

Flávio Silva Silveira

Estudo Analítico de Infraestrutura e Gerenciamento de
Rede da UESB

Vitória da Conquista- BA, Brasil
Setembro de 2011

Flávio Silva Silveira

Estudo Analítico de Infraestrutura e Gerenciamento de Rede da UESB

Monografia apresentada para obtenção do Grau
de Bacharel em Ciência da Computação pela
Universidade Estadual do Sudoeste da Bahia.

Orientador:
Hélio Lopes Santos

DEPARTAMENTO DE CIÊNCIAS EXATAS - DCE
COLEGIADO DO CURSO DE CIÊNCIA DA COMPUTAÇÃO
UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA – UESB

Vitória da Conquista- BA, Brasil
Setembro de 2011

Monografia de Projeto Final de Graduação sob o título “*Estudo analítico de infraestrutura e gerenciamento de rede da UESB*”, defendida por Flávio Silva Silveira e aprovada em setembro de 2011, em Vitória da Conquista, Estado da Bahia, pela banca examinadora constituída pelos professores:

Prof. Dr. Hélio Lopes Santos
Orientador

Prof. Mest. Adilson de Lima Pereira

Prof. Esp. Bruno Silvério Costa

Resumo

Este trabalho visa nortear a prática do gerenciamento de rede através do conteúdo teórico proposto pelo modelo funcional de gerência, dividido em cinco áreas: Falha, Contabilização, Configuração, Desempenho e Segurança. Visando assim facilitar as atividades do administrador da rede quanto ao planejamento, monitoração e análise de todo o sistema, sendo necessário o estudo de todas as tecnologias envolvidas no processo. De modo a garantir à gerência um planejamento embasado em um referencial, tornando possíveis as tarefas de monitoração e análise de forma consolidada. Neste trabalho foi utilizada a infraestrutura de rede da UESB como objeto de estudo direcionado ao processo de reestruturação da mesma, buscando viabilizar o seu gerenciamento na prática, consistindo o trabalho na análise de todas as tecnologias usadas pela administração em sua atividade de planejamento. A análise consiste em avaliar cada tecnologia envolvida quanto a sua atuação funcional na rede, seja em performances de desempenho, segurança, prevenção e reação a falhas, como também em auxílio às tarefas de configuração e contabilização dos recursos e seus rendimentos na infraestrutura, tornando possíveis as atividades de monitoração e análise do tráfego pelo gerenciamento da rede.

Abstract

This paper aims to guide the practice of network management through the theoretical content of the functional model proposed by management, divided into five areas: Fault, Accounting, Configuration, Performance and Security. Thus aiming at facilitating the activities of the network administrator for the planning, monitoring and analysis of the entire system that includes, and requires the study of all the technologies involved. To ensure to the manager a planning founded on referential, making possible the tasks of monitoring and analysis on a consolidated basis. In this paper we used the network infrastructure of UESB as an object of study, aimed at restructuring of the same, seeking to facilitate its management in practice, the work consists in the analysis of all technologies used by management in their planning activity. The analysis is to evaluate each technology involved and its functional role in the network, either in performance of performance, security, prevention and reaction to failure, as well as help in the tasks of configuration and resource accounting and its revenues in infrastructure, making possible monitoring activities and analysis of traffic by network management.

Dedicatória

Dedico o esforço empregado neste trabalho inteiramente a minha mãe, Maria Lúcia Ladeia Silva Silveira, que suportou bravamente, dormindo em uma cadeira, minhas angustias e aflições por me encontrar imóvel num leito de hospital por mais de 40 dias.

Agradecimentos

Agradeço primeiramente a glória do Supremo Arquiteto do Universo por me manter de pé frente a todos os obstáculos. Aos meus pais e meus irmãos, meu alicerce. A todos meus familiares e amigos que conquistei em toda minha jornada, mesmo os que tenham duvidado que concluísse, pois me serviram de incentivo a provar que estavam enganados. Sem citar nomes, para não cometer injustiça, a todos que de alguma forma me apoiaram para conclusão desta etapa.

*"Deem-me uma alavanca e um ponto
de apoio e moverei o mundo."*

(Arquimedes)

Lista de Figuras

Figura 1 - Relacionamento entre os Padrões IEEE 802 e o modelo OSI.....	22
Figura 2 - Foto dos modens da antiga infraestrutura de UESB	49
Figura 3 - Foto do enlace entre switch da antiga infraestrutura da UESB	49
Figura 4 - Fotografia de satélite do campus VCA.....	51
Figura 5 - Projeto da topologia de rede do campus VCA	52
Figura 6 - Relação das interfaces do switch core localizado no módulo acadêmico	52
Figura 7 - Relação das interfaces do switch core localizado no módulo da UINFOR.....	53
Figura 8 - Relação das interfaces do switch core localizado no módulo da Prefeitura de Campus	53
Figura 9 – Servidores de mesa da UESB	54
Figura 10 – Foto de nobreak de alimentação de servidores.....	54
Figura 11 – Foto do bastidor de fibras da Telemar na sala de servidores	55
Figura 12 – Foto do switch core da sala de servidores	55

Lista de Tabelas

Tabela 1 - Funções SNMPv2	44
Tabela 2 - Classificações das tecnologias de rede quanto às classes de gerência.	61

Lista de Gráficos

Gráfico 1 - Número de tecnologias empregadas pela UINFOR no processo de gerência.	62
--	----

Sumário

1. Introdução	14
1.1. Contextualização e motivação	14
1.2. Objetivos	16
1.3. Justificativa	17
1.4. Metodologia.....	17
1.4.1. Classificação da pesquisa	17
1.4.2. Tecnologias utilizadas	18
1.5. Estrutura do documento	19
2. Padrões de redes e conceitos do modelo OSI	20
2.1. Considerações iniciais	20
2.2. Padronização da Internet	20
2.3. Padrões internacionais	21
2.4. Áreas funcionais de gerenciamento	23
2.4.1. Gerenciamento de falhas	23
a) Funções da gerência de falhas.....	25
b) Registro de alarmes e controle de log.....	26
2.4.2. Gerenciamento de desempenho	27
2.4.3. Gerenciamento de configuração	29
2.4.4. Gerenciamento de contabilização	30
2.4.5. Gerenciamento de segurança	31
2.5. Tecnologias de rede.....	33
2.5.1. Intelligent Resilient Framework (IRF)	33
2.5.2. Agregação de banda.....	34
2.5.3. Distribuição das redes.....	34
2.5.4. Protocolos de redundância a falhas.....	36
2.5.5. Servidores de rede.....	37
a) Dynamic Host Configuration Protocol (DHCP)	38
b) Servidor Squid	38

2.5.6.	Segurança operacional	39
2.5.7.	Wi-Fi.....	40
2.5.8.	Protocolos de rede.....	41
a)	Internet Group Management Protocol (IGMP).....	41
b)	Internet Control Message Protocol (ICMP)	41
2.5.9.	Protocolos de gerenciamento	42
a)	Simple Network Management Protocol (SNMP)	42
b)	Remote Monitoring (RMON)	45
2.5.10.	Intelligent Management Center (IMC).....	46
2.6.	Considerações Finais	47
3.	Infraestrutura de redes da UESB campus VCA e tecnologias de rede.....	48
3.1.	Considerações iniciais	48
3.2.	Antiga infraestrutura de rede da UESB	48
3.3.	Departamento de Modernização da Informática	49
3.4.	Unidade Organizacional de Informática	50
3.5.	Topologia e infraestrutura de rede do campus VCA	51
3.6.	Classificações das tecnologias de rede quanto às classes de gerência	57
3.7.	Considerações finais	62
4.	Conclusão e trabalhos futuros	63
4.1.	Conclusão	63
4.2.	Trabalhos futuros	63
	Referências bibliográficas	65

1. Introdução

1.1. Contextualização e motivação

Independente do tamanho e da complexidade que uma rede de computadores possa apresentar, essa necessita ser gerenciada, a fim de satisfazer aos seus usuários a disponibilidade dos serviços a um nível de desempenho aceitável. E com a abrangência das redes de computadores nos dias atuais, o fator de compartilhar dispositivos assumiu cada vez mais um aspecto secundário em face às demais vantagens percebidas (KUROSE; ROSS, 2010; Comer 2007). Ora, assumindo as redes um papel de ferramenta que proporciona recursos e serviços ao cotidiano das pessoas, admitindo maior interação e um aumento de produtividade, por conseguinte. Com isso, cresce também a complexidade de seu gerenciamento, compelindo à adoção de ferramentas automatizadas para a sua monitoração e controle.

Para auxiliar neste processo, fundamenta-se a importância da área de gerência de redes de computadores. Ela é a ciência responsável por manter o controle, de forma integrada, de todos os serviços e recursos que a compõe (MELCHIORS, 1999), onde se entende que a sua função fundamental é a obtenção de informações da rede, que uma vez devidamente tratadas possibilite um diagnóstico seguro, propondo assim soluções aos problemas. Conceituado neste paradigma, as tarefas de gerência devem ser embutidas nos distintos componentes da rede, possibilitando desvendar, prever e reagir a problemas.

O gerenciamento eficaz de uma rede provê que os recursos sejam aplicados da melhor forma possível, atendendo o retorno proposto pelo investimento em Tecnologia da Informação (TI), de forma a amenizar possíveis prejuízos ocasionados por dificuldades em seu funcionamento.

Em uma definição mais elaborada sobre o assunto (KUROSE apud SAYDAM, 1996, p.556) explana e conclui que:

“Gerenciamento de rede inclui a disponibilização, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável.”

Em concordância, pode-se dizer que gerência de redes engloba o conjunto de atividades norteadas para o planejamento, monitoração e controle, objetivando maximizar o desempenho, prover recursos perante alterações de demanda, minimizar falhas, documentar e manter configurações, sempre zelando pela segurança dos elementos que a constitui, desde os serviços prestados pela infraestrutura de rede até as aplicações que dependem dessa infraestrutura.

Associada às diversas possibilidades de aplicabilidade das redes de computadores, o domínio proporcionado pela área de gerência de redes, incorpora novas tecnologias de redes muito rapidamente, gerando uma evolução muito acentuada nas redes, por tipos heterogêneos de equipamentos, o que pode vir a dificultar a manter um tempo de resposta satisfatório devido à variedade e complexidade dos problemas que surgem exponencialmente e torna necessária a utilização de um técnico especialista para controlar e manter a disponibilidade e qualidade dos serviços da rede, através do gerenciamento das mesmas.

O montante de recursos aplicados na infraestrutura de redes da UESB, em face do seu crescimento exponencial nos últimos anos em números de cursos, docentes e discentes é o que assegura a expansão e reestruturação da rede de computadores para atender a demanda de novos módulos erguidos pelo planejamento de ampliação do campus, o que ocasiona uma difícil tarefa de gerenciamento para conciliar novos e velhos equipamentos, uma vez que é necessário todo um processo para migrar e/ou interconectar a estrutura de rede já existe.

É primordial, à gerência de rede, o entendimento da importância e compreensão pela a utilização de padrões, visto que a interoperabilidade entre equipamentos e sistemas de diversos fabricantes é um fator essencial para evitar a dependência tecnológica a um determinado fabricante ou fornecedor, o que fundamentalmente resulta em redução de custo, promovendo assim a portabilidade de sistemas, treinamento de pessoal e admitindo a escalabilidade de sistemas e equipamentos, entre outros benefícios.

Como bem pode ser observado em TANENBAUM (2003) existem padrões que devido à grande aceitação do mercado ou de algum segmento de usuários, como por exemplo, os do meio científico, por determinada tecnologia com: IBM, UNIX, TCP/IP. Tornando-os padrões de fato. Já os padrões formais, legais, elaborados e adotados por organizações públicas ou privadas autorizadas para este fim constituem-se em padrões de direito, como são: ISO, IEEE, ANSI. Sendo relevante frisar que alguns padrões “de jure” originam-se a partir de padrões “de

facto”, como por exemplo, o POSIX (OSF), como um padrão para interface se sistemas operacionais UNIX.

Conscientizado pela importância de padronização, cabe ao administrador de rede tomar decisões quanto a planejar, analisar e reagir às informações gerenciais dirigidas à central de operações de rede, neste propósito é fundamental a identificação e gerenciamento de falhas (KATZELA,1995; MEDHI, 1997; STEINDER, 2002), detecção proativa de anomalias (THOTTAN, 1998), entendimento da correlação entre alarmes (JAKOBSON, 1993), gerenciamento de serviços (SAYDAM, 1996; RFC 3053), de forma a prover o fornecimento de recursos, como largura de banda, capacidade do servidor e outros recursos computacionais e de comunicação necessários para cumprir os requisitos de serviço específicos da missão de uma empresa.

Motivado por todo o conceito que abrange a área de redes de computadores, desde o tráfego de bits em meios físicos até a sua real aplicação, e em jus a tudo o que até então pode ser compreendido da relevância da infraestrutura à gerência de redes, faz-se necessário o aprofundamento das ideias que a envolve, sendo o objeto de estudo das próximas seções.

1.2. Objetivos

O objetivo deste projeto baseia-se no estudo direcionado a área de gerencia de redes de computadores em face à análise da estrutura de redes da UESB campus Vitória da Conquista (VCA), visando buscar soluções devidamente fundamentadas a sua melhor administração, uma vez que sua rede passa por um processo de reestruturação.

Cabe salientar que as redes de computadores proporcionaram inúmeras melhorias à era da informação, como o suporte à computação distribuída, cooperativa e tolerante a falhas, permitindo uma evolução de toda a computação. Mas novas aplicações e funcionalidades para as redes de computadores, que contravenha as padronizações e normas, podem causar queda no desempenho, reduzindo ou mesmo parando a comunicação, dentre outros estados anômalos, como falhas no sistema.

O presente projeto tem como objetivo inicial capturar o máximo de informações sobre os assuntos infraestrutura e gerência de rede, garantindo assim a elaboração de uma pesquisa bibliográfica contendo as principais características. Essa pesquisa define uma maior ligação

entre o que foi examinado ao que foi escolhido como tema do projeto. A pesquisa bibliográfica permite ao investigador uma gama de fenômenos do que aquela que poderia ser adquirida pesquisando diretamente.

Outro objetivo deste projeto é a elaboração de um estudo de caso da classificação das tecnologias empregadas na rede de computadores quanto aos aspectos gerenciais. Segundo Gil (2002) o estudo de caso é encarado como o delineamento mais adequado para a investigação de um fenômeno contemporâneo dentro de seu contexto real.

1.3. Justificativa

O conteúdo proporcionado neste trabalho tem como propósito essencial corroborar com a administração de redes de computadores, além servir de objeto aos docentes e discentes no curso de Ciências da Computação da UESB e a outros que possuam interesse no campo de gerência de redes ou ainda que queiram adquirir um pouco de informação sobre o tema. Também pode ser de grande valia, para quem queira conhecer um pouco mais sobre redes e algumas tecnologias que fazem parte da sua composição.

Para tanto, é primordial ao gerenciamento de rede o conhecimento prévio de todas as tecnologias e protocolos envolvidos nas tarefas de rede, como a transmissão e recepção de dados, detecção e resolução de erros, assegurando um serviço a um nível aceitável de desempenho e segurança da rede.

1.4. Metodologia

1.4.1. Classificação da pesquisa

Quanto à natureza, uma pesquisa pode ser classificada como básica ou aplicada, onde a primeira consiste no desenvolvimento de pesquisa sem uma finalidade prática imediata, enquanto a segunda consiste na aplicação dos resultados da pesquisa em problemas existentes (SILVA; MENEZES, 2005).

Este trabalho é classificado como pesquisa aplicada, pois objetiva gerar conhecimentos para aplicação prática e dirigidos à solução de problemas específicos no que se refere à infraestrutura e gerenciamento de rede.

Quanto à forma de abordagem do problema, uma pesquisa pode ser classificada em quantitativa ou qualitativa (SILVA; MENEZES, 2005).

Este trabalho possui características da abordagem qualitativa, pois descreve as relações dinâmicas entre o cenário real de uma rede de computadores e o seu administrador que não pode ser traduzido simplesmente em números, embora a quantificação seja uma forma mais indicada a determinar resultados. A interpretação dos fenômenos e a atribuição de significados são básicas no processo de pesquisa qualitativa. Não requer o uso de métodos e técnicas estatísticas.

Quanto aos objetivos, uma pesquisa pode ser classificada em exploratória, descritiva ou explicativa (SILVA; MENEZES, 2005). Esta é uma pesquisa exploratória, pois visa proporcionar maior familiaridade com problemas relacionados à infraestrutura e gerenciamento de rede com vistas a torná-lo explícito. Envolve levantamento bibliográfico, descrição de experiências práticas com o problema pesquisado, e análise de tecnologias que estimulem a compreensão e resolução de problemas.

1.4.2. Tecnologias utilizadas

Como ferramenta auxiliar ao processo de gerenciamento de redes foi detalhado o modelo funcional *Open Systems Interconnection* (OSI) proposto pela *International Organization for Standardization* (ISO), que é uma organização voluntária não governamental, responsável pela publicação de mais de 5000 padrões, incluindo o OSI (TANENBAUM, 2003).

O modelo OSI propõe três instâncias ao gerenciamento: organizacional, informacional e funcional, sendo que o modelo organizacional estabelece a hierarquia entre sistemas de gerência em um domínio de gerência, dividindo o ambiente a ser gerenciado em vários domínios. O modelo informacional é que define os objetos de gerência, as relações e as operações sobre esses objetos, sendo uma *Management Information Base* (MIB) necessária para o armazenamento dos objetos gerenciados. E o modelo funcional é que descreve as

funcionalidades de gerência, as quais o modelo OSI define em cinco áreas: gerência de falhas, gerência de configuração, gerência de desempenho, gerência de contabilidade e gerência de segurança (KUROSE; ROSS, 2010).

Para a análise da gerência de rede foi utilizado os próprios protocolos e tecnologias de rede empregadas na infraestrutura de rede da UESB, apresentadas no próximo capítulo, fomentando a sua importância no processo de gerenciamento e adequando sua utilização ao planejamento da rede elaborado pela administração.

1.5. Estrutura do documento

O projeto está organizado na seguinte forma: O capítulo 2 apresenta um resumo da padronização de rede e conceitos obtidos principalmente pela área funcional do modelo OSI.

No capítulo 3 temos a análise da infraestrutura de rede da UESB em especial a do campus VCA, bem como sua administração pela Unidade Organizacional de Informação (UINFOR), setor responsável pela rede de computadores da UESB e que servi de objeto de estudo quanto a utilização dos protocolos na rede envolvidos no processo de gerenciamento, especificação de tecnologias adotadas e suas adequações ao projeto de redes da UESB.

E no capítulo 4 temos a conclusão do trabalho além da descrição de futuros trabalhos.

2. Padrões de redes e conceitos do modelo OSI

2.1. Considerações iniciais

O capítulo aborda a adoção de padrões como método de viabilizar a interoperabilidade de rede em sistemas heterogêneos e descreve o modelo OSI como referencial para a gerência de rede aberta.

2.2. Padronização da Internet

Conforme supracitado no conteúdo deste projeto a importância da adoção de padrões resulta em inúmeros benefícios ao gerenciamento de uma rede. Lembrando que o emprego de padrões ocorre em todas as etapas de implementação de uma rede, do planejamento na escolha dos meios físicos, no desenvolvimento da infraestrutura até o monitoramento e controle do tráfego de dados na rede.

A Internet mundial possui seus próprios mecanismos de padronização, bastante diferentes dos adotados pela *Telecommunication Standardization Sector* (ITU-T) e pela ISO. Os grupos responsáveis pela padronização da Internet são muito mais informais.

O protocolo TCP/IP, por exemplo, foi desenvolvido em 1969 pelo *Defense Advanced Research Projects Agency* (DARPA), como uma arquitetura de transmissão de dados em rede, e foi o pilar da *Advanced Research Projects Agency Network* (ARPANET), rede privativa do ministério da defesa norte americano. Sendo que o desenvolvimento e a utilização desta rede era um esforço conjunto entre os meios acadêmicos e militares. E no início dos anos 80, ocorreu uma segregação do órgão militar, criando-se a rede *Military Network* (MILNET) exclusivamente para este fim. E a comunidade acadêmica tornou-se, então, única responsável pela ARPANET (PALMA; PRATES, 2000).

2.3. Padrões internacionais

Fundada em 1946, a ISO é composta por organizações de padrões internacionais de pelo menos 89 países como: ANSI, BSI, AFNOR, DIN e ABNT pelos respectivos países: Estados Unidos, Inglaterra, França, Alemanha e Brasil. E formada por cerca de 200 Comitês Técnicos (TC), numerados pela sua data de criação, que normatiza um largo espectro de assuntos. A *American National Standards Institute* (ANSI) é a principal organização normalizadora dos Estados Unidos, e principal membro da ISO. Cujos membros são fabricantes, concessionárias de telecomunicações e outras partes interessadas (TANENBAUM, 2003).

Seus padrões são estudados e propostos em áreas ou campos técnicos independentes, denominado *Accredited Standards Comitees* (ASC) (ANSI, 2011). O objeto de estudo do ASC denominado T1, por exemplo, é o de telecomunicações. Neste comitê se concentram, por exemplo, os grupos de trabalho que estudam os padrões das RDSI (Rede Digital de Serviços Integrados) em banda larga, *Asynchronous Transfer Mode* (ATM) e *Synchronous Optical Networking* (SONET). Um exemplo de padronização ANSI em redes locais são as redes *Fiber Distributed Data Interface* (FDDI), grupo de trabalho ANSI X3T9.5 (TANENBAUM, 2003).

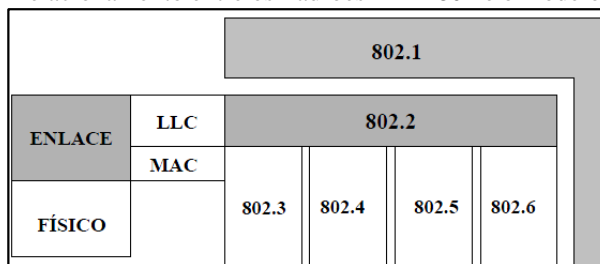
O *Institute Of Electrical And Eletronic Engineers* (IEEE) é a maior organização profissional do mundo e entre suas principais atividades estão a de publicação de artigos técnicos, a realização de diversas conferências durante o ano e o desenvolvimento e publicação de padrões na área de engenharia elétrica e computação (IEEE, 2010).

E foi a partir de 1980 que o comitê 802 da IEEE produziu diversos padrões para redes locais (IEEE802, 2011), as quais a ISO tomou-as como base para a publicação das normas ISO 8802. O comitê 802 e seus diversos grupos de trabalho se preocuparam em definir uma arquitetura com três camadas, perfeitamente relacionadas com o modelo OSI.

Para isto algumas funções de comunicação deveriam ser encaradas como premissas para o desenvolvimento dos padrões, como fornecer um ou mais *Service Access Point* (SAP), que é um rótulo de identificação para os terminais de rede usada na Interconexão de Sistemas Abertos de rede (OSI). Para a transmissão, montar os dados a serem transmitidos em quadros com campos de endereço e detecção de erros. E na recepção, desmontar os quadros, efetuando o reconhecimento de endereço e detecção de erros, além de gerenciar a comunicação do enlace.

Estas funções de comunicação são fornecidas pela camada de enlace de dados do modelo OSI. Os trabalhos também englobaram funções associadas à camada física com a multiplexação e decodificação de sinais, geração e remoção de preâmbulos para sincronização e transmissão e recepção de bits. De fato, as normas 802 são perfeitamente correlacionadas com o modelo OSI, segundo observado na figura 1:

Figura 1 - Relacionamento entre os Padrões IEEE 802 e o modelo OSI



Fonte: (TORRES, 2001, p. 47)

Definições dos padrões IEEE mostrados na figura 1:

- IEEE 802.1 faz uma introdução para o conjunto de padrões, seu relacionamento com o modelo OSI, descreve padrões para o gerenciamento de rede e informações para a interligação de redes (IEEE, 802.1, 2011).

- IEEE 802.2 (ISO 8802/2) delinea a subcamada superior da camada de enlace de dados, protocolo *Logical Link Control* (LLC) (IEEE, 802.2, 2011).

- IEEE 802.3 (ISO 8802/3) apresenta o método *Carrier Sense-Multiple Access with Collision Detection* (CSMA/CD) de acesso ao meio físico em uma rede em barra (IEEE, 802.3, 2011).

- IEEE 802.4 (ISO 8802/4) expõe o método Token Bus, ou seja, a passagem de permissão como método de acesso ao meio físico em uma rede em barra (IEEE, 802.4, 2011).

- IEEE 802.5 (ISO 8802/5) propõe o método Token Ring, ou seja, a passagem de permissão como método de acesso ao meio físico em uma rede em anel (IEEE, 802.5, 2011).

- IEEE 802.6 (ISO 8802/6) trata do método *Distributed Queue Dual Bus* (DQDB) como método de acesso em uma rede em barra (IEEE, 802.6, 2011).

O procedimento para padronização adotado pela ISO tem como objetivo alcançar o máximo de consenso possível. Para tanto, quando uma das organizações de padronização membro da ISO sente a necessidade de chegar a uma padronização internacional em

determinada área, se forma um grupo de trabalho com a finalidade de se produzir um *Comitee Draft* (CD), que é repassado a todas as entidades associadas, tendo estas seis meses para criticar o documento. Caso a maioria dos membros o aprove, é produzido um documento revisado *Draft International Standard* (DIS), para ser novamente analisado e votado, e com base nas análises do mesmo, é enfim elaborado, aprovado e publicado o *International Standard* (IS). Em áreas de grande controvérsia, um CD ou DIS pode receber diversas versões antes de ser aprovado, e o processo inteiro pode durar anos.

2.4. Áreas funcionais de gerenciamento

Entre as principais dificuldades em se automatizar o processo de gerência de redes destacam-se a complexidade e a manipulação do volume de informações. No sentido de minimizar a complexidade da gerência de redes, o modelo propõe cinco áreas funcionais: gerência de falhas, gerência de configuração, gerência de desempenho, gerência de contabilização e gerência de segurança (BRISA, 1993) (LEINWAND; CONROY, 1996)(KUROSE; ROSS, 2010).

A importância das gerências de rede também é fundamentada por (COMER, 2007) na seguinte afirmação:

“Embora o hardware de rede e o software de protocolo contenham mecanismos para detectar automaticamente falhas e retransmitir pacotes, administradores de rede trabalham para detectar e corrigir problemas subjacentes porque retransmissões resultam em desempenho mais baixo.”

Dentre as quais a gerência de falhas é a que requer maior atenção, juntamente com gerência de segurança, embora todas tenham fundamental importância. Esta segmentação dar-se da necessidade no processo de gerenciamento de rede facilitar a administração. Logrado o êxito, o modelo foi adotado pela maioria dos fornecedores de sistemas de gerenciamento de redes.

2.4.1. Gerenciamento de falhas

O objetivo do gerenciamento de falhas é registrar, detectar e reagir às condições de falha da rede (KUROSE; ROSS, 2010). Sendo funcionalmente responsável pela detecção de

eventos anormais e pelo diagnóstico de problemas que ocasionam esses eventos, permitindo assim o isolamento e a correção das operações anômalas. Entre as causas mais prováveis para falhas em uma rede estão os erros de projeto e desenvolvimento, de sobrecarga, utilização de equipamento com tempo de vida útil bastante avançado, além de possíveis distúrbios externos.

Uma gerência de falhas bem projetada aumenta a confiabilidade na rede fornecendo ferramentas ao administrador da rede que auxiliem a detectar os problemas e iniciar os procedimentos de recuperação. Portanto um software que visa oferecer suporte ao gerenciamento de falhas, deve mostrar ao administrador de rede o número, os tipos, a hora da ocorrência e a localização dos erros na rede.

Devendo quando ocorrem falhas seguir os procedimentos de determinar a localização exata da falha, se possível, isolar o resto da rede, assim a rede pode continuar a funcionar sem interferências. Reconfigurar ou modificar a rede de tal maneira a minimizar o impacto dessa operação de correção, mesmo com a ausência dos equipamentos falhos, e o mais breve possível corrigir as falhas, para que o funcionamento da rede possa retornar ao seu estado inicial.

O gerenciamento de falhas é dificultado quando, por exemplo, a existência de impasse entre processos cooperantes distribuídos pode não ser observada localmente ou ainda outras falhas podem não ser observadas devido à impossibilidade do equipamento registrar a ocorrência das mesmas (COMER, 2007). Quando uma falha em um elemento de rede pode ser observada, porém a observação pode ser insuficiente para identificar com precisão a fonte do problema. E ainda quando observações detalhadas de falhas são possíveis, podem existir incertezas ou inconsistências associadas às observações.

Após as falhas serem observadas, é necessário que cada uma seja isolada. Para que estas falhas sejam isoladas alguns problemas podem ocorrer, entre esses quando múltiplas tecnologias estão envolvidas, os locais e tipos de falhas aumentam significativamente. Isso torna mais difícil a localização da real fonte. Para tanto, a devida consideração ao modelo OSI deve ser tomada, pois uma falha em uma das camadas pode causar degradação ou falhas em todas as camadas de nível mais alto. Uma vez que mesmo um procedimento de correção local podem destruir importantes evidências referentes à natureza da falha, causando interferência ao diagnóstico.

Dentre as importâncias da gerência de falhas se encontram alguns papéis fundamentais envolvidos no processo de administração e são:

a) Funções da gerência de falhas

Estando determinado que a primeira exigência em um sistema de gerência de falhas é que ele detecte e informe a ocorrência das anomalias ocorridas. No mínimo, um agente de monitoramento de falhas deve manter log dos eventos e erros mais significativos. Tipicamente, um agente de monitoramento de falhas tem a capacidade, de forma independente, para informar a ocorrência de erros a um ou mais gerentes. Para evitar-se o engarrafamento da rede, alguns critérios para esse diálogos devem ser estabelecidos, fazendo-se necessário as referências como latência, perda de pacotes e disponibilidade da rede.

Além de avisar sobre alguns tipos de falhas, um bom sistema de gerência de falhas deve ser capaz de adiantar-se à falha, tornando sua administração proativa. Comumente, isto é feito determinando limites e uma vez alcançados estes limites o sistema deve lançar de si um alarme.

O sistema deve também permitir um diagnóstico da falha exposta e os procedimentos para recuperação, devem ser adotados através de testes como conectividade, integridade dos dados e dos protocolos, congestionamento da conexão, análise do tempo de resposta, por fim teste de diagnóstico.

A maneira de detecção de falhas consiste, em geral, na comparação entre um comportamento esperado e o comportamento apresentado. Discrepâncias entre estes comportamentos indicam que o sistema está com problemas. Devendo-se determinar as causas do problema, ou seja, um diagnóstico inicial. Assim, o objetivo deste diagnóstico é determinar os elementos responsáveis pelo mau funcionamento do sistema.

A aversão entre o comportamento esperado e o comportamento observado é utilizada para conduzir a pesquisa pelo diagnóstico, podendo-se, portanto fazer a análise entre o comportamento esperado para o sistema que está sendo diagnosticado e a observação do sistema no estado atual. Um fator fundamental nos diagnósticos baseados em modelo é que os modelos devem ser completamente corretos.

Entretanto, tal como em qualquer modelagem matemática, o modelo adotado para ser utilizado como referência, trabalha com uma quantidade de hipóteses simplificadas e aproximações que são incapazes de reproduzir a situação real do sistema com precisão. Em geral, se a aproximação for boa o suficiente, a abordagem baseada em modelo apresenta-se como uma boa técnica de diagnóstico.

Um formalismo adequado para determinar a conduta esperada do sistema de interesse, deve ser adotado. Para isso, as formas de se fazer diagnósticos baseados em modelo, depende do conhecimento que se obtém do comportamento do sistema, e se classificam em (SANTOS, 2004):

- Diagnóstico baseado em consistência: é um modelo que expõe o procedimento apropriado do sistema;
- Diagnóstico baseado em abdução: é um modelo que expõe o procedimento falho do sistema.

Para alguns problemas, a solução através de procedimentos exatos simplesmente não existe ou são computacionalmente inviáveis. Uma alternativa para esse problema consiste na utilização de procedimentos que oferecem soluções consideradas boas, mas em alguns casos pode não ser a melhor solução. Este método é chamado de heurística, uma classe mais geral ao método de heurística é chamada de meta-heurística e algumas têm sido propostas e especialmente projetadas para evitar que o procedimento fique preso em armadilhas de ótimos locais (SANTOS, 2004).

O diagnóstico heurístico utiliza do conhecimento de especialistas e do obtido através da observação de uma quantidade significativa de dados. Tipicamente, este conhecimento pode ser expresso através de regras, associando indícios com as falhas analisadas. Entre as dificuldades identificadas pela abordagem heurística esta à aquisição do conhecimento de especialistas humanos, que além de ser uma tarefa complicada gasta muito tempo. Em geral o conhecimento é intrínseco a um ambiente específico e não reutilizável o que gera a manutenção de uma grande base de regras, e ainda apenas o conhecimento sobre o comportamento do sistema até a data atual pode ser utilizado, portanto, alguns tipos de falhas raras podem não ser diagnosticados.

b) Registro de alarmes e controle de log

Alarmes constituem um subconjunto de notificações, mensagens emitidas por objetos gerenciados, e são causados por condições não habituais. Eles podem ser gerados em função de condições anormais que foram diagnosticados, como quando houver uma disparidade de um determinado serviço em relação a certo valor limite ultrapassado.

Alarmes podem ser motivados por mais de uma causa, para isolar as fontes os alarmes devem ser correlacionados. Esses alarmes são catalogados de uma maneira padrão, e devem conter dados para identificar a natureza e a fonte do problema. Se alguns problemas ocorrem constantemente, informações adicionais devem ser empregadas para analisar e estudar as prováveis causas.

Em geral, os alarmes são empacotados no serviço de registro de alarme, que está presente nos agentes e no gerente devido a sua importância, pois os dados gerados carregam não apenas uma ajuda para encontrar a fonte do problema, mas alguns deles podem indicar os passos do diagnóstico que podem ser adotado.

O controle de logs, diz respeito a solicitações de usuário, serviços oferecidos, e o protocolo necessário para proporcionar os serviços de registro de logs. Eventos e notificações que são recebidas precisam ser registrados para serem posteriormente utilizados.

Os objetos gerenciados que emitem notificações através de algum processamento podem gerar possíveis registros de log, os quais são mandados para um ou mais arquivos de log após terem sido devidamente filtrados. Os filtros têm um conjunto de regras que decidem que registros de log serão gravados.

A linha divisória entre gerenciamento de falha e gerenciamento de desempenho é bastante indefinida (KUROSE; ROSS, 2010). E um lembrete que se faz necessário é que as informações obtidas através das gerências de configuração e de desempenho devem ser utilizadas de forma proativa para evitar falhas previsíveis.

2.4.2. Gerenciamento de desempenho

A meta do gerenciamento de desempenho é qualificar, medir, informar, analisar e controlar o desempenho de diferentes componentes da rede (KUROSE; ROSS, 2010). Portanto, consiste na monitoração das atividades e no controle dos recursos através de ajustes

e trocas, com o objetivo de assegurar que a rede tenha capacidade para suportar e acomodar certa quantidade de usuários. Ou seja, ela é extremamente necessária para aperfeiçoar a qualidade do serviço.

Medir o desempenho dos equipamentos e softwares disponíveis através de registros de algumas taxas de medidas como as de *throughput*, de erros, de utilização e tempo de resposta. Além de estabelecer a real capacidade de utilização, níveis de tráfego e *throughput*, descobrindo assim se há gargalos, se o tempo de resposta está aumentando e com que latência.

Para tratar estas questões, o gerente deve focalizar um conjunto inicial de recursos a serem monitorados a fim de estabelecer níveis de desempenho. Isto inclui associar métricas e valores apropriados aos recursos de rede que possam fornecer indicadores de diferentes níveis de desempenho. Muitos recursos devem ser monitorados para se obter informações sobre o nível de operação da rede. Coletando e analisando estas informações, o gerente da rede pode ficar mais capacitado no reconhecimento de situações indicativas de falha de desempenho.

Estatísticas de desempenho podem ajudar no planejamento, administração e manutenção de grandes redes. Estas informações podem ser utilizadas para reconhecer situações de gargalo antes que elas causem problemas ao usuário final. Ações corretivas podem ser executadas como, por exemplo, a troca de tabelas de roteamento para balancear ou redistribuir a carga de tráfego durante horários de pico, ou ainda, em longo prazo, indicar a necessidade do aumento de banda.

Para cada tipo de monitoração definimos um valor máximo aceitável (*threshold*), um valor de alerta e um valor em que se remove a situação de alerta. Definem-se três modelos para atender aos requisitos de monitoração do uso dos recursos do sistema (KUROSE; ROSS, 2010):

- Modelo de Utilização: Provê a monitoração do uso instantâneo de um recurso.
- Modelo de Taxa de Rejeição: Provê a monitoração da rejeição de um pedido de um serviço.
- Modelo de Taxa de Pedido de Recursos: Provê a monitoração dos pedidos de uso dos recursos.

Desta forma, a gerência de desempenho deve utilizar-se de alguns indicadores de desempenho, tais como:

- **Vazão:** em sistema de filas que são formadas quando da chegada de pacotes em um servidor, serão ponderados o tempo de chegada de pacotes, e o tempo de serviço para atendê-los.

- **Disponibilidade:** é a probabilidade de o serviço estar em funcionamento durante um período de tempo. Devendo ser levados em consideração problemas externos, como a perda de alimentação.

- **Throughput:** é taxa de transmissão de dados, também conhecido como banda passante ou largura de banda sendo medido em função do número de bits que podem ser transmitidos sobre a rede em certo período de tempo.

Também são importantes indicadores de desempenho, os atrasos na entrega dos pacotes e os erros que ocorrem tanto na entrada quando na saída dos dados. Como a maioria dos problemas na gerência de desempenho, estão relacionados à situação que o especialista determinou como ideal para o sistema. Alguns itens devem ser considerados:

- **Monitorar os indicadores de desempenho:** providenciar alterações quando eles indicarem redução da eficiência.

- **Estabelecer um *baseline*:** isto significa delinear o que deve ser considerado normal no desempenho da rede, sendo escolhidas várias medidas para retratá-lo.

- **Definição de limiares:** é a definição de patamares, os quais serão responsáveis por gerar eventos ou alarmes de desempenho.

Assim, algumas estatísticas de desempenho são importantes, permitindo a formação de uma base de dados referente á tendências e eventos que servirão para planejamento de expansões.

2.4.3. Gerenciamento de configuração

O gerenciamento de configuração permite que o administrador da rede saiba quais dispositivos fazem parte da rede administrada e quais são suas configurações de hardware e software (KUROSE; ROSS, 2010). O objetivo da gerência de configuração é permitir a preparação, a iniciação, à partida, a operação contínua, e a posterior suspensão dos serviços de interconexão entre os sistemas, tendo então, a função de manutenção e monitoração da estrutura física e lógica de uma rede, incluindo a verificação da existência dos componentes, e a verificação da interconectividade entre estes componentes (KUROSE; ROSS, 2010).

O serviço de gerência de configuração possibilita a realização de uma série de atividades como desenvolvendo ações para materialização de resultados. As atividades desenvolvidas são classificadas por funcionalidade, responsabilidade e resultados, e devem oferecer total visibilidade para o administrador de redes no desenvolvimento de suas funções. Dentre as principais, pode-se se ressaltam (KUROSE; ROSS, 2010):

- Identificação dos elementos funcionais: processo de descoberta, classificação e identificação dos dispositivos da rede;
- Construção de mapas de topologia: apresentação documental de mapas com a topologia dos elementos e representação da estrutura de interconexão física ou lógica destes elementos;
- Inventário de hardware e software: relacionar hardware e software de diferentes dispositivos e ambientes, fornecendo informações sobre configuração e disponibilidade de recursos em cada elemento;
- Gestão de alteração na configuração dos dispositivos: mecanismos de sinalização e acompanhamento de mudanças com o objetivo de desenvolver processos capazes de acompanhar as modificações implementadas por um usuário na infraestrutura.
- Construção da base de dados de configuração: devem conter as relações dos dispositivos referenciando seus endereços IP e configurações, bem como as aplicações que auxiliam no processo de configuração de elementos de rede:
 - ✓ Implementação em larga escala: mecanismos para a reaplicação de configuração em larga escala, facilitando o processo de implementação e o fornecimento de recursos.
 - ✓ Verificação de integridade: análise crítica das configurações de todo o ambiente da rede.

2.4.4. Gerenciamento de contabilização

O gerenciamento de contabilização permite que o administrador da rede especifique, registre e controle o acesso de usuários e dispositivos aos recursos da rede (KUROSE; ROSS, 2010). Assim, este processo auxilia a assegurar que os usuários tenham acesso a quantidade suficiente dos recursos disponíveis. Tornando-se possível a realização de um melhor

planejamento do crescimento da rede, detectando abusos no uso dos recursos. Portanto envolve também, garantir ou remover permissões de acesso à rede.

Mesmo que nenhuma cobrança interna seja feita pela utilização dos recursos da rede, o administrador da rede deve estar habilitado para controlar o uso dos recursos por usuário ou grupo de usuários, com o objetivo de (KUROSE; ROSS, 2010):

- Evitar que um usuário ou grupo de usuários abuse de seus privilégios de acesso e monopolize a rede, em detrimento de outros usuários;
- Evitar que usuários façam uso ineficiente da rede, assistindo-os na troca de procedimentos e garantindo o desempenho da rede;
- Conhecer as atividades dos usuários com detalhes suficientes para planejar o crescimento da rede.

Portanto, podemos definir gerenciamento de contabilização como a área que trata a coleta de dados sobre o consumo de recursos para propósitos de análises de capacidade e tendências, alocação de custos, auditoria e cobrança. O gerenciamento de contabilização requer que o consumo de recursos seja medido, tarifado, designado e comunicado entre as partes apropriadas (ABOBA, 2000).

As propriedades desejáveis de um esquema de contabilização se definem basicamente sob o ponto de vista do gerente da rede e o ponto de vista dos clientes (FERRARI, 1999). Do ponto de vista do gerente da rede, os objetivos mais importantes relacionam-se com a grande probabilidade de recuperação de custos, o encorajamento ou desencorajamento de comportamentos dos clientes que irão acentuar ou interferir na eficiência da rede e a redução de custos de implementação. Sob o ponto de vista dos clientes, as principais propriedades se definem com a compreensibilidade e justiça na utilização.

2.4.5. Gerenciamento de segurança

A meta do gerenciamento de segurança é controlar o acesso aos recursos da rede de acordo com alguma política definida (KUROSE; ROSS, 2010). Sendo sua missão subsidiar as aplicações requeridas pelas políticas de segurança, protegendo os objetos gerenciados e o sistema de acessos indevidos por intrusos.

Nas palavras de (COMER, 2007) é definido que:

“Desenvolver uma política de segurança de rede pode ser complexo porque uma política racional exige que a organização relacione a segurança de redes e computadores ao comportamento humano e avalie o valor das informações.”

Deve-se, pois, munir-se de alarme, avisando assim ao gerente da rede sempre que se detectarem eventos relativos à segurança do sistema. Estes alarmes podem ser gerados com o auxílio de ferramentas *Intrusion Detection System* (IDS) ou firewalls.

O modelo OSI distingue dois conceitos referentes à segurança (KUROSE; ROSS, 2010):

- Arquitetura de segurança do modelo OSI;
- Funções de gerenciamento de segurança.

A finalidade da arquitetura de segurança do modelo OSI é o de produzir uma descrição geral dos serviços de segurança e dos mecanismos associados a este, e de definir em que posições do modelo de referência situam-se os serviços de segurança e os seus mecanismos associados. A norma de referência da arquitetura de segurança aborda exclusivamente da segurança dos canais de comunicação, através de mecanismos como a criptografia e a assinatura digital, que permitem aos sistemas que usam este canal se comunicar de forma segura.

Para isso, aspectos de segurança devem ser deliberados como os serviços de autenticação tanto de entidades pares quanto da origem dos dados, como o de controle de acesso aos recursos da rede, e que possibilitem a confidencialidade e integridade dos dados e que garantam a não rejeição ou não repudição na comunicação dos dados.

Os mecanismos a serem tomados dependem do uso da política de segurança, que é feita pelo uso das funções de segurança do gerenciamento de redes OSI, sendo que estas formam a área funcional de gerência de segurança. Estas funções, que compõem o gerenciamento de segurança, tratam do controle dos serviços de segurança do modelo OSI, e dos mecanismos e informações necessárias para se prestar estes serviços.

Para tanto, atendendo requisito de responsabilidade e autorização, deve ser fornecido relatórios de eventos referentes à segurança e o fornecimento de informações estatísticas, bem como, fazer-se a manutenção e análise dos registros deste histórico, permitindo a melhor

escolha na hora de setar os parâmetros dos serviços de segurança, e também a alteração, em relação à segurança, pela ativação e desativação dos serviços de segurança.

Para que estes objetivos sejam atingidos, devem-se apreciar as diferentes políticas de segurança a serem tomadas no sistema aberto. Lembrando que todas as entidades que seguem uma mesma política de segurança pertencem ao mesmo domínio de segurança.

Devido ao gerenciamento do sistema necessitar distribuir as informações de gerenciamento de segurança entre todas as atividades que se relacionam com a segurança, os protocolos de gerenciamento, assim como os canais de comunicação, devem ser protegidos usando os mecanismos que já devem ser previstos na arquitetura de segurança.

Conforme a proposta de gerenciamento de segurança OSI, vários são os mecanismos de proteção que podem ser usados para garantir segurança a um ambiente de comunicação em sistemas abertos como, por exemplo, o firewall pfSense e IDS Snort.

2.5. Tecnologias de rede

Para um melhor entendimento do planejamento da administração da rede da UESB é necessário compreender algumas tecnologias e protocolos adotados visando à resolução de problemas que serão tratados no seguinte capítulo.

2.5.1. Intelligent Resilient Framework (IRF)

O protocolo que possibilita o “empilhamento” de Switches modulares e empilháveis é o IRF, de forma a transformar diversos *Switches* físicos em um único Switch lógico, passando todos os equipamentos a serem visualizados como uma única “caixa”. Na sua segunda versão o protocolo possibilita efetuar o *Stacking* utilizando *links* de 10G (SWITCH H3C, 2011).

Porém, um dos problemas que o IRF pode trazer é quando ocorre uma quebra do *link* 10G que mantém o IRF ativo, chamado de SPLIT. Cada caixa irá agir como se fosse o MASTER do IRF, duplicando alguns serviços e trazendo diversos conflitos na rede. O *Multi-Active Detection* (MAD) é uma das formas para os switches do *Stack* detectarem que houve o SPLIT no IRF colocando o equipamento com o maior *Member ID* do IRF (não Master) em

modo *Recovery*, bloqueando assim todas as suas portas. Depois de restaurado o *link* do IRF as portas serão vinculadas novamente ao *Stack* e ao seu estado normal de encaminhamento.

2.5.2. Agregação de banda

Dentro da especificação IEEE 802.3ad o *Link Aggregation* é um termo da disciplina de redes de computadores que descreve o acoplamento de dois ou mais canais ethernet em paralelo para produzir um único canal lógico de maior velocidade e/ou aumentar a disponibilidade e redundância desse canal. Com isso agregação de *link* aborda dois problemas com conexões ethernet: as limitações de largura de banda e da falta de resiliência (LA, 2011).

Link Aggregation Control Protocol (LACP) permite que um dispositivo de rede negocie um agrupamento automático de ligações, enviando pacotes LACP para os pares, dispositivo diretamente conectado, que também implementa LACP (LA, 2011).

As vantagens que a agregação de *link* apresenta são as somas das velocidades dos meios físicos agregados resultando em uma abrangência de largura de banda, visando melhorar do desempenho da rede, como também tornar a rede tolerante a falhas, uma vez que a auto negociação, entre as portas fisicamente agregadas, além de prover o balanceamento de cargas, prover a redundância de caminho, caso alguma das interfaces agregadas caia.

2.5.3. Distribuição das redes

A *Virtual Local Area Network* (VLAN) nada mais é do que uma rede local virtual logicamente independente. Podendo várias VLANs coexistir em um mesmo switch, dividindo uma rede local, que fisicamente é a mesma, em mais de uma rede virtual, criando domínios de broadcast distintos. Podendo também tornar possível colocar em um mesmo domínio de broadcast, hosts com localizações físicas distintas, ligados a switches diferentes. Podendo ainda ter o propósito de restringir acesso a recursos de rede sem considerar a topologia da rede (VLAN, 2011).

Redes virtuais operam na camada 2 do modelo OSI. No entanto, uma VLAN geralmente é configurada para mapear diretamente uma rede ou sub-rede IP, dando-se a impressão que a camada 3 esteja envolvida. As primeiras VLANs geralmente eram configuradas para melhorar

o desempenho reduzindo o tamanho do domínio de colisão em um segmento ethernet muito extenso. Como os novos switches solucionam este problema, as atenções se voltaram para a redução do domínio de broadcast na camada *Media Access Control* (MAC). Podendo os usuários ganhar mobilidade física dentro da rede a depender do tipo de configuração. O protocolo predominante atualmente é o IEEE 802.1Q e podem ser classificadas em estáticas ou dinâmicas (VLAN, 2011):

- Estáticas: VLANs estáticas (ou baseadas em portas) são criadas atribuindo-se cada porta do switch a uma VLAN. Quando um novo dispositivo se conecta a rede ele assume a VLAN da porta à qual ele está ligado. Em caso de mudança, se esse dispositivo for ligado a uma nova porta, para mantê-lo na VLAN original será necessário que o administrador de rede reconfigure manualmente as associações porta-VLAN.

- Dinâmicas: VLANs dinâmicas são criadas e alteradas dinamicamente via software, através de um servidor VMPS (*VLAN Management Policy Server*) e de um banco de dados que armazena os dados dos membros das VLANs. VLANs dinâmicas baseiam-se em critérios estabelecidos pelo administrador de rede, como o MAC address ou o nome do usuário de rede de cada dispositivo conectado ao switch.

O processo de interligar mais de uma VLAN através de um *link* único é chamado de *trunking*, por onde passam informações originadas por e destinadas a mais de uma VLAN. O *link* de tronco não pertence a nenhuma das VLANs individualmente, devendo ser utilizado um roteador ou switch de camada 3 como o backbone entre o tráfego que passa através de VLANs diferentes. Os Métodos de implementação do *trunking* são (VLAN, 2011):

- Marcação de quadro (*frame-tagging*) - 802.1Q: Modifica a informação contida dentro do quadro da camada 2, de modo que os switches possam identificar as VLANs de origem e destino e encaminhar o tráfego da forma adequada. O quadro ethernet aumenta de tamanho para comportar o campo adicional, e quando sai do switch o campo é retirado.

- Filtragem de quadro (*frame-filtering*): O switch procura por certo critério (MAC, IP) no quadro e usa este sistema de comparação para encaminhar o tráfego para sua VLAN e destino corretos.

2.5.4. Protocolos de redundância a falhas

O *Spanning Tree Protocol* (STP) é um protocolo para equipamentos de rede que permite resolver problemas de loop em redes comutadas cuja topologia introduza anéis nas ligações. O que possibilita a inclusão de ligações redundantes entre os switches, provendo caminhos alternativos no caso de falha de uma dessas ligações. Neste contexto, ele serve para evitar a formação de loops entre os switches e permitir a ativação e desativação automática dos caminhos alternativos (STP, 2011).

Para isso, o *Spanning Tree Algorithm* (STA) determina qual é o caminho mais eficiente, de menor custo, entre cada segmento separado por bridges ou switches. Caso ocorra um problema nesse caminho, o algoritmo irá recalcular entre os existentes, o novo caminho mais eficiente, habilitando-o automaticamente. O nome deriva do algoritmo *spanning tree* em teoria dos grafos.

O STA coloca cada porta de bridge ou switch no estado *forwarding* ou *blocking*. Considerando-se que todas as portas estejam no estado *forwarding* em um dado momento no *spanning tree*, o conjunto de portas no estado *forwarding* cria um único caminho pelo qual os quadros são enviados entre os segmentos ethernet.

Para viabilizar o cálculo do caminho de menor custo, é necessário que cada switch tenha conhecimento de toda a topologia da rede. A disponibilidade dessas informações é assegurada pela troca de quadros especiais chamados *Bridge Protocol Data Units* (BPDU) entre os switches. O protocolo BPDU auxilia na definição do estado das portas em um switch com STP ativa, estes estados são os seguintes (STP 802.1d, 2011):

- **BLOCKING** - Apenas recebendo BPDUs;
- **LISTENING** - O switch processa BPDUs e espera por possíveis novas informações que podem fazê-lo voltar ao estado de Bloqueio;
- **LEARNING** - Quando a porta ainda está "aprendendo" e montando sua tabela de endereços de origem dos frames recebidos;
- **FORWARDING** - A porta envia e recebe dados, operado normalmente. O STP continua monitorando por BPDUs que podem indicar que a porta deve retornar ao estado de bloqueio prevenindo um loop.
- **DISABLE** - Não está utilizando STP, podendo o administrador de rede desabilitar a porta manualmente.

O protocolo padrão 802.1D (STP) foi projetado na época em que quando era necessária uma recuperação de conectividade após uma interrupção, um minuto estava dentro da performance adequada. Com o advento dos switches de camada 3 em ambientes de LAN, a alta disponibilidade torna-se essencial.

O *Rapid Spanning Tree Protocol* (RSTP), padrão 802.1w, pode ser considerada uma evolução do STP e são compatíveis entre si. A diferença básica entre ambos é o número de estado de uma porta, que no RSTP são apenas três: *LEARNING*, *FORWARDING* e *DISCARDING*. As portas *root* e *designated* funcionam e as portas que estão no estado de bloqueio são de backup, atuando como alternativas. O padrão 802.1w pode também retroceder para o padrão 802.1D com a ideia de interoperar com todo o legado de bridges que não possuem o novo sistema (RSTP, 2011).

A porta que recebe o melhor BPDU numa bridge é uma porta *root*, que está mais próxima da *root* bridge em termos de custo do caminho. Para cada VLAN, o STA elege uma única porta *root* em toda a rede comutada. A bridge *root* é a única bridge na rede que não possui a porta *root*, todas as outras bridges recebem BPDUs por pelo menos uma porta. Uma porta é *designated* se a mesma transmite o melhor BPDU no segmento em que está conectada.

O *Multiple Spanning Tree Protocol* (MSTP), assim como o RSTP deriva do STP e apresentam melhoras em relação ao seu predecessor, permitindo um maior número de funcionalidades, além de melhor tempo de resposta. Originário do padrão 802.1s sendo depois incorporado ao IEEE 802.1Q, tem como concepção permitir que quadros atribuídos a diferentes VLANs sigam rotas diferentes de dados dentro das regiões estabelecidas administrativamente da rede (MSTP, 2011).

2.5.5. Servidores de rede

Esta seção aborda fundamental a aplicabilidade dos serviços de rede, que atuam como servidor na infraestrutura da rede, em especial os que de alguma forma colaboram com o gerenciamento da rede em alguma das funcionalidades tratadas no segundo capítulo.

a) Dynamic Host Configuration Protocol (DHCP)

O serviço *Dynamic Host Configuration Protocol* (DHCP) atribui automaticamente um endereço distinto para cada host da rede, permitindo o gerenciamento centralizado dos endereços IP de uma rede e evitando a configuração individual de cada computador, esta configuração consiste, basicamente, em determinar a faixa de endereços IP que os hosts da rede irão utilizar. E a utilização deste serviço é altamente recomendada em grandes redes, pois além de evitar que possa ser atribuído a mais de um host o mesmo endereço, facilita inclusive a implementação de outros serviços como atribuição de endereços de servidores *Domain Name System* (DNS) e gateway padrão (PALMA; PRATES, 2000).

O funcionamento do DHCP consiste da solicitação de um cliente da rede que ainda não tem endereço IP através de mensagens do tipo broadcast (*DHCP Discover*). Os servidores DHCP verificam suas tabelas se possuem endereços IP disponíveis e respondem ao cliente oferecendo um endereço IP, também via broadcast (*DHCP Offer*). Como uma rede pode conter mais de um servidor DHCP, o cliente pode receber mais de uma oferta de endereço, em geral aceitando a oferta mais rápida, e envia uma mensagem broadcast requisitando o endereço oferecido (*DHCP Request*). Todos os servidores recebem essa mensagem, de forma que o servidor que ofereceu confirma a atribuição (*DHCP Ack*), os demais servidores desconsideram suas ofertas, mantendo os endereços oferecidos disponíveis para novos clientes.

b) Servidor Squid

A principal aplicação de um servidor proxy Squid é a armazenagem em cache de todas as solicitações feitas a servidores web, reduzindo a utilização da conexão e melhorando o tempo de resposta, uma vez que só irá gerar uma nova solicitação à internet caso haja alguma modificação no site web já armazenado em cache ou ainda não acessado, o que melhora significativamente a utilização da banda de internet, ou seja o canal de saída e entrada da rede administrativa, proporcionando a gerência da rede melhor desempenho (SQUID, 2011).

Outra função possível do Squid é a de blacklist, onde o servidor proxy nega as solicitações indesejáveis previamente classificado pelo administrador da rede através de regras acl, o que além de beneficiar a segurança da rede, também reduz o tráfego dos pacotes.

2.5.6. Segurança operacional

Um firewall é uma combinação de hardware e software que isola a rede interna de uma organização da Internet em geral, permitindo que um administrador de rede controle o acesso entre o mundo externo e os recursos da rede que administra gerenciando o fluxo de tráfego, e possui três objetivos (KUROSE; ROSS, 2010):

- Todo o tráfego de entrada e saída passa por um firewall, situado diretamente no limite entre a rede administrativa e o resto da Internet, facilitando o gerenciamento e a execução de uma política de acesso seguro.
- Somente o tráfego autorizado, como definido pela política de segurança local, poderá passar, limitando o acesso a tráfego autorizado.
- O próprio firewall deve ser imune à penetração, por se tratar de um mecanismo conectado a rede, se não projetado ou instalado adequadamente, pode comprometer toda a segurança da rede.

O pfSense é uma poderosa plataforma de firewall e roteamento flexível, que inclui as seguintes características (PFSENSE, 2011):

- Filtragem por IP de origem e destino, porta de origem protocolo e IP de destino para o tráfego TCP e UDP;
- Capacidade de limitar as conexões simultâneas em uma base por regras;
- Opção de log ou não registrar o tráfego correspondente a cada regra.
- Política altamente flexível de roteamento possível, selecionando gateway em uma base por regras (para balanceamento de carga, *failover*, WAN múltipla, etc);
- *Alias* permiti o agrupamento e a nomeação de IPs, redes e portas. Isso ajuda a manter o seu conjunto de regras de firewall limpa e de fácil compreensão, especialmente em ambientes com múltiplos IPs públicos e diversos servidores.
- Normalização de pacotes “*Scrubbing*” é a normalização de pacotes para que não haja ambiguidades na interpretação pelo destino final do pacote. A diretiva *scrub* também remonta pacotes fragmentados, protegendo alguns sistemas operacionais de algumas formas de ataque, e descarta pacotes TCP que têm combinações de *flag* inválidas.
- Desativar filtro, podendo desligar o filtro de firewall completo se desejar transformando o pfSense em um roteador puro.

Para detectar muitos tipos de ataque, é preciso executar uma inspeção profunda de pacote, não apenas inspecionar o cabeçalho do pacote como atua o firewall, mas é preciso observar dentro dos dados da aplicação que o pacote carrega, e quando percebido algo suspeito ser impedido que tal pacote entre na rede corporativa (KUROSE; ROSS, 2010).

Para isso, a solução adotada pelo gerenciamento de segurança são os sistemas de detecção de intrusos. Sendo um dispositivo que gera alertas quando observa tráfegos potencialmente mal intencionados chamado *Intrusion Detection System (IDS)*, e o dispositivo que filtra o tráfego suspeito de *Intrusion Prevention System (ISP)*, ambos constituem um sistema de detecção de intrusos.

2.5.7. Wi-Fi

A expansão do acesso à tecnologia de rede sem fio é notável aos dias atuais. Embora muitas tecnologias e padrões para LANs sem fio tenham sido desenvolvidos na década de 1990, uma classe particular de padrões surgiu claramente como a vencedora: a LAN sem fio IEEE 802.11, também conhecida como Wi-Fi. A arquitetura mais detalhada de uma rede sem fio apresenta os seguintes elementos (KUROSE; ROSS, 2010):

- Hospedeiros sem fio, são os equipamentos de sistemas finais que executam aplicações, por exemplo, laptop, smartphone, tablet ou um computador de mesa, já que o próprio hospedeiro pode ser ou não um dispositivo móvel.
- Enlace sem fio, é o meio pelo qual um hospedeiro se conecta a uma estação-base, e as características do enlace são definidas pelos padrões, como por exemplo: 802.11b, 802.11a, 802.11g e 802.11n que são os padrões utilizados na infraestrutura da UESB.
- Estação-base, frequentemente será responsável pela coordenação da transmissão de vários hospedeiros sem fio com os quais está associada. No caso da UESB esta associação ocorre no modo de infraestrutura, já que todos os serviços tradicionais são fornecidos pela rede com a qual estiverem conectados por meio da estação-base.
- Infraestrutura de rede, é a rede maior com a qual um hospedeiro sem fio quer se comunicar, no caso a rede da UESB.

2.5.8. Protocolos de rede

A presente seção tratará apenas dos protocolos cujas finalidades ajudam de forma significativa alguma especificidade do gerenciamento de uma rede, uma vez que a diversidade de protocolos de rede já estão intrínsecos ao processo da rede de computadores.

a) Internet Group Management Protocol (IGMP)

O protocolo *Internet Group Management Protocol* (IGMP) é utilizado para especificar quais hosts pertencem a um grupo *multicast*. Sendo assim este protocolo pode ser utilizado para aproveitar melhor os recursos de uma rede de modo a informar aos roteadores a enviar o *multicast* apenas para os hosts pertencentes aos grupos. Os grupos *multicast* viabilizam a transmissão simultânea de um mesmo conteúdo para diversos computadores (PALMA; PRATES, 2000).

Os hosts de um grupo *multicast* enviam mensagens IGMP para o roteador responsável pela rede a fim de comunicar que naquela rede existem membros daquele grupo *multicast*. Os roteadores então notificam, através do IGMP, os roteadores adjacentes, para que mensagens direcionadas ao grupo *multicast* sejam encaminhada a ele, e por fim destinadas aos membros do grupo em sua rede.

O exemplo de utilização do protocolo IGMP mais direto é a transmissão de vídeo e áudio, em que uma única copia de cada quadro é enviada à rede e todos os hosts pertencentes ao grupo *multicast* especificado para essa transmissão receberão o mesmo quadro, reduzindo claramente o nível de utilização da rede.

b) Internet Control Message Protocol (ICMP)

O protocolo *Internet Control Message Protocol* (ICMP) é utilizado internamente pelo protocolo IP para fornecer informações sobre as condições de transmissão de pacotes numa rede TCP/IP ou sobre erros ocorridos no envio desses pacotes. O ICMP somente reporta condições de erros ao host que origina a mensagem e não a intermediários. E suas principais funções são (PALMA; PRATES, 2000):

- Indicar erros na rede, reportando situações como um host da rede que não pode ser localizado (por estar desligado, por exemplo) ou um pacote TCP ou UDP direcionado a um determinado número de porta onde não é encontrado o serviço correspondente. Normalmente, roteadores fazem uso do protocolo ICMP para informar ao host que originou uma mensagem os eventuais problemas encontrados durante a transmissão;
- Indicar congestionamento da rede, quando um roteador estiver recebendo pacotes em uma taxa maior do que pode transmitir, ele poderá enviar um mensagem ICMP ao emissor para que este diminua a velocidade com que está enviando os pacotes (*Source Quench*);
- Suporte a procedimentos de eliminação de erros, em que o ICMP implementa a função *Echo*, através da qual um pacote é enviado a um host com finalidade de teste e o este que recebeu um requisição *Echo* responde a quem a originou com um pacote igual ao recebido. Esta função é utilizada no PING para determinar a possibilidade de comunicação com determinados host e o respectivo tempo de resposta.
- Indicar número de hops excedidos, o valor do campo TTL de um pacote IP indica o número máximo de roteadores pelos quais ele pode passar para atingir seu destino (*hops*) e é decrementado em cada roteador. Se esse valor atingir zero, o roteador descarta o pacote e gera uma mensagem indicando tal fato.

Alguns firewalls bloqueiam as respostas (*ICMP Reply*), dificultando o PING e o TRACEROUTE, isso por diversas razões, dentre uma delas para bloquear os ataques de hackers, que consiste na sobrecarga da memória, enviando dados em PING até o sistema não ter a capacidade de administrar suas próprias funções.

2.5.9. Protocolos de gerenciamento

Esta seção irá tratar dos protocolos intrínsecos ao processo de gerenciamento que atuam na camada de aplicação, de forma a elucidar sua atuação na infraestrutura da UESB, portanto analisados apenas os que são suportados pelos hardwares e softwares desta rede.

a) Simple Network Management Protocol (SNMP)

O protocolo *Simple Network Management Protocol* (SNMP) permite coletar informações sobre o status dos dispositivos da rede, permitindo ao administrador da rede

realizar a monitoração do funcionamento do sistema, para isto possui o sistema de gerenciamento e agentes SNMP (SANTOS, 2004). O gerenciamento de rede na Internet é muito mais do que apenas um protocolo para transportar dados de gerenciamento entre entidade gerenciadora e seus agentes (KUROSE; ROSS, 2010). Com isso o protocolo SNMP passou a ser muito mais complexo do que seu próprio nome possa sugerir.

A estrutura de gerenciamento do padrão Internet é constituída de quatro partes, sendo a primeira a definição dos objetos de gerenciamento de rede, conhecidos como objetos MIB, que por sua vez representa uma coletânea de objetos gerenciados que, junto, formam um banco virtual de informações da estrutura de gerenciamento, mantidas por um dispositivo gerenciado. Objetos MIB relacionados são reunidos em módulos MIB.

A segunda parte é uma linguagem de definições de dados, conhecida como *Structure of Management Information (SMI)*, uma estrutura de informações de gerenciamento que define os tipos de dados, um modelo de objeto e regras para escrever e revisar informações de gerenciamento. Objetos MIB são especificados nessa linguagem de definição de dados.

Sua terceira parte é o protocolo SNMP que é usado para transmitir informações e comandos entre uma entidade gerenciadora e um agente que os executa em nome da entidade dentro de um dispositivo da rede gerenciado. Estes dispositivos mantêm contadores que indicam seu status, possibilitando aos agentes e sistema de gerenciamento apresentar ao administrador informações sobre a rede.

Os agentes SNMP atuam normalmente de forma passiva, somente fornecendo respostas a solicitações do sistema de gerenciamento. Ocorrendo uma exceção quando alguma situação anormal é detectada e então é enviada uma mensagem trap. Os sistemas de gerenciamento também podem solicitar aos agentes SNMP alterações de parâmetros configuráveis, como os limites para o envio de mensagens trap. Essas operações ocorrem através dos seguintes comandos enunciados na tabela 1:

Tabela 1 - Funções SNMPv2

Tipo de SNMPv2-PDU	Remetente-receptor	Descrição
GetRequest	gerente a agente	pega o valor de uma ou mais instâncias de objetos MIB
GetNextRequest	gerente a agente	pega o valor da próxima instância de objeto MIB na lista ou tabela
GetBulkRequest	gerente a agente	pega valores em grandes blocos de dados, por exemplo, valores em uma grande tabela
InformRequest	gerente a gerente	informa à entidade gerenciadora remota valores da MIB que são remotos para seu acesso
SetRequest	gerente a agente	define valores de uma ou mais instâncias de objetos MIB
Response	agente a gerente ou gerente a gerente	gerada em resposta a <i>GetRequest</i> , <i>GetNextRequest</i> , <i>GetBulkRequest</i> , <i>SetRequest PDU</i> ou <i>InformRequest</i>
SNMPv2-Trap	agente a gerente	informa ao agente um evento excepcional

Fonte: (KUROSE; ROSS, 2010, p.567)

Os projetistas do SNMPv3 têm dito que o “SNMPv3 pode ser imaginado como um SNMPv2 com capacidades adicionais de segurança e de administração” [RFC 3410]. O papel desempenhado pela segurança no SNMPv3 é particularmente importante, visto que a falta de segurança adequada resultava na utilização do SNMPv1 primordialmente para monitorar, em vez de controlar, visto que o comando SetRequest raramente era usada, pois a interceptação de mensagens e/ou geração de pacotes SNMP por um intruso poderia causar grande tumulto na rede. Sendo assim, crucial que estas mensagens sejam transmitidas com segurança. Para tanto, o SNMPv3 fornece criptografia, autenticação, proteção contra ataques de reprodução e controle de acesso.

O SNMP se traduz na ferramenta que possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver seus eventuais problemas, e fornecer informações para o planejamento de sua expansão.

O software de gerência de redes não segue o modelo cliente-servidor convencional, pois para as operações GET e SET a estação de gerenciamento se comporta como cliente e o dispositivo de rede a ser analisado ou monitorado se comporta como servidor, enquanto que na operação TRAP ocorre o oposto, pois no envio de alarmes é o dispositivo gerenciado que toma iniciativa da comunicação.

O programa gerente da rede é a entidade responsável pelo monitoramento e controle dos sistemas de hardware e software que compõem a rede, e o seu trabalho consiste em detectar e

corrigir problemas que causem ineficiência ou impossibilidade na comunicação e eliminar as condições que poderão levar a que o problema volte a surgir.

b) Remote Monitoring (RMON)

O protocolo *Remote Monitoring* (RMON) permite monitorar informações sobre a rede de forma mais detalhada, pois surgiu para superar limitações do protocolo SNMP, que pelo fato de residir na camada de aplicação e se utilizar de datagramas UDP, não tem conhecimento do que ocorre nas camadas inferiores como as de rede e de acesso à rede (PALMA; PRATES, 200).

A MIB RMON permite que as funções de monitoração sejam realizadas através da captura dos pacotes que transitam por uma sub-rede sem a interferência constante do gerente. A RMON é composta por nove grupos: *Statistics*, *History*, *Alarm*, *Host*, *HostTopN*, *Matrix*, *Filter*, *Packet Capture* e *Event* (PINHEIRO, 2002), esclarecido a seguir:

1. O grupo *Statistics* mantém estatísticas das interfaces do agente, por exemplo, o número de colisões.
2. *History* armazena amostras de informações colhidas no grupo *Statistics*.
3. O grupo *Alarm* fornece mecanismos usados para a monitoração de variáveis de gerenciamento do tipo *Integer*, com valores-limites configurados que podem disparar eventos ao serem atingidos pelo valor monitorado.
4. O *Host* contém informações referentes aos nodos da sub-rede, como o número de pacotes enviados por cada nodo.
5. O grupo *HostTopN* classifica as informações obtidas pelo grupo *Host*, gerando, por exemplo, os nodos que mais transmitiram pacotes.
6. O *Matrix* possui informações referente a comunicação entre dois nodos da sub-rede.
7. O *Filter* provê mecanismos de filtros para os pacotes recebidos da sub-rede, que podem disparar um evento ou um processo de armazenamento de pacotes.
8. *Packet Capture* armazena informações dos pacotes recebidos na sub-rede;
9. O *Event* controla a geração e notificação dos eventos definidos, por exemplo, um relativo a um alarme especificado no grupo *Alarm*.

2.5.10. Intelligent Management Center (IMC)

O Intelligent Management Center (IMC) é a plataforma de gerenciamento de última geração da 3Com, uma plataforma independente e abrangente com flexibilidade e escalabilidade para atender às necessidades de redes corporativas avançadas. Foi projetado em uma arquitetura orientada para serviços (SOA), tendo por núcleo um modelo de fluxo para aplicativos corporativos e apresentando uma estrutura escalonável modularizada (3COM, 2011; HP, 2011). A combinação permite a implementação eficiente de um gerenciamento corporativo ponta a ponta enquanto o design modular do IMC possibilita a integração efetiva de ferramentas de gerenciamento tradicionalmente isoladas, oferecendo um total gerenciamento de recursos, serviços e usuários.

O IMC oferece um amplo conjunto de recursos para o gerenciamento de grandes redes heterogêneas. A solução independente oferece escalabilidade e alta disponibilidade através de um modelo de implantação distribuído e flexível. Com design modular, o IMC pode ser implantado em vários servidores, oferecendo maior escalabilidade e resiliência.

O gerenciamento multiusuário baseado em funções permite administração e monitoramento flexíveis da infraestrutura de rede da organização. O Administrador do Sistema tem controle sobre quais usuários do IMC têm permissão para gerenciar dispositivos e grupos de dispositivos, e pode também restringir as operações realizadas pelos usuários (IMC, 2010). O Administrador do Sistema também tem acesso a trilhas de auditoria completas que detalham todas as modificações na rede e identifica quem as executou. Isso ajuda a garantir que os processos e controles necessários estejam em vigor para atender à conformidade.

O IMC oferece poderosos recursos de descoberta e topologia de rede, inclusive um inventário detalhado da rede e descrições altamente precisas de como ela está configurada. As visualizações compatíveis incluem Camada 2 e Camada 3, além de topologia VLAN e visualização personalizada. A visualização personalizada permite que o usuário organize e controle a infraestrutura de rede com base em qualquer modelo organizacional. O painel de gerenciamento de dispositivos integrado ao IMC oferece um amplo gerenciamento de elementos tanto para dispositivos 3Com quanto H3C.

O IMC oferece suporte ao processo completo de gerenciamento de falhas, oferecendo correlação e análise detalhadas, alarmes em tempo real, solução de problemas e captura de

experiência. A monitoração de desempenho fácil de usar detecta gargalos e outros problemas de rede, inclusive os relacionados a CPU, memória e utilização de largura de banda, tempo de resposta de dispositivos e disponibilidade (3COM, 2011). As estatísticas TopN permitem a rápida identificação das áreas e dos dispositivos mais carregados na rede. Um limiar pode ser definido para gerar alarmes em qualquer monitor, alertando rapidamente os operadores sobre eventuais problemas. Para que o operador não receba um excesso de alarmes, o IMC oferece a opção de definir eventos personalizáveis, além de regras de filtragem de alarmes e eventos.

O gerenciamento centralizado de relatórios simplifica a administração de relatórios da organização. Os relatórios históricos flexíveis do IMC fornecem as informações necessárias à análise de tendências da rede e planejamento de capacidade, oferecendo relatórios predefinidos ou permitindo que os usuários definam os parâmetros de seus próprios relatórios por meio de um gerador de relatórios.

O tempo necessário para a introdução de alterações na rede e a probabilidade de erros de configuração é enormemente reduzido com a poderosa funcionalidade de configuração em massa do IMC. A definição das configurações de linha de base (*baselining*) garante que as alterações feitas às configurações de rede estável sejam sinalizadas imediatamente (IMC, 2010). O poderoso recurso de comparação de configurações apresenta uma rápida identificação de diferenças entre as configurações, permitindo que o administrador do sistema aceite a nova configuração ou volte à configuração estável original. As funcionalidades adicionais incluem backup e restauração em massa, uma função de gerenciamento de agentes extremamente flexíveis que permite ao administrador do sistema total controle sobre o processo de atualização.

2.6. Considerações Finais

Os tópicos propostos neste capítulo visam o aprimoramento do conhecimento a cerca de gerenciamento e entendimento de tecnologias que surgem constantemente atendendo à crescente demanda de padrões para rede, possibilitando ao administrador nortear-se quanto a real importância das configurações da rede resultando em melhor desempenho e segurança da mesma, como também a possibilita a prevenção de falhas do sistema e contabilização dos recursos da rede e seu rendimento, servindo de referencial ao estudo da infraestrutura e tecnologias adotadas pela administração de rede da UESB.

3. Infraestrutura de redes da UESB campus VCA e tecnologias de rede

3.1. Considerações iniciais

O presente capítulo desenvolve o conteúdo referendado no capítulo anterior e apresenta a problemática analisada neste trabalho a cerca da infraestrutura e gerência de redes da UESB, através do setor especializado.

Fundada em 27 de maio de 1980, a UESB foi criada a partir de uma decisão do governo da Bahia em interiorizar o ensino superior no Estado. Desde 1987 a UESB teve autorização para funcionamento em sistema multicampi (Vitória da Conquista, Jequié e Itapetinga), sendo o campus de Vitória da Conquista, o principal objeto do presente estudo. O capítulo abordara também as tecnologias de rede utilizadas pela UESB.

3.2. Antiga infraestrutura de rede da UESB

A antiga infraestrutura de redes da UESB como um todo era descentralizada o que inibia um gerenciamento proativo da rede. Os módulos externos ao campus de Vitória da Conquista ora eram atendidos por roteadores, nos casos dos campi de outro município, o que além de retardar os serviços de rede também acabava por ocultar sua LAN da rede local, ora atendidos por *Virtual Network Private* (VNP), como no caso do Núcleo de Práticas Jurídico e o museu Regional, criando-se dependências dos serviços de internet.

O próprio gerenciamento da rede no campus de VCA era impossibilitado devido sua infraestrutura de rede apresentar-se desorganizada e cascadeada, causando grande prejuízo ao tráfego da rede pelo próprio broadcast criado, e um prejuízo ainda maior pela ausência de uma devida documentação para análise da rede como um todo.

Por vezes, causando inconsistências na rede de difícil resolução, já que os mecanismos disponíveis eram o conhecimento técnico humano e ferramentas de rede como testador de cabo par trançado e alicate RJ-45. Ocasionalmente um enorme tempo para descoberta do problema, ainda por vezes mascarado em *loops* decorrentes do cascadeamento entre switches.

3.3. Departamento de Modernização da Informática

Em princípio, foi criando o Departamento de Modernização da Informática (DMI), que geria uma rede voltada ao atendimento de uma demanda simples, em que, basicamente, atendia alguns setores administrativos e, isoladamente, o setor acadêmico, em específico a Secretaria Geral de Cursos, principalmente no atendimento a necessidade de compartilhamento de dispositivos em rede, devido a escassez até mesmo de computadores para atender a todas as demandas da UESB.

Durante um longo período a ampliação do parque computacional da UESB deu-se por etapas muito espaçadas, em detrimento de poucos recursos, o que sem dúvida contribuiu para o crescimento desorganizado e heterogêneo das tecnologias de redes. Impossibilitando uma administração efetiva da mesma e por vezes provendo apenas ajustes técnicos, culminando em uma rede sucateada, devido ao aproveitamento de tecnologias ultrapassadas, conforme foi ressaltado nas figuras 2 e 3, que permaneceram como um legado por muito tempo.

Figura 2 - Foto dos modems da antiga infraestrutura de UESB



Fonte: próprio autor

Figura 3 - Foto do enlace entre switch da antiga infraestrutura da UESB



Fonte: próprio autor

3.4. Unidade Organizacional de Informática

Com o advento de novas tecnologias de rede, a informação torna-se a principal e mais importante ferramenta de uma organização, podendo esta ser de conhecimento público ou privativo. O domínio da informação exige processos que garantam os resultados buscados através de tarefas como manipular, minerar, centralizar na base de dados e a distribuir estes dados aos hosts da rede de computadores.

Com isso, a demanda de rede passou por vários processos de crescimento, como o surgimento de novos cursos, por conseguinte ampliação do número de laboratórios e novos setores, conseqüentemente a construção de novos módulos, além da necessidade de sistemas que possibilitem sua informatização. O que veio a ser o fator determinante na mudança do setor DMI para uma nova acessória, a UINFOR, tendo como meta a adequação de recursos à necessidade de informatização da instituição.

Hoje, o campus de VCA conta com 20 cursos de graduação, versados nas mais diversas áreas do conhecimento, o que perfaz um total de 4091 discentes matriculados nos cursos de graduação, os quais são assistidos atualmente por um corpo de 491 docentes e mais 346 funcionários administrativos e outros 283 prestadores de serviços, conforme informações prestadas pela Gerência de Recursos Humanos da UESB. Para atender toda esta clientela a infraestrutura acadêmica conta com 29 módulos distribuídos geometricamente pela ampla área do campus, além dos núcleos externos.

No que se refere à infraestrutura de redes da UESB administrada pela UINFOR cabe salientar que a atual composição da rede passa por um processo de reestruturação que já conta hoje com novos 37 switches de borda, 11 switches de distribuição, 2 switches que serve a servidores da rede e 3 switches core que compõe o núcleo da rede, todos com interfaces gerenciáveis, em interoperabilidade com os da estrutura antiga, e ora substituindo definitivamente os mesmos. Em face da mensura que a infraestrutura de rede se apresenta, contabiliza-se mais de 1200 interfaces disponíveis aos hosts de ethernet, contando ainda com 32 Access Point (AP), espalhados pelo campus VCA em recepção aos hosts wireless, com uma licença para até 48.

3.5. Topologia e infraestrutura de rede do campus VCA

Três são as características que distinguem os tipos de redes: tamanho, tecnologia de transmissão e topologia (SOARES, 1995; TANENBAUM, 2003). Em análise ao tamanho ocupado geograficamente pela infraestrutura de rede do campus VCA, está, portanto classificada como uma rede local, comumente chamada de LAN, conforme escala apresentada pela fotografia de satélite disponibilizada pela *Google Maps*, figura 4.

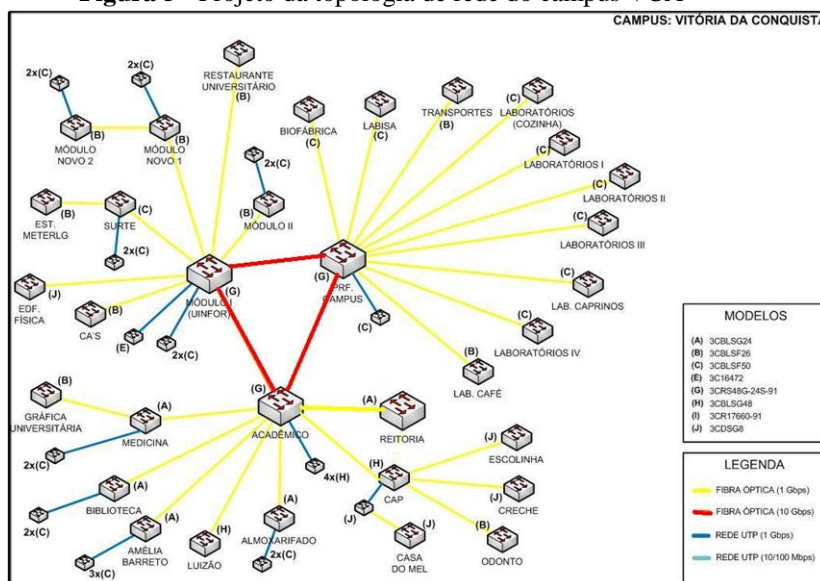
Figura 4 - Fotografia de satélite do campus VCA



Fonte: Google Maps

Mas em seu interesse e aos núcleos externos, ora situados inclusive em outros municípios, a UESB ingressou na rede ipê metropolitana da Rede Nacional de Ensino e Pesquisa (RNP, 2011), por fibra óptica contando com um *link* dedicado de 100 Mbps de banda, rede essa que prover entre outros diversos serviços, o acesso à internet. O planejamento da topologia da rede do campus VCA pode ser mais bem notado na figura 5.

Figura 5 - Projeto da topologia de rede do campus VCA



Fonte: Repositório da gerência de rede da UESB















Na topologia, é possível observar que além da utilização da estrutura de anel no núcleo, suas ramificações ocorrem com profundidade de poucos nós, sendo a maior parte em formato estrela, o que reduz a distância e, por conseguinte o tráfego em relação à comunicação dos switches de borda e distribuição com o switch core. O detalhamento das interfaces dos switches core é descrito nas figuras 6, 7 e 8, para melhor entendimento. Nas extremidades ficam os switches de borda, os quais realmente se interligam aos hosts, observando-se uma variação de velocidades entre *fast-ethernet* e *gigabit-ethernet*, conforme as velocidades de negociação entre as interfaces dos switches e as dos hosts propriamente.

Figura 6 - Relação das interfaces do switch core localizado no módulo acadêmico

4800G – UNIT 1 (MÓDULO ACADÊMICO)															
2	4	6	8	10	12	14	16	18	20	22	24	26/18	28/20	30/22	32/24
1	3	5	7	9	11	13	15	17	19	21	23	25/17	27/19	29/21	31/23
Legenda:															
Reitoria (LA 1)	Wireless (LA 5)														
Acadêmico (LA 2)	Saida – Firewall														
Amélia (LA 3)	Server Farm 1 (LA 6)														
Luizão	Server Farm 2 (LA 7)														
Medicina (LA 4)	Portas desligadas														
















Fonte: Repositório da gerência de rede da UESB

Figura 7 - Relação das interfaces do switch core localizado no módulo da UINFOR

4800G – UNIT 2 (UINFOR)															
2	4	6	8	10	12	14	16	18	20	22	24	26/18	28/20	30/22	32/24
1	3	5	7	9	11	13	15	17	19	21	23	25/17	27/19	29/21	31/23
Legenda:															
	Módulo TV (LA 8)		Módulo Educação												
	Módulo II (LA 9)		Estação Meteorológica 2												
	Estação Meteorológica 1		Módulo UINFOR (LA 10)												
	Educação Física		Server Farm Backup UINFOR												
	Biblioteca (LA 13)		Server Farm Remoto 1 (ACADEMICO) (LA 6)												
	Módulo IV		Server Farm Remoto 2 (ACADEMICO) (LA 7)												
	Módulo Eng. Florestal		Portas desligadas												

Fonte: Repositório da gerência de rede da UESB

Figura 8 - Relação das interfaces do switch core localizado no módulo da Prefeitura de Campus

4800G – UNIT 3 (PCU)															
2	4	6	8	10	12	14	16	18	20	22	24	26/18	28/20	30/22	32/24
1	3	5	7	9	11	13	15	17	19	21	23	25/17	27/19	29/21	31/23
Legenda:															
	GAD (LA 11)		Setor de transporte												
	Módulo de Odontologia (LA 12)		PCU												
	Melhoramento animal		COPEVE												
	Laboratório de Solos		Server Farm remoto 1 (ACADEMICO) (LA 6)												
	Caprinos		Server Farm remoto 2 (ACADEMICO) (LA 7)												
	Biofábrica		Nematologia												
	Labisa		Portas desligadas												
	Laboratório de Águas														

Fonte: Repositório da gerência de rede da UESB

Integrado a toda esta trama de switches encontram-se ainda os APs, os quais são geridos por um Wireless LAN Switch, interligado direto ao núcleo da rede. A tecnologia wireless ofertada em uma grande extensão do campus VCA oferece mobilidade aos seus usuários em essencial a classe docente e discente, atendendo em geral a smartphones, net e notebooks ou quaisquer outros dispositivos com tecnologia Wi-Fi.

Além de acesso à internet, a infraestrutura de rede provê aproximadamente 28 servidores que atendem as necessidades acadêmicas e administrativas dos três campi da UESB (podendo ser observado alguns na figura 9), o que por si requer uma melhor administração dos recursos computacionais como um todo, em fundamental a rede de computadores devido aos gargalos que esta possa sofrer ocasionado pela crescente demanda, ora apresentada.

Figura 9 – Servidores de mesa da UESB

Fonte: próprio autor

Como toda a infraestrutura da rede depende da infraestrutura elétrica, a disponibilidade da rede na UESB não pode ficar refém ao serviço de fornecimento elétrico e suas instabilidades, para isso existe um grupamento gerador elétrico e um conjunto de nobreaks para o núcleo da rede e os servidores, conforme figura 10, além de estabilizadores elétricos para os demais switches da rede, na tentativa de suprir a dependência elétrica, o que garante em si, uma melhor disponibilidade dos serviços na rede.

Figura 10 – Foto de nobreak de alimentação de servidores

Fonte: do próprio autor

Com a reestruturação, a UINFOR visa fornecer um serviço condizente com o seu parque computacional para longo prazo, atendendo a normatização e padrões de rede como pode ser notado nas figuras 11 e 12. Atendendo ao crescimento na demanda com um coeficiente ótimo de largura de banda tanto nos serviços da sua intranet quanto na utilização da Internet.

Figura 11 – Foto do bastidor de fibras da Telemar na sala de servidores



Fonte: próprio autor

Figura 12 – Foto do switch core da sala de servidores



Fonte: próprio autor

3.6. Classificações das tecnologias de rede quanto às classes de gerência

Esta seção tratará analiticamente as tecnologias discutidas do segundo capítulo bem como apresentará o serviço das mesmas na infraestrutura de redes da UESB classificando-as quanto aos aspectos gerenciais também discutidos no capítulo anterior.

O planejamento da utilização do protocolo IRF no núcleo da rede da UESB do campus VCA, visa trazer inúmeras vantagens como redundância a falhas, o que implica em alta disponibilidade e melhora do desempenho, além de facilitar o gerenciamento, uma vez que uma configuração única é adotada pela “caixa”. E se um Switch empilhado apresentar algum problema, como por exemplo, problemas elétricos, os outros switches serão capazes de permitir a continuidade do encaminhamento em camada 2 e 3, incluindo processos de roteamento dinâmico.

Uma das características que podem ser utilizadas neste cenário é a utilização de *link* de agregação distribuído (*Distributed Link Aggregation*) entre os equipamentos do IRF com switches de acesso, sem configuração adicional no *Link Aggregation*, o que traria como benefício um maior nível de redundância (HP, 2011). Mas a utilização desta característica fica impossibilitada por ora, uma vez que no projeto inicial de infraestrutura do campus VCA da UESB não foi sondado a possibilidade da mesma, o que implica na inexistência de fibras redundantes para o enlace entre os switches de distribuição a mais de um dos switches core, uma vez que embora estejam empilhados de forma lógica, suas reais localizações na topologia se encontram em módulos distintos.

A infraestrutura da rede da UESB no campus VCA conta com a utilização de 3 switches 4800G SFP da 3COM no núcleo da rede distribuídos em locais distintos da topologia com a utilização de módulos 10-Gigabit interligados por *transceivers* XFP, funcionam como logicamente empilhados formando uma única caixa devido o emprego do protocolo IRF, o que resulta nos benefícios já tratados, e notoriamente atende ao modelo de gerenciamento OSI tratado no capítulo anterior.

A agregação de banda na infraestrutura do campus VCA tanto pode ser observada na ligação dos switches core com os switches de distribuição através da agregação de fibras ópticas que na ideia inicial serviriam de redundância a falhas e devido a faculdade do *link*

aggregation passam a aumentar o tamanho de banda passante, operando como recurso para evitar gargalos na rede. Como também pode ser observado na ligação dos switches de distribuição aos switches de borda através da agregação de pares metálicos em dependência do número de hosts atendidos e da real necessidade de *throughput*, atendendo tanto a gerência de falhas, quanto a de desempenho e configuração.

A ideia de poder ter varias VLANs na infraestrutura da UESB, contempla o projeto de rede como um todo uma vez que todas estas ficam visíveis a administração da rede, facilitando as tarefas de gerência do modelo OSI como planejar, monitorar e reagir as falhas, sendo utilizadas VLAN estáticas devido a facilidade de configuração e segurança.

Outro benefício é o de isolar o domínio de broadcast, reduzindo o tráfego desnecessário na camada de rede, evitando assim problemas de *throughput*, o que melhora significativamente o desempenho da rede como um todo. Também há uma possibilidade de melhorar a configuração, uma vez que setores que atuem em atividades similares possam pertencer à mesma VLAN independentemente da topologia da rede, garantindo melhor assistência aos recursos necessários e evitando acesso indesejado de outras redes, o que implica em uma maior segurança.

No caso da infraestrutura planejada pela UESB os switches core que compõe a caixa no núcleo da rede atua como bridge *root* e cada VLAN elegerão suas portas *root* e *designated* entre os switches comutados em toda rede, e caso venham a apresentar *loop* na estrutura definam as portas bloqueadas. Mas como a configuração prever um tráfego direcionado entre os switches de acesso e os switches core e não apresentam ideia de regiões na sua topologia, foi adotado o protocolo RSTP ao invés do MSTP, atuando o protocolo RSTP também como um agente preventivo a falha no gerenciamento da rede.

Conforme visto no funcionamento do serviço DHCP, uma rede pode ser atendida por diversos servidores, o que é uma inconsistência para a rede, caso haja servidores DHCP impróprios na mesma. Sento este um problema já enfrentado na antiga infraestrutura de rede da UESB, vez que dispositivos roteadores wireless, têm habilitado a disponibilidade de servir DHCP, ocasionando atribuições de IP indesejáveis aos hosts da rede cabeada, que necessitam de endereço específico para utilização de recursos da rede da UESB.

Os switches gerenciáveis solucionam o impasse quanto à atribuição indevida por parte de servidores DHCP indesejáveis através do *DHCP Trust*, que estabelece quais portas são

confiáveis para comunicação de serviços DHCP, proporcionando um duplo benefício à rede que passa a ter um serviço DHCP confiável e como todas as comunicações das mensagens são através de broadcast, a customização de portas exclusivas para este propósito reduzem o tráfego desnecessário na rede, atendendo as expectativas da gerência de desempenho e segurança da rede.

O serviço SQUID conforme exposto no capítulo anterior atua principalmente na gerência de desempenho uma vez que reduz significativamente o tráfego com a rede externa e como benefício torna o acesso à internet mais rápido, e embora não seja utilizado como recurso de segurança pela infraestrutura de rede da UESB, pode ser uma opção a gerência de segurança, vez que pode atuar como tal.

Firewalls são a mais importante ferramenta de segurança usada para tratar de conexões de rede entre duas organizações que não confiam uma na outra (COMER, 2007). E como solução a esta questão a administração da UESB utiliza o pfSense que é um sistema de fonte aberta com base no *FreeBSD*, adaptado para uso como um firewall e roteador.

Na Infraestrutura de rede da UESB o pfSense atua como um firewall *state full*, permitindo que conexões originárias da rede administrativa possa permanecer ativa em uma nova portas negociada, mesmo que o serviço esteja negado para entrada na rede administrava, caso a solicitação fosse oriunda da Internet.

E como tecnologia de detecção de intrusos a gerência de rede da UESB utiliza o Snort que é um código aberto IDS/IPS que combina os benefícios de assinatura, protocolo e anomalia baseada em inspeção. O Snort possui três modalidades principais (SNORT, 2011):

- *Sniffer* é o responsável por leitura de pacotes que trafegam pela rede;
- *Packet Logger* registra os pacotes de log para o disco;
- *Network Intrusion Detection System* que permiti o Snort analise o tráfego da rede e detecte tentativas de invasão, por *rules* definidas pelo usuário.

Já rede Wi-Fi do campus VCA anteriormente era constituída por diversos roteadores AP wireless, configurados de forma independente, servindo restritamente a alguns setores específicos do campus. Na nova infraestrutura a abrangência da rede Wi-Fi deu-se pela substituição dos roteadores wireless independentes, por uma tecnologia Wireless LAN Switch que centraliza todas as configurações da rede Wi-Fi de forma que os APs obtêm todos os

parâmetros da rede a partir do Wireless LAN Switch, que por sua vez fica responsável por prover a mobilidade aos hospedeiros entre as diversas estações-base, conforme saem da área de cobertura de uma determinada estação-base para outra.

O protocolo IGMP é algo a ser estudado pela administração de rede da UESB, visto a possibilidade de se realizar conferências áudio visuais entre os seus campi ou mesmo com outras instituições através da internet que é uma necessidade cada vez mais crescente no âmbito acadêmico, além de poder proporcionar uma customização quanto à implementação do sistema vídeo vigilância para segurança no campus através de câmeras IP, devendo ser tomadas as devidas precauções já que a utilização do protocolo IGMP é susceptível a ataques.

A UESB utiliza o protocolo ICMP em face às vantagens que o mesmo proporciona a administração da rede, possibilitando o diagnóstico e resolução de problemas como os erros de roteamento através do TRACEROUTE e o PING quanto ao tempo de resposta que um host leva para comunicar-se, mas o seu firewall (*State Full*) bloqueia o PING originado de host externo a rede, justamente prevenindo possíveis ataques, tanto em demanda da gerência de falhas quanto a de segurança.

E a gerência de uma rede pode não ser simples, dada sua heterogeneidade em termos de hardware e software, e de componentes da rede, por vezes incompatíveis. As falhas intermitentes, se não forem detectadas, podem afetar o desempenho da rede. Um software de gerência de redes permite ao gestor monitorar e controlar os componentes da sua rede. Para isto, uma rede gerida pelo protocolo SNMP é formada por três componentes-chaves: dispositivos geridos, agentes e sistema de gestão de rede, que no estudo de caso da infraestrutura da UESB correspondem aos switches gerenciáveis, os agentes que atuam na rede e o *Intelligent Management Center* (IMC) que é a nova ferramenta de gestão de rede da *Hewlett-Packard* (IMC, 2010).

Outra tecnologia de gerência é o RMON, este protocolo em dispositivos de rede mais sofisticados permite ao sistema de gerenciamento monitorar todas as camadas do modelo DARPA, as definições do RMON1 em (RFC 1757, 2011) e do RMON2 em (RFC 2021, 2011; RFC 2034, 2011) (PALMA; PRATES, 2000). O protocolo RMON é nativo aos switches gerenciáveis da 3COM e ao IMC (IMC, 2010), sendo utilizado no monitoramento pela gerência de rede da UESB, suprimindo algumas deficiências do SNMP.

Já o IMC consiste por tanto como a principal ferramenta de monitoramento e administração de rede da UESB, uma vez que pelas características evidencias a respeito desta no capítulo anterior, suas funcionalidades se enquadram perfeitamente ao modelo de gerenciamento funcional abordadas também no segundo capítulo do presente trabalho, trabalhando perfeitamente com as tecnologias de rede também apresentadas neste capítulo.

O envolvimento das tecnologias estudadas e utilizadas na infraestrutura de rede da UESB com as classes de gerência do modelo OSI revisado no capítulo anterior, conforme as observações práticas obtidas pelas suas utilizações, descrita nesta seção, pode ser melhor analisada e evidenciada na Tabela 2:

Tabela 2 - Classificações das tecnologias de rede quanto às classes de gerência.

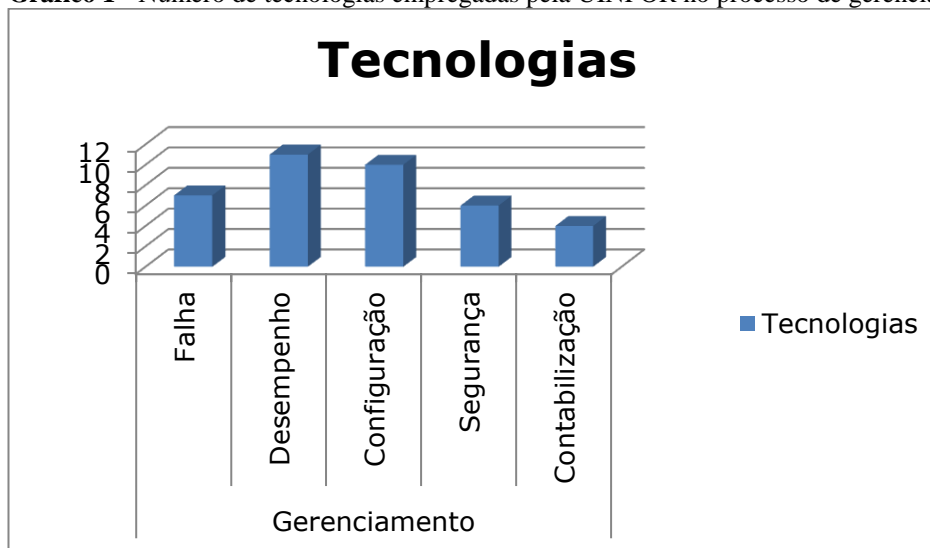
Tecnologias	Gerenciamento				
	Falha	Desempenho	Configuração	Segurança	Contabilização
IRF	X	X	X		
Link Aggregation	X	X	X		
VLAN		X	X	X	X
RSTP	X	X			
DHCP			X	X	X
SQUID		X		X	
pfSense		X	X	X	X
SNORT		X		X	
Wi-Fi		X	X		
IGMP		X			
ICMP	X	X	X		
SNMP	X		X		
RMON	X		X		
IMC	X	X	X	X	X

Fonte: Gerência de rede da UINFOR

Conforme Kurose (2010) a gerência de desempenho e configuração atuam de forma bastante intensa na infraestrutura de rede, uma vez que o gerenciamento de desempenho é responsável pela medição e disponibilização das informações sobre aspectos de desempenho dos serviços de rede e o gerenciamento de configuração possibilita ao administrador identificar quais os dispositivos que fazem parte da mesma, auxiliando o processo de planejamento e monitoração além de influir na gerência de falha que deve prevenir, detectar e reagir às anomalias que venham a ocorrer na rede de computadores, e por este aspecto uma grande gama de tecnologias trabalha de forma comitante para obtenção de maior êxito e por

vezes aproximando significativamente os processos desempenhados pelas demais gerências da rede conforme pode ser observado na Tabela 2 e quantificado no Gráfico 1:

Gráfico 1 - Número de tecnologias empregadas pela UINFOR no processo de gerência.



Fonte: Gerência de redes da UINFOR.

As interações encontradas entre os processos de gerência servem para validar a afirmação de Comer (2007), que nenhuma tecnologia de rede é a melhor para todas as necessidades. Devendo por tanto a administração da rede da UESB se ater bem ao planejamento da reestruturação de modo a evitar retrabalho o que sem dúvida gera ônus ao projeto. A implementação deve seguir os devidos padrões e principalmente documentar todo o projeto, facilitando a manutenção da rede e deixando-a estável, algo inédito à rede da UESB, pois nunca houve uma devida documentação de rede.

3.7. Considerações finais

Sendo este o principal capítulo do presente trabalho, o mesmo buscou reforçar a importância sobre os processos envolvidos na infraestrutura e gerência de rede, conforme o abrangente conteúdo referenciado no trabalho, utilizando-se, como estudo de caso, a reestruturação da rede da UESB. Para tanto foi abordada parcialmente uma gama de tecnologias que estão vinculados ao seu processo de planejamento e gerenciamento, não se esgotando das mais diversas possibilidades de configuração, nem de tecnologias de rede que podem vir a ser utilizadas, o trabalho no então não pode quantificar alguns aspectos devido a ausência de informações que pudessem ser comparadas e devido o trabalho de reestruturação ainda estar na etapa de execução.

4. Conclusão e trabalhos futuros

4.1. Conclusão

A investigação da área relativa à infraestrutura de redes e seu gerenciamento, habilita ao administrador de uma rede trabalhar de forma proativa, uma vez que o referencial teórico aliado ao conhecimento técnico sobre a rede global possibilita um melhor planejamento do que deve ser feito e de armadilhas que devem ser evitadas nas tomadas de decisões no âmbito gerencial. O emprego de protocolos de rede, que, em geral, atuam em diferentes camadas, seja no modelo OSI ou Internet, possibilitam um monitoramento da rede, permitindo ao administrador perceber e reagir a anomalias e assim, diagnosticar e solucionar mais facilmente os problemas que possam ocorrer e ,ainda, controlar o desempenho da rede através de lineares que determinam a qualidade da rede e de seus serviços como um todo.

O presente trabalho evidenciou a relevância do gerenciamento de rede, em face da importância de suas ferramentas, de modo a garantir soluções a possíveis falhas que podem ocorrer desde o projeto de infraestrutura, até a tarefa de gerenciamento que, em fundamental, deve atuar nas áreas de gerência de falha, configuração, desempenho, contabilidade e segurança. Sem, contudo, sondar especificidade de todos os protocolos e tecnologias de redes, visto que os processos de aquisição pelas instituições públicas passam por todo um processo licitatório, descartando a preferência por determinado equipamento ou fabricante.

Ainda ficou evidenciado que embora o modelo OSI para gerenciamento funcional da rede esteja dividido em cinco classes de gerência, visando facilitar o processo. O gerenciamento, como um todo, ocorre de forma associada, sendo que cada classe é complementar as outras, pois atuam diretamente em suas performances.

4.2. Trabalhos futuros

É notória a vasta amplitude de ferramentas e tecnologias que abrangem a área computacional de redes de computadores. Linear ao presente trabalho esta a possibilidade de se realizar diversos estudos de casos de ferramentas e tecnologias, em específico, como um estudo de caso sobre o equipamento Wireless LAN Switches da 3COM.

Outra possibilidade de trabalho futuro é um estudo comparativo entre as diversas ferramentas de gerência de rede, seus padrões e protocolos utilizados, como por exemplo: o TIVOLI da IBM, SMS da Microsoft, UniCenter da Computer Associates, ManageWise da Novell, CiscoWorks da Cisco, IMC da 3COM recentemente incorporado a HP e o próprio OpenView da HP.

Referências bibliográficas

- 3COM, 2011. Acesso em 30/08/2011. Disponível em: <<http://blog.gruppen.com.br/Anexos/IMC%20-%20A%20nova%20ferramenta%20de%20gerenciamento%20da%203Com.pdf>>.
- ABOBA, Bernard. *IPsec-NAT Compatibility Requirements*. draft-ietf-ipsecnat-reqts-00, 2000.
- ANSI, 2011. Acesso em 30/8/2011. Disponível em: <<http://webstore.ansi.org/NewsDetail.aspx?NewsGuid=5a44537c-7dcd-40e4-9ade-e72828b4b3f0>>.
- BRISA. *Gerenciamento de Redes - Uma abordagem de Sistemas Abertos*, Makron Books, 1993.
- COMER, Douglas E. *Redes de computadores e internet*, 4ª ed. Porto Alegre: Bookman, 2007.
- GIL, A. C. *Como elaborar projetos de pesquisa*. [S.l.]: Editora Atlas, 2002.
- HP, 2011. Acesso em 15/9/2011. Disponível em: <<http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA2-9402ENW.pdf>>.
- IEEE 802.1. Acesso em 14/9/2011. Disponível em: <<http://www.ieee802.org/1/>>.
- IEEE 802.2. *Logical Link Control (LLC)*. Acesso em 14/9/2011. Disponível em: <<http://www.ieee802.org/2/>>.
- IEEE 802.3. *Carrier Sense-Multiple Access with Collision Detection*. Acesso em 14/9/2011. Disponível em: <<http://www.ieee802.org/3/>>.
- IEEE 802.4. *Token bus*. Acesso em 14/9/2011. Disponível em: <<http://tools.ietf.org/html/rfc1230>>.
- IEEE 802.5. *Token ring*. Acesso em 14/9/2011. Disponível em: <<http://www.ieee802.org/5/>>.
- IEEE 802.6. *Distributed Queue Dual Bus*. Acesso em 14/9/2011. Disponível em: <<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=180821&userType=inst>>.
- IEEE802, 2011. *IEEE 802 LAN/MAN Standards Committee*. Acesso em 14/9/2011. Disponível em: <www.ieee802.org/>.
- IMC, 2010, *IMC Platform Administration Course Materials*, Hewlett-Packard.
- JAKOBSON, Gabriel. *Alarm correlation*. IEEE Network, 1993.
- KATZELA, Irene. *Distributed Fault Identification in Telecommunication Networks*. J. Network Syst. Manage, 1995.
- KUROSE, James F. e ROSS, Keith W., *Redes de computadores e a Internet: uma abordagem top-down*, 5ª ed. São Paulo: Addison Wesley, 2010.
- LA, 2011. *Link Aggregation*. Acesso em 16/9/2011. Disponível em: <<http://www.ieee802.org/3/ad/>>.
- LEINWAND, A.; CONROY, K. F. *Network Management – A Practical Perspective*. 2ª ed. Addison-Wesley:1996.
- MEDHI, *Models for network design, servicing and monitoring of ATM networks based on the virtual path concept*. IEEE Trans. Commun, 1997.
- MELCHORS, Cristina. *DUMBO: Uma Abordagem para Gerenciamento de Falhas Utilizando Raciocínio Baseado em Casos*. Porto Alegre: UFRGS. Dissertação de Mestrado apresentada ao departamento de Ciência da Computação, 1999.
- MSTP, 2011. Acesso em 17/9/2011. Disponível em: <<http://www.ieee802.org/1/pages/802.1s.html>>.
- PALMA, Luciano; PRATES, Rubens, *TCP/IP , Guia de Consulta Rápida*, Novatec Editora, 2000.

PFSense, 2011, Acesso em 17/9/2011. Disponível em: <<http://www.pfsense.org/>>.

PINHEIRO, José M. dos S, 2002. *Gerenciamento de Redes*. Acesso em 30/8/2011. Disponível em: <<http://www.allnetcom.com.br/upload/GerenciamentodeRedes.pdf>>.

RFC 1757. *Remote Network Monitoring Management Information Base*. Acesso em 14/9/2011. Disponível em: <<http://tools.ietf.org/html/rfc1757>>.

RFC 2021. *Remote Network Monitoring Management Information Base Version 2 using SMIV2*. Acesso em 14/9/2011. Disponível em: <<http://tools.ietf.org/html/rfc2021>>.

RFC 2034. *SMTP Service Extension for Returning Enhanced Error Codes*. Acesso em 14/9/2011. Disponível em: <<http://tools.ietf.org/html/rfc2034>>.

RFC 3053. *Internet Engineering Task Force*. Acesso em 14/9/2011. Disponível em: <<http://www.ietf.org/rfc/rfc3053.txt>>.

SANTOS, Fábio J. J. dos. 2004. *Sistema de gerenciamento de redes baseado em conhecimento*. Acesso em 21/8/2011. Disponível em: <www.ginux.ufla.br/files/mono-FabioSantos.pdf>.

SAYDAM, T., *From Networks and Network Management into Service and Service Management*, jornal of Networks and System Management, 1996.

SILVA, E. L. D.; MENEZES, E. M. *Metodologia da Pesquisa e Elaboração de Dissertação*. Editora da UFSC, 2005.

SNMP, 2011, Acesso em 12/9/2011. Disponível em: <http://pt.wikipedia.org/wiki/Simple_Network_Management_Protocol>.

SNORT, 2011. Acesso em 14/9/2011. Disponível em: <<http://www.snort.org>>.

SOARES, Luiz Fernando G. *Redes de computadores: das LANs, MANs e WANs às redes ATM*. Rio de Janeiro: Campus, 1995.

STP, 2011. Acesso em 12/9/2011. Disponível em: <http://pt.wikipedia.org/wiki/Spanning_Tree_Protocol>.

SQUID, 2011. Acesso em 17/9/2011. Disponível em: <<http://www.squid-cache.org/>>.

STEINDER, Malgorzata. *Distributed fault localization in hierarchically routed networks*. M Steinder, A Sethi, LNCS: Proceedings of DSOM, 2002.

STP 802.1d, 2011. Acesso em 12/9/2011. Disponível em: <http://en.wikipedia.org/wiki/Spanning_tree_protocol>.

SWITCH H3C, 2011. Acesso em 15/9/2011. Disponível em: <<http://comutadores.blogspot.com/2010/12/switches-h3c-7500-irf-v2-utilizando.html>>.

TANENBAUM, Andrew S. *Redes de computadores*, 4ª ed. Rio de Janeiro: Campus/Elsevier, 2003.

THOTTAN, M. and C. Ji, *Proactive Anomaly Detection Using Distributed Intelligent Agents*. IEEE Network Magazine 1998.

TORRES, Gabriel, *Redes de Computadores Curso Completo*, 1ª ed. , :Axcel Books, 2001.

VLAN, 2011. Acesso em 12/9/2011. Disponível em: <http://pt.wikipedia.org/wiki/Virtual_LAN>.