes vantagens
    - Segurança (as máquinas não estão diretamente acessíveis pela Internet)
    - Margem de manobra para alocar endereços (uma classe A inteira!)
        - Melhor do que depender de (poucos) endereços fornecidos por um ISP
        - Apenas alguns endereços públicos são necessários (basta uma classe C)
    - Permite alocar endereços em blocos, o que diminui o tráfego de atualização de tabelas de roteamento (como veremos adiante)
    - O uso de endereçamento privativo evitou o pânico que estava tomando conta da comunidade Internet com o esgotamento do espaço de endereçamento
- Desvantagens
    - Outsourcing de gerência de rede é mais difícil
        - A empresa de outsourcing tem que:
            - Usar VPN, ou
            - Instalar consoles de gerência e pessoas dentro da empresa
            - Instalar um esquema "out-of-band" para obter dados de gerência (mais caro)

Uso de um modelo hierárquico para atribuir endereços

- Endereços IP já são hierárquicos
    - Parte rede e parte host
    - Onde a faca foi passada nos endereços de 32 bits depende da classe
- Isso foi feito para diminuir o tamanho das tabelas de roteamento
    - Não tanto pelo espaço que tomam nos roteadores mas pela banda passante necessária para trocar tabelas de roteamento entre roteadores
    - Observe que o roteamento usa apenas a parte de rede
- Em outras palavras, os roteadores não entendem a topologia completa (não sabem nada sobre os hosts das redes)
- Mas precisamos de mais hierarquia ainda para melhorar as coisas
    - Exemplo: o sistema telefônico tem muito mais hierarquia
        - O que é feito com o número 55833331404?

Por que usar um modelo hierárquico?

- Já falamos algumas considerações acima
- As vantagens:
    - Fornece melhor troubleshooting, atualizações, gerenciabilidade
    - Ajuda a otimizar o desempenho
    - Permite convergência mais rápida dos protocolos de roteamento

    - Permite melhor escalabilidade
    - Permite melhor estabilidade
    - Permite usar menos recursos de rede (CPU, memória, buffers, banda passante, ...)
- Uma das técnicas básicas que um modelo hierárquico permite usar é a de sumarização de rotas (ou agregação de rotas)
    - Permite que um roteador junte muitas rotas e as divulguem como uma só rota
- Outra técnica permitida pelo uso de um modelo hierárquico: Variable-Length Subnet Masking (VLSM)
    - Permite que uma rede seja dividida em subredes de tamanhos diferentes, o que não é permitido quando se usam apenas máscaras de subrede

Roteamento sem classes

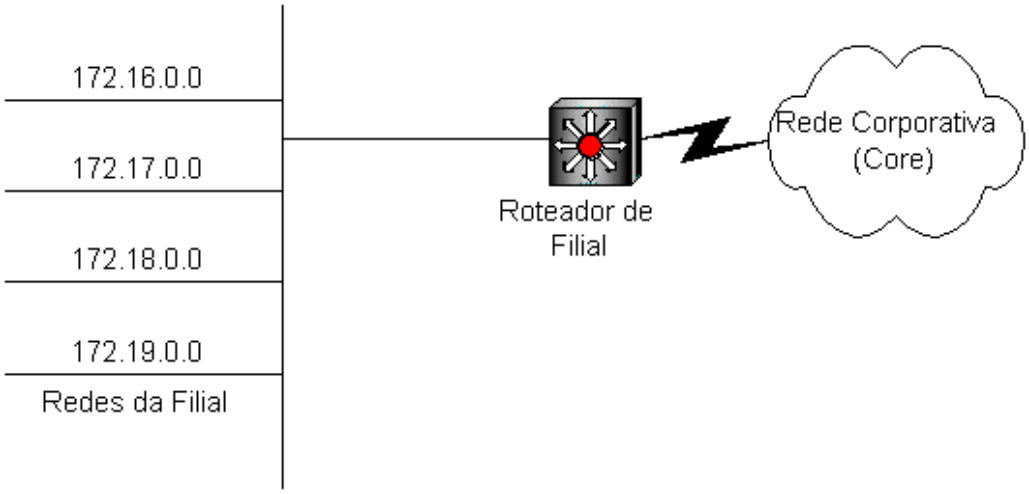
- No meio dos anos 90, o crescente tamanho das tabelas de roteamento na Internet forçou a IETF a introduzir um esquema com mais hierarquia no endereçamento
- A solução foi Classless Inter-Domain Routing (CIDR)
- Com CIDR, os endereços são alocados em blocos e roteadores podem agrupar rotas de blocos para diminuir a quantidade de informação de roteamento trocada entre roteadores
- A RFC 2050 dá regras para a alocação e endereços
    - Basicamente, um ISP recebe um bloco de endereços e as distribui entre seus clientes de acordo com as necessidades de cada um
    - As rotas são anunciadas para o resto da Internet num único bloco
    - Compare isso com a alternativa de dar várias classes C para os vários clientes
        - A rota para cada classe C seria anunciada separadamente

Roteamento com classes versus sem classes

- Lembre que apenas a parte rede do endereço IP é normalmente usada para rotear
    - "Normalmente" significa "usando roteamento baseado em classes"
- Este "prefixo" tem tamanho fixo para cada classe
    - Classe A (primeiro bit = 0): prefixo de 8 bits
    - Classe B (primeiros 2 bits = 10): prefixo de 16 bits
    - Classe C (primeiros 3 bits = 110): prefixo de 24 bits
- O tamanho do prefixo está embutido na classe e não é transmitido nas trocas de rotas
    - Exemplo: 172.16.0.0/14 significa um prefixo de 14 bits
- Localmente, podemos usar subnetting (máscaras de subrede) para estender o prefixo
    - Isso é uma solução apenas local e não é usado para endereços remotos
- Com CIDR, o tamanho do prefixo é transmitido com o endereço IP
    - Isso é a chave para descobrir qual parte do endereço considerar no roteamento
- Protocolos que aceitam roteamento sem classes
    - RIP Versão 2
    - Enhanced IGRP (Cisco)
    - OSPF
    - BGP-4
    - IS-IS
- Protocolos que não aceitam roteamento sem classes
    - RIP Versão 1
    - IGRP

Sumarização (ou agregação) de rotas

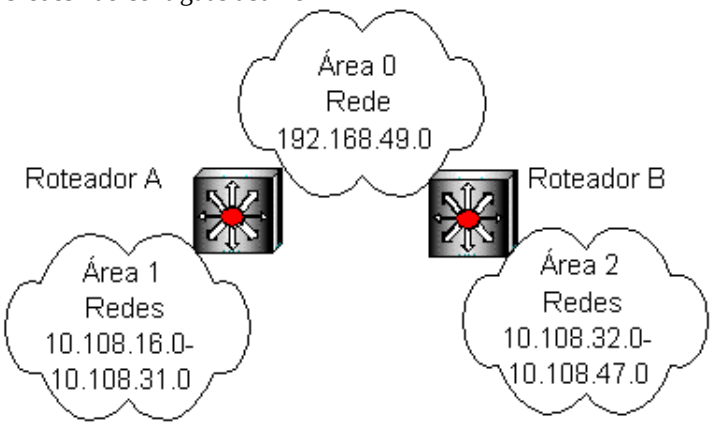
- O roteamento com classes automaticamente sumariza rotas para subredes
    - Rotas são anunciadas para redes classes A, B e C e não para subredes
    - É isso que permite ter menos informação de roteamento
- Como consequência, subredes não contíguas não são suportadas (vide adiante)
- Com CIDR, poderemos também fazer sumarização de rotas, mas de uma maneira mais eficiente (com prefixos menores, juntando rotas de várias classes)
    - Devido ao prefixo menor, chamamos isso de "supernetting"
    - Isso deve ser feito dentro da rede corporativa também, para minimizar tráfego de roteamento
- Exemplo: Veja a rede abaixo



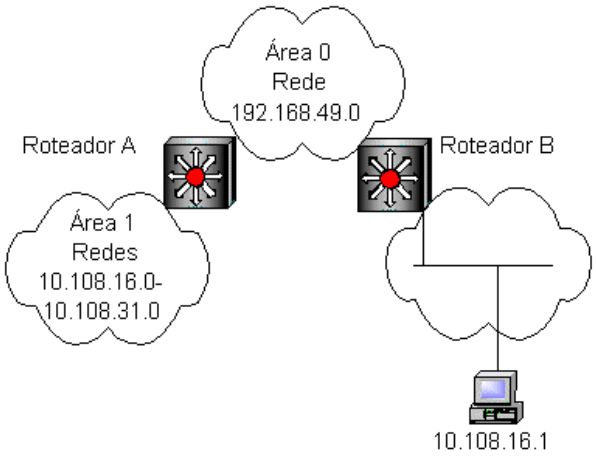
- O roteador pode anunciar que ele tem atrás 172.16.0.0/14 atrás dele para o resto da empresa
  - Os 14 primeiros bits das redes são iguais

Subredes não contíguas

- Lembre que o roteamento com classes não suporta redes não contíguas
- Veja uma rede com subredes não contíguas abaixo



- Usando roteamento com classes
  - Roteador A anuncia que pode chegar à rede 10.0.0.0
  - Roteador B ignora isso porque ele também pode chegar na rede 10.0.0.0
  - Portanto o roteador B não pode chegar às subredes 10.108.16.0 a 10.108.31.0
  - Não houve forma do roteador A anunciar exatamente a situação
- Usando roteamento sem classes
  - Roteador A anuncia que pode chegar à rede 10.108.16.0/20
  - Roteador B anuncia que pode chegar à rede 10.108.32.0/20
  - Nenhum dos roteadores joga essa informação fora porque eles podem analizar o prefixo e sacar o que está acontecendo
- Podemos ainda dar suporte a um hospedeiro móvel
  - Um hospedeiro móvel tem um endereço IP fixo mas pode mover de subrede para subrede
  - Considere a figura abaixo
    - Roteador A anuncia que pode chegar à rede 10.108.16.0/20
    - Roteador B anuncia que pode chegar à rede 10.108.32.0/20 e também 10.108.16.1/32 (prefixo de 32 é uma rota para um host)
    - Depois de trocar a informação de roteamento, os roteadores terão a informação aparentemente conflitante que
      - 10.108.16.0/20 está atrás de A
      - 10.108.16.1/32 está atrás de B
    - Mas eles usam a rota de maior prefixo primeiro, resolvendo a situação



Variable-length subnet masking

- Uma consequência do roteamento sem classes é que podemos ter prefixos de tamanhos diferentes, ou subredes de tamanhos diferentes na mesma rede
- Isso se chama Variable-length subnet masking (VLSM)
- Fornece mais flexibilidade
- Exemplo:
    - Para um enlace WAN ponto-a-ponto, precisamos de dois endereços IP (um para cada lado)
    - Podemos usar um prefixo de 30 bits, deixando 2 bits para os endereços IP
        - Dispositivos com números 01 e 10 (00 e 11 não podem ser usados)
    - Observe que certos roteadores permitem estabelecer um enlace ponto-a-ponto sem usar endereços IP
        - A única desvantagem é que não se pode "pingar" os endereços mas uma solução de gerência com SNMP ainda consegue saber tudo que ocorre no enlace

Um modelo para atribuir nomes

- Nomes são dados a recursos de vários tipos
    - Roteadores
    - Switches
    - Hospedeiros
    - Impressoras
    - etc.
- Para ter melhor usabilidade, é preferível acessar os recursos por nome e não por endereço
- Precisa-se de uma forma de mapear nomes a endereços, dinamicamente de preferência
- Algumas perguntas que devem ser respondidas com respeito a nomes:
    - Que tipo de recurso precisa de nomes?
    - Estações de trabalho precisam de nomes fixos?
        - Algumas estações oferecerão serviços tais como um servidor Web pessoal?
    - Qual é estrutura de um nome? O tipo de recurso está identificado no nome?
    - Como nomes são armazenados, gerenciados e acessados?
    - Quem atribui nomes?
    - Como mapear nomes a endereços? De forma estática? Dinâmica?
    - Como um hospedeiro descobre seu próprio nome?
    - Se o endereço é atribuído de forma dinâmica, o nome muda se o endereço mudar?
    - Quanta redundância é necessária nos servidores de nomes?
    - O banco de dados de nomes será distribuído entre vários servidores?
    - De que forma o sistema de nomes afeta o tráfego na rede?
    - De que forma o sistema de nomes afeta a segurança na rede?

Distribuição de autoridade para atribuir nomes

- Temos o velho problema da solução centralizada (controlada mas burocrática, ponto único de falha, mais tráfego de rede) versus decentralizada
- Dicas para atribuir nomes
    - Colocar o tipo de recurso no nome (rtr, sw, ...)
    - Às vezes, pode ser útil colocar a localização no nome (SAO, CPV, REC, BSB, ...)
    - Cuidado com o $ final em nomes NetBIOS
        - Significa que o nome é escondido e é usado para propósitos administrativos
    - Use nomes com caixa única (maiúsculas ou minúsculas)

Nomes num ambiente NetBIOS

- NetBIOS é o protocolo usado em rede Microsoft
- Pode ser implementado em cima de:
    - NetBEUI (num único domínio de broadcast, já que NetBEUI não roteia)

        - NWLink (Novell)
        - NetBT (NetBIOS over TCP/IP)
            - Cada vez mais comum hoje
- NetBIOS com NetBEUI
    - Não pode ser uma rede muito grande devido ao alto número de broadcasts usados
    - Por isso, as empresas estão migrando para NWLink ou NetBT
- NetBIOS over TCP/IP (NetBT)
    - Há 4 opções para cadastrar e mapear nomes
        - Broadcasts (não desejável)
        - Arquivos lmhosts (cada estação tem a informação de mapeamento de nomes para endereços IP num arquivo - não desejável)
        - Windows Internet Name Service (WINS)
            - Servidor WINS armazena a base de dados e permite o mapeamento dinamicamente
            - Cada estação pode receber o endereço do servidor WINS na resposta DHCP
        - WINS com Domain Name Service (DNS)
            - Uma estação pode ter um nome NetBIOS e um nome DNS
            - Não precisam ser iguais
            - Windows-NT permite integrar as bases de dados
            - Com tempo, é possível que WINS deixe de existir e que apenas DNS seja usado

Nomes num ambiente IP

- Usa o Domain Name Service (DNS)

Seleção de Protocolos de Bridging, Switching e Roteamento

- Supõe-se que o leitor já conheça princípios básicos de protocolos de bridging, switching e roteamento
- Essa seção resume algumas das considerações na escolha de tais protocolos
- Protocolos de bridging/switching/roteamento diferem quanto a:
    - Características de tráfego gerado
    - Uso de CPU, memória e banda passante
    - O número máximo de roteadores pares suportados
    - A capacidade de adaptar rapidamente a novas condições na rede
    - A capacidade de autenticar atualizações de rotas por motivos de segurança
    - Sua padronização (versus protocolo proprietário)
- Ao escolher os protocolos nesta fase do projeto, você terá subsídio para listar as características funcionais dos dispositivos a ser adquiridos

Uso de tabelas de decisão no projeto de rede

- De forma geral, para tomar boas decisões em qualquer projeto (não só de redes), você deve:
    - Conhecer os objetivos (requisitos)
    - Explorar muitas alternativas
    - Investigar as consequências das decisões
    - Elaborar planos de contingência
- Para casar alternativas com requisitos de forma clara e simples, pode-se usar uma tabela de decisão
- Exemplo de uma tabela de decisão (fictícia)

	Requisitos críticos			**Outros requisitos**		
	Adaptabilidade - deve reconfigurar em segundos após mudança na rede	Deve ser escalável até grandes redes (centenas de roteadores)	Deve ser um padrão e ser compatível com equipamento existente	Não deve gerar muito tráfego	Deve rodar em roteadores baratos (low-end)	Deve ser fácil de configurar e gerenciar
BGP	X	X	X	8	7	7
OSPF	X	X	X	8	8	8
IS-IS	X	X	X	8	6	6
IGRP	X	X				
Enhanced IGRP	X	X				
RIP			X			

- Na tabela acima, um X é usado para requisitos críticos
    - Se a alternativa não satisfizer, ela é cortada imediatamente
- Para requisitos não críticos (que podem ser ou não atendidos), usam-se pesos (1=fraco atendimento ao requisito, 10=bom atendimento ao requisito)
- Após tomar a decisão, pergunte-se:
    - O que pode dar errado com a opção escolhida?
    - Essa opção foi tentada por outras empresas? Teve problemas?
    - Como o cliente vai reagir à decisão?
    - Qual o plano de contingência se o cliente não aprovar a decisão?

Seleção de protocolos de bridging e switching

- Lembre que, em termos de protocolos, bridges e switches são praticamente equivalentes
    - Uma switch é essencialmente uma ponte com muitas portas
    - A switch é mais rápida porque pode usar cut-through switching
        - Chavea antes de ter recebido todo o frame
    - A switch implementa VLANs e a ponte não
    - Ambas são dispositivos de camada 2
    - Ambas permitem "mixed-media" (portas para redes de tecnologias diferentes)

Protocolos comuns

- O leitor deve estar familiarizado com os seguintes protocolos de bridging e switching:
    - Transparent bridging/switching (Ethernet)
    - Spanning tree protocol
    - Source-route bridging (Token Ring - pouco usado no Brasil)
    - Como as alternativas são poucas, não falaremos mais sobre a escolha
        - Use transparent bridging/switching com spanning tree e fim de papo

Protocolos de switching para transportar informação de VLANs

- Montar VLANs com várias switches e com as VLANs espalhadas entre as switches significa que as switches devem trocar informação sobre VLANs
    - Em geral , o protocolo chama-se "Trunking protocol"
    - Os quadros devem ser etiquetados com a informação de VLAN à qual pertencem
- Até recentemente, não havia padrão para este protocolo e cada fabricante adotava sua própria solução
    - Exemplo: Cisco usa vários protocolos:
        - Adaptação de IEEE 802.10
        - Inter-Switch Link protocol (ISL)
        - VLAN Trunk protocol (VTP)
    - Era impossível fazer VLANs com switches de fabricantes diferentes
    - mesmo, hoje, é preferível usar switches de um mesmo fabricante
- O IEEE padronizou o protocolo 802.1q para este fim
    - É melhor exigir que os switches dêem suporte a este protocolo

Seleção de protocolos de roteamento

- Um protocolo de roteamento permite que um roteador descubra como chegar a outras redes e trocar essa informação com outros roteadores
- É mais difícil escolher um protocolo de roteamento do que um protocolo de bridging/switching porque tem muitas alternativas
- Uma tabela de decisão pode ser usada para juntar os fatos e selecionar os protocolos

Caracterização de protocolos de roteamento

- Já falamos que protocolos de roteamento diferem quanto a:
    - Características de tráfego gerado
    - Uso de CPU, memória e banda passante
    - O número máximo de roteadores pares suportados
    - A capacidade de adaptar rapidamente a novas condições na rede
    - A capacidade de autenticar atualizações de rotas por motivos de segurança
    - Sua padronização (versus protocolo proprietário)
- Examinaremos algumas dessas questões rapidamente aqui, como lembrete ao leitor
    - Supõe-se conhecimento de protocolos de roteamento

Tipos de protocolos

- Os algoritmos dos protocolos são de dois tipos:
    - Vetor de distância (roteador anuncia a distância que ele tem para cada destino)
        - IP Routing Information Protocol (RIP) versões 1 e 2
        - IP Interior Gateway Routing Protocol (IGRP)
        - Novell NetWare Internetwork packet Exchange Routing Information Protocol (IPX RIP)
        - AppleTalk Routing Table Maintenance Protocol (RTMP)
        - AppleTalk Update-Based Routing Protocol (AURP)
        - IP Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)
        - IP Border Gateway Protocol (BGP)
    - Link-state (roteador anuncia o estado de cada interface de rede que ele têm)
        - Open Shortest Path First (OSPF)
        - IP Intermediate System to Intermediate System (IS-IS)
        - NetWare Link Services Protocol (NLSP)
- De forma geral, os protocolos link state (que são mais recentes) convergem mais rapidamente e não causam tantos loops de rotas durante a convergência
    - Por outro lado, eles são mais complexos de configurar

Métricas de protocolos

- Os protocolos mais velhos de vetor de distância usam número de hops como única métrica
    - Não conseguem usar rotas com mais hops mas que tenham mais banda passante ou filas menores
- Alguns têm um limite no número máximo de hops (15 para RIP)
- Protocolos mais recentes podem usar atraso, banda passante, etc. como métricas

Protocolos de roteamento hierárquicos e não hierárquicos

- Em alguns protocolos, cada roteador é igual a outro (são pares)
- Em outros protocolos, há uma hierarquia onde certos roteadores são agrupados em áreas (ou sistemas autônomos)
- Um roteador que conecta duas áreas pode sumarizar as rotas para sua área e anunciar menos informação

Protocolos Interior versus Exterior

- "Interior routing protocols" (RIP, IGRP, OSPF) são feitos para achar as melhores rotas baseando-se em métricas, dentro de um sistema autônomo (uma empresa, por exemplo)
- "Exterior routing protocols" (BGP) roteam entre sistemas autônomos e devem levar em consideração considerações administrativas
    - Por isso, nem todas as rotas são anunciadas, para obedecer a certas políticas de roteamento
    - Exemplo: Uma empresa está conectada ao backbone Embratel (um sistema autônomo) e ao backbone RNP (outro sistema autônomo) e quer anunciar suas rotas mas não quer servir de "transit network" entre Embratel e RNP

Protocolos baseados em classes e classless

- Já falamos acima de roteamento com classes e sem classes
- As vantagens do roteamento sem classes são
    - Há mais sumarização de rotas com prefixos menores (supernetting)
    - Tem suporte a subredes não contíguas
    - Tem suporte a Variable-Length Subnet Masking, incluindo suporte a hosts móveis

Roteamento estático versus dinâmico

- Em certos casos (em stub networks), podemos dispensar protocolos de roteamento e usar rotas estáticas
    - Exemplo: se uma empresa se conecta ao um ISP via um único enlace, não há por que trocar informação de roteamento entre a empresa e o ISP

Restrições de escalabilidade em protocolos de roteamento

- Protocolos podem ser investigados quanto às suas restrições de escalabilidade
- Exemplos de questões que podem ser investigadas
    - Há limites impostos nas métricas?
    - Com que rapidez o protocolo converge depois de mudanças na rede?
        - Um bom protocolo (OSPF, por exemplo) converge em poucos segundos
    - Que quantidade de dados é transmitida nuna atualização de rota? A tabela inteira? Apenas as mudanças?
    - Quanta banda passante é consumida pelo protocolo?
        - Veja tabela na seção 2.4
    - Para quem as atualizações de rotas são enviadas? Para roteadores vizinhos? Para todos os roteadores num sistema autônomo?
    - Quanta CPU é necessária para processar as atualizações de rotas recebidas?
    - Rotas estáticas de rotas default são suportadas?
    - A sumarização de rotas é suportada?

Roteamento IP

- Daremos um breve resumo dos protocolos mais usados numa rede TCP/IP
    - RIP, IGRP, Enhanced IGRP, OSPF e BGP

Routing Information Protocol (RIP)

- Primeiro protocolo de roteamento na Internet, no início dos anos 1980
- Interior routing protocol
- Ainda é usado devido à simplicidade e disponibilidade em todos os equipamentos
- É do tipo vetor de distância
- Broadcast da tabela de rotas a cada 30 segundos
- 25 rotas por pacote
    - Tabela grande leva vários pacotes
- Quando se usam enlaces lentos, a banda passante consumida pode ser alta em redes grandes
- Métrica única: hop count
- Hop count limitado a 15
- Versão 2 melhora um pouco as coisas, já que a máscara de sub-rede é transmitida na tabela de rotas (classless routing)

IP Interior Gateway Routing Protocol (IGRP)

- Inventado pela Cisco no anos 1980
- Muito usado, já que 80% dos roteadores vendidos são da Cisco
- Interior routing protocol
- Tem mais métricas do que RIP e não tem limite de 15 hops

- Atualizações a cada 90 segundos
- Permite balanceamento de carga
- Permite convergência mais rápida devido ao uso de "triggered updates"
    - Diminui a ocorrência de loops durante a convergência

IP Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)

- Inventado pela Cisco no anos 1990
- Interior routing protocol
- Feito para grandes redes com múltiplos protocolos de roteamento
    - Interfaceia com RIP, IS-IS, BGP e OSPF
- Convergência muito rápida, mesmo com grandes redes (milhares de roteadores)
- Algoritmo garante que não haja loops

Open Shortest Path First (OSPF)

- Protocolo da IETF, fins dos anos 1980
- Para substituir RIP e oferecer um protocolo para grandes redes
- Interior routing protocol
- Tipo Link State
- Vantagens:
    - É um padrão suportado por todos os fabricantes
    - Converge rapidamente
    - Autentica atualizações de rotas para fins de segurança
    - Suporta redes não contíguas e VLSM
    - Usa multicast em vez de broadcast
    - Redes OSPF podem ser configuradas em áreas hierárquicas
    - Propaga apenas mudanças e não tabelas inteiras
    - OSPF não usa muita banda passante

IP Border Gateway Protocol (BGP)

- Exterior routing protocol
- Complexo, usa muita banda passante e não deve ser usado em empresas pequenas

Um sumário de protocolos de roteamento

- Em redes muito pequenas, usam-se frequentemente rotas estáticas
- Quando a rede cresce um pouco e tem enlaces redundantes, usa-se RIP ou IGRP
- Com redes um pouco maiores, usa-se OSPF
- Entre sistemas autônomos, usa-se BGP-4
- Um resumo dos protocolos segue

	Tipo	Interior/Exterior	Classful/classless	Métricas	Escalabilidade
RIP versão 1	Distance-vector	Interior	Classful	Hop count	15 hops
RIP versão 2	Distance-vector	Interior	Classless	Hop count	15 hops
IGRP	Distance-vector	Interior	Classful	Banda passante, atraso, confiabilidade, carga	255 hops (default 100)
Enhanced IGRP	Distance-vector	Interior	Classless	Banda passante, atraso, confiabilidade, carga	Milhares de roteadores
OSPF	Link-state	Interior	Classless	Custo (depende do fabricante)	Aprox. 50 roteadores por área, aprox. 100 áreas
BGP	Path-vector	Exterior	Classless	Valor de atributos do caminho e outros fatores configuráveis	Milhares de roteadores
IS-IS	Link-state	Interior	Classless	Valor de caminho configurado, atraso, custo e erros	Milhares de roteadores
RTMP	Distance-vector	Interior	N/A	Hop count	15 hops
AURP	Distance-vector	Interior ou exterior	N/A	Hop count	15 hops de cada lado
IPX RIP	Distance-vector	Interior	N/A	Ticks e hop count	15 hops
NLSP	Link-state	Interior	N/A	Custo e banda passante	127 hops

	Tempo de convergência	Consumo de recursos	Autenticação de rotas?	Facilidade de projeto, configuração, troubleshooting
RIP versão 1	Pode ser grande	Memória: baixo CPU: baixo BW: alto	Não	Fácil
RIP versão 2	Pode ser grande	Memória: baixo CPU: baixo BW: alto	Sim	Fácil
IGRP	Rápido (usa triggered updates e poison reverse)	Memória: baixo CPU: baixo BW: alto	Não	Fácil
Enhanced IGRP	Muito 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	Pode ser grande	Memória: médio CPU: médio BW: alto	Não	Fácil
AURP	Rápido	Memória: baixo CPU: médio BW: baixo	Sim	Médio
IPX RIP	Rápido	Memória: médio CPU: médio BW: alto	Não	Fácil
NLSP	Rápido	Memória: alto CPU: alto BW: baixo	Sim	Médio

Desenvolvimento de Estratégias de Segurança e Gerência

- Segurança e Gerência são aspectos importantes do projeto lógico de uma rede
- São frequentemente esquecidos por projestistas por serem considerados questões operacionais
    - Não são!
    - Essas questões afetam a escalabilidade, o desempenho, e os tradeoffs entre vários requisitos
    - Exemplo: pode-se querer monitoração "out-of-band" para a gerência e isso afeta todo o projeto
- Uma boa referência: RFC 2196: Site Security Handbook
- Abordamos alguns aspectos da segurança, mas de forma incompleta
    - O assunto merece uma disciplina inteira

Projeto da segurança de uma rede

- A segurança é cada vez mais importante devido a:
    - Conexões para Internet
    - Formação de uma Extranet
    - Uso da rede corporativa por usuários móveis e empregados que trabalham em casa
- Etapas para o projeto da segurança:
    - Identificar os recursos de rede
    - Analizar os riscos de segurança
    - Analizar os requisitos e tradeoffs de segurança
    - Elaborar um plano de segurança
    - Elaborar políticas de segurança
    - Elaborar procedimentos para aplicar as políticas de segurança
    - Elaborar uma estratégia de implementação
    - Obter o compromisso de usuários, gerentes e equipe técnica
    - Treinar usuários, gerentes e equipe técnica
    - Implementar a estratégia a procedimentos de segurança
    - Testar a segurança e rever as decisões, se necessário
    - Manter a segurança através de auditorias independentes periódicas, examinando logs, respondendo a

incidentes de segurança, atualizando-se quanto a alertas de segurança, continuando a treinar os usuários, continuando a testar a segurança, atualizando o plano e a política de segurança

Identificação de recursos de rede e de riscos

- O assunto já foi discutido num capítulo anterior
- Recursos de rede e os riscos associados ao seu acesso inapropriado devem ser avaliados
- Recursos de rede incluem:
  - Hospedeiros (incluindo sistemas operacionais, aplicações, dados)
  - Dispositivos de interconexão (roteadores, switches)
  - Dados que transitam na rede

Análise de tradeoffs de segurança

- O custo da proteção contra uma ameaça deve ser menor do que recuperar-se da concretização da ameaça!
- Há tradeoffs entre segurança e:
  - Custo
  - Usabilidade (mais difícil para os usuários)
  - Desempenho (filtros de pacotes e criptografia podem usar uns 15% da CPU; é mais difícil fazer balanceamento de carga com criptografia)
  - Disponibilidade (se houver ponto único de falha num firewall, por exemplo)
  - Gerenciabilidade (manter logins, senhas, ...)

Desenvolvimento de um plano de segurança

- Um plano de segurança é um documento de alto nível que especifica o que uma empresa vai fazer para cumprir requisitos de segurança
- O plano especifica o tempo, as pessoas e outros recursos necessários para desenvolver as políticas de segurança e implementá-las
- O plano faz referencia à topologia da rede e especifica quais serviços serão providos
- O plano especifica ainda:
  - Quem provê os serviços
  - Quem pode acessar os serviços
  - Como o acesso é provido
  - Quem administra os serviços
  - Como será o treinamento sobre aspectos de segurança
- É importante receber a compromisso dos envolvidos sobre o plano de segurança
  - O maior perigo da segurança está nas pessoas

Desenvolvimento de uma política de segurança

- Uma política de segurança especifica formalmente as regras que devem ser seguidas pelas pessoas que acessarão os recursos da empresa
- As obrigações das pessoas (usuários, gerentes, equipe técnica) para manter a segurança são especificadas
  - Os mecanismos pelos quais as obrigações podem ser cumpridas são especificados

Componentes de uma política de segurança

- Uma política de acesso
  - Define os direitos de acesso
  - Deve prover regras (quem, quando, como) para conectar redes externas, conectar dispositivos à rede e adicionar novo software a hospedeiros ou dispositivos
- Uma política de responsabilidade
  - Define as responsabilidades de usuários, equipe de operação e gerência da empresa
  - Deve prover uma forma de fazer auditoria e regras para reportar problemas de segurança
- Uma política de autenticação
  - Define a política de uso de senhas e regras para a autenticação de localizações remotas (call-back, por exemplo)
- Uma política de aquisição de tecnologia de computadores
  - Define regras para adquirir, configurar e auditar sistemas de computadores e redes, de forma a manter a integridade das políticas de segurança

Desenvolvimento de procedimentos de segurança

- Procedimentos de segurança implementam as políticas de segurança
- Os procedimentos definem os processos de configuração, login, auditoria e manutenção
- Procedimentos específicos devem ser escritos para:
  - Usuários
  - Administradores de rede
  - Administradores de segurança
- Os procedimentos devem descrever como responder a um incidente de segurança (o que fazer, quem contactar, ...)
- Os envolvidos devem receber treinamento sobre os procedimentos de segurança

Mecanismos de segurança

- Falaremos de algumas técnicas que podem ser usadas para implementar soluções de segurança

- O projeto das soluções em si será abordado adiante

Autenticação

- Mecanismo normal: nome de login e senha
- Pode usar "one-time passwords" para obter mais segurança
    - Normalmente empregado para usuários remotos, usando um *security card*
        - O security card gera one-time passwords após receber identificação do usuário
        - Para obter acesso, o usuário deve ter duas coisas: a identificação e o card

Autorização

- Baseada em permissões de acesso, usando, por exemplo, Access Control Lists
- Gerenciamento das permissões facilitada com o uso de grupos de usuários

Auditoria

- Coleta de dados sobre o uso de recursos
- Para descobrir quem fez o quê, quando
- Informação tipicamente coletada:
    - Todas as tentativas de autenticação e autorização
    - Nome de login (não senha!)
    - Logouts
    - Mudanças de permissões
    - Timestamp para toda a informação
- Pode incluir um *sucurity assessment* feito por profissionais contratados para penetrar no sistema
- Os logs devem ser periodicamente analizados e as políticas de segurança ajustadas

Sigilo

- Criptografia para "esconder" os dados
- Dados não criptografados são chamados "clear text"
- Uso obrigatório qo utilizar uma Virtual Private Network
- Duas técnicas básicas
    - Chaves simétricas (rápido, problemas de distribuição de chaves)
        - Exemplo: Data Encryption Standard (DES)
    - Chaves públicas (lento mas permite criptografia e assinatura digital)
        - Exemplos: RSA, Diffie-Hellman
    - Solução híbrida (chave pública para trocar senhas simétricas)
        - Exemplo: Digital Signature Standard (DSS) = Diffie-Helman + DES

Filtros de pacotes

- Já discutidos anteriormente

Firewalls

- Filtro de pacote inteligente com definição de ações e boa interface gráfica

Escolha de soluções de segurança

- Como usar os mecanismos acima numa solução de segurança?
- Falaremos de:
    - Segurança da conexão Internet
    - Segurança do acesso discado
    - Segurança de serviços de rede
    - Segurança de serviços do usuário

Segurança da conexão Internet

- Uso de uma combinação de mecanismos:
    - Firewalls
    - Segurança física
    - Logs de auditoria
    - Autenticação
    - Autorização
- Apenas alguns serviços públicos podem ser usados sem autenticação/autorização
- A chave é desligar todos os serviços não necessários
- Não rode NIS (que é muito perigoso) no Demilitarized Zone

Segurança do acesso discado

- Uso de uma combinação de mecanismos:
    - Firewalls
    - Segurança física
    - Logs de auditoria
    - Autenticação
    - Autorização
    - Criptografia
- Usuários remotos que utilizem o PPP devem ser autenticados usando um protocolo tal como Challenge Handshake

Authentication Protocol (CHAP)
    - Não usar o Password Authentication Protocol (PAP) que é mais fraco (a senha é enviada como clear text)
- Uma outra opção é o uso de Remote Authentication Dial-In User Server (RADIUS)
    - Mantém um banco de dados centralizado de usuários/senhas
    - O banco de dados especifica o tipo de serviço permitido (telnet, rlogin, ...)
- Não deve ser permitido que um usuário conecte um modem a sua máquina na empresa!
    - Deve haver um único ponto para dial-in
- O uso de call-back para combater hackers é muito comum

Segurança de serviços de rede

- A regra chave novamente: desligue os serviços não necessários
- Proteja o acesso a roteadores e switches com senhas
    - Mesmo que o acesso seja a partir de uma porta serial no dispositivos
- Dois níveis de autorização são frequentemente implementados
    - Visualização de status dispositivos (primeiro nível)
    - Visualização e alteração de configuração (segundo nível)
- Para controlar o acesso a vários roteadores e switches, pode-se usar o Terminal Access Controller Access Control System (TACACS)
    - Semelhante a RADIUS
- De forma geral, desabilite o uso da operação SNMP set
    - Porque SNMPv1 e SNMPv2 não têm segurança boa
    - SNMPv3 tem melhor segurança

Segurança de serviços do usuário

- Tenha uma política de senhas e ensine-a aos usuários
    - Como escolher uma senha
    - Quando trocar uma senha
- Cuidado com "root"
- Habilite o logout automático

Projeto da gerência de rede

- Será visto em outra disciplina

4. Projeto Físico da Rede

- Seleção de tecnologias e dispositivos para redes de campus
- Seleção de tecnologias e dispositivos para redes corporativas

Seleção de Tecnologias e Dispositivos para Redes de Campus

- O projeto físico envolve a seleção de:
  - Cabeamento
  - Protocolos das camadas física e de enlace
  - Dispositivos de interconexão (hubs, switches, roteadores)
- Não escolha "certa" para todas as circunstâncias (ou mesmo uma circunstância particular)
- Neste capítulo, estudamos como fazer o projeto físico para uma rede de campus
  - Rede de alguns kilometros de diâmetro
- No final veremos um exemplo completo de um projeto de uma rede de campus

Projeto de cabeamento para LANs

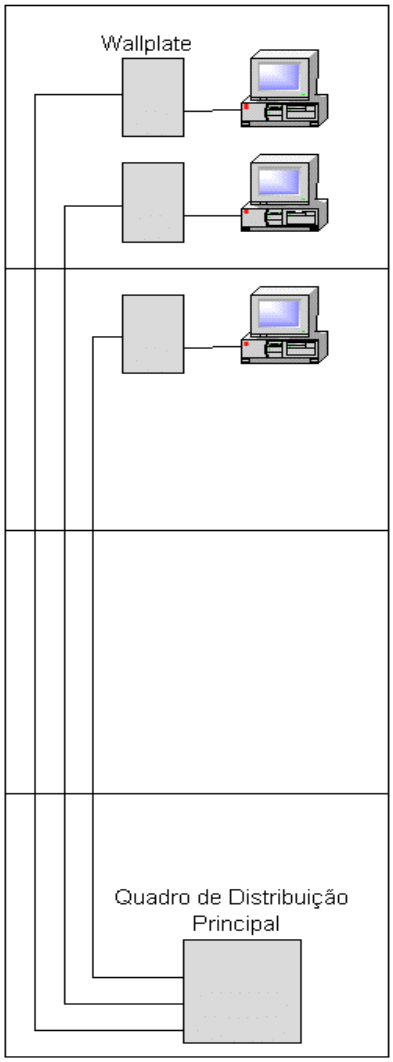
- Não cobrimos o assunto em detalhes
- De forma geral, o planejamento de cabeamento tem que levar em consideração que este poderá ser usado durante mais tempo (vários anos) do que as tecnologias de rede que o usarão
- Em muitos casos, o projeto tem que se adaptar a um cabeamento existente, como já foi levantado num capítulo anterior:
  - Topologias de cabeamento de prédios
  - Topologias de cabeamento de campus (entre prédios)
  - Tipos e comprimentos dos cabos entre prédios
  - Localização dos armários de cabeamento (wiring closets) e salas especiais de conexões
  - Tipos e comprimentos de cabos verticais entre andares
  - Tipos e comprimentos de cabos da área de trabalho, entre armários de cabeamento até as estações

Topologias de cabeamento

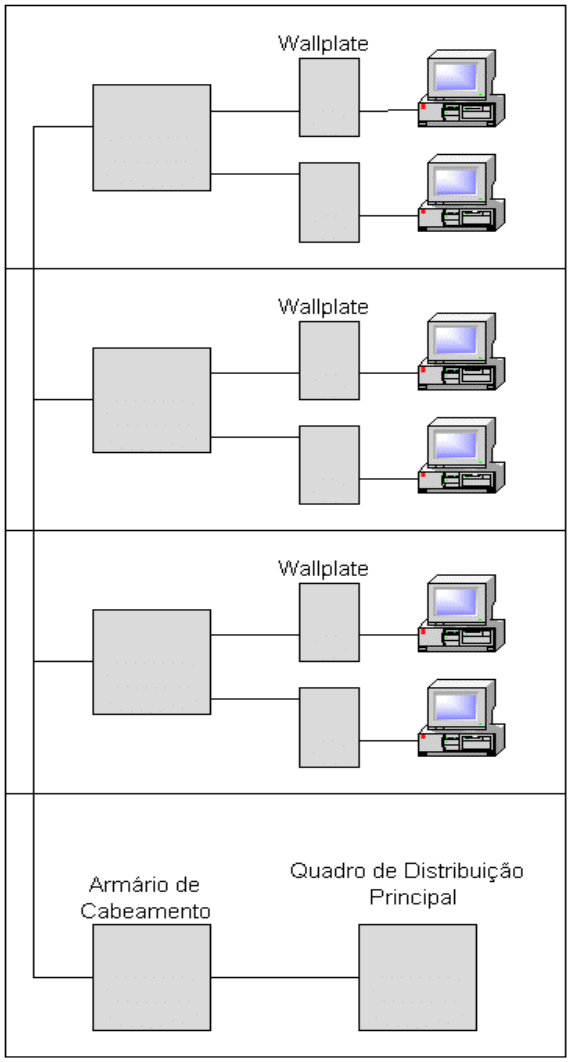
- Há dois grandes tipos de topologias:
  - Cabeamento centralizado, onde todos os cabos vão para uma única área física
  - Cabeamento distribuído, onde os cabos podem terminar em várias áreas físicas

Topologias de cabeamento para prédios

- Dentro de um prédio pequeno, uma arquitetura centralizada ou distribuída pode ser usada, já que todos os cabos poderão ter menos de 100 m
- Num prédio grande, onde os cabos individuais seriam grandes demais, deve-se usar uma arquitetura distribuída



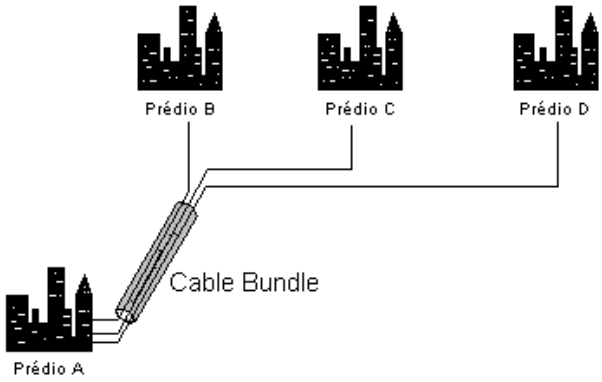
Topologia Centralizada para
Cabeamento de Prédio



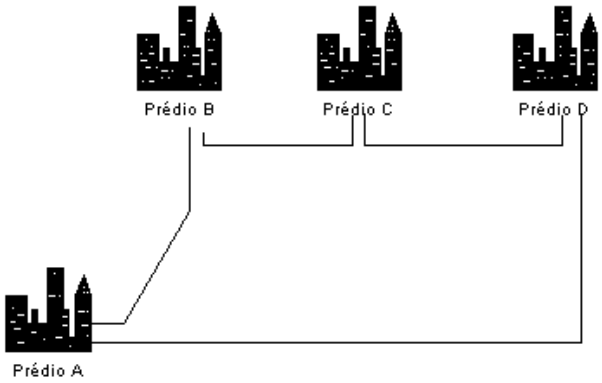
Topologia Distribuída para
Cabeamento de Prédio

Topologias de cabeamento para o campus

- Entre prédios, há mais perigos físicos
  - Escavações, enchentes, ...
- Pode haver outras restrições
  - Cruzamento de áreas pertencendo a outras empresas
  - Nesses casos, pode-se utilizar tecnologia sem fio (microondas, rádio, laser)
- Por esses, motivos, deve-se ter mais cuidado com o cabeamento entre prédios
- A disponibilidade é melhor para uma arquitetura distribuída, pois evita um ponto úmico de falha
  - Porém, o manuseio pode ser mais complicado



Cabeamento centralizado entre prédios



Cabeamento distribuído entre prédios

Tipos de cabos

- Cabo metálico (cobre) com blindagem (shield), incluindo
  - Shielded tswited pair (STP)
  - Coaxial (não é mais popular)
  - Twin-axial (twinax)
- Cabo metálico (cobre) sem blindagem (UTP)
  - O tipo mais usado dentro de prédios
  - Há várias categorias de UTP
    - Cat 1 e Cat 2 não são recomendados para dados
    - Cat 3 (Voice grade): até 16 MHz
      - Pode ser usado com Ethernet 10BASET
    - Cat 4: até 20 MHz (não usado)
    - Cat 5: até 100MHz (o mais usado)
    - Cat 5 estendido: até ?MHz
- Fibra ótica
  - Muito usada entre prédios e para cabeamento vertical
  - Não usada, normalmente, até as estações (muito caro)
  - Dois tipos: multimodo (com LED) e monomodo (com laser)
  - Não sujeito a ruído, interferência eletromagnética, cross-talk
  - Com Wave Division Multiplexing, atinge 40 Gbps (ou mais)

Tecnologias LAN

- Essas tecnologias devem ter sido cobertas em outras disciplinas
  - IEEE 802.3 (Ethernet) e derivados (Fast Ethernet, Gigabit Ethernet)
    - Half e full duplex, 10, 100 e 1000 Mbps
  - ATM
    - Usado com LAN Emulation (LANE) ou Multiprotocolo over ATM (MPOA)
    - 155, 622 Mbps e até 10 Gbps (OC-192)
    - Menos usado no campus devido a Gigabit Ethernet
  - Token ring (obsoleto)
  - FDDI (obsoleto)
- Entender Ethernet e ATM é fundamental para poder escolher tecnologias para redes de campus

- A seleção hoje é frequentemente 100BASETX nas pontas e ATM ou Gigabit Ethernet para o backbone
    - Mas tem muitas redes existentes com 10BASET

Seleção de dispositivos de interconexão para uma rede de campus

- Neste ponto, você já deve ter uma idéia de quais segmentos serão compartilhados e chaveados (switched) e onde estarão feito o roteamento
- Observe a regra "Switch when you can, route when you must"
- Resumo das diferenças entre hubs, pontes, switches e roteadores

	Camadas OSI	Domínios de bandwidth (ou de colisão)	Domínios de broadcast	Onde usado tipicamente	Características adicionais
Hub	1	Todas as portas compartilham o mesmo domínio de bandwidth	Todas as portas compartilham o mesmo domínio de broadcast	Conectar dispositivos individuais em LANs pequenas	Autoparticionamento para isolar portas com problemas
Ponte	1-2	Cada porta participa de um domínio de bandwidth diferente	Todas as portas compartilham o mesmo domínio de broadcast	Conectar redes entre si (hoje usa switch)	Filtragem de pacotes configurada pelo usuário
Switch camada 2	1-2	Cada porta participa de um domínio de bandwidth diferente	Todas as portas compartilham o mesmo domínio de broadcast	Conectar dispositivos individuais ou redes	Filtragem, portas ATM, cut-through switching, multicast
Switch camada 3	1-3	Cada porta participa de um domínio de bandwidth diferente	Depende da estrutura de VLANs	Conectar dispositivos individuais ou redes	Filtragem, portas ATM, cut-through switching, multicast, várias formas de criar VLANs
Roteador	1-3	Cada porta participa de um domínio de bandwidth diferente	Cada porta está num domínio de broadcast diferente	Conectar redes	Filtragem, enlaces WAN de alta velocidade, compressão, enfileiramento especial, multicast, load balancing, Bandwidth on demand, ...

- Agora, dispositivos de fabricantes particulares devem ser escolhidos, baseando-se nos critérios abaixo
- Critérios gerais
    - Número de portas
    - Velocidade de processamento
    - Latência
    - Tecnologias de LAN suportadas (Ethernet 10/100/1000, ATM, ...)
    - Auto-sensing da velocidade (Ethernet 10/100)
    - Cabeamento suportado
    - Facilidade de configuração
    - Gerenciabilidade (suporte a SNMP e RMON)
    - Custo
    - MTBF e MTTR
    - Componentes hot-swappable
    - Suporte a fontes de alimentação redundantes
    - Disponibilidade e qualidade do suporte técnico
    - Disponibilidade e qualidade da documentação
    - Disponibilidade e qualidade do treinamento (para equipamentos complexos)
    - Reputação do fabricante
- Critérios adicionais para switches
    - Vazão em quadros por segundo (ou células para ATM)
    - Suporte a cut-through switching
    - Auto-detecção de modo half- e full-duplex
    - Suporte a Spanning Tree
    - Suporte a VLANs, incluindo formas de definir VLANs e suporte a protocolos de trunking
    - Padronização dos protocolos usados
    - Suporte a IGMP para multicast (para aplicações multimídia)
- Critérios adicionais para roteadores (e switches de camada 3)
    - Protocolos de camada 3 suportados
    - Protocolos de roteamento suportados
    - Suporte a RSVP, multicast IP
    - Habilidade de agir como LES, BUS, LECS, LES em ambiente ATM
    - Suporte a features de otimização (enfileiramento especial, ...)
    - Suporte a compressão
    - Suporte a criptografia
    - Funções de firewall

- Load balancing

Exemplo do projeto de uma rede de campus

- O exemplo que segue é um caso real (mas o nome do cliente foi mudado)

Informação inicial

- Cliente: Faculdades Integradas Onipresentes Fernando do Ó
- 400 alunos (tempo integral e tempo parcial)
- 30 professores
    - Metade com salas permanentes no campus
- Áreas: Humanidades, Negócios, Ciências Sociais, Matemática, Ciência da Computação, Ciências da Terra, Física, Medicina
- 15 funcionários de apoio
- 3 administradores de rede em tempo parcial
- Percepção de que mais alunos não se inscrevem por causa da deficiência na infraestrutura computacional
- Orçamento de US$350.000 para atualizar os laboratórios e a rede no campus
    - Não haverá mais verba para administração e gerência da rede
    - Portanto, o projeto deve ser simples e a rede facilmente gerenciada

Requisitos de negócios e técnicos

- Requisitos de negócio
    - Aumentar a matrícula de 400 a 500 anos em 2 anos
    - Reduzir a taxa de evasão de 30% para 15% em 2 anos
    - Atrair alunos que deixam o estado à procura de faculdades com vantagens tecnológicas
    - Prover mais e maiores laboratórios de computação no campus
    - Permitir que usuários conectem seus computadores portáteis à rede do campus para acessar serviços da Faculdade e da Internet
    - Manter (ou reduzir, se possível) o orçamento operacional para a rede
- Requisitos técnicos
    - Centralizar todos os serviços e servidores de forma a facilitar a administração e reduzir custos
        - Servidores decentralizados serão tolerados mas não gerenciados e seu tráfego não será levado em consideração no planejamento da rede
    - Centralizar a conexão à Internet e proibir conexões departamentais à Internet
    - Aumentar a velocidade da conexão à Internet para suportar novas aplicações e um aumento no uso de aplicações existentes
    - Padronizar o protocolo TCP/IP para a rede de campus
        - MacIntoshes serão permitidos mas devem usar o protocolo TCP/IP ou o AppleTalk Filing Protocol (AFP) rodando em cima de TCP/IP
    - Prover portas adicionais nas switches de forma a permitir que alunos conectem seus PCs notebook à rede
    - Instalar DHCP nos servidores Windows NT para dar suporte aos notebooks
    - Prover um tempo de resposta de, no máximo, 100 ms para aplicações interativas
    - Prover uma disponibilidade da rede de 90,90%, com MTBF de 3000 horas (4 meses) com MTTR de 3 horas
        - Falhas no acesso à Internet que fujam ao controle da faculdade não serão contabilizadas
    - Prover segurança para proteger a conexão Internet e a rede interna de hackers
    - Prover uma rede com escalabilidade que permita o uso futuro de aplicações multimídia
    - Prover uma rede que utilize tecnoloigia estado-da-arte
- Convencer os usuários de Matemática e Computação não foi simples
    - Deve-se prover uma rede com alta disponibilidade de forma a que tais usuários não procurem implantar suas próprias soluções

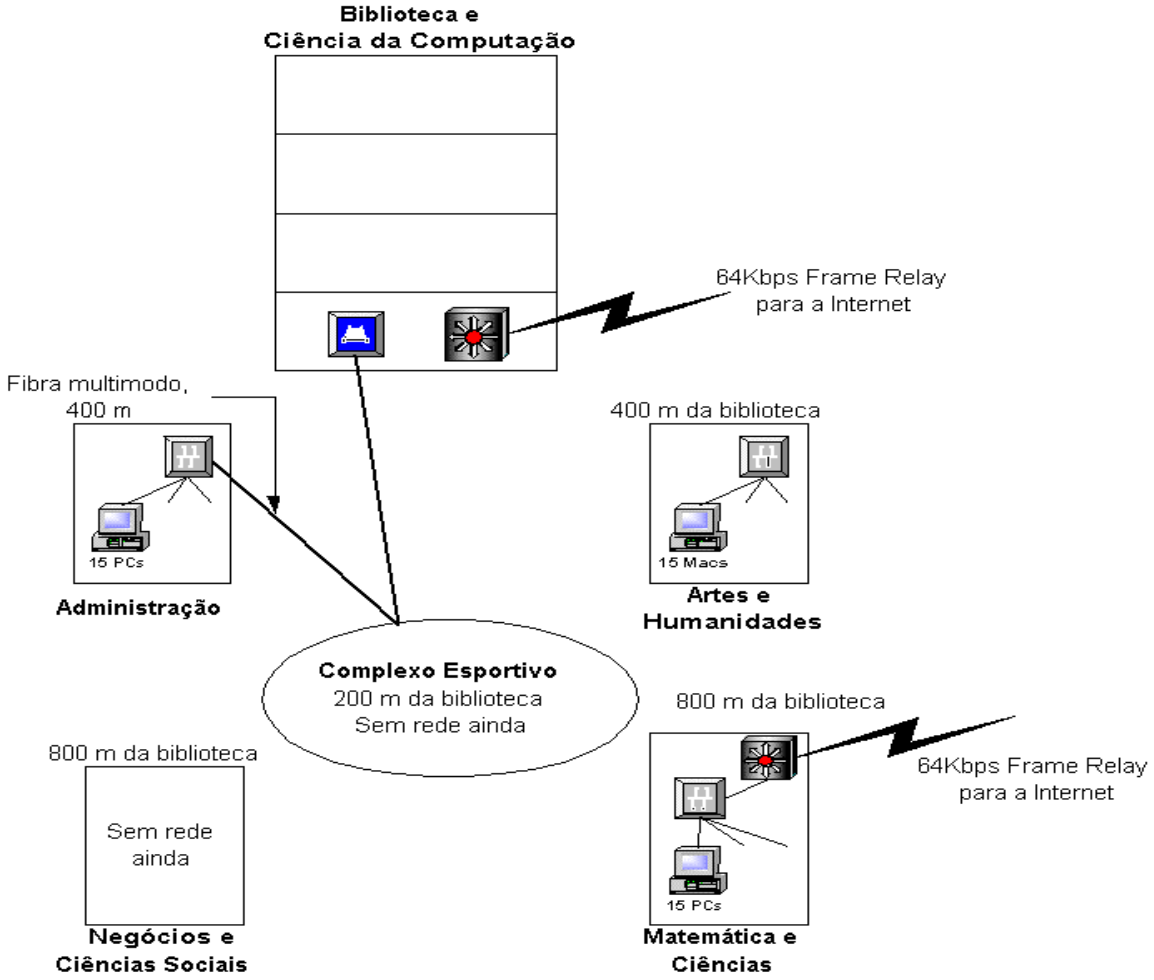
Aplicações de rede

- Aplicações existentes de uso geral
    - Processamento de texto (papers, listas de exercícios, etc.) incluindo a impressão e armazenamento de arquivos em servidores de arquivos
    - Envio e recepção de E-mail
    - Navegar na Web para acessar informação, participar de chat, jogar, etc.
    - Acessar o cadastro da biblioteca
- Aplicações existentes para o Centro de Ciências e Tecnologia
    - Modelagem do tempo
        - Alunos e professores de Meteorologia participam de um projeto para modelar padrões climáticos juntamente com outras faculdades e universidades do estado
    - Monitoração de telescópio
        - Alunos e professores de Astronomia usam um PC para continuamente fazer download de imagens gráficas de um telescópio localizado na universidade estadual
- Aplicações administrativas
    - Um sistema acadêmico executa em ambiente Novell NetWare

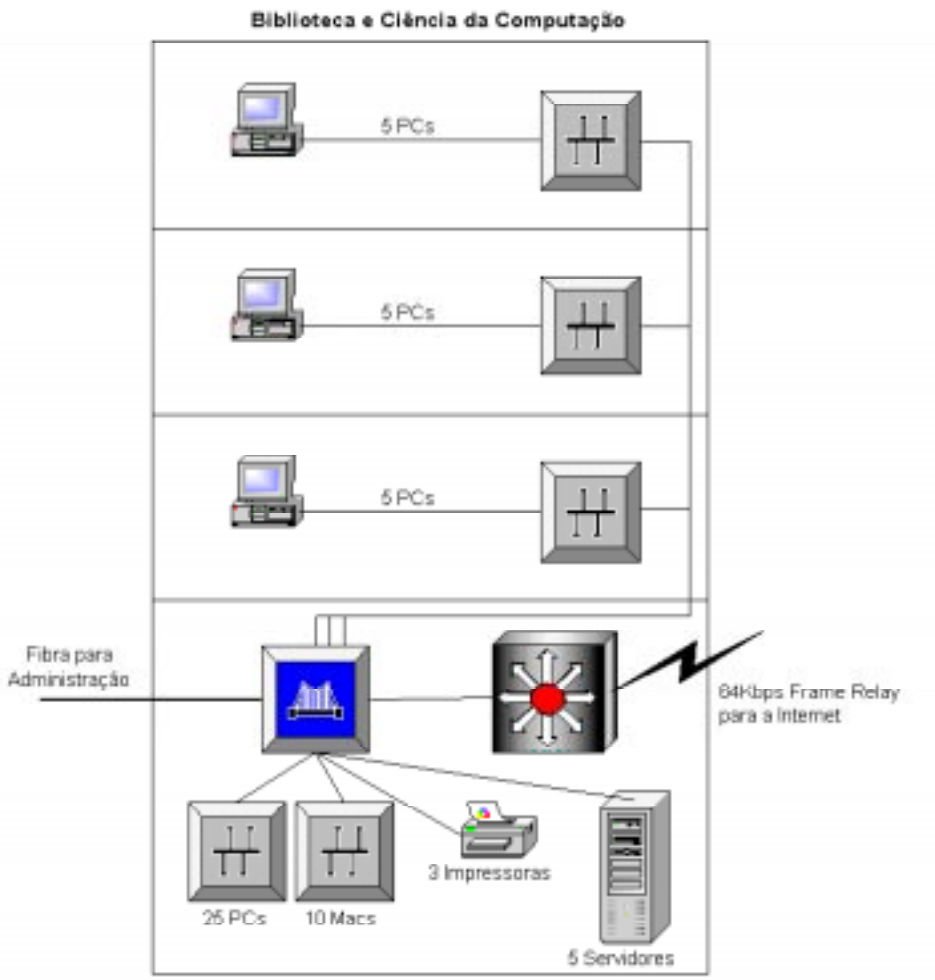
- Aplicações novas planejadas
  - Upload de gráficos
    - O Departamento de Artes deseja fazer upload de volumosas imagens gráficas para impressão laser numa gráfica fora do campus
  - Ensino à distância
    - O Departamento de Ciência da Computação deseja participar de um projeto piloto de ensino à distância juntamente com a universidade estadual
    - Alunos da faculdade poderão receber fluxos de vídeo de aulas dadas na universidade estadual
    - Durante a aula, os alunos podem participar da aula via sala de chat apenas

A rede atual

- No passado, devido à comunidade não permanente da faculdade, a suposição era que alunos e professores usariam mais seus computadores em casa do que na faculdade
- Devido a essa suposição, a rede atual consiste apenas de alguns laboratórios de computação espalhados e um único laboratório principal localizado no Centro de Computação no térreo do prédio da biblioteca
- Veja a rede atual abaixo



- Todas as LANs são Ethernet 10 Mbps
- Todos os prédios têm cabeamento Categoria 5 e wallplates em escritórios, salas de aula, laboratórios
  - Não estão sendo usados em alguns prédios
- Há uma fibra ótica multimodo correndo da biblioteca até o complexo esportivo e daí até o prédio de administração
- Usuários da Biblioteca e do prédio de administração acessam a Internet através de um enlace Frame Relay de 64 Kbps até a universidade estadual
- Os usuários de Matemática não esperaram ganhar acesso à Internet tão cedo e instalar sua própria solução (64 Kbps, Frame Relay) até um ISP
- A biblioteca possui um laboratório central de computação com 10 Macs, 25 PCs, um switch LAN para conectar hubs, estações, servidores, impressoras
  - O roteador age como firewall simples (filtro de pacotes)
  - O roteador não executa protocolo de roteamento
  - Cada andar da biblioteca tem 5 PCs para acessar a Internet e o acervo da biblioteca



Comunidades de usuários

- A tabela abaixo resume as comunidades de usuários
- Espera-se um crescimento devido à aquisição de novos PCs e Macs e devido aos notebooks dos alunos

Nome da comunidade de usuários	Número de usuários na comunidade	Localização da comunidade	Aplicações usadas pela comunidade
Usuários de PCs no centro de computação	25, crescimento até 30	Térreo da biblioteca	Atividades escolares, E-mail, navegação Web, acervo biblioteca
Usuários de Macs no centro de computação	10, crescimento até 15	Térreo da biblioteca	Atividades escolares, E-mail, navegação Web, acervo biblioteca
Usuários da biblioteca	15	Andares 1 a 3 da biblioteca	E-mail, navegação Web, acervo biblioteca
Usuários de PCs em Negócios e Ciências Sociais	16 planejados	Prédio de Negócios e Ciências Sociais	Atividades escolares, E-mail, navegação Web, acervo biblioteca
Usuários de Macs em Artes e Humanidades	15, crescimento até 24	Prédio de Artes e Humanidades	Atividades escolares, E-mail, navegação Web, acervo biblioteca, upload de gráficos
Usuários de PCs em Artes e Humanidades	24 planejados	Prédio de Artes e Humanidades	Atividades escolares, E-mail, navegação Web, acervo biblioteca, upload de gráficos
Usuários de PCs em Matemática e Ciências	15, crescimento até 24	Prédio de Matemática e Ciências	Atividades escolares, E-mail, navegação Web, acervo biblioteca, modelagem climática, monitoração de telescópio, piloto de ensino à distância
Usuários de PCs na administração	15, crescimento até 24	Prédio de Administração	E-mail, navegação Web, acervo biblioteca, sistema acadêmico
Usuários externos	Desconhecido	Internet	Acesso ao site Web da FIOFO

Armazens de dados (servidores)

- A tabela abaixo mostra os servidores de dados identificados

Servidor de dados	Localização	Aplicações	Comunidades que usam
Servidor Windows NT com acervo da biblioteca	Centro de computação	Acervo da biblioteca	Todas
Servidor de Impressão/Arquivo AppleShare	Centro de computação	Tarefas escolares	Usuários de Macs no centro de computação e, no futuro, usuários Mac no prédio de Artes e Humanidades
Servidor de Impressão/Arquivo Windows NT	Centro de computação	Tarefas escolares	Usuários de PCs no centro de computação e, no futuro, usuários de PCs nos outros prédios
Servidor Windows NT para Web e E-mail	Centro de computação	E-mail, navegação Web (hospedeiro do site da FIOFO)	Usuários de PCs no centro de computação e, no futuro, todos os usuários (incluindo usuários externos acessando o site Web local)
Servidor Novell com sistema acadêmico	Centro de computação	Sistema acadêmico	Administração
Servidor de E-mail	Universidade Estadual	E-mail	Servidor de E-mail do campus recebe e envia E-mail de/para este servidor

Características de tráfego das aplicações

- Técnicas usadas para levantar as características do tráfego:
  - Analizador de protocolos
  - Entrevistas com os usuários
  - Tabela de Tamanho Típico de Objetos
  - Tabela de Overhead de Protocolos
- As seguintes aplicações não são sensíveis ao atraso
  - Tarefas escolares
  - E-mail
  - Nabegação Web
  - Acervo da biblioteca
  - Sistema acadêmico
- E-mail
  - Apesar do uso eventual de attachments, E-mail foi considerada uma aplicação de baixo consumo de banda passante
  - 80% do tráfego de E-mail de/para a Internet
  - Espera-se que o percentual caia para 60% depois que todos tiverem conta interna de E-mail
- Navegação Web
  - 2% do tráfego Web vem do o site da faculdade, o resto vem da Internet
  - No futuro, estima-se que 10% do tráfego será local
  - Estimativa de 60 Kbps de banda passante para usuários externos acessando o site da faculdade
- Sistema acadêmico tem demanda muito baixa de banda passante
  - Um único servidor Novell não cria problemas com broadcast SAP

Características de tráfego das aplicações novas e em expansão

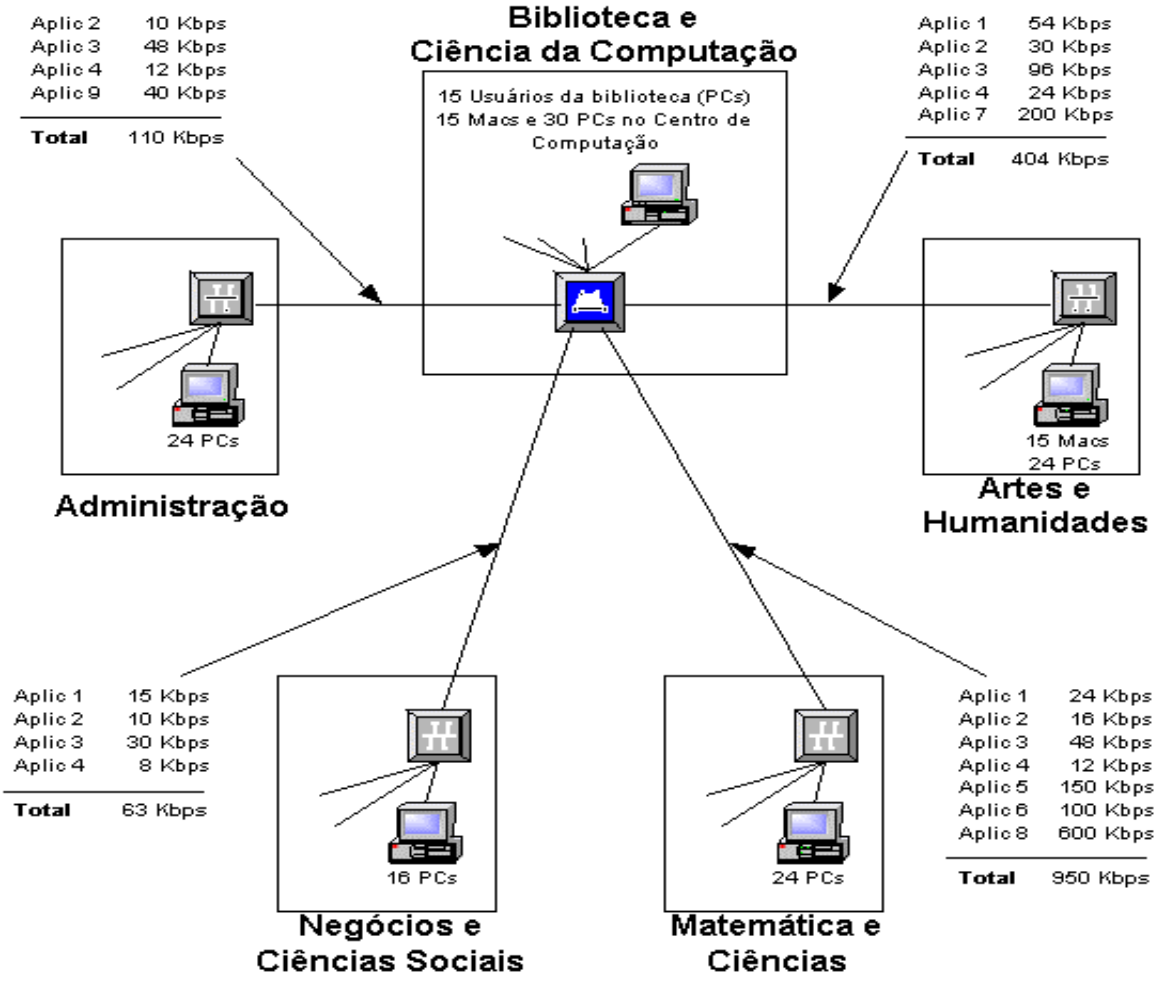
- Modelagem climática e monitoração de telescópio
  - Essas aplicações estão sofrendo com o acesso lento à Internet
  - Um analizador de protocolos e entrevistas com os usuários sobre planos futuros levantaram os dados que aparecem na tabela de sumário, abaixo
- Upload de gráficos
  - Entrevistas com os usuários levantaram que não mais do que 1 arquivo por hora será transferido
  - Arquivos podem ser muito grandes (50 MB)
  - Usuários topam esperar de 5 a 10 minutos para a transferência completar
- Ensino à distância
  - Fluxo de vídeo assimétrico (direção entrando apenas) usando Real-Time Streaming Protocol (RTSP) e Real-Time Protocol (RTP)
  - Alunos da faculdade participam da aula via chat
  - Cada fluxo de vídeo usa 56 Kbps, no máximo, já que a universidade estadual supõe que alunos remotos estarão usando um modem para receber o fluxo (embora não se use modem na faculdade para receber o vídeo)
  - A faculdade vai limitar o número de usuários receptores de vídeo a 10, localizados no prédio de Matemática e Ciências
  - No futuro, o sistema vai usar multicast e, neste ocasião, a faculdade vai abrir o sistema para qualquer aluno no campus

Sumário das características de tráfego fluxos de tráfego

- A tabela abaixo (Características e Fluxos de Tráfego) reflete uso de pico

Nome da aplicação	Tipo de fluxo de tráfego	Protocolos usados pela aplicação	Comunidades que usam a aplicação	Armazens de dados	Banda passante necessária	Requisitos QoS
1. Atividades escolares	Cliente/Servidor	SMB/NetBT	Usuários de PCs no centro de computação	Servidor de arquivo/impressão Windows NT	30 Kbps	Flexível
		AFP sobre TCP	Usuários de Macs no centro de computação	Servidor de arquivo/impressão AppleShare	18 Kbps	Flexível
		SMB/NetBT	Usuários de PCs em Negócios/Ciências Sociais	Servidor de arquivo/impressão Windows NT	15 Kbps	Flexível
		AFP sobre TCP	Usuários de Macs em Artes/Humanidades	Servidor de arquivo/impressão AppleShare	30 Kbps	Flexível
		SMB/NetBT	Usuários de PCs em Artes/Humanidades	Servidor de arquivo/impressão Windows NT	24 Kbps	Flexível
		SMB/NetBT	Usuários de PCs em Matemática/Ciências	Servidor de arquivo/impressão Windows NT	24 Kbps	Flexível
2. E-mail	Cliente/Servidor	SMTP e POP	Usuários de Macs e PCs no centro de computação	Windows NT Web/E-mail/Servidor DHCP	30 Kbps	Flexível
			Usuários da biblioteca	Windows NT Web/E-mail/Servidor DHCP	6 Kbps	Flexível
			Usuários de PCs em Negócios/Ciências Sociais	Windows NT Web/E-mail/Servidor DHCP	10 Kbps	Flexível
			Usuários de Macs e PCs em Artes/Humanidades	Windows NT Web/E-mail/Servidor DHCP	30 Kbps	Flexível
			Usuários de PCs em Matemática/Ciências	Windows NT Web/E-mail/Servidor DHCP	16 Kbps	Flexível
			Administração	Windows NT Web/E-mail/Servidor DHCP	10 Kbps	Flexível
	Servidor/Servidor	SMTP	Servidor Windows Ht Web/E-mail	Servidor E-mail no ISP	60 Kbps	Flexível
3. Navegação Web	Cliente/Servidor	HTTP	Usuários de Macs e PCs no centro de computação	10% no site Web local, 90% na Internet	90 Kbps	Flexível
			Usuários da biblioteca		30 Kbps	Flexível
			Usuários de PCs em Negócios/Ciências Sociais		30 Kbps	Flexível
			Usuários de Macs e PCs em Artes/Humanidades		96 Kbps	Flexível
			Usuários de PCs em Matemática/Ciências		48 Kbps	Flexível
			Administração		48 Kbps	Flexível
			Usuários externos	Site Web local	60 Kbps	Flexível
4. Acervo da biblioteca	Cliente/Servidor	HTTP	Todos os usuários internos	Servidor Windows NT com acervo da biblioteca	Aprox. 500 bps por usuário	Flexível
5. Modelagem climática	Computação distribuída	Proprietário sobre TCP/IP	Subconjunto dos usuários de PCs em Matemática/Ciências	Servidores na Internet	120 Kbps	Flexível
6. Monitoração do telescópio	Cliente/Servidor	HTTP	Subconjunto dos usuários de PCs em Matemática/Ciências	Servidores na Internet	100 Kbps	Flexível
7. Upload de gráficos	Cliente/Servidor	AFP sobre TCP ou FTP	Usuários de Macs e PCs em Artes/Humanidades	Servidor na gráfica externa	200 Kbps	Flexível
8. Ensino à distância	Cliente/Servidor	RTSP, RTP, TCP (futuro RSVP e multicast IP) HTTP para chat	Subconjunto dos usuários de PCs em Matemática/Ciências	Servidor na universidade estadual	600 Kbps	Controlled load (na terminologia IETF)
9. Sistema acadêmico	Cliente/Servidor	NetWare Core Protocol (NCP)	Administração	Servidor Novell do Sistema Acadêmico	40 Kbps	Flexível

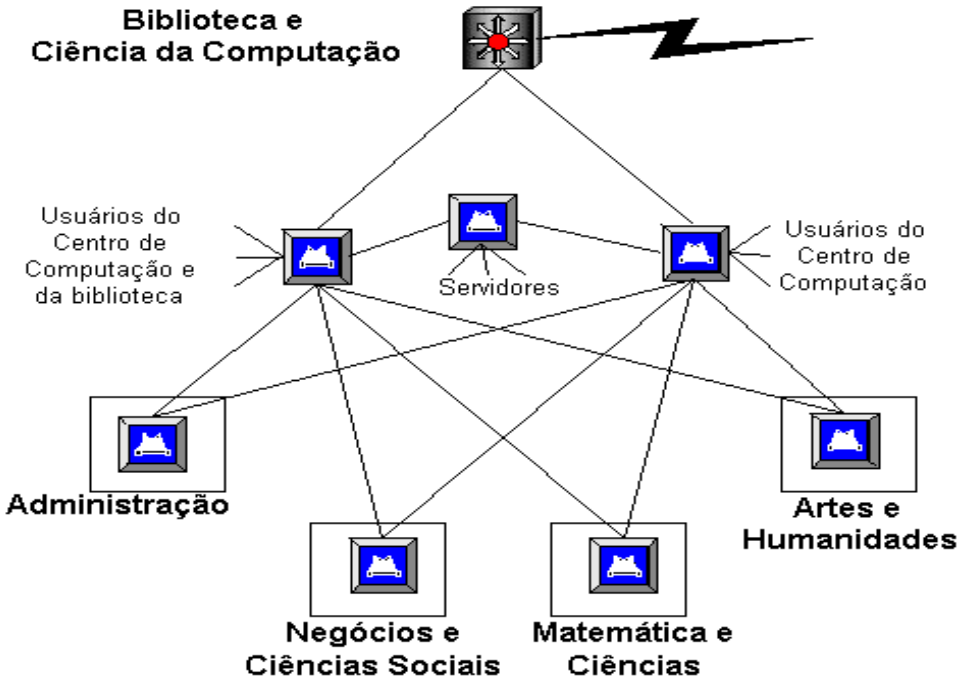
- De forma gráfica, podemos representar os fluxos de tráfego cruzando o campus como na figura abaixo



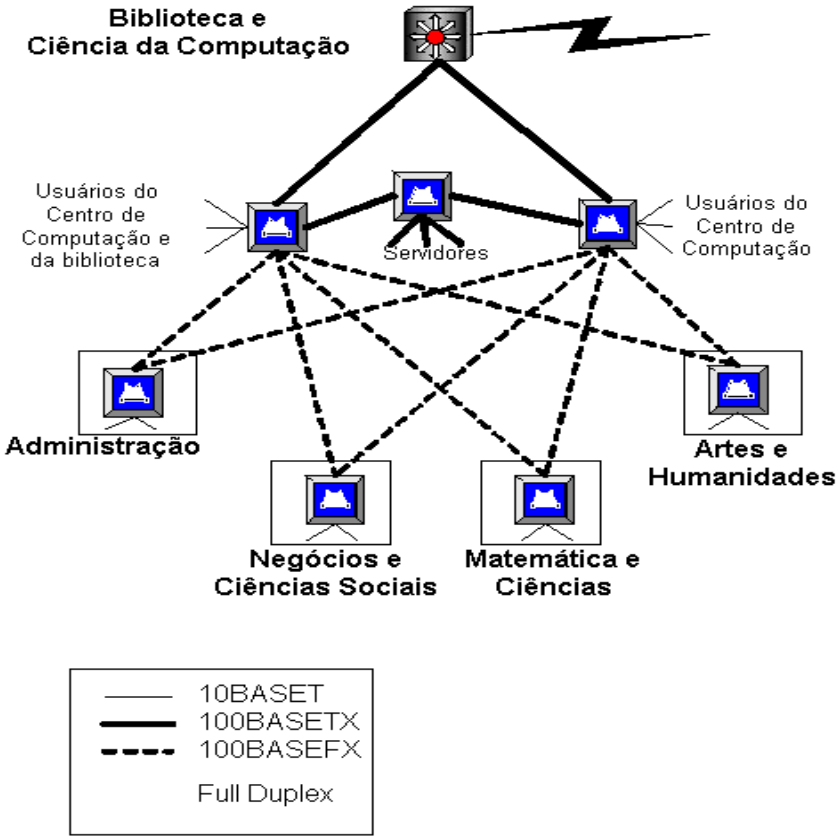
- Dentro do prédio da biblioteca, os fluxos são como segue:
  - Aplicação 1: 48 Kbps
  - Aplicação 2: 36 Kbps
  - Aplicação 3: 120 Kbps
  - Aplicação 4: 30 Kbps
  - **Total: 234 Kbps**
- Os fluxos de tráfego com a Internet são como segue:
  - Aplicação 2: 60 Kbps
  - Aplicação 3: 370 Kbps
  - Aplicação 5: 120 Kbps
  - Aplicação 6: 100 Kbps
  - Aplicação 7: 200 Kbps
  - Aplicação 8: 600 Kbps
  - **Total: 1450 Kbps**

O projeto de rede

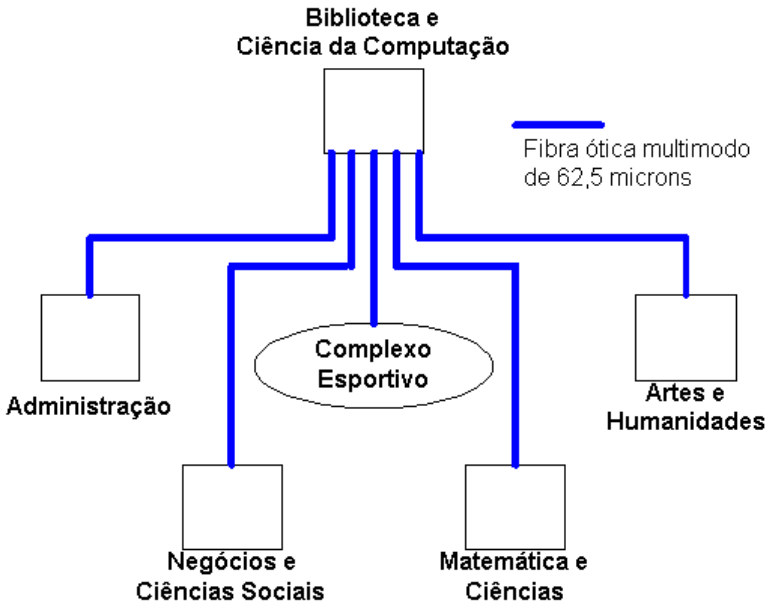
- Analizando os requisitos, uma mesh hierárquica com enlaces redundantes entre prédios foi escolhida como topologia lógica



- Outras decisões tomadas:
  - A rede usa Ethernet com switches
    - Hubs seriam aceitáveis, em termos de banda passante, mas o switches serão melhores para escalabilidade e o custo é aceitável
  - Todos os dispositivos participam de um único domínio de broadcast (são pouco mais de 200 dispositivos)
  - Todos os dispositivos farão parte de uma mesma subrede IP usando o endereço de rede fornecido pela universidade estadual para a faculdade
    - Para PCs e Macs, os endereços IP são atribuídos com DHCP
    - Os servidores DHCP rodam nos servidores de arquivos/impressão Windows NT e no servidor Web
  - As switches executam o protocolo Spanning Tree
  - As switches são gerenciáveis com SNMP e suportam RMON
    - Um sistema de gerência de rede baseado em Windows (Cisco Works, por exemplo) será usado, desde que todos os equipamentos sejam comprados da Cisco
  - O roteador age como firewall simples (filtro de pacotes)
    - O roteador não executa protocolo de roteamento
- Com a topologia escolhida, a capacidade dos enlaces foi examinada para escolher a tecnologia de camada 2
  - O resultado (a topologia física) segue abaixo



- Vários switches foram examinados e escolheram-se switches de 24 e 48 portas
- Ainda sobre o projeto físico, as seguintes decisões foram tomadas:
  - Prédios serão conectados com Ethernet 100BaseFX, Full Duplex
    - Permite enlaces de até 2000 metros
    - 10BaseFL seria suficiente em termos de banda passante mas tem mais suporte a 100BaseFX nos switches do mercado e a banda passante permite crescer no futuro
  - Dentro dos prédios, switches Ethernet de 10 Mbps são usados
    - Com exceção dos 15 PCs nos andares 1-3 da biblioteca que usarão hubs de 10 Mbps já existentes
  - Todos os switches podem ser expandidos no futuro para terem um módulo de roteamento e implementar VLANs
    - Permitindo segmentar os domínios de broadcast no futuro quando tiver aplicações multimídia
  - Todos os switches suportam multicast IP (com IGMP) facilitando o suporte às futuras aplicações multimídia
  - O enlace WAN passa a ser uma LPCD E1 (1 Mbps)
    - A segunda conexão à Internet na Matemática será desligada
  - O roteador no Centro de Computação será substituído para suportar 2 portas 100BaseTX e uma porta E1
    - Uma fonte de alimentação redundante será adicionada ao roteador, já que ele é um ponto único de falha
    - (Em tempo: no dia que escrevi essas linhas, a fonte de alimentação do equipamento que conecta a UFPb à Internet tinha acabado de pifar!)
  - O cabeamento do campus usará uma topologia centralizada (em estrela)
    - Fibra ótica será puxada entre os prédios
    - Fibra multimodo padrão de 30 "strands" com núcleo de 62,5 microns com proteção plástica para uso interno/externo
    - O cabeamento aparece na figura abaixo



Seleção de Tecnologias e Dispositivos para Redes Corporativas

- Veremos os seguintes tópicos relacionados ao projeto de redes corporativas:
  - Tecnologias para o Acesso Remoto
    - O protocolo Point-to-Point
    - Acesso remoto com Digital Subscriber Line (xDSL)
  - Seleção de dispositivos para o acesso remoto
  - Tecnologias WAN
    - Sistemas para a alocação de banda passante
    - Linhas Privadas de Comunicação de Dados (LPCDs)
    - Redes ATM
  - Seleção de dispositivos e provedores para a WAN
    - Seleção de roteadores WAN
    - Seleção de switches WAN
    - Seleção do provedor de serviços WAN
  - Exemplo de um projeto de rede WAN

Tecnologias de acesso remoto

- Tecnologias usadas para permitir o acesso à rede corporativa por usuários remotos e usuário móveis
- O projeto do acesso remoto se baseia principalmente na localização de comunidades de usuários e as aplicações que usam
- Se o acesso for durante menos de 2 horas por dia e altas velocidades não forem necessárias, podem-se usar um modem analógico (max 56 Kbps) e acesso discado
- Para velocidades mais altas ou períodos mais longos, as alternativas são
  - ISDN (não usado devido a melhores velocidades de xDSL)
  - Cable modems (ainda raros no Brasil)
  - Modems para Digital Subscriber Line (DSL)
- Em praticamente todos os caso, o protocolo de enlace usado é PPP

Point-to-Point Protocol (PPP)

- Protocolo de enlace para ligações seriais ponto-a-ponto
- É o protocolo mais usado para ligações seriais remotas
- PPP pode conectar à sede:
  - Um usuário remoto
  - Um escritório remoto com vários usuários
- PPP aceita vários protocolos de camada de rede, incluindo IP
- Serviços básicos do PPP:
  - Multiplexação de protocolos de camada de rede
  - Configuração do enlace
  - Teste da qualidade do enlace
  - Negociação de opções de enlace
  - Autenticação
    - Usando Password Authentication Protocol (PAP) ou Challenge Handshake Authentication Protocol (CHAP)
      - CHAP é melhor: use se puder (mais seguro, já que PAP manda a senha como clear text)
  - Compressão de cabeçalho

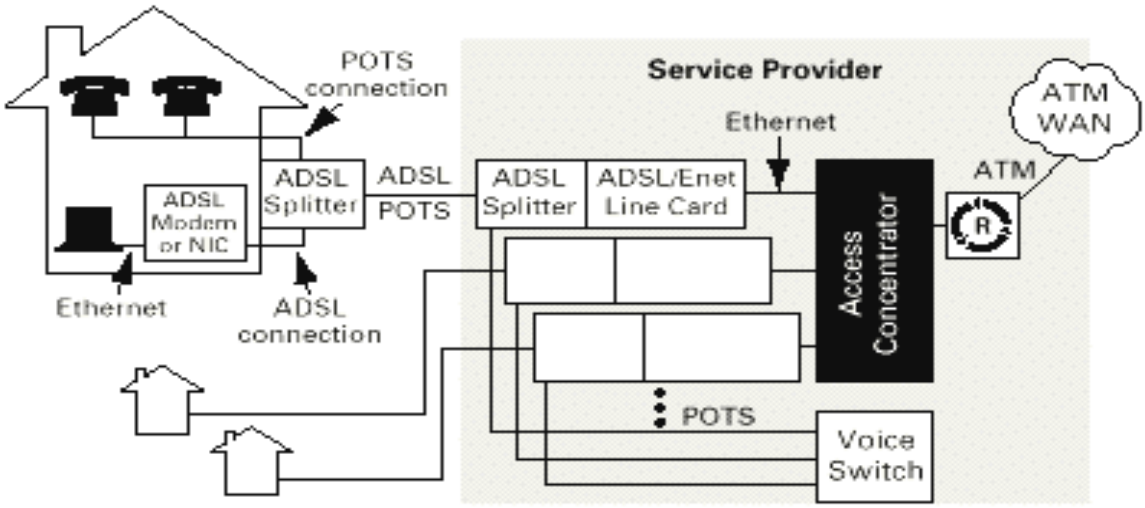
- Detecção de erro

Acesso remoto com Digital Subscriber Line (xDSL)

- Permite tráfego de alta capacidade usando o cabo telefônico normal entre sua casa (ou escritório) e a central telefônica
  - Necessidade de um modem especial de cada lado
  - Transmissão digital (sem CODEC de 64Kbps usados para voz)
- Velocidades dependem da tecnologia DSL particular, da distância e bitola do cabo, etc.
  - Podem atingir 32 Mbps (uns 2 Mbps no Brasil?) recebendo e entre 16 Kbps e 1,5 Mbps no envio
- DSL é chamado xDSL porque tem várias tecnologias embutidas na sigla:
  - 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)
  - Consumer DSL (CDSL)
- As tecnologias mais usadas são ADSL e VDSL

Asymmetric Digital Subscriber Line (ADSL)

- Capacidade assimétrica (recebe mais do que envia)
  - As velocidades dependem da qualidade da linha, distância, etc.
  - Até 18.000 pés
- ADSL tem vários canais, incluindo canais normais para telefone
  - Tudo operando simultaneamente no mesmo cabo



ADSL

High-Bit-Rate Digital Subscriber Line (HDSL)

- Capacidade simétrica: 2 Mbps usando 3 pares
- Alternativa barata a um enlace E1
- Até 12.000 pés

Seleção de dispositivos para o acesso remoto

- O site central que recebe as chamadas remotas incluir Remote Access Servers
- Um RAS oferece 5 tipos de serviços
  - Acceso remoto para estações
    - Permite que estações remotas se conectem ao site central usando PPP, SLIP, Xremote (para terminais X), AppleTalk Remote Access (ARA) ou NetWare IPXWAN
  - Acesso remoto para terminais
    - Provê serviços de terminais tais como telnet, rlogin (Unix), Local Area Transport (LAT) para DEC, X.25 PAD para acesso a redes públicas e TN3270 (teminal IBM)
  - Serviços de tradução de protocolo
    - Para que terminais acessem um host remoto que espera um terminal de tipo diferente
  - Serviços de roteamento assíncrono
    - Provê roteamento (camada 3) para interconectar LANs usando um enlace assíncrono (ex. para uma filial que disca 2 vezes por dia)
  - Serviço de dial-out
    - Controla uma bateria de modems usados por estações que acessam enlaces assíncronos para fora (evitando que cada estação tenha um modem)

- Critérios para a seleção de um servidor RAS
    - Número de portas e tipo de portas
    - Suporte para os 5 serviços acima
    - Flexibilidade de configuração e modularidade
        - Suporte a modems ISDN, portas de voz, cable modems, modems DSL, ...
    - Suporte a Network Address Translation (NAT) para hosts em redes remotas
    - Suporte a DHCP para hosts em redes remotas
    - Suporte a aplicações multimídia (multicast IP, RSVP)

Tecnologias WAN

- Para conexões à distância
- Não cobrimos tecnologias wireless aqui, mas elas são importantes
    - Satélite, por exemplo
        - Serviço Datasat e Datasat Plus da Embratel
    - Rádio
    - Celular
    - etc.
- Tem havido muita mudança nos últimos anos no oferecimento de tecnologias para acesso WAN devido a novas demandas de QoS
- No Brasil, há menos alternativas:
    - LPCDs
    - Frame Relay
    - ATM

Sistemas para a alocação de banda passante

- A hierarquia disponível no Brasil é o "Sistema E":
    - Nem todas as velocidades podem estar disponíveis num determinado provedor

Sinal	Capacidade	Número de E1s
E0	64 Kbps	
E1	2.048 Mbps	1
E2	8.448 Mbps	3
E3	34.368 Mbps	16
E4	139.264 Mbps	64

- Para fibras óticas, usa-se a Synchronous Digital Hierarchy

Nível SDH	Nível OC	Capacidade
	OC-1	51,84 Mbps
STM-1	OC-3	155,52 Mbps
STM-3	OC-9	466,56 Mbps
STM-4	OC-12	622,08 Mbps
STM-6	OC-18	933,12 Mbps
STM-8	OC-24	1.244,16 Mbps
STM-12	OC-36	1.866,24 Mbps
STM-16	OC-48	2.488,32 Mbps
STM-32	OC-96	4.976,64 Mbps
STM-64	OC-192	9.953,28 Mbps

Linhas Privadas de Comunicação de Dados (LPCDs)

- Circuito dedicado alugado de um provedor por muito tempo (meses, anos)
- Enlace dedicado para o tráfego do cliente
- Uso de topologia ponto-a-ponto
- Empresas usam LPCDs para dados e também para voz
    - Um canal de voz = 64 Kbps
- Protocolo de enlace é frequentemente PPP ou HDLC
- Vantagens:
    - Tecnologia madura e estável
    - Não há compartilhamento de tráfego com outros clientes (QoS garantido)
- Desvantagens
    - Alto custo
    - QoS não flexível
    - Capacidades limitadas

Redes ATM

- Boa escolha para clientes que têm aceleração de demanda de banda passante
- Boa escolha para aplicações com requisitos fortes de QoS

- Altas capacidades
    - Com cabos metálicos de cobre, chega a 34 Mbps
    - Com fibra ótica, pode chegar a OC-192 (9.952 Gbps), com uso de WDM
- Mais barato que LPCDs

Seleção de dispositivos e provedores para a WAN

- Backbone WAN usa roteadores e switches de alto desempenho
- Veremos critérios de seleção para tais equipamentos

Seleção de roteadores WAN

- A seleção do roteador é semelhante à seleção de um roteador de rede de campus, mas com atenção particular a:
    - Alta vazão
        - Lembre a velha regra 80/20 que virou 20/80, gerando muito tráfego no backbone
    - Alta disponibilidade
    - Features avançados para otimizar o uso de enlaces WAN (que são caros)
        - Ver esses features no capítulo sobre Otimização da Rede
- Escolher o roteador com a portas desejadas (com as tecnologias desejadas) e uma vazão (PPS) adequada

Seleção de switches WAN

- Switches revolucionaram o projeto de redes de campus nos anos 90
- Estão mudando a forma de construir backbones corporativos
- Uso de switches que dão suporte a ATM, Frame Relay, Acesso Remoto, suporte a voz (com Voice Activity Detection, voice compression, ...)
- Esses switches podem também fazer alocação dinâmica de banda passante para vários serviços (dados, voz, ...)
- São uma boa alternativa para fundir redes de dados e de voz numa única rede corporativa

Seleção do provedor de serviços WAN

- Critérios de seleção
    - Custo dos serviços
    - Tipos de serviços oferecidos
        - Ex. outsourcing da gerência da WAN
        - Ex. Suporte a Virtual Private Network
    - Tipos de tecnologias oferecidas
    - Área geográfica cobreta
    - Contratos Service Level Agreements (SLA) oferecidos
        - Ex: SLA da Embratel oferece disponibilidade de 99,7% para LPCDs
    - O nível de segurança oferecido
    - O nível de suporte técnico oferecido (pode fazer parte do SLA). Em particular, descubra:
        - A experiência da equipe de suporte
        - Disponibilidade de um ponto único de contato com o suporte para todos os problemas
        - Certificação ISO 9002
    - Confiabilidade e desempenho da rede interna do provedor. Embora isso seja difícil de descobrir, às vezes, fale com os engenheiros do provedor sobre:
        - Roteamento físico dos enlaces
        - Redundância da rede
        - O nível de "Oversubscription" na rede (satélite, ATM)
        - Mecanismos de alocação de banda passante para garantir QoS
        - Frequência e duração típica de quedas na rede
        - Métodos de segurança utilizados para proteger a rede

Exemplo de um projeto de rede WAN

- Exemplo real de projeto
- Empresa: PUFF (Por-Um-Fio Federated)

Informação inicial

- PUFF fabrica papel e produtos de papel (caixas, papel jornal, etc.)
- PUFF tem 15 sites no Brasil
    - Sede em Belém
- 1.500 empregados
- Clientes no mundo inteiro, muitos dos quais estão na Ásia
- No final dos anos 90, PUFF viu uma redução nas suas margens de lucro devido a uma queda de vendas na Ásia e dificuldade de encontrar madeira para a fabricação dos produtos
- Bolou-se um plano de recuperação:
    - Processos internos mais eficientes
    - Uso de papel reciclado
- A execução do plano depende de um programa de educação à distância para que empregados aprendam a conservar matéria prima, utilizem melhor papel reciclado e trabalhem mais eficientemente
    - O programa de treinamento é crucial à recuperação da empresa

    - A diretoria aprovou orçamento para instalar salas de vídeo-conferência na maior parte dos sites
- Uma vez a infra-estrutura de vídeo-conferencia instalada, PUFF pretende oferecer treinamento para outras empresas do ramo, aproveitando subsídios federais para o re-treinamento de empregados

Objetivos de negócio e técnicos

- Objetivos principais de negócio:
    - Aumentar lucros através da implementação de uma WAN para apoiar o plano de recuperação, em particular com o uso de vídeo-conferencia
    - Melhorar o desempenho da WAN existente para melhorar a eficiência das operações
    - Conter os custos crescentes da operação da WAN atual
    - Prover uma rede que permita que empregados troquem idéias mais facilmente sobre melhorias de eficiência e o uso de materiais reciclados
    - Prover uma nova fonte de faturamento com o sistema de vídeo-conferencia
- O pessoal técnico acrescentou os seguintes objetivos técnicos:
    - Aumentar a capacidade e oferecimento de QoS da rede atual que não pode suportar o sistema de vídeo-conferencia
    - Projetar uma rede que utilize tecnologias disponíveis através dos provedores de serviços WAN da região
    - Prover uma rede que ofereça um tempo de resposta máximo de 100 ms para aplicações interativas
    - Disponibilidade de 99,98% com MTBF de 4000 horas e MTTR de 1 hora
    - Melhorar a gerenciabilidade da rede através de uma topologia mais simples (correntemente, há uma mesh complexa de circuitos de dados e voz)
    - Projetar uma rede com escalabilidade de banda passante para aplicações futuras
    - Projetar uma rede que possa carregar voz no futuro

Aplicações de rede

- Ensino à distância
    - Vai usar um serviço bidirecional de vídeo digital comprimido baseado nos padrões H.320 para vídeo-conferencia
    - Cada site receberá uma câmera digital e um CODEC para converter sinais analógicos para digital
    - Os fluxos de vídeo poderão ser acessados on-line ou off-line num servidor de vídeo
- Sistema de suporte à manufatura
    - Aplicação SNA terminal/host ridando no mainframe em Belém
    - Sistema permite o escalonamento e acompanhamento de ordens de manufatura
    - Usuários de vários departamentos de manufatura acessam a aplicação usando seus PCs através de gateways TCP/IP-SNA
    - O sistema é de missão crítica
- Sistema de modelagem financeira
    - Usa um BD Oracle executando em máquinas UNIX em Belém
    - Analistas usam seus PCs com TCP/IP para acessar o sistema
- Sistema de entrada e rastreamento de pedidos
    - Executa em servidores Novell NetWare
    - Usuários de vendas e marketing usam seus PCs para acessar o sistema
- Sistema de produção gráfica
    - Executa em sistemas Mac usando servidores via AppleShare
- Outras aplicações
    - Windows 98 com E-mail, agenda corporativa, navegação Web, compartilhamento de arquivos e impressoras
    - As aplicações usam TCP/IP e NetBIOS over TCP/IP (NetBT)

Comunidades de usuários

- As comunidades são como segue:

Nome da comunidade	Número de usuários na comunidade	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

Data Stores

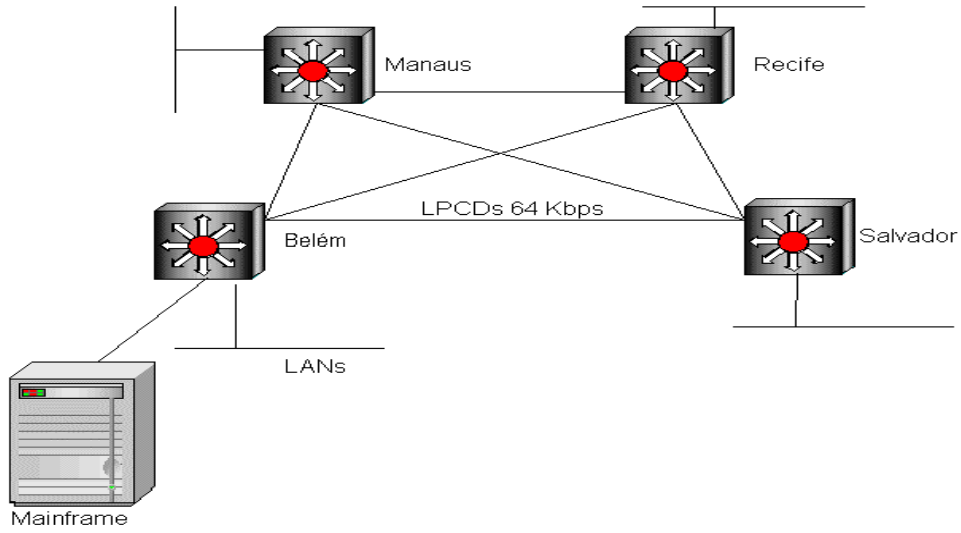
- Os data stores são como segue:

Data Store	Localização	Aplicações	Comunidades que usam
Mainframe	Belém	Sistema de Suporte à Manufatura	Todos os locais de manufatura
Servidores de arquivos UNIX	Dois em 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	Ensino à distância	Todas

A rede atual

- LPCDs de 64 Kbps conectando 15 sites usando uma mesh parcial
- Tráfego de voz é carregado por canais separados de 64 Kbps
- O mesmo provedor que aluga as LPCDs fornece acesso Internet com um canal E1 em Belém
- O roteador em Belém age como filtro de pacotes (firewall simples)
- O roteador também possui um Channel Interface Processor (CIP) para conectar ao mainframe
    - O roteador encapsula tráfego SNA em conexões TCP/IP na WAN
    - Isto é, o tráfego SNA tunela na rede WAN TCP/IP
- O core (núcleo) da rede de dados é uma full mesh de enlaces 64 Kbps
    - Um roteador em cada site liga a WAN a uma LAN Ethernet local



Características de tráfego na WAN atual

- O desempenho da rede tem piorado com o crescimento da PUFF
    - Usuários reclamam da lentidão da rede, especialmente entre 10 e 11 horas da manhã
    - Os usuários do Sistema de Manufatura reclamam que o tempo de reposta chega a 2 ou 3 minutos
    - Os usuários do sistema de entrada de pedido (NetWare) e do sistema de modelagem financeira também reclamam
- Um analizador de protocolos foi colocado na WAN em cada site importante para medir a utilização dos enlaces de 64 Kbps
    - Cada circuito em Belém está acima de 80% de utilização, numa janela de 10 minutos
    - Os outros enlaces da full mesh estão acima de 70%
    - A tabela abaixo mostra a utilização de banda passante por protocolo, no pior enlace de Belém
        - Observe que SNA e NetBIOS trafegam sobre TCP/IP mas isso foi removido do tráfego IP
        - O tráfego IP é relativo às aplicações IP "puras"

	Utilização relativa (comparada ao tráfego)	**Tráfego absoluto**	**Taxa de multicast**
IP	30%	15 Kbps	0,5 Kbps
IPX	25%	13 Kbps	0,7 Kbps
AppleTalk	8%	4 Kbps	0,7 Kbps
NetBIOS	15%	8 Kbps	0,6 Kbps
SNA	20%	10 Kbps	0,3 Kbps
Outros	2%	1 Kbps	0,4 Kbps

- Outras observações
    - Nenhum protocolo em particular está causando problemas sérios
    - Nenhuma aplicação parece estar retransmitindo rapidamente demais (indicando um valor baixo demais para o timeout de retransmissão)
    - As aplicações parecem estar usando quadros grandes e janelas grandes
    - O tráfego de broadcast é de aproximadamente 5%, o que parece normal
    - A taxa de erros é aceitável (1 erro de CRC a cada 2 Mbytes de dados)
- Verificou-se o estado dos roteadores do núcleo da rede usando os seguintes comandos dos roteadores Cisco:
    - show processes (não tem sobre-utilização de CPU)
    - show buffers (não tem problemas com falta de buffers)
    - show interfaces
        - 5% dos frames estão sendo descartados, provavelmente devido ao tráfego pesado

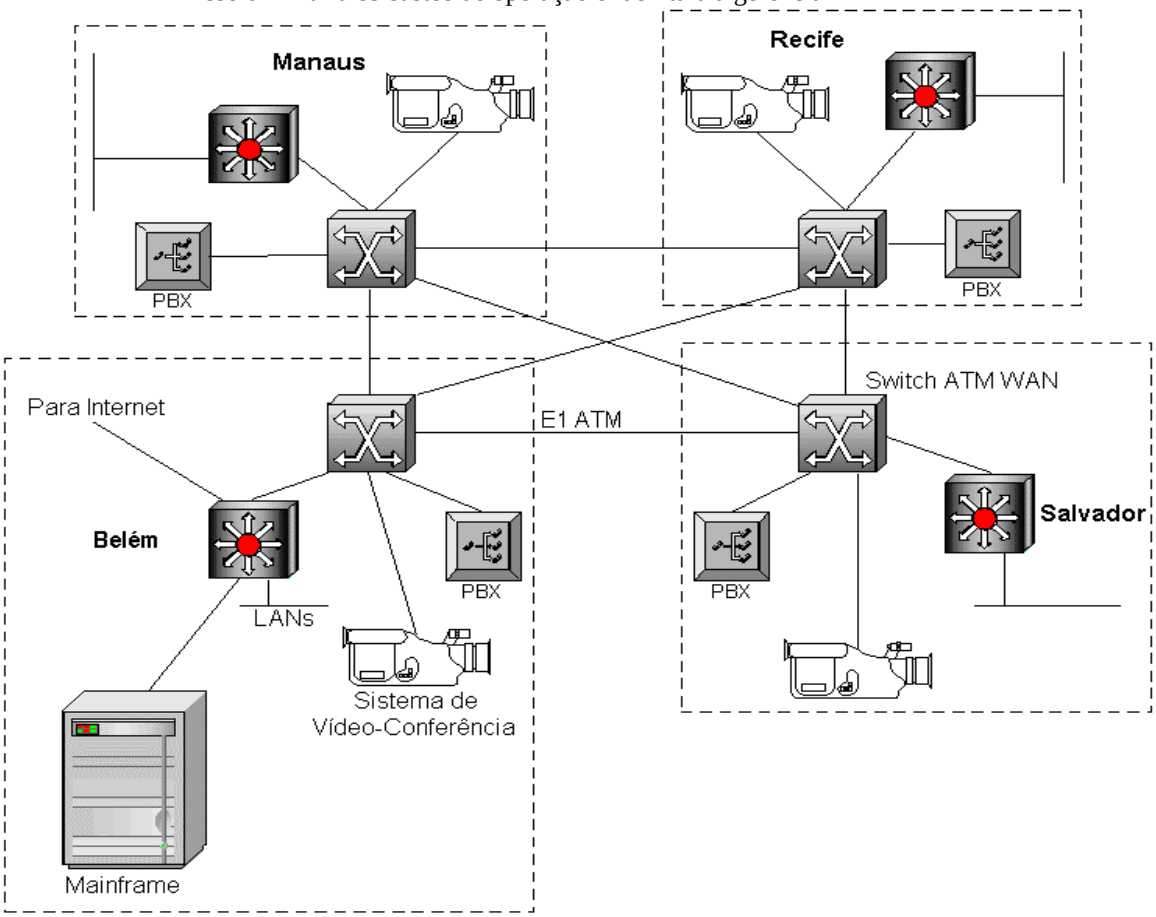
- Conclusão: não há problema com a rede, com exceção da demanda grande, mas normal, de tráfego para a capacidade instalada

O projeto da rede WAN

- A seguinte tabela de decisão foi elaborada:

	Objetivos críticos para a WAN				
	Deve ter capacidade e QoS para carregar vídeo sem afetar o tráfego SNA	**Deve usar tecnologias disponíveis através dos provedores locais**	**Tempo de resposta <= 100 ms para aplicações interativas**	Disponibilidade de 99,98% ou mais	Contenção dos custos de operação da WAN
Adicionar mais LPCDs de 64 Kbps		X	X	X	
SONET	X		X	X	
SMDS			X	X	
Frame Relay		X		X	X
ATM	X	X	X	X	X

- Resultado
  - Decidiu-se alugar enlaces E1 e rodar ATM em cima deles para obter o QoS desejado para as várias aplicações
  - O mesmo provedor foi usado já que:
    - Oferece os serviços desejados (ATM sobre E1) a um preço competitivo
    - Permite manter os endereços IP existentes
    - Tem suporte 24x7 (24 horas por dia, 7 dias por semana)
    - Garante MTTR de 1 hora
    - Tem ponto único de contato para o suporte
- Cada site se conecta à rede ATM com uma switch ATM
  - Selecionou-se um switch com suporte a E1 e a E3 (34 Mbps) para crescimento futuro
  - O switch tem duas portas de fibra a 155 Mbps (OC-3) para conectar ao roteador e qo equipamento de vídeo-conferência em cada site
  - O switch pode tratar tráfego de voz
    - No futuro as centrais PBX de cada site se conectrão ao switch e a rede de voz será posta fora de operação
    - Todos os dados e a voz transitarão na rede ATM
    - Isso diminuirá os custos de operação e facilitará a gerência



5. Testes e Documentação do Projeto de Rede

- Testes do projeto de rede
- Documentação do projeto de rede

Testes do projeto de rede

- Teste servem para provar para você mesmo e para seu cliente que o projeto da rede vai satisfazer os objetivos de negócio e técnicos
- Embora se possam usar alguns testes prontos "da indústria", é mais frequente realizar testes específicos para o projeto da rede
    - Isso envolve construir um protótipo e medir desempenho (vazão a nível de aplicação, atraso e disponibilidade)
    - Uma alternativa possível é de usar ferramentas de modelagem
- A seleção de procedimentos e ferramentas de testes depende dos objetivos dos testes
- Objetivos comuns para os testes:
    - Verificar que oprojeto satisfaz os objetivos mais importantes de negócio e técnicos
    - Validar a seleção de tecnologias e de dispositivos de LAN e de WAN
    - Verificar que o provedor de serviço ofereça, de fato, os serviços prometidos
    - Identificar problemas de conectividade ou de gargalos
    - Testar a redundância da rede
    - Analisar os efeitos de quedas de enlaces no desempenho
    - Determinar técnicas de otimização (multicast, RSVP, ...) que serão necessárias para satisfazer objetivos de desempenho
    - Analisar os efeitos de atualizações (upgrades) de enlaces e/ou dispositivos no desempenho (análise "what-if")
    - Provar que seu projeto é melhor do que um projeto concorrente (quando o cliente pedir tal comparação)
    - Para passar um "teste de aceitação" que permite continuar com o projeto e implantar a rede
    - Convencer a gerência e seus colegas que o projeto é eficaz
    - Identificar riscos que podem dificultar a implementação e fazer o planejamento de contingências
    - Determinar quantos testes adicionais são necessários (ex. pode-se decidir continuar o projeto apenas como piloto para investigar mais)

Testes da indústria

- Testes comarativos são executados e publicados por fabricantes, laboratórios independentes e revistas especializadas
    - Network Device Testing Laboratory (Harvard University)
    - Strategic Network Consulting, INC. (SNCI) - www.snci.com
    - Interoperability Lab (IOL) da University of New Hampshire - www.iol.unh.edu
- Normalmente testam dispositivos
- Os resultados só podem ser usados para o convencimento de que o projeto da rede está ok para redes muito simples, consistindo de uma topologia essencialmente igual à dos testes publicados
    - Para redes mais complexas, você deverá elaborar seus próprios testes
    - Motivo: deve-se fazer testes de sistema e não apenas testes de componentes

Construção e teste de um protótipo para a rede

- Listamos as tarefas necessárias à construção e testes de um protótipo que verifique e demonstre o comportamento de uma rede
- Um protótipo é uma implementação inicial de um novo sistema que modela como a rede final será implementada
- O protótipo deve ser funcional mas não precisa ser uma implamentação completa da rede

Determinação do escopo do protótipo

- Quanto da rede deve ser implementado para convencer o cliente de que o projeto está ok (satisfaz os requisitos)?
- Isole os aspectos que são mais importantes
    - Funções importantes
    - Funções que envolvem risco
        - Onde o projeto foi muito influenciado por restrições do negócio ou técnicas
        - Onde o projeto foi muito influenciado pelos tradeoffs entre objetivos
    - Funções que foram alvo de rejeição em projetos anteriores
        - Ex.: o cliente já recusou um projeto no passado devido à sua fraca gerenciabilidade e fraca usabilidade
- Os recursos disponíveis (gente, equipamento, dinheiro, tempo) vão também ditar o alcance do protótipo
- Um protótipo pode ser implementado e testado de três formas diferentes
    - Como rede de testes num laboratório
    - Integrado a uma rede de produção mas com realização de testes fora do horário comercial
    - Integrado a uma rede de produção e com realização de testes no horário comercial normal
- É interessante implementar uma rede de testes em laboratório antes de implementá-la na rede de produção
    - Para acertar bugs

        - Para avaliar produtos nunca usados antes
        - Para acertar a configuração inicial de dispositivos
- O teste final deve ser em produção, durante o horároi comercial normal
- Cuidado com o seguinte ao fazer testes num ambiente de produção:
    - Avise os usuários com antecedência sobre os horários de testes para que eles estejam esperando problemas de desempenho, mas peça que eles trabalhem normalmente para não invalidar os testes devido a um comportamento anormal dos usuários
    - Avise os administradores da rede com antecedência para que eles também não estejam executando testes ao mesmo tempo!
    - Avise os operadores da rede com antecedência para que eles estejam esperando alarmes inesperados na console de gerência e outro comportamento estranho
    - Se possível, execute vários testes pequenos (até 2 minutos) para minimizar o impacto nos usuários
    - Execute testes leves primeiro e aumente a carga do teste aos poucos, e somente se testes anteriores estiverem ok. Não passe para carga máxima "de cara"
    - Monitore os resultados dos testes e pare assim que:
        - Os objetivos dos testes foram alcançados; ou
        - Os testes estão impactando a rede em demasia

Escrevendo um plano de testes para o protótipo

- Uma vez que o escopo do protótipo está decidido, um plano de testes é escrito, contendo:
    - Objetivos dos testes e critérios de aceitação
    - Tipos de testes que serão executados
    - Equipamento de rede e outros recursos necessários
    - Scripts de teste
    - Cronograma do projeto de testes
- Elaboramos sobre esses pontos abaixo

Elaboração de objetivos de testes e critérios de aceitação

- Listar os objetivos dos testes é o passo mais importante
    - Os objetivos devem ser específicos e concretos
    - Deve-se incluir critéios de aceitação
- Exemplos de objetivos e critérios de aceitação:
    - "Medir o tempo de resposta para a aplicação Xpto durante horário de pico (entre 10:00 e 11:00 da manhã). Critério de aceitação: tempo de resposta <= 500 ms"
    - "Medir a vazão da aplicação Xpto durante horário de pico (entre 10:00 e 11:00 da manhã). Critério de aceitação: vazão >= 2 Mbps"
    - "Medir o tempo para que um usuário do sistema de Voz Sobre IP (VoIP) ouça o tom de discar após tirar o fone do gancho. Critério de aceitação: O tempo deve ser menor ou igual ao tempo oferecido pelo sistema PBX normal"
- Os critérios de aceitação são baseados nos objetivos de negócio e técnicos já levantados para o projeto da rede
- O mais importante é que o próprio cliente e o testador concordem sobre o significado dos critérios de aceitação para que não haja dúvida sobre se cada teste passou ou não
- Os critérios de aceitaão podem ser baseados num baseline de desempenho da rede atual
    - Exemplo: diminuir o tráfego de broadcast em 50%

Determinação dos tipos de testes a realizar

- Há três tipos básicos de testes:
    - Testes de desempenho
        - Caracterização da vazão, atraso, variação no atraso, tempo de resposta e eficiência
    - Testes de estresse
        - Degradação do serviço com aumento de carga
    - Testes de falhas
        - Caracterização da disponibilidade e acurácia da rede
- Embora seja mais raro, outros testes especiais podem ser feitos para gerenciabilidade, usabilidade, adaptabilidade e segurança
- Testes típicos
    - Tempo de resposta de aplicações
        - Medir o tempo para operações típicas realizadas pelo usuário (iniciar a aplicação, abrir arquivo, salvar arquivo, pesquisar, ...)
        - Pode usar um simulador ou examinar usuários reais trabalhando
    - Testes de vazão
        - Vazão para uma aplicação particular ou para um grupo de aplicações
        - Medido em KBytes/seg ou MBytes/seg
    - Testes de disponibilidade
        - Monitoram-se os erros e as falhas durante vários dias

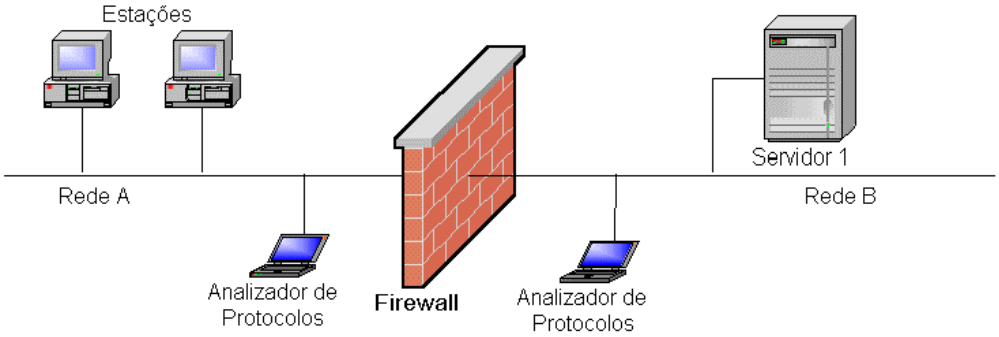
- Testes de regressão
    - Verificação de que as aplicações que executavam corretamente na rede antiga continuam rodando na nova rede

Documentação dos equipamentos de rede e outros recursos

- Listar tudo que é necessário para fazer os testes
    - Mapa de rede
    - Lista de dispositivos
    - Outros equipamentos (cabos, etc.)
    - Enlaces
    - Ferramentas (de monitoração, de injeção de tráfego, de simulação, ...)
    - Aplicações especiais que aumentam a eficiência dos testes (aplicação de distribuição de software, aplicação de controle remoto como PCAnywhere, ...)
    - Outros recursos
        - Tempo blocado num laboratório especial
        - Ajuda de colegas
        - Ajuda de usuários
        - Nomes ou endereços IP durante os testes

Escrita de scripts de testes

- Para cada teste, escreva uma script de teste, listando todas as etapas para a execução do teste
- O script deve também identificar:
    - As ferramentas usadas
    - Como cada ferramenta é usada para fazer as medições relevantes
    - Que informação deve ser logada surante cada teste
    - Valores iniciais para parâmetros dos testes e como alterar esses parâmetros ao longo do teste (exemplo: carga ofeecida)
- Exemplo de um script de teste segue para a configuração abaixo



    - Objetivos dos testes: Avaliar a capacidade do firewall bloquear tráfego da aplicação Xpto durante condições de tráfego leve e moderadamente pesado
    - Critério de aceitação: O firewall deve bloquear o pedido TCP SYN e qualquer estação na rede A que tentar abrir uma sessão com a aplicação Xpto no Servidor 1 na rede B. O firewall deve devolver um reset TCP (RST). Observe que SYN significa "abertura de conexão e suncronização de números de sequência".
    - Etapas de teste:
        1. Iniciar a captura de tráfego no analizador de protocolos na rede A
        2. Iniciar a captura de tráfego no analizador de protocolos na rede B
        3. Executar a aplicação Xpto numa estação localizada na rede A para acessar o servidor 1 na rede B
        4. Parar a captura de tráfego nos analizadores de protocolos
        5. Exibir dados no analizador de protocolos da rede A para verificar que o analizador capturou um pacote TCP SYN proveniente da estação. Verificar que o destino do pacote é o Servidor 1 na rede B e que a porta destino é 1234 (a porta da aplicação Xpto). Verificar que o firewall respondeu à estação com um pacote TCP RST
        6. Exibir dados no analizador de protocolos da rede A para verificar que o analizador não capturou qualquer tráfego para a aplicação Xpto
        7. Logar os resultados do teste no arquivo de log do projeto
        8. Salvar os arquivos de rastreamento dos analizadores de protocolos no diretório de arquivos de rastreamento
        9. Gradualmente aumentar a carga no firewall, aumentando o número de estações na rede A, 1 de cada vez, até chegar a 50 estações tentando abrir conexão com a aplicação Xpto no Servidor 1. Repetir as etapas 1 a 8 ao adicionar cada estação

Cronograma de testes

- Para um projeto complexo de testes (demorando mais do que 1 semana), elaborar um cronograma evidenciando data inicial, data final e milestones principais
    - Incluir responsável por cada tarefa principal
- Tarefas típicas são:

- Escrever os objetivos dos testes e critérios de aceitação
- Projetar a topologia para o ambiente de testes
- Determinar o hardware e software necessários para os testes
- Emitir o pedido de compra para o hardware e software, se necessário
- Escolher as ferramentas de testes
- Emitir o pedido de compra para as ferramentas de testes, se necessário
- Determinar outros recursos que serão necessários e providenciá-los
- Escrever scripts de testes
- Instalar e configurar o hardware e o software
- Iinciar testes
- Logar resultados dos testes
- Revisar e analizar resultados
- Reduzir os dados de resultados, se necessário
- Apresentar resultados ao cliente
- Arquivar os resultados

Implementação do plano de testes

- É basicamente uma questão de seguir o plano

Ferramentas para testar uma rede

- Há três tipos de ferramentas que ajudam a realizar testes
- Ferramenta de gerência e monitoração de rede
    - Cisco Works, HP OpenView
    - Pode obter informações variadas sobre tráfego, erros, etc.
    - Na sua ausência, pode-se usar comandos que dão informação equivalente nos roteadores
        - show interfaces, show processes, show buffers, ...
    - Outra alternativa: analizadores de protocolos
        - Bom para analizar comportamento de tráfego, erros, utilização, eficiência, taxas de broadcast e multicast, etc.
        - Ajuda a gerar tráfego artificial durante os testes
- Ferramentas especiais de testes e simulação
    - Simulação pode ser menos caro do que testar uma rede de verdade
    - De forma geral, é muito difícil fazer uma boa simulação que esteja perto do mundo real
- Ferramentas de gerência de nível de serviço
    - Ferramentas novas que analizam o desempenho fim-a-fim de aplicações, incluindo requisitos de QoS
    - Exemplo: NetPredictor de NetPredict

Um exemplo de um cenário de testes

- Exemplo abaixo é um estudo de caso real

Informação inicial

- Empresa:Umqua Systemas projeta e fabrica circuitos integrados especiais para aparelhos eletrônicos
- O projeto se foca numa rede de campus com 4 prédios, 3 deles próximos e 1 a uma distância de 5 km
- 400 empregados (engenharia, vendas, marketing, finanças)

Objetivos dos testes

- Dois objetivos principais para os testes
    - Determinar a carga e desempenho da rede atual, com foco especial no backbone FDDI
    - Determinar o que acontecerá com o desempenho da rede se 10 a 20 pessoas executarem uma nova aplicação de entrada de pedido usando tecnologia Oracle
- Hoje, a empresa usa OpenView para gerar alarmes mas não para observar o desempenho da rede

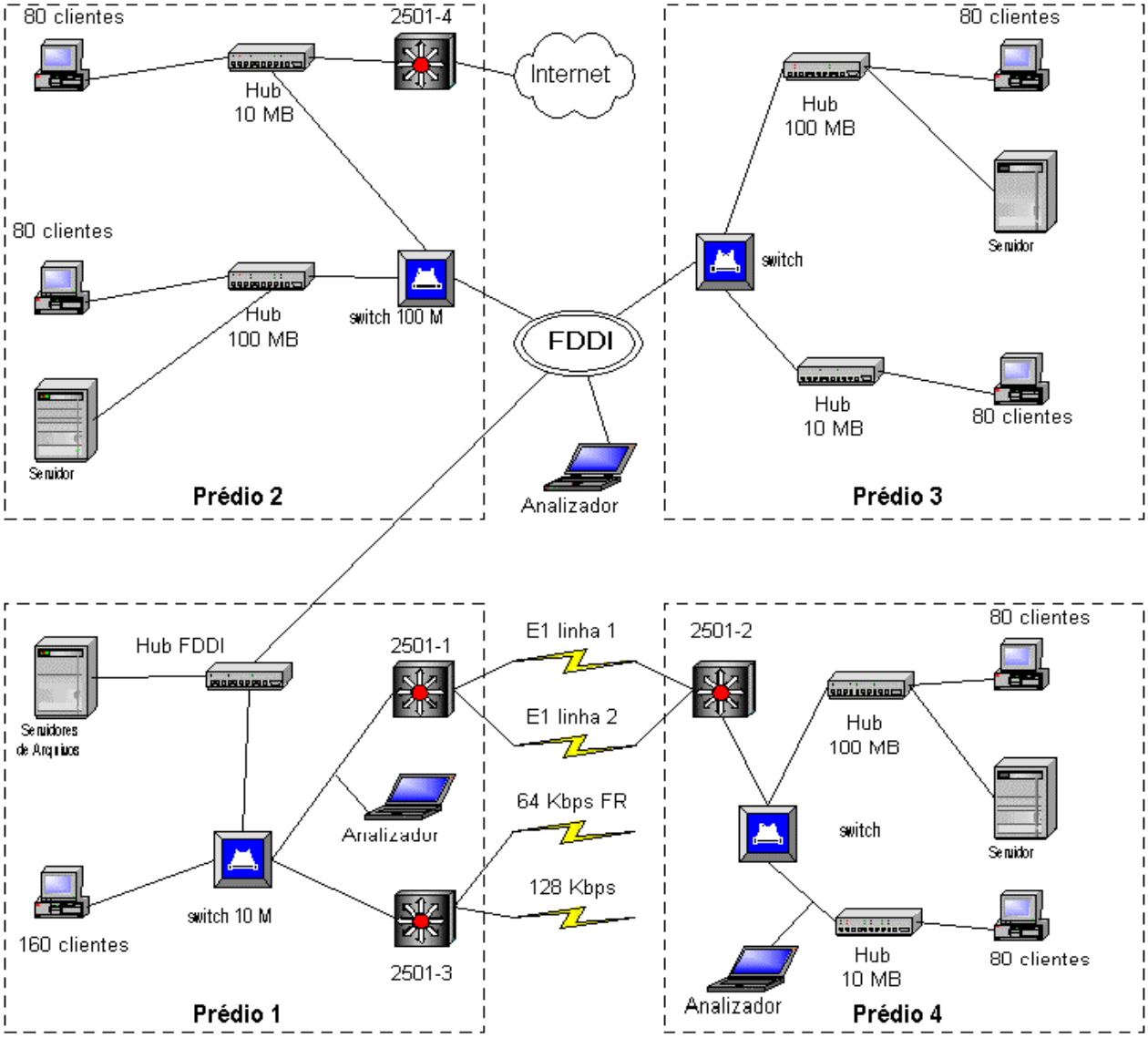
Aplicações de rede

- Aplicações típicas de escritório (mail, compartihamento de arquivos e impressoras)
- Computer-Aided Design (CAD) para projetar circuitos integrados
    - Os engenheiros têm dois computadores na mesa: PC com Windows 98 para trabalho de escritório e Workstation Sun para a aplicação CAD
- Características especiais da aplicação CAD
    - Edições pequenas são feitas diretamente no arquivo original (no servidor)
    - Para edições grandes, o arquivo é trazido para a estação local e editado localmente
    - À noite, um programa de sincronização de arquivos verifica as datas dos arqiuvos nas várias estações e consolida tudo no servidor central
    - Os arquivos variam de 1 a 20 MBytes

A rede atual

- Backbone FDDI conectando os prédios 1 a 3
- Prédio 4 conectado ao backbone com 2 enlaces paralelos E1 de 2 Mbps, com fibra ótica
- Um enlace E1 adicional com subcanais é usado como segue:
    - Canal de 64 Kbps com Frame Relay para acessar filais domésticas

- Canal de 128 Kbps para acessar filiais na Europa
- Acesso Internet 64 Kbps a partir do prédio 2
- Estações Sun se conectam a segmentos 100BaseTX
- PCs se conectam a segmentos 10BaseT
- Servidores se conectam diretamente no backbone FDDI



Métodos de testes usados

- Um plano de testes foi escrito, com objetivos específicos de medir o desempenho atual e predizer o desempenho futuro da rede com a nova aplicação
  - Ferramenta básica: NetPredictor para fazer análise "what-if"
- Um modelo de carga de tráfego (para NetPredictor) foi obtido através de conversas com os gerentes de rede na empresa
  - O modelo foi calibrado através de medições de desempenho obtidas na rede real
    - Ver localização dos analizadores de protocolos na figura acima
    - Dados foram obtidos com médias a cada minuto, durante 24 horas
  - O modelo calibrado aparece na tabela abaixo

Modelo de distribuição de carga na empresa Umqua Systems (Números em azul foram computados pela ferramenta)			
Prédio 2			
Número de máquinas clientes	160		
Tamanho médio de arquivo acessado	20	Mbytes	
Atividade média por pessoa	40	Mbytes/hora	
Carga total iniciada no prédio	6.400	Mbytes/hora	
Carga em segmento 10 Mbps e em segmento 100 Mbps	10%	90%	
Carga local saindo do prédio	67%		
Carga local na LAN 10 Mbps	640	Mbytes/hora	
Carga local na LAN 100 Mbps	5.760	Mbytes/hora	
Tráfego de outros prédios	3.008	Mbytes/hora	

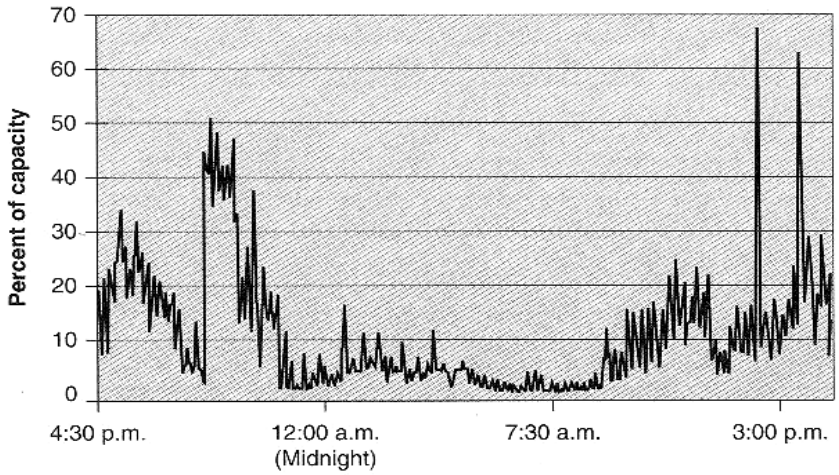
Tráfego do prédio 1	80%	3.430,4	Mbytes/hora
Tráfego do prédio 3	20%	857,6	Mbytes/hora
Tráfego do prédio 4	0%	0	Mbytes/hora
Utilização da LAN 10 Mbps	20,9%		
Utilização da LAN 100 Mbps	18,8%		
Prédio 1			
Número de máquinas clientes	160		
Tamanho médio de arquivo acessado	17	Mbytes	
Atividade média por pessoa	34	Mbytes/hora	
Carga total iniciada no prédio	5.440	Mbytes/hora	
Carga em segmento 10 Mbps e em segmento 100 Mbps	10%	90%	
Carga local saindo do prédio	65%		
Carga local na LAN 10 Mbps	544	Mbytes/hora	
Carga local na LAN 100 Mbps	4.896	Mbytes/hora	
Tráfego de outros prédios	3.540	Mbytes/hora	
Tráfego do prédio 2	80%	2.828,8	Mbytes/hora
Tráfego do prédio 3	20%	707,2	Mbytes/hora
Tráfego do prédio 4	0%	0	Mbytes/hora
Utilização da LAN 10 Mbps	20,0%		
Utilização da LAN 100 Mbps	18,0%		
Prédio 3			
Número de máquinas clientes	160		
Tamanho médio de arquivo acessado	1	Mbytes	
Atividade média por pessoa	2	Mbytes/hora	
Carga total iniciada no prédio	320	Mbytes/hora	
Carga local saindo do prédio	80%		
Carga local na LAN 10 Mbps	320	Mbytes/hora	
Tráfego de outros prédios	1,570	Mbytes/hora	
Tráfego do prédio 1	60%	153,6	Mbytes/hora
Tráfego do prédio 2	35%	89,6	Mbytes/hora
Tráfego do prédio 4	5%	12,8	Mbytes/hora
Suponha 2 LANs de 10 Mbps:			
Utilização em cada LAN 10 Mbps	21,0%		
Prédio 4			
Número de máquinas clientes	160		
Tamanho médio de arquivo acessado	2	Mbytes	
Atividade média por pessoa	4	Mbytes/hora	
Carga total iniciada no prédio	640	Mbytes/hora	
Carga em segmento 10 Mbps e em segmento 100 Mbps	15%	85%	
Carga local saindo do prédio	8%		
Carga local na LAN 10 Mbps	88,32	Mbytes/hora	
Carga local na LAN 100 Mbps	500,48	Mbytes/hora	
Tráfego de outros prédios	13	Mbytes/hora	
Tráfego do prédio 1	50%	25,6	Mbytes/hora
Tráfego do prédio 2	40%	20,48	Mbytes/hora
Tráfego do prédio 3	10%	5,12	Mbytes/hora
	Do modelo	Medido	
Utilização da LAN 10 Mbps	2,0%	2,0%	
Utilização da LAN 100 Mbps	1,1%		
Utilização do backbone FDDI 100 Mbps	18%	18%	
Utilização das linhas E1	4,6%	4,32%	

Dados medidos

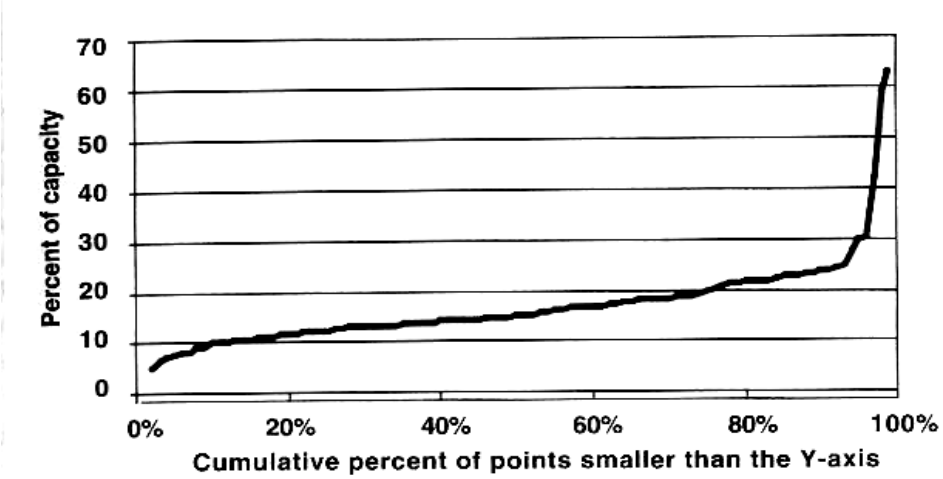
- Apresentam-se dados colhidos com os analizadores de protocolos e algumas conclusões decorrentes da análise dos dados

Carga no backbone FDDI

- A figura abaixo mostra a carga no backbone FDDI durante aproximadamente 24 horas
  - À noite, temos utlização de uns 2%
  - Maior carga perto do fim do dia



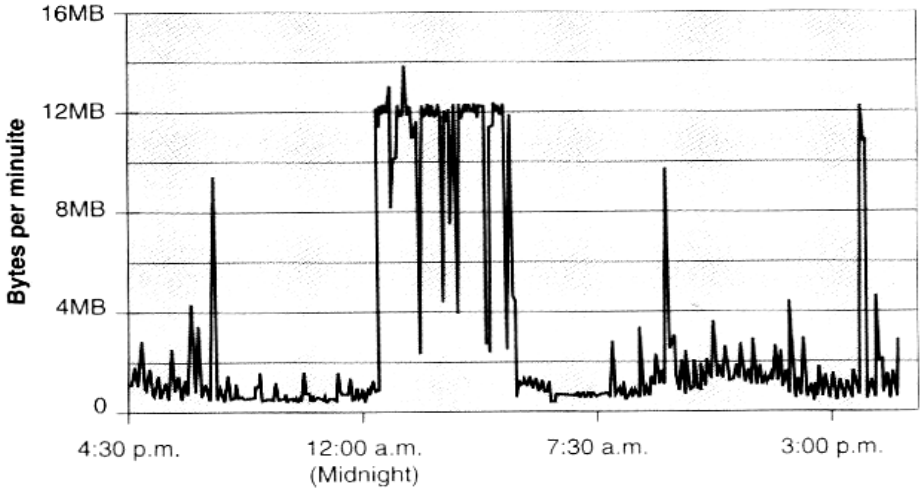
- A curva abaixo mostra uma função cumulativa de probabilidade da carga (um histograma cumulativo dos pontos da figura anterior), mostrando que:
  - A carga média é de 15%
  - Aproximadamente 5% dos pontos indicam carga maoir que 25%
  - Curva boa para diferenciar a carga média da carga de pico



- Conclusão: não há problemas de sobrecarga
  - Já sabíamos disso pois os usuários não estavam reclamando

Carga nas LPCDs

- A figura abaixo mostra que a carga nos enlaces é pequeno, com exceção do período da noite durante a sincronização de arquivos, que dura umas 4 horas
- Durante o dia, a utilização está abaixo de 10% 90% do tempo
  - Sem problemas, portanto



Análise do novo sistema de entrada de pedidos

- Obteve-se uma análise de tráfego usando um analizador de protocolos de uma sessão de um único usuário para modelar o tráfego

- Resultados:
  - A entrada de um único pedido causa um tráfego de uns 2 Mbytes
    - 220 KBytes de tráfego TCP/IP entre o usuário e o BD Oracle no prédio 1
    - 1,7 Mbytes de tráfego NetWare entre o usuário e o servidor de arquivo NetWare no prédio 1 (tráfego para carregar a aplicação e os formulários virgens de entrada de pedido)
  - O trabalho foi completado em 3 minutos com carga média de 90 Kbps
  - Para uso contínuo (aplicação já carregada), estima-se que a carga média será de 40 Kbps
  - Para 10 usuários, a carga seria de 400 Kbps
    - Isso não vai sobrecarregar as LANs
    - Os enlaces E1 terão utilização aumentada de 4,3% para uns 17%

Conclusões

- A rede aguenta o novo tráfego sem problemas
- É até possível considerar alternativas mais baratas para os enlaces E1 que estão sub-utilizados

Documentação do projeto de rede

- Você poderá estar preparando um projeto de rede
  - Para responder a um Request For Proposal (RFP), ou Carta Consulta, Licitação, etc.
  - Sem RFP, como parte de suas atribuições na empresa
- Há uma forma ligeiramente diferente de lidar com essas duas situações
- Em ambos os casos, deve-se preparar um documento de projeto que:
  - Descreve os requisitos do cliente
  - Explica como seu projeto os atende
  - Documenta a rede atual
  - Detalha o projeto lógico e físico
  - Informa custos previstos

Respondendo a um RFP

- Um RFP lista os requisitos básicos do projeto e tem a seguinte estrutura comum:
  - Objetivos de negócio para a rede
  - Escopo do projeto
  - Informação sobre a rede e as aplicações existentes
  - Informação sobre as 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
  - Requisitos de treinamento e suporte
  - Cronograma inicial com milestones e artefatos a entregar (deliverables)
  - Termos e condições contratuais legais
- Alguns RFPs já estabelecem o formato da reposta e deve ser seguida
- Em geral, os seguintes tópicos são incluídos:
  - Uma topologia para a rede nova
  - Informação sobre os protocolos, tecnologias e produtos que formam o projeto
  - Um plano de implementação
  - Um plano de treinamento
  - Informação sobre serviços de suporte
  - Preço e formas de pagamento
  - Qualificação de quem está respondendo ao RFP
  - Recomendações de outros clientes para os quais projetos de redes já foram feitos
  - Termos e condições contratuais legais
- Observe que essa reposta não é um projeto completo mas um esboço para ganhar a RFP (licitação)

Conteúdo de um documento de projeto de rede

- A ser seguido para apresentar um projeto completo de rede (após ganhar a RFP ou quando não há RFP)
- As seções do documento 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
- Apêndices

Resumo executivo

- Uma única página resumindo os pontos importantes do projeto
- Orientado a gerentes que serão os decisores sobre a continuação do projeto
- O objetivo da seção é de vender as vantagens para o negócio do projeto de rede
  - Portanto, não mencione aspectos técnicos, ou mencione-os de forma extremamente sumária
  - Se foque nos negócios

Objetivo do projeto

- Descrição do objetivo principal
- Deve ser um objetivo de negócios
- Deve ter a ver com a questão: "Como a empresa ficará mais competitiva no seu negócio"
- Um parágrafo único
- Deixe claro ao leitor que você entende como a nova rede vai afetar a empresa
- Exemplo: "O objetivo deste projeto é de desenvolver uma WAN que suportará aplicações multimídia de alta banda passante e baixo atraso. As novas aplicações são chave para a implantação bem sucedida de um novo programa de treinamento para a equipe de vendas. A nova rede WAN deve facilitar atingir o objetivo de aumentar vendas domésticas em 50% no próximo ano fiscal"

Escopo do projeto

- Qual é tamanho do projeto?
- É uma rede nova ou uma extensão a uma rede existente?
- Mencione departamentos e redes afetadas pelo projeto
- Esclareça também o que *não* faz parte do projeto
- Exemplo: "O escopo do projeto é de atualizar a WAN que interconecta os escritórios de vendas principais no país à sede. A nova rede WAN será acessada por empregados das áreas de vendas, marketing e de treinamento. Não faz parte do escopo do projeto atualizar qualquer LAN usada por tais empregados. Tampouco faz parte do projeto atualizar as redes acessadas via satélite e por empregados que trabalham em casa"

Requisitos de design (de negócio e técnicos)

- Liste os objetivos de negócio e técnicos
  - Em ordem de prioridade
  - Evidenciando os objetivos críticos
- Os objetivos técnicos incluem objetivos relacionados à escalabilidade, disponibilidade, desempenho, segurança, gerenciabilidade, usabilidade, adaptabilidade, relação custo-benefício
- Mostre os tradeoffs que o cliente topa fazer, usando uma tabela de priorização de objetivos
- Liste as comunidades de usuários e os data stores
- Liste as aplicações e seus atributos

Estado da rede atual

- Use um (ou poucos) mapas de alto nível para mostrar a estrutura e baseline de desempenho da rede atual
  - Mapas detalhados ficam em apêndice
- Mostre VPNs, VLANs, segmentos, firewalls, clusters de servidores, endereçamento, etc.

Projeto lógico

- A topologia da rede
- Um modelo para endereçar segmentos de rede e dispositivos
- Um modelo para dar nomes aos dispositivos de rede
- Uma lista de protocolos de switching e de roteamento, incluindo qualquer recomendação sobre o uso dos protocolos
- Mecanismos e produtos recomendados para a segurança
  - Incluir um resumo de políticas de segurança e procedimentos associados
  - Um plano completo de segurança pode ser incluído como apêndice
- Recomendações sobre arquitetura e produtos para a gerência
- Explicações sobre o porquê de várias decisões tomadas, relacionando as decisões aos objetivos do cliente

Projeto físico

- Incluir:
  - Tecnologias
  - Dispositivos
  - Escolha de provedor
  - Informação de preços

Resultados de testes

- Mostre evidências de que o projeto da rede vai funcionar
- Se um protótipo tiver sido construído, inclua:
  - Objetivos dos testes realizados
  - Critérios de aceitação dos testes
  - Ferramentas de testes usadas

- Scripts de testes
- Resultados e conclusões

Plano de implementação

- Inclua recomendações sobre a implantação da rede
  - O plano não é detalhado se você não for responsável pela implantação
- Um plano de implementação inclui:
  - Um cronograma
  - Planos com fornecedores ou provedores de serviço para a instalação de enlaces, equipamentos ou serviços
  - Planos ou recomendações de outsourcing da implementação e/ou da gerência da rede
  - Um plano para informar usuários, gerentes, administradores sobre o projeto
  - Um plano de treinamento para administradores de rede e usuários
  - Um plano para medir a eficácia da nova rede depois de implantada
  - Uma lista de riscos conhecidos que podem atrasar o projeto
  - Um plano de contingência, caso a implementação venha a falhar
  - Uma plano para a evolução da rede face ao surgimento de novos requisitos e aplicações
- Um cronograma típico indicando milestones importantes segue:

Data de término	**Milestone (ponto de controle)**
1 junho	Projeto terminado e versão inicial do Documento de Projeto distribuído aos principais gerentes, administradores e usuários finais
15 junho	Recepção de comentários sobre o Documento de Projeto
22 junho	Documento de Projeto final distribuído
25 junho	Instalação de LPCDs entre todos os prédios pelo provedor WAN
28-29 junho	Administradores de rede treinados sobre o novo sistema
30 junho-1 julho	Usuários finais treinados sobre o novo sistema
6 julho	Implementação piloto terminada no prédio 1
20 julho	Feedback recebido dos administradores de rede e usuários finais sobre o piloto
27 julho	Implementação terminada nos prédios 2-5
10 agosto	Feedback recebido dos administradores de rede e usuários finais sobre a implementação nos prédios 2-5
17 agosto	Implementação terminada nos prédios remanescentes
Contínuo	Monitoração do novo sistema para verificar que satisfaz requisitos

Orçamento

- Deve-se documentar o orçamento disponível, incluindo:
  - Aquisição de hardware e software
  - Contratos de suporte e manutenção
  - Contratos de serviços
  - Treinamento
  - Recursos humanos
  - Fees de consultoria
  - Despesas de outsourcing

Retorno no investimento

- A forma mais fácil de convencer o decisor financeiro de bancar o projeto é de apresentar uma análise de Retorno no Investimento (ROI)
- Um exemplo de análise ROI:
  - Cliente ABC está considerando gastar R$1.000.000,00 em novo equipamento de comutação WAN
  - Se, em vez de comprar equipamento de rede, R$1.000.000,00 forem investidos por 5 anos, o retorno será de 5% e considera-se portanto que o investimento seja de R$1,05 milhão
  - Suposição: depreciação do equipamento em 5 anos
  - Os equipamentos atualmente em uso já estão pagos e depreciados
  - Porém, precisamos comparar os custos de operar a rede antiga e a nova rede
  - Com o novo equipamento, serão usados 12 enlaces E1 em vez de 20 enlaces como na rede antiga
  - Cada enlace custa R$1.500,00 por mês (12 enlaces custam R$18K e 20 custam R$30K)
  - Os custos recorrentes serão R$12K menores por mês e o custo de aquisição de R$1,05 milhão estará pago em 1.050.000/12.000 = 7 anos, maior que o tempo de depreciação
    - Well ... o homem não gostou ... Vamos tentar de novo!

Apêndices

- Incluir informação suplementar aqui
  - Mapas topológicos detalhados
  - Configurações de dispositivos
  - Detalhes de endereçamento IP
  - Resultados de testes
  - etc.