

**Alexandre Augusto Gimenes Marquez Filho**

***Infraestrutura de redes de computadores focada em  
SaaS***

São José – SC

julho / 2012

**Alexandre Augusto Gimenes Marquez Filho**

***Infraestrutura de redes de computadores focada em  
SaaS***

Monografia apresentada à Coordenação do  
Curso Superior de Tecnologia em Sistemas  
de Telecomunicações do Instituto Federal de  
Santa Catarina para a obtenção do diploma de  
Tecnólogo em Sistemas de Telecomunicações.

Orientador:

Prof. Ederson Torresini, Me.

CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES  
INSTITUTO FEDERAL DE SANTA CATARINA

São José – SC

julho / 2012

Monografia sob o título “*Infraestrutura orientada a SAAS*”, defendida por Alexandre Augusto Gimenes Marquez Filho e aprovada em 23 de julho de 2012, em São José, Santa Catarina, pela banca examinadora assim constituída:

---

Prof. Ederson Torresini, Me.  
Orientador

---

Frederico Gendorf  
ESSS

---

Prof. Marcelo Maia Sobral, Dr.  
IFSC

*Investiguemos de que modo a alma deverá prosseguir sempre de modo igual e no mesmo ritmo. Ou seja, estar em paz consigo mesmo, e que essa alegria não se interrompa, mas permaneça em estado plácido, sem elevar-se, sem abarbar-se. A isso eu chamo de tranquilidade.*

*Investiguemos como alcançá-la.*

*Lúcio Anneo Sêneca*

# *Agradecimentos*

Primeiramente, dedico este trabalho à minha esposa, Maria Fernanda, companheira de muito valor que esteve ao meu lado desde o início de minha graduação me incentivando a sempre acreditar que esta conquista seria possível e que outras estão por vir no decorrer de nossa caminhada.

À minha família querida, que, apesar da distância, sempre me incentiva e orienta a seguir o caminho do sucesso. Agradeço à minha mãe pelo carinho, meu pai pelos ensinamentos e minha irmã pelo seu exemplo. Acredito que, se hoje concluo esta etapa, com certeza, devo ser eternamente grato à minha família.

Aos meus professores, orientadores e demais profissionais do IFSC-SJ, os quais tive a oportunidade de vivenciar uma metodologia de ensino diferenciada, focada em conhecimentos atuais e práticos condizentes às necessidades do mercado.

Aos meus colegas de trabalho, pelo constante aprendizado que vivenciei junto a eles tanto profissional quanto pessoalmente.

E um agradecimento especial a todos os autores e colaboradores de software livre que auxiliam na promoção desta plataforma de desenvolvimento aberta.

# *Resumo*

Este trabalho é desenvolvido considerando a infraestrutura de rede de computadores e servidores do *Instituto Federal de Santa Catarina de São José* (IFSC-SJ) e seus serviços. Durante a análise deste projeto foi verificado que a aplicação de maior importância e mais problemática no IFSC-SJ é o HTTP. Soluções mais eficientes para esta aplicação vão ao encontro ao modelo SaaS, sendo o foco deste trabalho. Assim esta proposta direciona a infraestrutura atual ao serviço Web e elabora estudos sobre a disponibilidade e segurança dos diversos serviços de rede de computadores utilizando sistemas distribuídos. Esta proposta abrange um conjunto de alterações na rede de computadores do IFSC-SJ, a qual afeta toda a infraestrutura, tendo assim impacto significativo na atual organização. Foram sugeridos a readequação da plataforma de virtualização, que abrangem as aplicações Web e de banco de dados. Em ambos os casos foram mostradas soluções baseadas em sistemas distribuídos, somado ao controle de versão com a função de administração de sistema, visando assim facilitar o sincronismo e a restauração de arquivos passíveis de configurações.

# *Abstract*

This work is developed considering the current network infrastructure of computers and servers at the *Instituto Federal de Santa Catarina de São José* (IFSC-SJ) and its services. During the analysis of this project since the application was of greater importance in this scenario, quantitatively and qualitatively, is the HTTP server. In this study, therefore, will be a proposal to recast this, that meets the requirements of SaaS-based solutions. Will be presented a proposal to redesign the network infrastructure and servers in the IFSC-SJ, in order to improve services in terms of network availability and security. For an infrastructure better suited to providing services in Web applications, is presented a solution configuration virtualization platform in order to meet the load. This platform will contain virtualized systems and Web and database servers. These will make a auto-balancing of requests coming from clients. To ensure greater fault tolerance of our services, you must also propose changes to the Link layer (OSI model), it is possible to use technology in the switches to ensure more security and redundancy to the system. In this layer will need to configure the equipment in order to provide the requirements demanded. In addition, use will be also new management techniques with the help of applications for distributed version control.

# *Sumário*

## **Lista de Figuras**

## **Lista de Tabelas**

<b>1</b>	<b>Introdução</b>	p. 11
1.1	Definição do Problema . . . . .	p. 13
1.2	Justificativa . . . . .	p. 14
1.3	Objetivos . . . . .	p. 14
1.3.1	Objetivo Geral . . . . .	p. 14
1.3.2	Objetivos Específicos . . . . .	p. 14
1.4	Proposta da Solução . . . . .	p. 14
<b>2</b>	<b>Fundamentação Teórica</b>	p. 16
2.1	Redes de Computadores . . . . .	p. 16
2.1.1	Camadas Altas . . . . .	p. 18
2.1.2	Camadas Baixas . . . . .	p. 20
2.2	Virtualização . . . . .	p. 21
2.3	Sistemas Distribuídos . . . . .	p. 22
2.3.1	Aglomerado . . . . .	p. 22
2.3.2	Computação em grade . . . . .	p. 23
2.4	Computação em Nuvem . . . . .	p. 24
2.5	Gerência de Redes de Computadores . . . . .	p. 26
2.5.1	Documentação . . . . .	p. 26

2.5.2	Segurança . . . . .	p. 26
2.5.3	Monitoramento . . . . .	p. 27
2.5.4	Salvaguarda da Informação . . . . .	p. 28
2.6	Controle de versão . . . . .	p. 28
<b>3</b>	<b>Recursos Disponíveis</b>	<b>p. 31</b>
3.1	Rede Externa . . . . .	p. 31
3.2	Rede Interna . . . . .	p. 32
3.3	Serviços . . . . .	p. 33
<b>4</b>	<b>Proposta da Nova Rede</b>	<b>p. 36</b>
4.1	Visão geral . . . . .	p. 36
4.2	Distribuição dos Serviços e dos Servidores . . . . .	p. 37
4.3	Serviço de Conexão e de Processamento . . . . .	p. 38
4.3.1	Servidor HTTP . . . . .	p. 38
4.4	Serviços de diretórios . . . . .	p. 40
4.5	Serviços de armazenamento de dados . . . . .	p. 40
4.5.1	Sistema de Gerenciamento de Banco de Dados . . . . .	p. 40
4.5.2	Controle de Versão . . . . .	p. 42
4.6	Camada de Enlace . . . . .	p. 43
4.7	Serviços para Usuários Finais . . . . .	p. 44
4.8	Gerência . . . . .	p. 45
<b>5</b>	<b>Conclusões</b>	<b>p. 48</b>
	<b>Lista de Abreviaturas</b>	<b>p. 49</b>
	<b>Referências Bibliográficas</b>	<b>p. 52</b>

## *Lista de Figuras*

2.1	Modelos de camadas em redes de computadores e classificação. . . . .	p. 17
2.2	Modelo de sistemas de controle de versão centralizado. . . . .	p. 29
2.3	Modelo de sistemas de controle de versão descentralizado. . . . .	p. 29
3.1	PoP-SC - fonte: <a href="http://rnp.br">http://rnp.br</a> . . . . .	p. 31
3.2	PoP-SJ - fonte: <a href="http://rnp.br">http://rnp.br</a> . . . . .	p. 32
3.3	Modelo atual de rede do IFSC-SJ. . . . .	p. 33
3.4	Contabilização do servidor integrado. . . . .	p. 35
4.1	Modelo de <i>proxy</i> reverso. . . . .	p. 39
4.2	Modelo de aglomerado em MySQL. . . . .	p. 41
4.3	Modelo do <i>Cluster Manager</i> em MySQL. . . . .	p. 41
4.4	Proposta para diretórios Web em sistemas de controles de versão. . . . .	p. 43
4.5	Novo modelo de rede proposto para redes virtuais. . . . .	p. 44
4.6	Visão geral dos serviços no novo modelo de rede concebido. . . . .	p. 46

## *Lista de Tabelas*

3.1	Aplicações e URLs do IFSC-SJ. . . . .	p. 34
3.2	Serviços oferecidos na rede IFSC-SJ. . . . .	p. 34
4.1	Proposta de repositórios em sistema de controle de versão. . . . .	p. 42

# 1 *Introdução*

A Internet como a conhecemos atualmente muito deve a um dos seus protocolos de base, o *Internet Protocol* (IP). Passados mais de 30 anos, a quarta versão desse protocolo (IPv4) ainda se encontra amplamente em uso, apesar de já demonstrar claramente suas limitações frente às novas demandas dos serviços que operam sobre a infraestrutura de dados, com destaque a tolerância a falhas e segurança dos dados transportados. Tais requisitos têm se mostrado cada vez mais necessários para a maioria das instituições. O Instituto Federal de Santa Catarina de São José (IFSC-SJ) possui consideráveis dependências dos serviços de redes por meio da comunicação IP, pois são esses que possibilitam o gerenciamento das diversas informações acadêmicas e administrativas da instituição, e questões como disponibilidade e segurança dos serviços são essenciais.

Se por um lado a adoção do IPv6 indica avanço na comunicação dos dados, muitos esforços e pesquisas foram realizados para aperfeiçoar os entes terminais da transmissão, em particular os servidores: sistemas operacionais, protocolos de alto desempenho e aplicações que aproveitam melhor os recursos disponíveis. As principais tecnologias que auxiliam para essa finalidade estão no campo de sistemas distribuídos, computadores independentes interligados em rede visando oferecer um sistema único, que unidos aos avanços em sistemas virtualizados, os quais possibilita a instalação de diversos sistemas operacionais em um mesmo computador, somam para garantir maior confiabilidade aos serviços ofertados, seja para alcance local ou para atender um cliente a quilômetros de distância.

Com o constante avanço destas tecnologias, especificamente em sistemas distribuídos e virtualizados, as aplicações do tipo Web obtiveram consideráveis melhorias para conseguir atender o elevado número de usuários, visto que esse é o serviço de maior crescimento na Internet (KUROSE; ROSS, 2010). Utilizando destas tecnologias, as aplicações Web conseguem distribuir a carga de processamento e entregar um serviço de grande abrangência e com suporte a uma infinidade de clientes.

O desenvolvimento de aplicações Web também começou a evoluir de forma a possibili-

tar a criação de aplicações mais complexas e também a mudar padrões no fornecimento dessas aplicações aos usuários, as quais podem ser vistas como serviços. Um primeiro passo neste sentido foi em 1998 com a proposta do termo *Application Service Provider* (ASP), que tinha por intuito oferecer uma aplicação como serviço por meio de comunicação IP utilizando geralmente do navegador Web para acesso do usuário, embora não obtivesse tanto sucesso devido ainda as limitações de implementações de sistemas distribuídos, ainda em aperfeiçoamento à época. Entretanto, a partir de 2001 ocorreram significativas melhorias nas tecnologias envolvidas e ainda o surgimento da computação em nuvem, a qual permite solidificar os conceitos de aplicação, plataforma e infraestrutura como serviços, juntamente com soluções baseadas em *Web Service*, modelo adotado no desenvolvimento de aplicações que visa a comunicação e integração de diversos sistemas por meio da Web. Foi assim, por esse conjunto de tecnologias emergentes, que se tornou possível atender a proposta concebida pelo ASP, porém agora compreendida pelo *Software as a Service* (SaaS), o qual resultou em uma aceitação maior, principalmente do mercado (SIIA, 2001).

O SaaS se encaixa hoje em um dos tipos previstos em computação em nuvem para entrega de aplicações como serviços, entretanto, como visto, antes mesmo do conceito de computação em nuvem essa característica de *software* oferecido como serviço já era almejada. Por meio dessa tecnologia é possível oferecer um ambiente focado na Web, que independente de onde os usuários estejam, as informações estarão sempre disponíveis na Internet com acesso facilitado. Por meio da aceitação desta tecnologia, é possível afirmar, que hoje, o modelo de aplicação Web é extremamente aceito pelos usuários, e possibilita orientar a configuração da aplicação para que fique o armazenamento e processamento da aplicação a cargo do servidor e o acesso pelo cliente por meio de um navegador Web, simplificando os requisitos de instalações para estações clientes (SIIA, 2001).

O uso de sistemas distribuídos e virtualizados é comum em redes de computadores, onde disponibilidade e segurança são relevantes ao funcionamento dos serviços e é, em muitos casos, condição essencial para as suas aplicações. Entretanto, garantir apenas em nível de aplicação a disponibilidade e segurança pode não ser suficiente, visto que redes de computadores possui uma infraestrutura composta por vários outros dispositivos que precisam ser tolerantes as falhas para garantir os serviços pertencentes a essa rede. Nesse sentido, a energia elétrica, o provedor de Internet, os roteadores e *switches* precisam de soluções que busquem minimizar as falhas possíveis, e seus tempos de queda, para que se minimize a ocorrência de erros no sistema e consequentemente defeitos nos serviços.

Com isso, as redes de computadores atualmente podem ser construídas aproveitando todo

esse conhecimento acumulado em busca das melhores configurações. Construir uma rede de computadores consiste em utilizar diversas tecnologias disponíveis para que os equipamentos e serviços sejam devidamente configurados e, ainda, definir quais as rotinas de administração para garantir estabilidade e segurança a esse funcionamento. A administração de redes visa estabelecer boas práticas para que uma rede seja criada, configurada e gerenciada de forma a estabelecer maior disponibilidade e segurança, que saiba identificar as falhas, que possam vir a ocorrer e antes dos erros ocorrerem, emitir alertas e ações para garantir a estabilidade da rede por meio de aplicações de monitoramento.

A título de exemplo, na atual rede de computadores do IFSC-SJ existem vários pontos que podem ser melhorados quanto a disponibilidade e segurança dos serviços prestados, entre os quais a pouca disponibilidade de memória para algumas máquinas e existência de ponto único de falha - *Single Point of Failure* (SPOF) - em nível de enlace e de aplicação.

## 1.1 Definição do Problema

O trabalho é desenvolvido considerando a atual infraestrutura de rede de computadores e parque de servidores do campus IFSC-SJ e seus serviços. A rede do IFSC-SJ possui limitações físicas e lógicas, que envolvem desde as condições das salas destinadas ao abrigo desses equipamentos, bem como a falta de atualização das configurações de *software* e *hardware*, sendo assim necessário rever as políticas presentes para administração desta rede de computadores.

Após o convívio com a equipe técnica de gerência desta rede para a realização deste trabalho foi possível identificar alguns problemas, que abrangem a rede lógica e a rede física. Quanto a rede lógica, atualmente o IFSC-SJ possui os principais serviços ofertados por servidores virtualizados e notamos, na atual configuração, que são pouco aplicadas as diversas tecnologias existentes para tornar um ambiente virtualizado mais enxuto e equilibrado, que evitasse a atual competição por recursos das diversas máquinas virtuais configuradas neste ambiente, sendo que, nesse caso, esse problema compromete todos os serviços que estão em sistemas operacionais virtualizados, em sua maioria, aplicações Web.

Quanto a rede física, ficou evidenciada a dificuldade de operar toda a rede como uma única rede local, sem fazer uso de redes virtuais, configuradas em nível de *switches*, pois uma simples falha se propaga rapidamente, e é difícil diagnosticar a origem. Inclusive, os *switches* pouco utilizam configuração que acrescente melhorias a esta rede sendo que essas podem auxiliar na obtenção de maior segurança e disponibilidade a esta rede.

Essa atual situação da rede do IFSC-SJ compromete a disponibilidade dos serviços aos

usuários desta, evidenciado por reclamações tanto dos usuários quanto da equipe de gerência, a qual, para apresentar uma solução definitiva a este problema, precisa replanejar a configuração desta rede. Enquanto isto, são utilizadas soluções temporárias para estes problemas.

## 1.2 Justificativa

Em busca de maior **disponibilidade** e **segurança** aos serviços prestados na rede de computadores do IFSC-SJ, faz-se necessário reavaliar a atual configuração de serviços e de servidores e, assim, identificar maneiras de obter maior eficiência no uso dos recursos disponíveis.

Este trabalho é relevante pelo fato de considerar que redes de computadores devem ser projetadas para atender um crescimento futuro, usando principalmente das configurações de *software* e assim ter condições de atender quando necessário muitos clientes com uso de poucos servidores, e por consequência evitar o constante investimento em *hardware* para cobrir a necessidade de desempenho.

## 1.3 Objetivos

### 1.3.1 Objetivo Geral

Replanejamento da infraestrutura lógica de rede e de servidores em nível de Enlace e de Aplicação, a fim de melhorar os serviços prestados em termos de disponibilidade, no tocante a tolerância a falhas e distribuição de atendimento aos clientes Web, e segurança, em especial na oferta de autenticação e autorização criptografada nas duas camadas já mencionadas.

### 1.3.2 Objetivos Específicos

- Reconhecimento da infraestrutura física e lógica, com vistas à sugestão de melhorias em nível de enlace e de rede.
- Estabelecimento de políticas de criação e de uso de serviços ofertados na Web.

## 1.4 Proposta da Solução

Neste trabalho iremos analisar as questões referentes a instalação e configuração de *software* e *hardware* dos servidores e equipamentos de rede do campus São José do Instituto. O

foco principal deste projeto está nas aplicações e optou-se por soluções que garantam independência do sistema operacional e da plataforma de virtualização, características de ambientes distribuídos heterogêneos, sendo assim focado apenas nas tecnologias pertencentes as camadas altas e baixas presentes em redes de computadores para atender as necessidades mencionadas anteriormente: disponibilidade e segurança.

Haja vista que atualmente existe uma infraestrutura suficiente para garantir qualidade aos serviços oferecidos pelo IFSC-SJ, e que pode ser melhor utilizada no que tange à eficiência, podemos oferecer assim estudos para uma melhor configuração dos equipamentos utilizados pela infraestrutura, a fim de oferecer também estabilidade juntamente com escalabilidade.

A principal aplicação de interesse deste trabalho é o *Hypertext Transfer Protocol* (HTTP), por este ser considerado o serviço mais importante na rede do IFSC-SJ e também pelo fato do enorme crescimento de aplicações do tipo Web providas por meio deste serviço. Essa proposta vai ao encontro do modelo SaaS, cujos princípios serão utilizados como linha mestre, embora esse seja um modelo de negócio, é também um modelo de fornecimento de aplicações Web utilizando de inúmeras tecnologias, inclusive de sistemas distribuídos, para garantir escalabilidade juntamente com segurança e disponibilidade (SIIA, 2001).

## 2 *Fundamentação Teórica*

Neste capítulo são apresentados os conceitos básicos, de forma não exaustiva, como redes de computadores e suas camadas, com ênfase àquelas que serão objeto de estudo: as altas, que correspondem às aplicações e serviços, e as baixas, que tratam de interconexão entre os componentes ativos de rede. Além disso, serão vistos também outros conceitos, estes aplicados a ambientes de entrega de serviço por IP, como é o caso do SaaS, o qual se aplica a esse ambiente as tecnologias de sistemas distribuídos para assim obter maior escalabilidade dos serviços e virtualização de sistemas para melhor aproveitamento dos recursos do hardware. Serão vistos também conceitos sobre gerência de rede, pelo meio do qual é possível garantir o registro das informações monitoradas em rede e emitir os alertas de falhas aos administradores da rede. Por último, o sistema de controle de versão, o qual será adaptado controlar os arquivos passíveis de configurações dos dispositivos e serviços em redes de computadores.

### 2.1 **Redes de Computadores**

Embora o termo “redes de computadores” seja bastante conhecido nos dias atuais, cabe destacar alguns termos utilizados na sua definição mais formal: dispositivos computacionais interligados capazes de trocar informações por meio de uma ou mais tecnologias. A transmissão entre os dispositivos é realizada por **protocolos** que determinam padrões para as trocas de informações. A maioria das redes são concebidas e organizadas como **pilha de camadas hierárquicas**, cuja organização se dá na oferta de serviços para as camadas (imediatamente) superiores ou inferiores, protegendo essas camadas dos detalhes de como os serviços são realmente implementados (TANENBAUM, 2003).

O modelo de referência *Open Systems Interconnection* (OSI) e o popular TCP/IP são os dois modelos mais importantes de arquitetura e ambos os serviços de redes de computadores em camadas hierárquicas. O modelo OSI foi concebido de forma bastante geral, não sendo inclinado para um determinado conjunto de protocolos, embora seja concreto e amplamente implementado. São sete camadas neste modelo, de cima para baixo: Aplicação, Apresentação,

Sessão, Transporte, Rede, Enlace e Física. Os princípios deste modelo podem ser resumidos na necessidade de cada camada possuir uma abstração diferente, executar uma função diferente, abranger protocolos padronizados internacionalmente e minimizar os fluxos de informações entre as interfaces (TANENBAUM, 2003).

Diferente do modelo OSI, o modelo TCP/IP foi criado como descrição dos protocolos já existentes (TANENBAUM, 2003) - é o padrão de comunicação na Internet. Ao contrário do modelo OSI, este modelo possui quatro camadas: Aplicação, Transporte, Internet e Interface (BLANK, 2004). Para este trabalho, será utilizado o TCP/IP exceto nos casos em que esse se mostrar genérico ou carente de detalhes, como por veremos nos próximos capítulos.

		Camadas de Rede	
		OSI	TCP/IP
Camadas Altas	7	Aplicação	Aplicação
	6	Apresentação	
	5	Sessão	
	4	Transporte	Transporte
Camadas Baixas	3	Rede	Internet
	2	Enlace	Interface
	1	Física	

Figura 2.1: Modelos de camadas em redes de computadores e classificação.

Em ambos os modelos, as camadas baixas, conforme ilustrado pela figura 2.1, descrevem a interconexão entre os dispositivos de rede. A dimensão da rede, e dos enlaces definem em rede local ou de longa distância, ainda que em níveis mais teóricos que práticos, a área que eles compreendem. Em primeiro, a rede local - *Local Area Network* (LAN) - a qual interconecta recursos computacionais em área geográfica de tamanho moderado. Pode ser uma sala, diversas salas em um prédio ou diversos prédios em um campus universitário. Uma importante característica de redes locais são as velocidades a qual as estações clientes possuem disponíveis para troca de informações entre os dispositivos. Contrastando com uma rede local, há a rede de longa distância - *Wide Area Network* (WAN) -, que interconecta recursos computacionais distantes geograficamente uns dos outros. Geralmente, as redes WAN são conectadas por uma infraestrutura com equipamentos de alto nível, com fibras ópticas ligando interconectadas por *backbones*, uma rede principal com alta capacidade de processamento por onde passa dados de diversos clientes (TANENBAUM, 2003). Ao contrário de alguns anos atrás, a WAN em alguns casos atinge velocidades de transmissão próximas da LAN. Prova disso é a expansão da banda larga que viabilizou desde VoIP, transmissão de voz sobre IP até *home office*, por meio do qual é possível um funcionário em sua residência estar conectado a rede da empresa utilizando da Internet. No nosso cenário, na rede do IFSC-SJ, em particular, cabe destacar que os enlaces

de LAN são equivalentes aos de WAN em termos de velocidade: 1 Gbps simétrico (*upload* e *download*).

### 2.1.1 Camadas Altas

As sete camadas do modelo OSI estão distribuídas neste trabalho em três grupos:

- Altas: Aplicação, Apresentação e Sessão, associadas às aplicações.
- Médias: Transporte e Rede, associadas aos sistemas operacionais.
- Baixas: Enlace e Física, associadas à infraestrutura física e lógica da rede local e enlaces WAN.

Por questões de decisão estratégica da instituição, não deve haver um sistema operacional específico, seja esse virtualizador ou virtualizado. Assim, este trabalho se pautou nas camadas altas e baixas, assim, se ater ao modelo TCP/IP.

As redes de computadores, e principalmente a Internet, podem ser descritas como uma plataforma para aplicações distribuídas, que disponibilizam diversos serviços. No modelo OSI, são as camadas mais altas responsáveis por isso: Aplicação, Apresentação e Sessão. Embora no modelo TCP/IP reste apenas a camada de Aplicação, manteremos o termo no plural (altas) para representar a complexidade dos serviços prestados. Desses serviços, cabe elencar aqueles em uso corrente ou futuro do IFSC-SJ: sistemas de arquivos, diretórios, bancos de dados, Web e impressão.

A abstração de arquivo, conjunto de dados encapsulado e nomeado, ainda é muito presente nos atuais sistemas operacionais. Devido a isso, um tipo de serviço bastante popular nas redes é tornar um sistema de arquivos compartilhado, para mais de um sistema operacional (TANENBAUM, 2003). Serviços amplamente utilizados como *Network File System* (NFS) e *Common Internet File System* (CIFS) - outrora *Server Message Block* (SMB) - são vistos desde sistemas embarcados a virtualizadores.

Embora o próprio sistema operacional organiza-se na forma de diretórios, os serviços de diretórios propriamente ditos organizam dados em outros formatos: registros, objetos entre outros. Além disso, possui outras características: repositório distribuído fisicamente, logicamente centralizado de rara alteração de dados, comumente usados para armazenar informações sobre usuários, aplicativos e recursos de rede como servidores de arquivos e impressoras (CISCO, 2003). Assim, serviços de diretórios podem ser utilizados para diversos fins, como o popular

*Domain Name Server* (DNS) e em sistemas integrados de autenticação utilizando *Lightweight Directory Access Protocol* (LDAP).

O DNS é o serviço de diretório da Internet, com a finalidade principal de agrupar endereços IP em domínios (e zonas) e fornecer-lhes informações como nome, descrição e outros (MOKAPETRIS, 1987). Estabelece uma hierarquia entre os servidores DNS em escala global, regida pela *Internet Assigned Numbers Authority* (IANA). Diversas aplicações fazem uso do DNS, comumente HTTP, *Simple Mail Transfer Protocol* (SMTP), *Session Initiation Protocol* (SIP) e outros (KUROSE; ROSS, 2010). Outro serviço de diretório é LDAP, mais especificamente de acesso a diretório baseado no original *Directory Access Protocol* (DAP) do padrão X.500 da *ITU Telecommunication Standardization Sector* (ITU-T). Comumente, e que também se aplica ao IFSC-SJ, é utilizado para autenticação de usuários e organizar itens comuns de recursos de rede, tais como impressoras, computadores, telefones e outros objetos (FRISCH, 2002).

Outro tipo de aplicação muito comum em redes de computadores são os de Sistema de Gerenciamento de Bancos de Dados (SGBD). O SGBD pode ser visto como uma camada de *software* entre os usuários do sistema e os dados físicos de fato armazenados, responsável por todas as solicitações de acesso a esses dados. Semelhante ao que ocorre em linguagens de programação de alto nível, o SGBD fornece aos usuários uma visão de banco de dados acima do nível de *hardware*, e admite operações (DATE, 2003). As operações mais comuns realizadas em banco de dados são adicionar novos arquivos, inserir novos dados, buscar e alterar dados em arquivos existentes e, por último, remover dados existentes. O SGBD está disponível e acessível aos usuários geralmente por intermédio de aplicações, e as operações são realizadas por uma linguagem padrão, e a mais reconhecida por todos os produtos de banco de dados existentes hoje no mercado é a linguagem *Structured Query Language* (SQL) (DATE, 2003). Existem três classes de usuários amplas para SGBD, a primeira consiste de desenvolvedores de aplicações, a segunda por usuários de aplicações e a terceira é dos administradores de banco de dados. Em aplicações Web é muito comum a utilização de banco de dados, onde o processamento no servidor HTTP irá realizar requisições ao servidor do banco para consultas e atualizações de dados e, em seguida, montando a página de forma dinâmica.

Bancos de dados distribuídos implica uma única aplicação capaz de operar os dados dispersos em áreas de armazenamento diferentes, sendo admitida uma variedade de sistemas operacionais diferentes e conectados entre si, o qual deve funcionar de forma transparente como se todos os dados fossem gerenciados por apenas um SGBD (DATE, 2003).

Contudo, os serviços DNS, LDAP e SGBD são transparentes ao usuário final, porém pré-requisitos do HTTP, considerando o cenário proposto focado em SaaS, o qual utiliza desses serviços para oferecer acesso as aplicações por meio da Web. O HTTP foi concebido como parte de um conjunto de padrões, destacando o *Hypertext Markup Language* (HTML) e *Uniform Resource Locators* (URL). Enquanto que o HTTP é responsável pela troca de mensagens para transferência de dados, o HTML trata da formatação do hipertexto. Por fim, o URL, como o nome diz, serve de localizador dos recursos disponíveis na rede. Desde a sua introdução, a Web evoluiu consideravelmente. Há uma riqueza de métodos e ferramentas para produzir informação a ser processado tanto por servidor, como por exemplo *web service* quanto pelo cliente, como Javascript. Atualmente, existem serviços que se utilizam deste protocolo para fins de compartilhamento de arquivos e impressoras em um sistema operacional, respectivamente *Web-based Distributed Authoring and Versioning* (WebDAV) e *Common Unix Printing System* (CUPS). Essas e outras possibilidades realizadas sobre o protocolo HTTP o torna muito versátil, sendo inclusive considerado o protocolo chave para a implementação de SaaS.

### 2.1.2 Camadas Baixas

Em relação às camadas baixas, algumas tecnologias podem auxiliar na disponibilidade, administração e segurança dos serviços disponíveis em redes de computadores, principalmente aqueles pertencentes à camada de aplicação.

A *IEEE 802* desenvolve e mantém padrões e práticas recomendadas para redes locais e metropolitanas a nível mundial. Entre os padrões mais utilizados está a *IEEE 802.3* que define as características para redes *Ethernet*, amplamente implementada em LAN (ELECTRICAL; ENGINEERS, 2008).

Para garantir disponibilidade a nível de enlace duas tecnologias se destacam: *Spanning Tree Protocol* (STP) (IEEE 802.1d) e agregação de enlace (IEEE 802.1ax). Quanto a administração outras duas tecnologias podem ser utilizadas, o empilhamento de *switches* e a organização por *Virtual Local Area Network* (VLAN) (IEEE 802.1Q), sendo essa última também útil para segurança. A seguir será melhor explicado tais tecnologias.

A criação de VLANs auxiliam na divisão de um rede física em outras redes virtuais com domínios de *broadcast* diferentes coexistindo em um mesmo *switch* - ou empilhamento de *switches*. Com isto, é possível, a utilização de domínios menores e maior facilidade para administrar serviços que nele se propagam, como o caso do *Dynamic Host Configuration Protocol* (DHCP), que fornece informações para configuração automática das interfaces de rede dos clientes quando são solicitadas. Desse modo é possível diagnosticar, isolar e corrigir problemas

de forma mais eficiente, não repercutindo em toda a rede física, apenas nas respectivas VLANs. Outra propriedade da VLAN é a capacidade de **restringir** acesso a recursos da rede, tais como servidores e impressoras e também facilitar a implantação de uma topologia de rede, além de melhorar o aproveitamento dos *switches* (COMER, 2009).

O empilhamento de *switch* é uma tecnologia fornecida especificamente por cada fabricante e aplicáveis apenas ao mesmo modelo, e tem por objetivo agrupá-los em um único dispositivo virtual. Logo, a gerência desses dispositivos é realizada por apenas uma interface, simplificando a administração da rede e permitindo aos outros protocolos implementações mais robustas e sofisticadas, pelo fato dos *switchs* em pilhas serem vistos como um único *switch*.

O STP é utilizado para evitar caminhos redundantes entre *switches*, pois caso existam tais caminhos, pode ocorrer de um determinado *switch* enviar uma mensagem em *broadcast* por um caminho e recebe-la em outro, caracterizando um laço na rede, comprometendo a troca de informações e ocasionando inclusive falhas, assim o STP organiza os enlaces em uma árvore de acordo com regras pré-definidas para ativa-los ou desativa-los. Os caminhos redundantes são desejáveis para aumentar a disponibilidade, mas apenas quando necessário, se gerenciados pelo STP serão então vistos como caminhos alternativos. Na prática, ainda funciona como protocolo de tolerância a falhas (ELECTRICAL; ENGINEERS, 2004).

Para aproveitar o uso de múltiplos enlaces para aumentar a capacidade e obter maiores taxas de transmissão de dados, pode-se combinar várias interfaces para criação de um único canal lógico, com agregação de enlaces. Esse termo, é genérico e atualmente implementado de várias formas, como por exemplo *Link Aggregation Protocol* (LACP). Por combinar as conexões em paralelo para aumentar a vazão, também fornece tolerância a falhas no caso de um dos enlaces falhar. O LACP, um dos padrões abertos, fornece um método para controlar a agregação de várias portas físicas em conjunto para formar um único canal lógico, enviando pacotes LACP para os pares que também implementam LACP e quando ocorrer uma falha é possível identificar e readaptar os caminhos lógicos, até que tal falha seja solucionada (COMER, 2009).

## 2.2 Virtualização

A virtualização de sistema tem por objetivo fornecer várias máquinas virtuais (VMs) sobre a máquina física disponível. Cada máquina virtual executa uma instância de sistema operacional isolado. Essa tecnologia decorre da observação de que computadores têm o desempenho necessário para suportar um número potencialmente grande de máquinas virtuais (COULOURIS et al., 2011). Há dois tipos de virtualização. Na virtualização plena, o *sistema* é totalmente

virtualizado, não requerendo qualquer modificação do sistema virtual. Já na paravirtualização apenas parte do *sistema* é virtualizado. Embora seja comum maior desempenho no último caso, é necessário uma VM projetada para tal fim.

As ações essenciais no ambiente virtualizado são realizadas pelo *hypervisor*, componente mais importante de qualquer solução de virtualização. O *hypervisor* é o software instalado diretamente sobre o hardware físico que hospeda as máquinas virtuais e implementa as funções de gerenciamento e monitoramento destas (ROSENBERG; MATEOS, 2011).

## 2.3 Sistemas Distribuídos

Uma vez vistas as aplicações e formas de implementar uma rede lógica com disponibilidade e segurança, pode-se partir para distribuição de sistemas.

Existem dois grandes avanços tecnológicos que possibilitaram o surgimento de sistemas distribuídos. O primeiro avanço é fruto do advento de microprocessadores, o qual possibilitou a fabricação de computadores com maior processamento e ainda mais baratos. O segundo avanço foi a invenção de redes de alta velocidade que possibilitou consideráveis melhorias na comunicação entre computadores (S.TANENBAUM; STEEN, 2006). Um sistema distribuído é um conjunto de computadores independentes interligados em rede visando oferecer um sistema único e coerente aos usuários. Os componentes de hardware ou software podem se comunicar em redes e coordenar suas ações apenas pelo envio de mensagens (COULOURIS et al., 2011).

Uma possível classificação de sistemas distribuídos os divide em: sistemas de computação distribuídos, sistemas de informação distribuídos e sistemas embutidos distribuídos, implantados, respectivamente, em cenários de alto desempenho, bancos de dados e computação ubíqua. São previstos dois tipos de computação distribuída, aglomerado e grade (S.TANENBAUM; STEEN, 2006).

### 2.3.1 Aglomerado

O aglomerado, ou *cluster*, é um tipo de computação distribuída para construir computadores com grande quantidade de recursos (processadores, memórias e capacidade de armazenamento), utilizando de redes de alta velocidade para o compartilhamento destes recursos (DANTAS, 2005).

O diferencial de ambientes de aglomerado é a escalabilidade, que possibilita a configuração crescer a medida que mais recursos estiverem disponíveis, permitindo aumentar o desempe-

nho de uma aplicação por meio da informação de configurações com uma vantajosa relação custo-desempenho. A implementação dos aglomerados está relacionada a execução com maior desempenho das aplicações alvo de uma organização. Existem duas classes de aplicações: a primeira caracterizada pela necessidade de poder computacional alto desempenho para uma execução eficiente; a segunda, pela necessidade de alta disponibilidade (DANTAS, 2005).

O funcionamento de um ambiente de configuração de um aglomerado é realizado por um *Single System Image* (SSI) que podem ser estabelecidos por um *middleware*, que é um mediador entre sistemas diferentes, implantados no sistema operacional (software) ou no nível de *hardware*. Utilizar o *middleware* como SSI produz uma maior flexibilidade de configuração devido a independência do sistema operacional, que esteja sendo executado em cada computador, caracterizado por ambientes heterogêneos, os quais precisam ter os pacotes de *software* compilados em diferentes sistemas operacionais de maneira correta para garantir o funcionamento e transparência para os usuários (Ibid.). Esta configuração explica como os aglomerados podem ser aplicados a nível de aplicação, pois uma vez que essas possuem um *middleware* pronto, podem ser instaladas em diferentes plataformas que conseguirão se comunicar e trabalharem como apenas um processo.

Os aglomerados podem ser empregados para a melhoria de desempenho de aplicações Web, um processo mestre recebe as solicitações dos usuários externos e distribui para os demais computadores do aglomerados, que tem a função de efetuar um balanceamento de carga da configuração. Entretanto, esse processo tem uma importância essencial, em uma solução de alta disponibilidade, e deve existir um segundo processo que possa assumir as funções do processo mestre caso venha a falhar utilizando técnicas de *heartbeat*, aplicações para o constante monitoramento do processo mestre, caso de falta de sinal de operação por alguns segundos, o segundo processo assume a função de balanceamento de carga. Cabe destacar que o *heartbeat* é usado em muitas aplicações onde a disponibilidade é essencial, como será visto no capítulo 4.

### 2.3.2 Computação em grade

A computação em grade difere do aglomerado na maneira do gerenciamento dos recursos e serviços. No aglomerado, o gerenciamento é realizado por uma autoridade central enquanto na grade cada organização virtual faz o gerenciamento. Enquanto o aglomerado é uma configuração de *hardware* e *software* local, a grade tem um configuração geograficamente distribuída. Uma analogia interessante é comparar o aglomerado a LAN, que compartilha recursos em redes locais, e a grade a WAN, que compartilha recursos em redes de longas distâncias (DANTAS, 2005).

A plataforma de grade é caracterizada por um ambiente heterogêneo com tecnologia de acesso comum aos serviços e recursos, com alto foco no compartilhamento. Os participantes de um grade são definidos como organizações virtuais, a qual é uma entidade que compartilha recursos (COULOURIS et al., 2011)..

A arquitetura da grade pode ser representada por 4 camadas, aplicações e serviços, *middleware*, recursos e rede. Milhares de aplicações compõem a camada de aplicações e serviços que incluem também os conjuntos de ferramentas de desenvolvimento, funções de gerenciamento e todos os parâmetros para uso dos recursos compartilhados. A camada a seguir, *middleware*, é composta pelos protocolos que permitem a unificação e o suporte dos elementos heterogêneos de uma grade, diferentes sistemas operacionais, sistemas de arquivos e comunicação entre redes. Na penúltima camada, recursos, composta pelos recursos e serviços que partem da grade e por fim a última camada, de rede, a qual garante conectividade para os recursos da grade (DANTAS, 2005).

## 2.4 Computação em Nuvem

O conceito de computação em nuvem aborda o próximo passo evolutivo da computação distribuída. Tem por objetivo fazer uma melhor utilização dos recursos distribuídos, obter maior rendimento e ser capaz de resolver problemas em grande escala de computação (STANOEVSKA-SLABEVA; WOZNIAK; RISTOL, 2010).

A computação em nuvem refere-se ao *hardware*, *software* de sistemas e aplicações entregues como serviços através da Internet. Em geral, existem três categorias para os provedores destes serviços (ANTONOPOULOS; GILLAM, 2010):

- *Software as a Service* (SaaS): *software* como serviço;
- *Platform as a Service* (PaaS): plataforma como serviço;
- *Infrastructure as a Service* (IaaS): infraestrutura como serviço.

O SaaS indica um novo passo evolutivo na entrega de *software* como um serviço baseado em serviços Web e tecnologias de computação em grade (SIIA, 2001). Representa os serviços e aplicações que estão disponíveis em uma base sobre demanda. Em vez de ser uma inovação tecnológica, essa é uma inovação do modelo de negócio. No modelo SaaS, o *software* não está a venda, pois esse é visto como um serviço, o qual é pago enquanto é utilizado. O cliente compra o acesso ao *software* por um período ou volume de uso especificado: tráfego, processamento e

outros indicadores de consumo de recurso. A maioria dos provedores de computação em nuvem se utilizam deste modelo (ROSENBERG; MATEOS, 2011).

O SaaS não é uma tecnologia nova e estende a ideia do modelo ASP introduzido em 1998, o qual é baseado na ideia de que uma aplicação Web possa ser fornecida *online* em uma infraestrutura baseada em IP por um provedor central aplicativo de serviço. A convergência de serviços da Web e de tecnologias de computação em grade oferece novas oportunidades para resolver os problemas de entrega ASP. Serviços Web permitem a modularização de aplicações em vários serviços que podem ser combinados e personalizados pelos usuários. A computação em grade e também em nuvem tem o potencial de fornecer a necessária flexibilidade e escalabilidade no lado de infraestrutura de ofertas de SaaS (STANOEVSKA-SLABEVA; WOZNIAK; RISTOL, 2010).

O PaaS, por sua vez, oferece aos desenvolvedores uma plataforma, incluindo todos os sistemas e ambientes, compreendendo o ciclo para desenvolver, testar, implantar e hospedar aplicações Web sofisticadas como um serviço prestado na base da nuvem. Representa uma maneira mais fácil para desenvolver aplicações por meio da Internet. Quando comparado ao desenvolvimento de aplicações convencionais, esta estratégia pode reduzir o tempo de desenvolvimento, oferecer de ferramentas prontamente disponíveis e serviços rapidamente escaláveis (ANTONOPOULOS; GILLAM, 2010).

Já o IaaS oferece recursos, tais como o processamento e armazenamento, que podem ser obtidos como um serviço. Normalmente os provedores de IaaS oferecem infraestrutura virtualizada como um serviço. Pela virtualização, os recursos de *hardware* são abstraídos e encapsulados e podem, assim, ser expostos à camada superior e utilizados por usuários finais por meio de uma interface unificada. Apesar de a infraestrutura já estar disponível antes da computação em nuvem, o IaaS denota sua evolução para suporte integrado as três modalidades: IaaS, PaaS e SaaS. O PaaS e os fornecedores SaaS recorrem as ofertas de IaaS com base em interface padronizada: a *Application Programming Interface* (API) (STANOEVSKA-SLABEVA; WOZNIAK; RISTOL, 2010).

Existem também duas classificações importantes em computação em nuvem: pública e privada. As nuvens privadas, diferentemente das nuvens públicas, não há disponibilização de recursos computacionais para todos os utilizadores da Internet, sendo aquela uma variante de computação em nuvem onde os recursos internos de uma organização não são ofertados ao público em geral. A implementação de nuvem privada pode se comportar tanto como uma nuvem pública, embora em escala reduzida. Houve um investimento enorme em recursos para centro de dados ao longo da última década, que possibilitaram a reorientação desses ativos em

direção ao modelo de uso em nuvem. Caso a capacidade de uma nuvem privada seja esgotado ainda é possível combinar nuvens públicas e privadas para o excesso de capacidade ser provisionado em outro lugar, caracterizando assim nuvens híbridas.

O funcionamento de uma nuvem depende das seguintes tecnologias e requisitos: virtualização, API de acesso, armazenamento, banco de dados e, finalmente **elasticidade**. Uma nuvem precisa de elasticidade para ser dinamicamente escalável, maximizando ou minimizando os recursos. Um dos principais atrativos da computação em nuvem é que aplicações podem ser escaladas conforme a demanda que o aplicativo recebe (ROSENBERG; MATEOS, 2011).

## 2.5 Gerência de Redes de Computadores

A gerência de rede tem por finalidade estabelecer as atividades, métodos, procedimentos e ferramentas que pertencem a administração, operação, manutenção e fornecimento dos serviços em redes de computadores. A administração envolve o controle dos recursos. A operação trata dos serviços que a rede oferece e precisam funcionar com fluência, o que inclui o monitoramento constante para ações pró-ativas. A manutenção preocupa com reparações que exerçam melhoramento nos serviços. O fornecimento está preocupado com os recursos necessários para a rede suportar determinado serviço (CLEMM, 2007).

Uma importante aplicação para a administração de servidores é o *Secure Shell* (SSH). Quando este serviço está ativo em uma máquina, permite o acesso seguro por meio de autenticação para assim obter o controle do sistema operacional via terminal de comandos. No cenário, como será visto no capítulo 4, tal protocolo será utilizado nos sistemas reais e virtualizados. O SSH pode ter o acesso automatizado por meio do uso de chaves criptografadas, privada e pública. A chave privada fica restrita ao servidor e os clientes que possuírem a chave pública poderá ter acesso ao servidor sem a necessidade de digitar senha, sendo uma opção para a execução de comandos em séries entre diversos servidores administrados.ssh

### 2.5.1 Documentação

A documentação em redes de computadores tem por função manter os registros sobre a instalação, administração e atividades, pela qual possibilita a criação de uma memória institucional que permite a equipe de administração aumentar o nível de conhecimento e habilidade. Uma maneira simples de criar padrões e auxiliar no processo de documentação é criar um repositório de documentos, uma área de armazenamento. Esta localização central fornece um

ponto de partida para organizar e atualizar os documentos (LIMONCELLI; HOGAN; CHALUP, 2007).

### 2.5.2 Segurança

As políticas são as bases para tudo que uma equipe de segurança faz. As mais comuns em redes de computadores podem ser agrupadas em indentificação e acesso por usuário, o monitoramento e privacidade que usuários e recursos estão sujeitos, padrões para acesso remoto, padrões para acesso a rede (conectividade), e por fim uma política de retenção dos registros de sistemas para consulta em caso de incidentes.

Entre os serviços de segurança, a criptografia é comumente utilizada por aplicações em redes de computadores para proteger a informação caso esta venha a ser capturada. No caso do acesso e controle remoto dos servidores, a utilização de uma aplicação que implemente criptografia nos dados trafegados é altamente recomendada, como por exemplo SSH, que ainda possibilita a utilização de chaves criptografadas como visto na seção 2.5.

O *Transport Layer Security* (TLS) e o *Secure Socket Layer* (SSL) são protocolos para segurança na comunicação na Web e também para outros serviços da Internet. Por meio do serviço de criptografia implementado por estes protocolos é possível garantir a privacidade e integridade entre as mensagens trocadas pelas aplicações.

### 2.5.3 Monitoramento

Sistemas de monitoramento são úteis para detectar e corrigir problemas, identificar a origem dos problemas, prever e evitar problemas futuros, e fornecer dados a gerência de redes. As duas principais formas de monitoramento são reunir os dados de registros relacionados ao uso e disponibilidade, e realizar o monitoramento em tempo real para garantir que os gerentes sejam alertados (LIMONCELLI; HOGAN; CHALUP, 2007).

Para o gerenciamento de redes TCP/IP o protocolo mais comum é o *Simple Network Management Protocol* (SNMP). Este protocolo define como são trocadas as solicitações e o formato de respostas entre duas entidades, um gerente e um agente. Basicamente o protocolo SNMP define duas operações básicas: buscar (GET) e armazenar (SET) cada objeto com um identificador único. O conjunto de todos os objetos que o SNMP pode acessar é definido como *Management Information Base* (MIB), entretanto o padrão só especifica o formato da mensagem e descreve como as mensagens são codificadas, um outro padrão separado especifica variáveis para MIB. Este gerenciamento pode ser utilizado em qualquer dispositivo executando um *software* que per-

mita obter informações SNMP, não apenas equipamentos físicos, mas também aplicações como servidores Web e banco de dados (FRISCH, 2002).

A entidade gerente (*software*) lida com as estações gerenciadas da rede, onde é previsto uma estação para esta função ou *Network Management Station* (NMS). O NMS é responsável por executar uma ação com base nas informações que recebe do agente. A segunda entidade, o agente, é uma aplicação instalada nos equipamentos monitorados. O agente fornece informações gerenciais para o NMS, com intuito de mantê-lo informado sobre o controle operacional de vários aspectos do dispositivo monitorado. O MIB pode ser visto como um banco de dados de objetos gerenciados com as informações enviadas pelos agentes. Qualquer informação que possa ser acessado pela NMS é definida em uma MIB, tais como as informações do sistema operacional e estatísticas de interface, embora possa o agente implementar suas próprias MIBs para cobrir aspectos específicos dos dispositivos de um fabricante em particular (MAURO; SCHMID, 2005).

Em ambientes de monitoramento existem quatro níveis de atividades, inativo, reativo, interativo e pró-ativo, que podem ser identificados na gestão de um serviço ou dispositivo específico. O modo inativo é quando não há monitoramento e a administração da rede recebe alguma notificação sobre determinada falha e ignora, diferenciando do modo reativo apenas no fato deste último reagir a falha tentando resolvê-la. No modo interativo é realizado um acompanhamento manual do sistema em busca de prevenir falhas. Por último, a melhor solução, no modo pró-ativo é realizado o monitoramento automatizado, o qual emite alarmes em casos de falhas, envia notificações aos responsáveis e pode iniciar processos pré-definidos para minimizar o tempo de inatividade (MAURO; SCHMID, 2005).

#### 2.5.4 Salvaguarda da Informação

O uso de aplicações para cópias de segurança ajudam proteger os dados contra imprevistos como exclusões de arquivos acidentais e falhas de *hardware*. Estas aplicações podem acessar remotamente outros sistemas afim de realizar a cópia de dados previamente listados (automação) e ainda copiá-los tanto em disco local como em outras mídias de armazenamento.

Em uma instituição a cópia de segurança pode ser uma atividade relativamente demorada, visto que a tendência dos dados é sempre aumentar, e pode ser que também seja muito despendioso a restauração desses quando necessário. Em ambientes com foco em disponibilidade, ao utilizar de plataformas de virtualização, é possível utilizar de ferramentas para *snapshot* combinadas aos dados relacionados para o correto armazenamento e recuperação das informações.

## 2.6 Controle de versão

Sistema de controle de versão é comumente utilizado para o desenvolvimento de *software*, por prover um repositório em um servidor, o qual aceita conexões de clientes para envio e recebimento de arquivos e informações e associando tais ações a um histórico de todas as transações ocorridas, sendo assim possível resgatar qualquer versão dos documentos.

Segundo Kleine, Hirschfeld e Bracha (2012) existem características diferentes entre sistemas de controle de versão centralizado e descentralizado. Em resumo, o peso das propriedades benéficas e indesejáveis de repositórios centralizados, bem como descentralizados depende dos casos de utilização. Um repositório central pode ser benéfico se o controle de acesso é crítico, mas pode, ao mesmo tempo não ser desejável se nenhuma autoridade central para um projeto existe.

A principal diferença entre esses sistemas está na forma de armazenamento dos registros das transações e alterações no repositório. Enquanto no sistema centralizado o histórico está armazenado apenas no servidor, em sistemas descentralizados o histórico está em cada repositório, conforme se observa nas figuras 2.2 e 2.3 respectivamente.

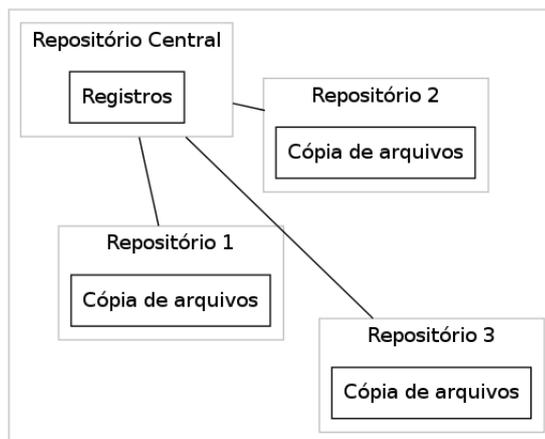


Figura 2.2: Modelo de sistemas de controle de versão centralizado.

Para uma correta utilização deste sistema é recomendado estabelecer políticas para envio de arquivos ao servidor, pois o repositório geralmente é compartilhado entre diversos colaboradores. Para submeter um arquivo ao envio é necessário realizar o *commit* para assim efetivar as alterações no repositório, geralmente esse envio é acompanhado de uma mensagem editada por quem enviou, a fim de facilitar a análise do histórico por outros colaboradores.

No momento do envio, embora raro, pode ocorrer conflito de alteração por coincidir o envio de alterações no mesmo arquivo por usuários distintos. Neste caso, o sistema de controle de versão pode reagir de diferentes maneiras. Ao identificar que o arquivo foi alterado em

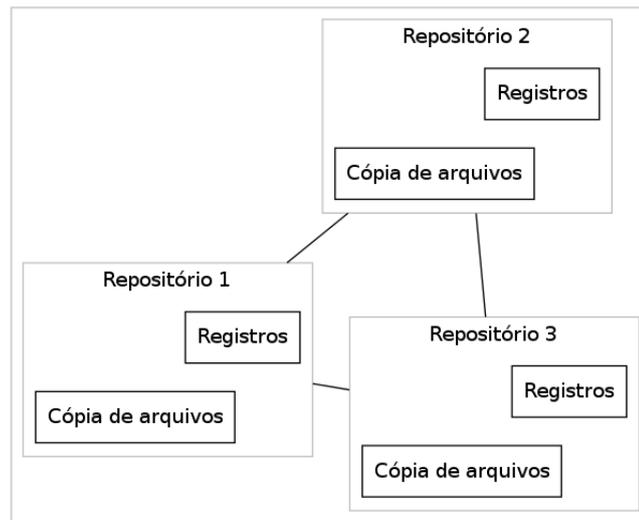


Figura 2.3: Modelo de sistemas de controle de versão descentralizado.

campos diferentes ele poderá utilizar do mecanismo de mesclagem. Nos casos em que não é possível serializar os processos de submissão (*commits*) o sistema pode criar uma cópia para cada modificação e apresentar a diferença entre essas, solicitando assim intervenção manual. Outro mecanismo útil para projetos em sistemas de controle de versão são a marcação de um determinado momento - a versão - do repositório, função a qual pode ser útil para identificar versões estáveis do projeto em desenvolvimento.



José (PoP-SJ) e na figura 3.2 ilustramos as outras redes que estão ligados a este.

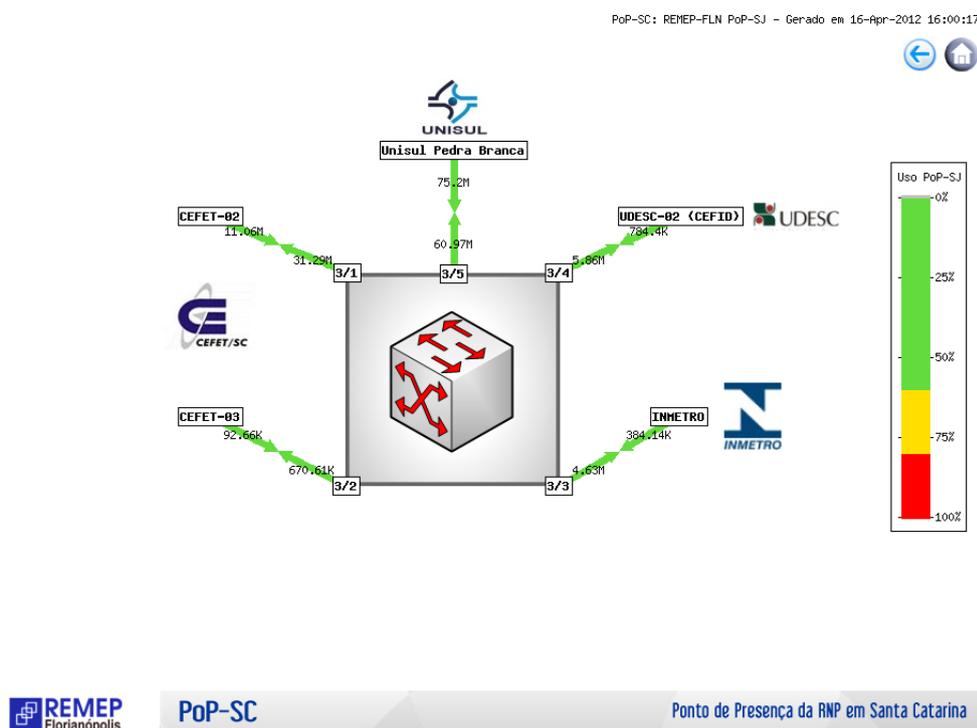


Figura 3.2: PoP-SJ - fonte: <http://rnp.br>

A WAN do IFSC é uma solução estável e suficiente em transmissão e adequada para implementação de tecnologias de computação em grade e até mesmo em nuvem. Como visto na seção 2.4, a computação em grade é constituída por organizações virtuais que compartilham recursos em redes de longas distâncias. O IFSC-SJ possui enlaces de fibras ópticas e disponibilidade de taxas transmissão para troca de informações entre outras instituições do IFSC, possibilitando o compartilhamento de recursos em nível de WAN, caracterizando assim a viabilidade de computação em grade.

## 3.2 Rede Interna

Vistas as condições de infraestrutura externas pertencentes a WAN dessa rede em questão, agora analisaremos as características internas. Existe disponível no IFSC-SJ uma sala para os servidores, a qual tem em seu espaço alocado para os servidores, equipamentos de redes e inclusive o *backbone* do PoP-SJ. Os *switches* dessa sala estão conectados com outros dois armários, a fim de distribuir os pontos de redes por bloco (predial). Atualmente a configuração desses *switches* estão sem fazer uso das tecnologias para agregação de enlace, VLANs e STP e empilhamento, conforme mencionadas no item 2.1.2 como boas práticas para tolerância a falhas

e facilidade de configuração.

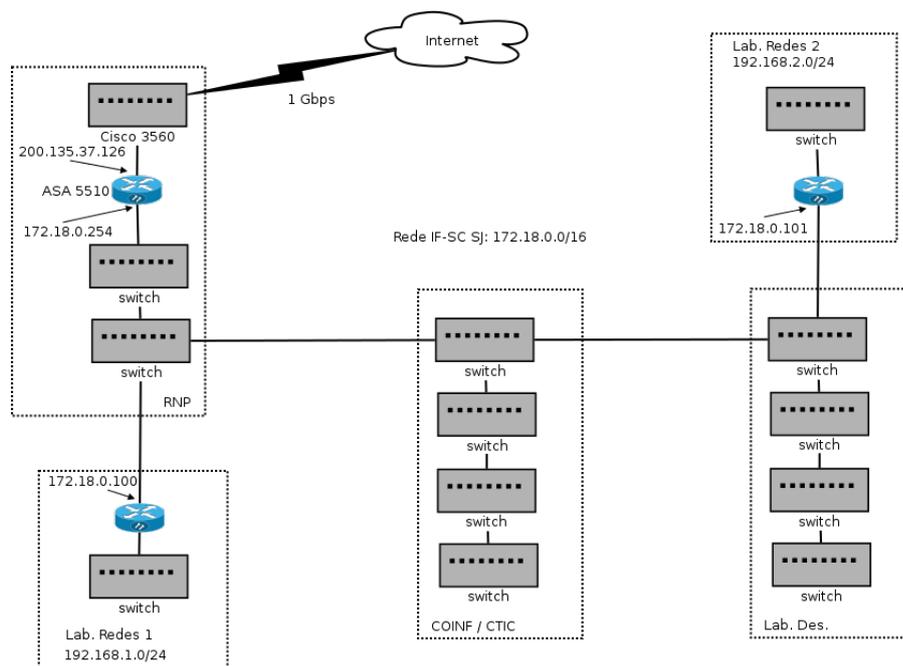


Figura 3.3: Modelo atual de rede do IFSC-SJ.

### 3.3 Serviços

Os serviços oferecidos pela infraestrutura lógica de redes de computadores da Instituição podem ser divididos entre aqueles acessados apenas pela LAN, usuários internos, e aqueles acessados também por conexões oriundas da WAN, usuários externos.

Os serviços disponíveis para acesso de fora da instituição são predominantemente do tipo Web: *sites*, portais, wiki, blogs, arquivos disponibilizados por meio de servidores HTTP - conforme apresentado na tabela 3.1. Apesar de ser a única aplicação vista para os usuários comuns e externos, uma vez realizado a solicitação por este serviço via cliente (navegador) é desencadeado o atendimento, processamento e assim pode ser necessário acesso a outros serviços internos da rede, como os bancos de dados das aplicações Web, autenticação em LDAP para usuários registrados entre outros. Desta forma o serviço HTTP está disponível aos usuários para a WAN que por sua vez interage com os demais serviços restritos a LAN quando necessário.

No ambiente da LAN, é utilizado o DHCP para fornecer IP para todas as estações, tanto via rede cabeada quanto conexões realizadas por dispositivos sem fio. Outros serviços estão presentes, como os diretórios DNS e LDAP para resolução de nomes de máquinas a autenticação de usuários, respectivamente.

Aplicação	URL
Portal	<a href="http://www.sj.ifsc.edu.br">http://www.sj.ifsc.edu.br</a>
Wiki	<a href="http://wiki.sj.ifsc.edu.br">http://wiki.sj.ifsc.edu.br</a>
Aplicação SIGA	<a href="http://siga.sj.ifsc.edu.br">http://siga.sj.ifsc.edu.br</a>
Blog Integrado	<a href="http://integrado.sj.ifsc.edu.br">http://integrado.sj.ifsc.edu.br</a>
Repositório DAV do Integrado	<a href="http://integrado.sj.ifsc.edu.br/arquivos">http://integrado.sj.ifsc.edu.br/arquivos</a>
Blog Tele	<a href="http://tele.sj.ifsc.edu.br">http://tele.sj.ifsc.edu.br</a>
Repositório DAV de Tele	<a href="http://tele.sj.ifsc.edu.br/arquivos">http://tele.sj.ifsc.edu.br/arquivos</a>
Moodle de Tele	<a href="http://tele.sj.ifsc.edu.br/moodle">http://tele.sj.ifsc.edu.br/moodle</a>
Projetos de Tele	<a href="https://tele.sj.ifsc.edu.br/projetos">https://tele.sj.ifsc.edu.br/projetos</a>
Gerência da Rede	<a href="https://monitoaramento">https://monitoaramento</a>

Tabela 3.1: Aplicações e URLs do IFSC-SJ.

Quanto aos sistemas operacionais dos servidores, são em sua maioria Linux (Debian GNU/Linux) virtualizados sobre a plataforma VMWare ESXi. São dois servidores físicos responsáveis por virtualizar 21 sistemas, sendo que desses 10 possuem servidor Web em operação (tabela 3.2, o qual caracteriza a importância do serviço HTTP nesta rede.

Serviços	Quantidade	Ambiente
Servidor HTTP	10	Virtualizado
Servidor SGBD	1	Virtualizado
Servidor LDAP	1	Virtualizado
Servidor DNS	1	Virtualizado
Servidor SMB/CIFS	1	Físico

Tabela 3.2: Serviços oferecidos na rede IFSC-SJ.

O modelo atual de gerenciamento de máquinas virtuais, como se percebe na figura 3.2 não é eficiente, pois serviços críticos como DNS e LDAP não têm suporte a redundância. As próprias aplicações Web não estão replicadas em vários servidores: cada um deles possui a sua própria lista distinta. Além disso, essa configuração é alocada de forma ineficiente as máquinas virtuais, como memória e espaço em disco - hoje recursos escassos, estabelecendo uma competição muito grande por recursos entre as máquinas virtuais.

Como exemplo, tem-se o servidor `integrado.sj.ifsc.edu.br`, cujos uso dos recursos podem ser vistos na figura 3.4. Os casos relatados sobre esse servidor, em particular, é que o mesmo trava antes mesmo de informar ao gerente de monitoramento e de contabilização - a coleta periódica utilizando SNMP ocorre a cada 5 minutos, e não há configuração de *traps*. Tais ocorrências são bastante perceptíveis na figura: são as lacunas visíveis nos gráficos.

Outros servidores físicos fazem também parte da rede e responsável por outros serviços, porém não pertencentes a sistemas virtualizados. A lista disponível na tabela 3.2 contempla os

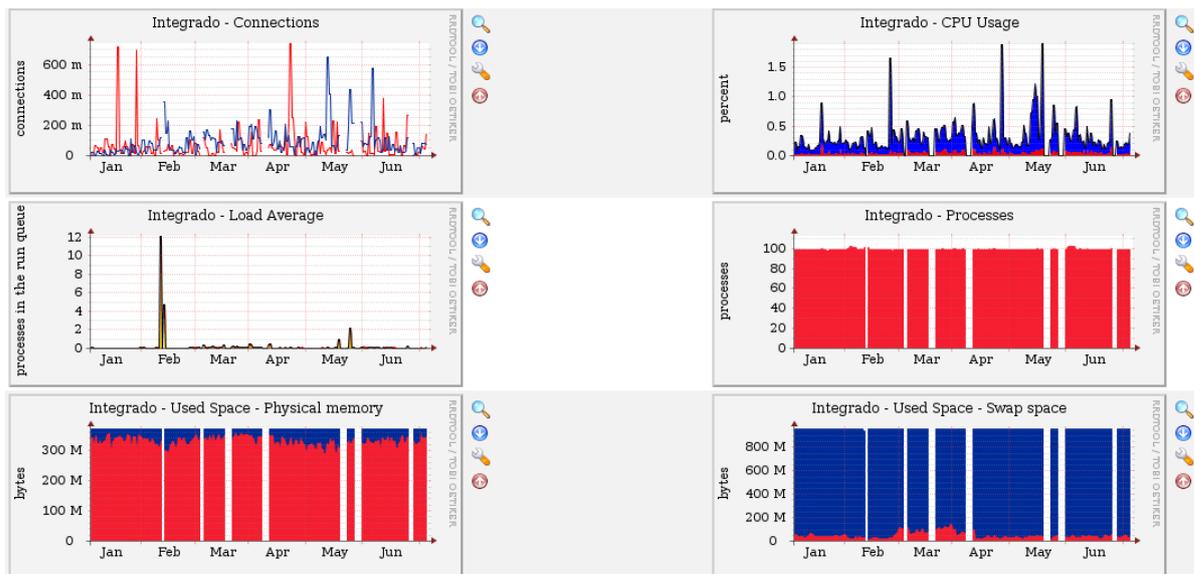


Figura 3.4: Contabilização do servidor integrado.

serviços, as quantidades e ambiente de execução desses.

## ***4 Proposta da Nova Rede***

Durante a análise deste projeto foi visto que a aplicação de maior importância no IFSC-SJ, quantitativo e qualitativamente, é o servidor HTTP. Nesse trabalho, portanto, será apresentada uma proposta para reformulação desse, que vai ao encontro as exigências de soluções baseadas em SaaS.

### **4.1 Visão geral**

Atualmente a rede do IFSC-SC é caracterizada por poucos acessos de clientes, em média esparsos e raros casos com grande acesso (poucos picos mas significativos). Para o número de clientes podemos afirmar que existem muitos servidores com poucos recursos. A ideia para este projeto é mudar a quantidade de servidores, almejando ter condições de atender quando necessário muitos clientes com uso de poucos servidores, sendo mais eficientes e melhor adequado a esse cenário. Esta configuração será concebida de forma a garantir escalabilidade, visando atender crescimento ou expansões futuras desta rede, com vistas a contemplar futuras nuvens privadas na instituição.

Com o objetivo de garantir uma infraestrutura mais adequada para o fornecimento de serviços em aplicações Web, é apresentada uma solução de configuração para a plataforma de virtualização de maneira a atender a carga, a qual se caracteriza, como já mencionado, por raros momentos de pico e grandes períodos de ociosidade. Esta plataforma contém sistemas virtualizados e configurados para serem servidores Web e de banco de dados. Estes fazem um auto balanceamento das requisições oriundas dos clientes.

Para maior aproveitamento dos recursos são previstos de 2 a 3 servidores por aplicação, dependendo da carga já estimada pela gerência de contabilização, e quando os recursos expandirem e as necessidades aumentarem poderão ser adicionados mais servidores a este ambiente de forma prática, uma vez que se trata de um aglomerado, como visto na página 22.

A fim de garantir maior tolerância a falha dos serviços prestados, será necessário propor

também alterações na camada de Enlace (modelo OSI), para que seja possível utilizar tecnologias nos *switches* que garantam mais segurança e redundância a esta rede (página 20). Nessa camada será necessário configurar os equipamentos a fim de oferecer os requisitos demandados. Esse assunto será melhor visto na seção 4.6.

Visto que a grande maioria dos serviços prestados pelo IFSC-SJ são Web e acessíveis fora da instituição, foi também necessário apresentar uma nova proposta de segurança para essa rede. Por ser orientado a SaaS, a estrutura dessa rede conta como principal protocolo o HTTP. Serão também apresentadas as soluções para os serviços auxiliares a este serviço, tendo em vista segurança e autenticação a esta rede, abrangendo: banco de dados, diretórios e resolução de nome para domínios. Além disso, utilizar-se-ão também novas técnicas de gerência com auxílio de aplicações para controle de versões distribuídos e, não obstante, atender a necessidade de uso de mais tecnologias na camada de enlace, por meio da configuração e rearranjos dos *switches*.

As instalações e configurações de sistemas operacionais e equipamentos devem seguir um criterioso procedimento de documentação. O servidor de monitoramento, o qual conterá o sistema de controle de arquivos, está previsto para armazenar tais arquivos, de forma que estejam disponíveis para rápida consulta e/ou restaurações dos serviços dessa rede, o qual dependerá do seguimento destas políticas por parte dos administradores, devem enviar e registrar arquivos importantes a configuração para o devido repositório e ainda documentar procedimentos em plataforma colaborativa, no caso a já operacional *wiki*<sup>1</sup>.

## 4.2 Distribuição dos Serviços e dos Servidores

Para a adequação do atual cenário ao novo modelo, é necessário a reformulação da plataforma de virtualização utilizada. Atualmente são dois computadores com instâncias independentes, sem qualquer relação direta entre si. Com a utilização de soluções em aglomerado, é possível tornar este ambiente mais confiável. Utilizando ainda as duas máquinas, porém agora com o intuito de obter redundância de plataforma física, assim, caso ocorra uma falha em uma dessas será possível continuar a operação por meio da outra máquina - que possui os mesmos serviços ativos. Para exemplificar, o *hypervisor* VMware ESXi, atual sistema utilizado como plataforma de virtualização pelo IFSC-SJ, possui tecnologias para identificação de quedas de enlaces e aproveitamento do cruzamento das vias de transmissão a fim de contornar falhas caso uma interface fique indisponível. Porém, cabe destacar que essa versão em particular (ESXi) não faz migração de serviços ou de sistemas “a quente” (*live migration*).

---

<sup>1</sup>[http://wiki.sj.ifsc.edu.br/wiki/index.php/Portal\\_da\\_Coordenadoria\\_de\\_Inform%C3%A1tica](http://wiki.sj.ifsc.edu.br/wiki/index.php/Portal_da_Coordenadoria_de_Inform%C3%A1tica)

Esta proposta visa oferecer uma plataforma que contenha os servidores Web, de diretórios e de bancos de dados, arquitetados de forma a utilizar corretamente as vantagens de ambientes virtuais, previsto pela utilização de aglomerado para disponibilidade e desempenho destas aplicações. Ainda acrescenta à solução facilidades na administração e atualização dos sistemas, visto que facilmente é possível fazer o *backup* de *snapshot* associado aos seus dados, e caso aconteça alguma modificação indesejada ou atualização mal sucedida é possível restaurar a instância de forma relativamente rápida comparado ao sistemas não virtualizados, como já mencionado na página 28.

Devido a redundância projetada para a rede, os servidores precisam ter configuração equivalente, necessitando que para cada servidor instalado seja previsto previamente um modelo de instalação, para assim facilitar a distribuição de serviços para este tipo de servidor. Esse conceito de modelos de máquinas é bastante comum na criação de máquinas virtuais, cujo objetivo principal é a sua rápida implantação (*deployment*).

## 4.3 Serviço de Conexão e de Processamento

### 4.3.1 Servidor HTTP

O protocolo HTTP serve como base para vários serviços presentes em redes de computadores, que vão além do escopo de ser apenas um servidor de páginas HTML, como visto na seção 2.1.1. O servidor HTTP conta com funcionalidades que centralizam diversos serviços da rede nesse protocolo. Entre essas funcionalidades, estão presente a transferência de arquivos, autenticação, autorização e criptografia.

Com o aumento de aplicações Web nos últimos anos são visíveis as melhorias que foram feitas nos servidores HTTP em busca de atender este crescimento. Um dos principais avanços nesse sentido foi o refinamento de balanceamento de carga para servidores, visto que em muitos cenários apenas um servidor não é capaz de suportar o número de requisições solicitadas, seja por limitação da aplicação e/ou por recursos de máquina. Para este trabalho, foi vislumbrada uma opção de balancear a carga do servidor HTTP para, assim, cobrir a necessidade de atendimentos conforme demanda de requisições de clientes *vs.* recursos.

Utilizando balanceamento de carga no servidor HTTP como visto na seção 2.3.1, é esperado otimizar a utilização de recursos, maximizar o desempenho, minimizar o tempo de resposta e evitar sobrecarga no servidor. Uma opção muito simples e prática para balanceamento de carga é o uso de *proxy* reverso. A distribuição de carga entre vários servidores pode ser feita por esse

tipo de *proxy*, sendo cada servidor responsável pela sua própria aplicação. Caso seja necessário, o *proxy* reverso ainda pode modificar URLs válidas externamente para os endereços da rede interna de forma transparente ao usuário final.

O servidor Web atualmente utilizado pelo IFSC-SJ é o Apache - inclusive é a aplicação mais popular para esse serviço, responsável por hospedar cerca de 70% de todos os *sites* da Internet (S.TANENBAUM; STEEN, 2006). No Apache o balanceamento de carga é contemplado pelo módulo *proxy balancer* que implementa justamente o conceito de *proxy* reverso com garantia dos estados das sessões: o balanceamento se dá por sessão, e não por requisição, preservando assim todas as funcionalidades da maioria das aplicações Web.

Para cada domínio no IFSC-SJ existem arquivos de configurações disponíveis no Apache que passarão ser reconfigurados com parâmetros para balanceamento de carga e os IPs dos demais servidores. Para isso, com um único IP publicado no serviço DNS, é possível organizar diversos outros IPs sobre interfaces virtuais que serão configurados nos sistemas operacionais, os quais farão o balanceamento. Nesse cenário de *proxy* reverso é necessária a utilização de técnicas de *heartbeat* (também já visto na seção 2.3.1) para acompanhar a disponibilidade do processo de gerenciamento do servidor Web, e evitar a falha global do sistema. Assim, uma aplicação *heartbeat* precisa monitorar constantemente o serviço e caso identificada a falha poderá transferir a atribuição dessa a outra, mantendo o serviço em operação. A figura 4.1 ilustra um cenário reduzido da solução: um servidor “visível” com *proxy* reverso para dois serviços “invisíveis”.

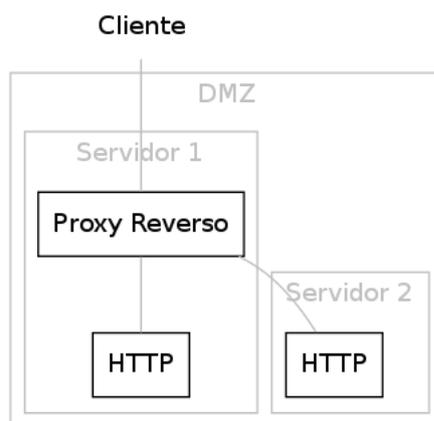


Figura 4.1: Modelo de *proxy* reverso.

## 4.4 Serviços de diretórios

O DNS é um serviço presente nessa rede, porém não tolerante a falhas. O mesmo se aplica ao LDAP, outro serviço de extrema importância para o controle de acesso a rede e aplicações, visto a necessidade de unificar a base de dados referente a informações de todos os usuários das diversas unidades do IFSC. Em busca de melhorar este serviço já foi apresentado um trabalho a esta instituição para análise (OLIVEIRA, 2010).

Para esta nova proposta, os serviços estarão replicados em duas máquinas virtuais com os mesmos dados, e serão publicados os dois endereços no DNS com balanceamento de carga com o mesmo nome de máquina, uma vez que os dados são espelhados - embora essa solução não seja tão robusta quanto *proxy* reverso, que provê nenhuma perda nas trocas de mensagens.

## 4.5 Serviços de armazenamento de dados

### 4.5.1 Sistema de Gerenciamento de Banco de Dados

Segundo Date (2003), quanto a implementações comerciais, a maior parte dos produtos para SGBD oferece algum suporte para bancos de dados distribuídos e com variados graus de funcionalidades. Isso faz com que dificulte uma abordagem genérica para implementação de SGBD. Assim, este trabalho irá focar em uma solução para banco de dados distribuído específica para o SGBD já em uso no IFSC-SJ: MySQL.

Como definido anteriormente, na seção 2.3.1, foi falado sobre **disponibilidade**, o que em um SGBD pode se aplicar o conceito de aglomerado. Em 2004, foi disponibilizado o *MySQL Cluster*, com o intuito de permitir configurações do MySQL para alta disponibilidade e desempenho, sendo esse um mecanismo de armazenamento adicional implementado no MySQL chamado por *Network Data Base* (NDB). O MySQL Cluster é configurado independentemente dos servidores MySQL. Para o funcionamento do MySQL Cluster são previstos variados tipos de processos, em uma instalação mínima são necessários três destes processos, conforme Oracle (2012), os quais são listados conforme funcionalidades a seguir:

- **Processo de acesso** (*mysqld*): esse é um nó que acessa os dados do cluster. No caso do MySQL Cluster, um nó de SQL é um servidor MySQL tradicional que usa o mecanismo de armazenamento NDB.
- **Processo de gerenciamento** (*ndb\_mgmt*): esse processo tem por finalidade gerenciar todos os demais processos, com o fornecimento de dados de configuração, portanto é o

primeiro processo a ser iniciado.

- **Processo de armazenamento (ndbd):** esse processo é reponsável por armazenar dados no cluster. Uma réplica é suficiente para armazenamento de dados, mas não fornece nenhuma redundância, portanto, é recomendado ter dois (ou mais) réplicas para proporcionar redundância e, assim, a disponibilidade elevada.

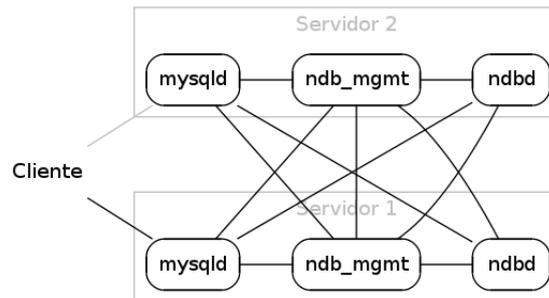


Figura 4.2: Modelo de aglomerado em MySQL.

Na figura 4.2 é possível verificar uma proposta de configuração para o MySQL Cluster utilizando de configurações mínimas para obter a redundância deste serviço. Para uma configuração mais robusta em busca de desempenho é possível, ao utilizar o MySQL Cluster Manager, implementar um conjunto de agentes. O administrador conecta o cliente MySQL regular para qualquer um desses agentes e, em seguida, os agentes de cada comunicam-se uns com os outros, conforme figura 4.3. Os agentes trabalham em conjunto para executar operações em todos os processos que compõem o aglomerado.

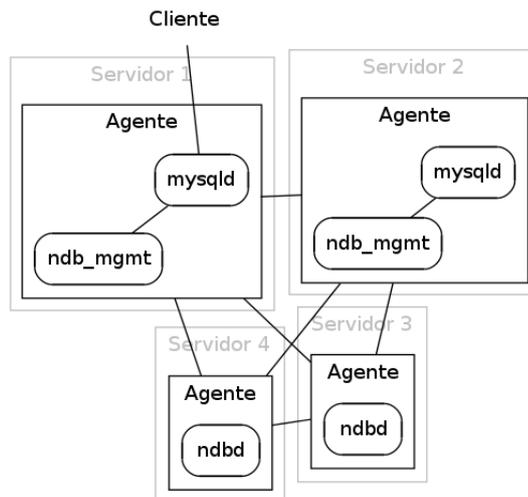


Figura 4.3: Modelo do *Cluster Manager* em MySQL.

## 4.5.2 Controle de Versão

Com o intuito de facilitar a gerência desta rede foi concebido um conjunto de repositórios descentralizados (corente ao padrão de redundância proposto a esta rede de forma geral) para gestão da configuração de equipamentos e aplicações. Permitirá, assim, a organização de diferentes versões de arquivos que são passíveis de alterações da rede.

Embora não seja comum, um sistema de controle de versão pode ser aplicado para gestão da configuração de equipamentos e aplicações em redes de computadores. Utilizando de sistemas de controle de versão distribuídos é possível obter algumas vantagens para esse fim que são a distribuição dos arquivos para espelhamento dos serviços nas máquinas de redundância, recuperar cenários de forma equivalente a um *backup* e concentrar em única estrutura de dados as informações sensíveis a administração da rede.

O servidor responsável por armazenar este sistema de controle de versões será o servidor de monitoramento, por possuir acesso a todas as outras máquinas utilizando SSH (página 26). Por meio desse a rede terá diversos arquivos importantes armazenados em repositórios especificados conforme tabela 4.1.

Repositório	Descrição
Processamento	Arquivos do S.O. e código das aplicações Web.
Armazenamento	Arquivos do S.O. e arquivos de configuração dos diretórios e dos bancos de dados.
Rede	Arquivos de configuração dos equipamentos de rede.

Tabela 4.1: Proposta de repositórios em sistema de controle de versão.

A criação deste repositórios visa atender a necessidade por estabelecer políticas de armazenamentos e registros de atividades de manutenção a essa rede. Um caso específico será a utilização deste repositório como controlador dos arquivos Web acessados pelo servidor HTTP, sendo esta uma solução para que todos os servidores ligados ao *proxy* estejam com os arquivos iguais, fundamental para o funcionamento da distribuição de carga entre esses.

Os arquivos Web serão separados em dois grupos distintos, os códigos de aplicação e arquivos de usuários. Os códigos de aplicação são os arquivos acessíveis apenas a programadores, com versões controladas, enquanto arquivos de usuários são adicionados por meio de *upload* pelos usuários por essas aplicações disponíveis na rede. Quando houver a necessidade de editar os códigos de aplicação, é prevista uma máquina a parte para este fim, chamada de **servidor de atualização**. Essa máquina estará acessível apenas aos programadores dessas aplicações. Esta máquina é necessária para que não ocorra o risco de, quando uma aplicação for atualizada, gerar inconsistências entre os diretórios Web em produção. Uma vez carregados os novos arquivos

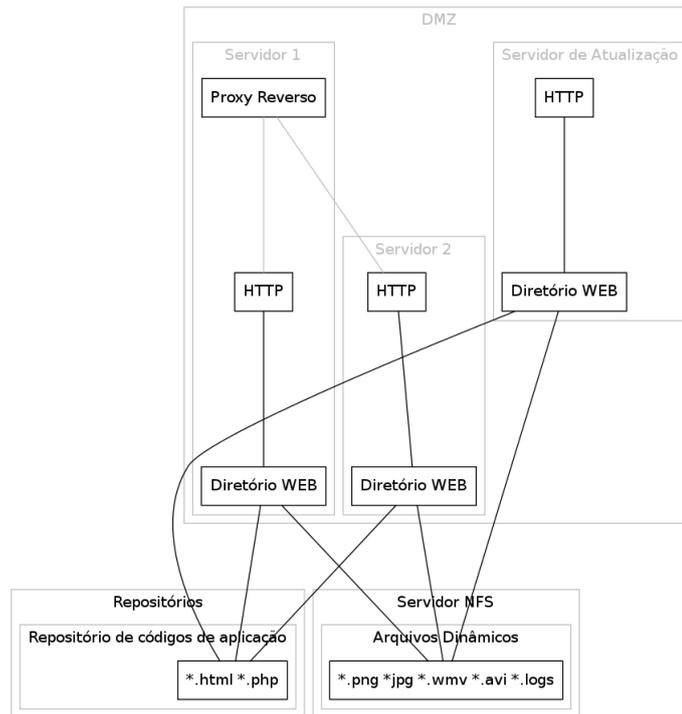


Figura 4.4: Proposta para diretórios Web em sistemas de controles de versão.

no servidor de atualização, uma rotina será rodada em todos os servidores Web para sincronizar os repositórios.

Quanto aos arquivos de usuários, não haverá controle de versão. Ao invés disso, será utilizado um serviço único, o qual será responsável por compartilhar a todos os servidores Web, via NFS, esses arquivos.

## 4.6 Camada de Enlace

Para a camada de Enlace, estão previstas alterações nas configurações dos *switches*. Segundo Limoncelli, Hogan e Chalup (2007), em uma LAN a criação de uma rede sobreposta geralmente significa criar uma rede simples com topologia física plana e fazer uso de VLAN para cobrir as sub-redes que os clientes precisam, para ser possível usar enlaces de alta velocidade redundantes, todos mediados na camada de enlace. As tecnologias devem seguir uma ordem de implementação, visto a dependência e relações entre essas, conforme enumerado abaixo:

1. **STP**: tolerância a falhas inter-*switch*, cuja implementação é feita diretamente nos *switches* e pontes ao se definir a árvore de dispositivos mediante atribuição de pesos e prioridades.

2. **Empilhamento de switch:** sempre que houver equipamentos com mesmo *hardware* e versão do *software* ou *firmware*, cuja implementação é específica por fabricante (uso de conectores e cabos específicos). Sem o empilhamento de *switch*, não será possível implementar plenamente agregação de enlace com redundância a falha física.
3. **Agregação de enlace:** tolerância a falhas e combinação de velocidades inter-portas, onde duas ou mais portas de rede são combinadas em uma única porta lógica.
4. **Redes virtuais (VLAN):** segregação dos domínios de *broadcast* para efeitos de segurança e facilidade de administração, conforme a figura 4.5, utilizando para tal marcação de pacotes com o padrão 802.1Q - bem aceito em ambientes heterogêneos como em IFSC-SJ. Na figura 4.5, estão identificadas as *tags* (marcações) numéricas relacionadas aos contextos (sub-redes) da rede do campus.
5. **802.1X:** uma vez que já estão identificados todos os pontos de acesso, é possível agora utilizar autenticação de acesso tanto em meio cabeado como sem fio, sendo que o ingresso à rede se faz mediante autenticação e autorização por um controle centralizado. No caso do IFSC-SJ, isso se dá com o protocolos RADIUS.

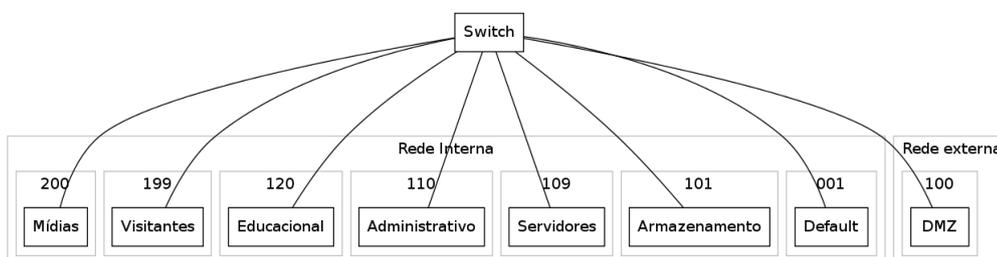


Figura 4.5: Novo modelo de rede proposto para redes virtuais.

## 4.7 Serviços para Usuários Finais

Os usuários dessa rede podem ter acesso a mesma utilizando meio cabeado ou sem fio. As redes sem fio disponíveis no IFSC-SJ atualmente exigem autenticação por chave compartilhada, a qual é uma situação de extremo risco, dada a quantidade de pessoas que circula no campus: aproximadamente 250 servidores e 1350 alunos<sup>2</sup>.

Em suma, tanto para acessos sem fios quanto cabeados serão reformulados para fazer uso das VLANs: os pontos de rede cujos usuários finais são regulares, como salas da administração

<sup>2</sup>Dados obtidos pelo sistema SIGA (<http://siga.sj.ifsc.edu.br>).

do campus, serão diretamente identificados e marcados na VLAN específica. Já os pontos públicos, ou de usuários finais sem procedência conhecida, como por exemplo salas de aula e auditórios, será exigida a autenticação (802.1X) para posterior autorização na VLAN relacionada: administrativa (110) para técnicos administrativos e pedagógica (120) para docentes e alunos. Haverá ainda uma terceira opção, a VLAN de visitante, que não requer autenticação, porém terá somente acesso à Internet e vazão reduzida para inibir o seu uso de forma irrestrita.

Após a autenticação, ficarão disponíveis os seguintes serviços:

- **Indiretos**, de configuração automática ou informado manualmente com o auxílio do corpo técnico da rede: DHCP, *Network Time Protocol* (NTP), DNS, *Windows Internet Name Service* (WINS) e LDAP.
- **Diretos**, usados pelo usuário final: SMB/CIFS e HTTP. O serviço CUPS, por ser baseado em HTTP, será mapeado sobre o mesmo.

Para finalizar, a figura 4.6 mapeia as dependências entre as principais aplicações da rede, com ênfase em SaaS.

Embora exista ainda aplicações que não são do tipo Web no IFSC-SJ, tanto para o setor administrativo quanto para o setor educacional, acreditamos que com as tendências de desenvolvimento em soluções SaaS, os fornecedores destas podem vir a apresentar versões em Web. Prova disso são empresas que tradicionalmente ofertavam aplicativos no modelo tradicional, como por exemplo Adobe e Microsoft, já estão apresentando versões adaptadas para esse modelo de negócio e sobre HTTP. Em contrapartida, existe a possibilidade de adaptar o acesso a interface de aplicações tradicionais para que sejam acessíveis pela Web, por meio de utilização de acesso remoto gráfico incorporado a navegadores com utilização de Javascript e *applets* Java. Tais aplicações não são maiorias nessa instituição e ainda são necessárias, assim mantiveram-se inalteradas as configurações e instalações para estes sistemas, visto que não se encaixam em um ambiente SaaS. Por enquanto.

## 4.8 Gerência

A proposta de gerência para essa rede busca auxiliar na disponibilidade e segurança dos serviços existentes por meio de políticas para manutenção, atualização, monitoramento, acessos e contabilização das informações desses serviços.

A manutenção de todos os serviços consiste em acesso remoto aos servidores, virtualizado-

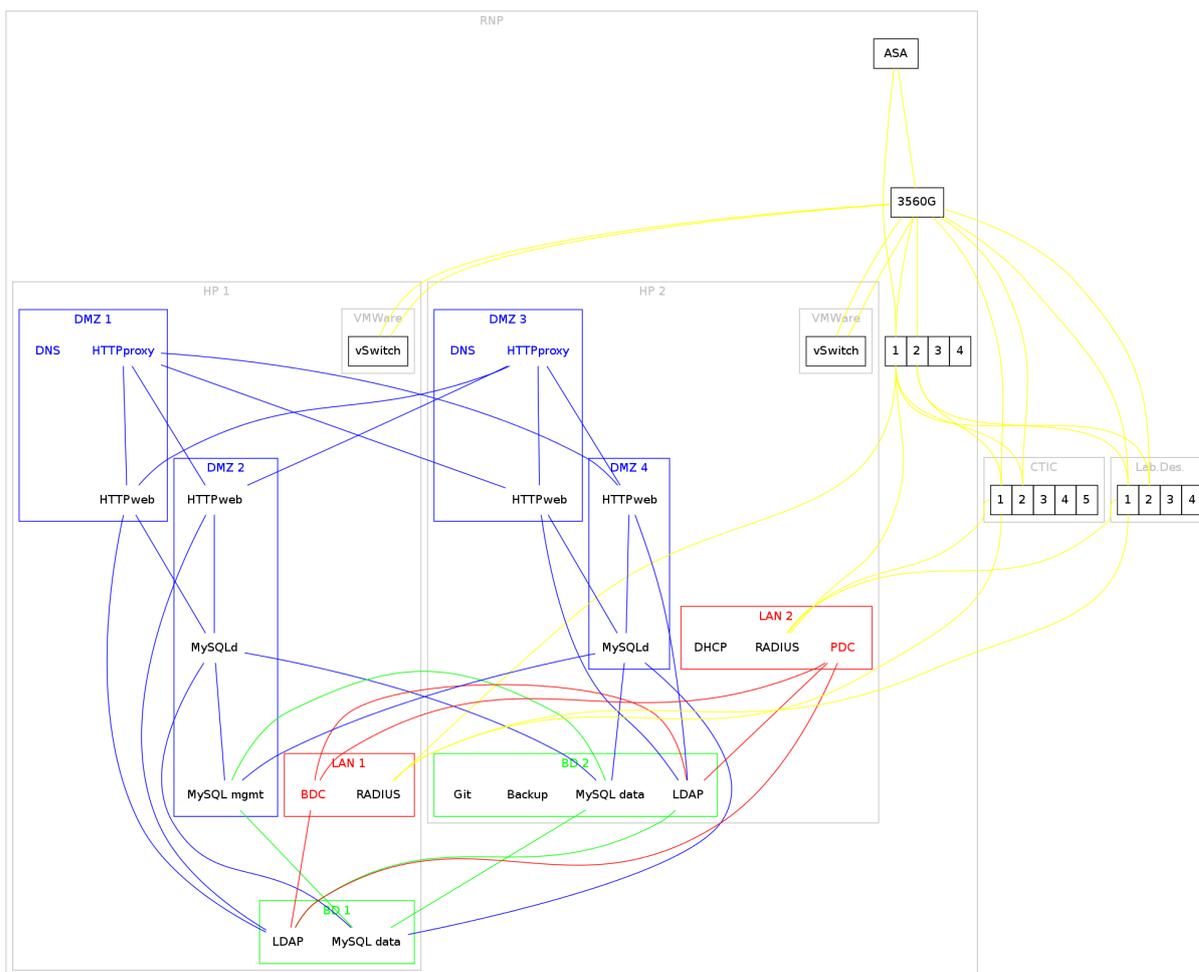


Figura 4.6: Visão geral dos serviços no novo modelo de rede concebido.

res e virtualizados, por meio do qual é prevista a implementação de um política rígida de acesso para esses, somente a máquina de monitoramento poderá ter controle remoto dos servidores dessa rede utilizando esquema de chaves públicas para autenticação. Assim, será previsto a utilização de *scripts* para emissões de comandos em série para um ou mais servidores quando necessário: atualização do sistema, sincronização com os repositórios de controle de versão e outros. Essa política de controle remoto centralizado visa focar o controle a partir de uma única máquina, caracterizando-a por uma estação do tipo NMS (secção 2.5.3, a qual para esse fim também realizará o monitoramento da rede por meio do SNMP, utilizando de uma *Structure of Management Information* (SMI) e gerenciar informações das MIBs - específicas para cada agente - para contabilização dos serviços e geração de relatórios.

Para salvaguarda da informação será utilizado um sistema gerenciador próprio para este fim, como atualmente é feito, a partir do qual são armazenados em mídia removível. Entretanto, será adicionada mais uma política para este serviço conforme citado no item 4.5.2. Por meio do sistema de controle de versão, é possível obter rápido acesso as mudanças de configuração

---

dessa rede, bem como arquivos para rápida restauração, sendo que em muitos casos apenas esses repositórios podem ser necessários para determinadas restauração. Quando a situação for mais crítica, e os repositórios não atender esta necessidade, será então necessário a restauração via sistema gerenciador de *backup*.

## 5 *Conclusões*

Este trabalho concentrou os esforços no sentido de melhorar a infraestrutura do IFSC-SJ por meio de uma proposta para melhorias nas instalações e configurações de equipamentos, sistemas operacionais e aplicações com foco em sistemas distribuídos, no intuito de obter maior disponibilidade e segurança aos recursos e serviços oferecidos nesta organização.

Esta proposta abrange um conjunto de alterações na rede de computadores do IFSC-SJ, o qual afeta toda a infraestrutura, em particular camadas baixas e altas, tendo assim alto impacto na atual organização. Todas as soluções propostas neste trabalho são possíveis de serem configuradas, visto que não foram inventadas; porém, não é possível prever as variações que podem ocorrer pelos diferentes tipos de aplicação para o mesmo serviço, ou suas diferentes versões. Entretanto, o conceito e a finalidade da configuração pouco têm a mudar a curto prazo.

Foram sugeridos a readequação da plataforma de virtualização, que abrangem as aplicações Web e de banco de dados. Em ambos os casos foram mostradas soluções baseadas em sistemas distribuídos, somado ao controle de versão com a função de administração de sistema, visando assim facilitar o sincronismo e a restauração de arquivos passíveis de configurações.

Com o foco em SaaS, esta proposta direciona a infraestrutura atual ao serviço Web e elaborou estudos sobre a disponibilidade e segurança utilizando sistemas distribuídos. Trabalhos futuros podem avançar o estudo sobre a implementação de computação em grade, os quais podem buscar soluções para aproveitamento das infraestrutura dispersas geograficamente, pois outros *campi* também possuem centro de dados, que podem ser vistos como organizações virtuais em um ambiente de grade em WAN para assim ser possível unificar o sistema em nível estadual.

Ainda em trabalhos futuros pode ser elaborado um estudo de implementação de nuvem privada no IFSC, pois como visto este modelo acrescenta mais praticidade na entrega dos recursos ao separar os serviços antes visto como um só, em *software*, plataforma e infraestrutura. A nuvem ainda disponibiliza de um conceito chave que é a **elasticidade**, sendo um ambiente com alocações de recursos altamente dinâmico.

## *Lista de Abreviaturas*

**API** *Application Programming Interface*

**ASP** *Application Service Provider*

**CIFS** *Common Internet File System*

**CUPS** *Common Unix Printing System*

**DAP** *Directory Access Protocol*

**DHCP** *Dynamic Host Configuration Protocol*

**DNS** *Domain Name Server*

**HTML** *Hypertext Markup Language*

**HTTP** *Hypertext Transfer Protocol*

**IaaS** *Infrastructure as a Service*

**IANA** *Internet Assigned Numbers Authority*

**IFSC** *Instituto Federal de Santa Catarina*

**IFSC-SJ** *Instituto Federal de Santa Catarina de São José*

**IP** *Internet Protocol*

**ITU-T** *ITU Telecommunication Standardization Sector*

**LACP** *Link Aggregation Protocol*

**LAN** *Local Area Network*

**LDAP** *Lightweight Directory Access Protocol*

**MIB** *Management Information Base*

**NDB** *Network Data Base*

**NFS** *Network File System*

**NMS** *Network Management Station*

**NPD** Núcleo de Processamento de Dados

**NTP** *Network Time Protocol*

**OSI** *Open Systems Interconnection*

**PaaS** *Platform as a Service*

**PoP-SC** Ponto de Presença da RNP em Santa Catarina

**PoP-SJ** Ponto de Presença da RNP em São José

**RNP** Rede Nacional de Pesquisa

**SaaS** *Software as a Service*

**SGBD** Sistema de Gerenciamento de Bancos de Dados

**SIP** *Session Initiation Protocol*

**SMB** *Server Message Block*

**SMI** *Structure of Management Information*

**SMTP** *Simple Mail Transfer Protocol*

**SNMP** *Simple Network Management Protocol*

**SPOF** *Single Point of Failure*

**SQL** *Structured Query Language*

**SSH** *Secure Shell*

**SSI** *Single System Image*

**SSL** *Secure Socket Layer*

**STP** *Spanning Tree Protocol*

**TLS** *Transport Layer Security*

**URL** *Uniform Resource Locators*

**VLAN** *Virtual Local Area Network*

**WAN** *Wide Area Network*

**WebDAV** *Web-based Distributed Authoring and Versioning*

**WINS** *Windows Internet Name Service*

## *Referências Bibliográficas*

- ANTONOPOULOS, N.; GILLAM, L. *Cloud Computing: Principles, systems and applications*. 1. ed. Estados Unidos: Springer, 2010.
- BLANK, A. G. *TCP/IP Foundations*. Estados Unidos: SYBEX, 2004.
- CISCO, S. *Internetworking Technology Handbook*. 2003.
- CLEMM, A. *Network Management Fundamentals*. Estados Unidos: Cisco Press, 2007.
- COMER, D. E. *Computer Networks and Internets*. 6. ed. Estados Unidos: Pearson Education, 2009.
- COULOURIS, G. et al. *Distributed Systems: Concepts and design*. 5. ed. Estados Unidos: Pearson, 2011.
- DANTAS, M. *Computação Distribuída de Alto Desempenho*. Brasil: Axcel, 2005.
- DATE, C. J. *An Introduction to Database Systems: Tools for building robust data centers*. 8. ed. United States of America: Addison Wesley, 2003.
- ELECTRICAL, I. of; ENGINEERS, E. *802.1D: Media access control (mac) bridges*. [S.l.]: IEEE, 2004.
- ELECTRICAL, I. of; ENGINEERS, E. *802.3: Ethernet*. [S.l.]: IEEE, 2008.
- FRISCH Aileen. *Essential System Administration*. 3. ed. Estados Unidos: O'Reilly, 2002.
- KLEINE, M.; HIRSCHFELD, R.; BRACHA, G. *An abstraction for version control system*. [S.l.], 2012.
- KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a Internet: uma abordagem top-down*. [S.l.]: PEARSON, 2010.
- LIMONCELLI, T. A.; HOGAN, C. J.; CHALUP, S. R. *The Practice of System and Network Administration*. 2. ed. Estados Unidos: Addison-Wesley, 2007.
- MAURO, D.; SCHMID, K. *Essential SNMP*. 6. ed. Estados Unidos: O'Reilly, 2005.
- MOCKAPETRIS, P. *Domain names - concepts and facilities*. IETF, nov. 1987. RFC 1034 (Standard). (Request for Comments, 1034). Updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936. Disponível em: <<http://www.ietf.org/rfc/rfc1034.txt>>.
- OLIVEIRA, L. M. de. *Estudo sobre serviço de diretórios distribuídos para instituições acadêmicas*. São José: IFSC, 2010. Disponível em: <<http://wiki.sj.ifsc.edu.br/wiki/images/6-/64/Monografia-luiz-marcelo-2010-02.pdf>>.

ORACLE. *MySQL 5.1 Reference Manual: Including mysql cluster ndb 6.x/7.x reference guide*. United States of America, 2012.

ROSENBERG, J.; MATEOS, A. *The cloud at your service: The when, how, and why of enterprise cloud computing*. Estados Unidos: Manning, 2011.

SIIA. *Software as a Service: Strategic Backgrounder*. [S.l.], 2001.

S.TANENBAUM, A.; STEEN, M. V. *Distributed Systems: principles and paradigms*. 2. ed. Estados Unidos: Pearson, 2006.

STANOEVSKA-SLABEVA, K.; WOZNIAK, T.; RISTOL, S. *Grid and Cloud Computing: A business perspective on technology and applications*. 1. ed. Estados Unidos: Springer, 2010.

TANENBAUM, A. S. *Redes de Computadores*. [S.l.]: Elsevier, 2003.