UMA ESTRATÉGIA PARA FIRMAR ACORDOS DE NÍVEL DE SERVIÇO POR MEIO DA ANÁLISE DE FLUXO

Adson Bispo de Andrade
Universidade Estadual do Sudoeste da Bahia (UESB), Campus Jequié/Brasil
adsbispo@hotmail.com

Saulo Correa Peixoto
Universidade Estadual do Sudoeste da Bahia (UESB), Campus Jequié/Brasil
Faculdade de Tecnologia e Ciência (FTC), Campus Jequié/Brasil
saulopeixoto@hotmail.com

Alex Ferreira dos Santos
Universidade Estadual do Sudoeste da Bahia (UESB), Campus Jequié/Brasil
afsantos@uesb.edu.br

Robson Hebraico Cipriano Maniçoba
Universidade Estadual do Sudoeste da Bahia (UESB), Campus Jequié/Brasil
robson@ieee.org

Abstract: **Information technology is a key element to the business processes of organizations today and due to new computing paradigms, converges to a state in which their activities tend to manifest in the form of services. The management of these services is a fundamental practice, since it allows to clarify the responsibilities of the parties and determinate the main goals and variables, but requires, however, detailed agreements on specific levels and its correct monitoring, failing to become inconsistent and ineffective. This study presents a strategy to measure and monitor network services provided by an Internet Service Provider described in a Service Level Agreement. The monitoring is related to indicators and unique metrics in an environment composed by sensors, collectors and reporting systems. These reports, issued through the use of Netflow protocol, demonstrated to be flexible enough to indicate the behavior of different services and provide to associate the packet flow filtering to indicators effectively, indicating in what level each service specifications were met.**

Keywords: **Monitoring; Traffic Flow Analysis; Netflow; Service Level Agreement.**

Resumo: **A Tecnologia da Informação é um elemento chave para os processos de negócios das organizações atuais e, devido aos novos paradigmas computacionais, converge para um estado em que suas atividades tendem a se manifestar em formas de serviços. O gerenciamento destes serviços é uma prática fundamental, pois possibilita esclarecer as responsabilidades das partes e determinar as principais metas e variáveis, mas requer, em contrapartida, acordos detalhados em níveis específicos e seu correto monitoramento, sob pena de se tornarem inconsistentes e ineficazes. Este trabalho apresenta uma estratégia para medir e monitorar serviços de rede prestados por um Provedor de Internet descritos em um Acordo de Nível de Serviço. O monitoramento está relacionado com indicadores e métricas exclusivas em um ambiente composto por sensores, coletores e geradores de relatórios. Tais relatórios, emitidos através do uso do protocolo Netflow, demonstraram-se suficientemente flexíveis para reportar o comportamento de serviços distintos e proporcionaram associação da filtragem dos fluxos de pacotes aos indicadores de forma eficaz, indicando em que nível as especificações de cada serviço foram atendidas.**

Palavras-chave: **Monitoramento; Análise de Fluxo de Tráfego; Netflow; Acordo de Nível de Serviço.**

I. INTRODUÇÃO

Todas as aplicações e sistemas em geral, que dão suporte às organizações, funcionam sobre a plataforma de uma infraestrutura de rede comum. Esta tende a estar mais interligada à medida que novos paradigmas baseados na Internet são criados e implementados. Devido a esta convergência, as atividades na Tecnologia da Informação (TI) são classificadas pelos clientes e usuários como um serviço único e indivisível, abstraindo-se formas de aplicações, modelos e plataformas [1].

Um serviço, por sua vez, constitui a entrega de algo intangível e devido a esta característica é mais difícil de medir e de qualificar, diferente de um produto manufaturado, por exemplo. Para sanar estas dificuldades, é relevante estabelecer como este serviço será entregue, suas metas e as variáveis que influenciam no seu funcionamento [2].

O uso de técnicas para diagnosticar os ativos de rede sempre foi um fator essencial para a garantia de um bom gerenciamento de redes e desempenho de serviços. Este monitoramento pode estar aplicado tanto para os equipamentos quanto para os dados que trafegam na rede em diversos níveis. O fornecedor do serviço deve contar com uma infraestrutura de rede confiável, planejada e mantida segundo critérios e métodos bem definidos e devem existir mecanismos de verificação da qualidade e monitoração do ponto

de demarcação (ponto de acesso do cliente ao serviço) [2].

Dentro deste cenário é relevante que esses serviços prestados pela TI sejam firmados por meio de acordos com resultados bem especificados, em um documento descrito como Acordo de Nível de Serviço (ANS). Este é um documento formal entre duas ou mais entidades onde estão definidos os níveis de prestação de serviços especificados em termos mensuráveis [1]-[3].

Além do ANS, também é de suma importância a criação de mecanismos e métodos precisos para reportar a eficiência da prestação dos serviços e monitoramento, em ambos os lados. Como destaca Sahai [4], os ANSs são difíceis de especificar de forma clara e inequívoca. Além disso, a maioria dos ANSs lida apenas com as garantias do lado do provedor e negligenciam a medição do lado do cliente.

Neste intuito, este trabalho objetiva medir a eficácia na prestação de serviços de redes firmados em ANS por meio da análise de fluxo de tráfego, utilizando, para tanto, um Provedor de Serviço de Internet (ISP) de nível dois, como cenário de pesquisa e fonte de dados. Em adição, busca estabelecer os níveis de gerenciamento para fluxo de tráfego de rede ao passo que categoriza e mede os principais indicadores em cada um desses níveis.

II. Gerenciamento de Nível de Serviço em Rede

É possível observar que o objetivo da TI é fornecer métodos e estrutura que garantam um melhor desempenho nas atividades e processos das organizações. Este, vem sendo reforçado com crescente vigor. As soluções de TI continuam a aumentar a eficiência e eficácia das operações de negócios e comunicações e as empresas vão continuar a contar com elas para o sucesso [5].

Portanto, é necessário conhecer bem estas estruturas e métodos para determinar se há um alinhamento adequado entre o uso da tecnologia e as atividades por ela suportadas.

A. Rede como Infraestrutura e Serviço

Os ativos de uma rede de computadores são definidos como um conjunto de diversos dispositivos físicos como *switches*, roteadores, pontos de acesso sem fio, servidores, e outros, que são interligados para prover comunicação e compartilhamento de recursos. Para Tanenbaum [6], a diversidade de usos de redes de computadores crescerá rapidamente no futuro, e é provável que esse crescimento se dê por caminhos que ninguém é capaz de prever agora.

Em nível empresarial, o desafio de gerenciar a rede será maior a medida que a estrutura da organização aumenta. Logo, quanto mais funcionários, processos e filiais, maior deverá ser a estrutura de rede necessária para a realização de funções, tais como: acesso remoto a aplicações e bases de dados, videoconferências, transmissão de dados e vídeo em *streamming*, monitoramento e acesso à Internet.

Para Atrostic e Nguyen [7], a coleta de informações sobre as maneiras como as empresas usam as redes de computadores é um princípio vital para a compreensão de como usar a TI para melhorar o desempenho organizacional e econômico.

Além de ser grande parte da infraestrutura, a rede, por vezes, é vista como parte de um serviço prestado. Em um ambiente de rede, a indisponibilidade de um servidor de email é um problema que pode apontar para indícios que vão desde erro de cabeamento até erros de aplicação. A falha do serviço, que consiste em receber e enviar mensagens, não transparece para o usuário se é um problema estrutural ou de configuração de conexão. Portanto, a rede é vista como parte de uma única entrega e, em geral, a maior responsável nos casos de falhas.

Em [8] é abordado que a rede faz parte de tudo. Negócios assumem que a rede irá funcionar perfeitamente e fazem as decisões de acordo. Este problema é generalizado pela invisibilidade da rede. Roteadores e switches são como caixas-pretas, ligam-se os cabos e se tem conectividade.

O crescente uso da Web ou dos ambientes virtualizados como suporte às aplicações amplia esta indissociabilidade, como é visto nos novos padrões de tecnologia que despontam nos dias atuais, entre os quais se pode citar:

Sistemas Distribuídos: Consiste na adição de poder computacional pela interligação de vários computadores através da rede, no intuito de compartilhar a execução de tarefas. Mesmo formado por computadores e grupos de equipamentos independentes, apresenta-se ao usuário como um sistema único e consistente.

- **Computação em Nuvem (*Cloud computing*):** do inglês é o uso dos recursos computacionais entregues como um serviço através de uma rede, em geral, a Internet.
- **Software como Serviço (*Software as a Service*):** É um modelo no qual o fornecedor de software se responsabiliza por toda a estrutura necessária para a disponibilização do sistema (servidores, conectividade, cuidados com segurança da informação) e o cliente utiliza o software via Internet, pagando um valor recorrente pelo uso.

Barths [9] chama a atenção para a percepção do fato de que a tecnologia revolucionou a comunicação, mas além de seus benefícios, é preciso adaptar as informações existentes à sua linguagem e objetivos, além de estimular o público interno a interagir como essa ferramenta.

Diante disso, para que haja um bom entendimento e uso tanto da infraestrutura quanto de serviços, os

contratos devem ser firmados no intuito de descrever especificamente os requisitos do usuário e as ferramentas e técnicas que o provedor irá utilizar para prestar tais serviços.

B. Acordo de Nível de Serviço

Segundo a ITIL [3], um ANS é um documento formal entre duas ou mais entidades onde estão definidos os níveis de prestação de serviços especificados em termos mensuráveis. Um serviço constitui uma maneira de entregar valor aos clientes, provendo um meio que estes alcancem um resultado sem ter que assumir riscos. O termo ANS, traduzido do inglês Service Level Agreemen (SLA), começou a ser utilizado nos anos 90 com as operadoras de telefonia e foi dedicado inicialmente a ambientes computacionais até ser utilizado atualmente em diversas áreas de prestação de serviços.

O escopo de um ANS está diretamente ligado tanto aos processos de negócios do fornecedor quanto às expectativas do cliente. Para agregar valor, o fornecedor deve fazer com que o serviço funcione de maneira correta, caso contrário, uma falha ou não cumprimento de algum requisito do acordo incidirá em perdas para ambas as partes. Portanto, o ANS deve estar alinhado à estratégia de crescimento da empresa, tanto para companhias que prestam quanto para as que compram serviços [2]. A Fig. 1 ilstra a gestão de relacionamento e gerenciamento ANS segundo a ITIL.

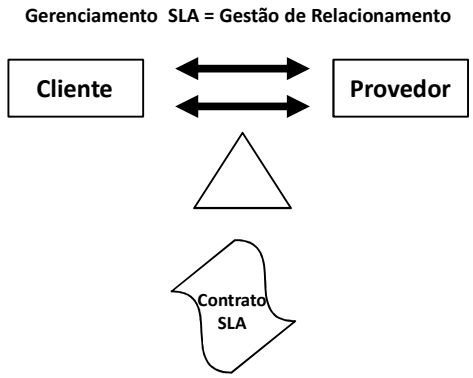


Fig. 1. Gestão de Relacionamento e Gerenciamento ANS [3].

C. Composição e Função de um ANS

Além das funções citadas, Muncinelli [2] defende que em um ANS constam também:

- ✓ Definição das responsabilidades de cada parte do fornecimento do serviço.
- ✓ Gerenciamento da expectativa dos clientes, no intuito de dirimir possíveis frustrações no cumprimento do contrato.
- ✓ Análise e supervisão dos requisitos do cliente. Isto é, identificar as reais necessidades do cliente ao contratar determinado serviço.
- ✓ Implementação do controle e execução do serviço.
- ✓ Fornecimento de verificação, geração e análise de relatórios que garantem se os serviços foram oferecidos nos parâmetros estipulados.
- ✓ Avaliação do retorno.

Quanto à composição, um ANS pode ser construído de diversas formas, inclusive seguido de acordos exclusivos separados por categorias como finanças, distribuição geográfica, administração, contingência, prioridade, segurança, entre outros.

Em [10] é detalhado o ANS em sete componentes chaves através dos quais derivam todos os demais requisitos e informações pertinentes ao contrato descritos como: tipo de serviço, período do contrato, frequência ou tempo de entrega, renegociação de cláusulas, períodos de revisão, penalidades e valores. A ligação entre estes componentes será base para o planejamento dos processos de negócio. Contudo, esta estrutura não especifica itens importantes como, indicadores mensuráveis, ou a forma como o ANS será administrado.

Uma estrutura mais completa dos componentes do ANS é descrita por [11], e ilustrada na Fig. 2, na qual os nove elementos são enumerados e descritos como :

- **Propósito:** Objetivos a serem alcançados através do ANS.
- **Restrições:** Medidas necessárias ou ações que precisam ser tomadas para garantir que o nível requerido de serviços é prestado.
- **Validade:** Período para o cumprimento do acordo.
- **Escopo:** Serviços que serão entregues aos consumidores e serviços que não serão abordados no ANS.
- **Partes:** Quaisquer organizações ou indivíduos envolvidos e suas funções (por exemplo, fornecedor e consumidor).
- **Objetos de Nível de Serviço (ONS):** Níveis de serviços que ambas as partes concordem. Alguns indicadores de nível de serviço, tais como disponibilidade, desempenho, confiabilidade, são usados.
- **Penalidades:** Multas ou ações coercitivas caso o ONS não atinja ou esteja abaixo das medições especificadas.
- **Serviços Opcionais:** Serviços que não são obrigatórios, mas podem ser necessários.
- **Administração:** Processos que são utilizados para garantir a realização de ONSs e as responsabilidades relacionadas com a organização para o controle desses processos.

Neste modelo cabe destacar que do ANS é gerado um Acordo de Nível Operacional (ANO) cuja função é detalhar os objetivos do ANS com grupos de objetivos mais curtos ou específicos, além de possuir cláusulas mais técnicas.

Um ANO embasa o ANS, visto que, define como os departamentos vão trabalhar juntos para cumprir os requisitos de níveis de serviços documentados em um ANS [12].

Em termos práticos, enquanto o ANS declara que um sistema deve suportar até 150 transações por segundo, em um ANO este parâmetro irá verificar a largura de banda mínima da LAN (*Local Area Network*) e da WAN (*Wide Area Network*), ou, ainda, a quantidade de memória, como indicadores.

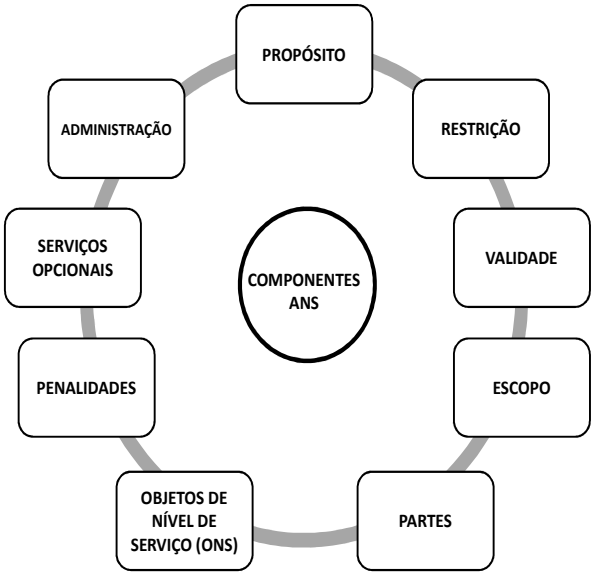


Fig. 2. Estrutura e Componentes chaves ANS [11].

D. *Métricas*

O gerenciamento e a aplicação de um ANS requerem que as métricas sejam persistentes e concisas. Durante a fase de monitoramento elas possuem um papel fundamental, de modo que será através destas métricas que o provedor saberá se os objetivos foram alcançados ou não.

As métricas de ANS são usadas para medir as características de desempenho dos objetos do serviço. Elas são recuperadas diretamente dos recursos gerenciados, tais como servidores, *middleware* e aplicativos instrumentados ou são criadas agregando tais métricas diretas em métricas de nível superior de composição [13].

Boas métricas são alinhadas a um Objeto de Nível de Serviço (ONS) específico, ou seja, cada indicador após ser medido irá emitir um resultado em forma de relatório ou gráfico auxiliando gerenciamento do ANS. Contudo há dificuldades em se compor métricas para categorias diferentes. Em [13] é descrito um dos maiores problemas identificados que é a falta de entrosamento entre métricas e objetos de serviços / processos de TI, bem como a falta de automação em gestão de ANS e de acompanhamento.

Quanto ao tipo, as métricas podem ser classificadas de duas formas [2]:

A primeira tem enfoque na qualidade do serviço prestado pela infraestrutura de rede, gerando estatísticas de rede que podem incluir parâmetro de taxa de *bits*, capacidade *throughput*, taxa de erro, *frames* descartados e taxas de utilização. A segunda mede a capacidade do provedor em fornecer recursos para implantar os serviços tendo como foco principal medir o desempenho da infraestrutura do prestador de serviço em relação às atividades que afetam a capacidade de rede. A Tabela I descreve os tipos de estruturas de métricas da ANS.

TABELA I. TIPOS E ESTRUTURAS DE MÉTRICAS ANS [2].

MÉTRICAS ANS	
Infraestrutura da Rede	**Infraestrutura do ISP**
✓ Taxa de bits ✓ Capacidade ✓ Throughput ✓ Taxa de erro ✓ Frames descartados ✓ Latência ✓ Perda de Pacotes ✓ Disponibilidade de Recursos	✓ Tempo médio entre falhas ✓ Tempo médio de provisão ✓ Tempo médio de resposta a incidentes ✓ Fluxo de ordens de serviços ✓ Trouble Tickets

E. *Níveis de Gerenciamento*

Ainda conforme a ITIL [3], o gerenciamento de níveis de serviços começa a partir do momento em que se obtêm os requisitos dos clientes através do ANS, objetivando os serviços que serão entregues. Tudo que constar no ANS deverá ser medido, a fim de evitar disputas ou perda de confiança no processo.

Os serviços de TI precisam facilitar os resultados a serem alcançados no negócio do cliente. Se o serviço é utilizado para automatizar suas atividades administrativas, para aumentar sua eficiência, ele espera que os serviços de TI propiciem estes resultados [14].

O monitoramento inclui documentar, medir, reportar e revisar os níveis de serviço, observando se estão de acordo com metas específicas, que serão base para decisões futuras a serem tomadas tanto pelo provedor de serviço quanto pelo cliente.

De acordo com as normas ITIL, é possível classificar os níveis de serviços de rede em categorias de gerenciamento da capacidade, disponibilidade e desempenho.

No gerenciamento de capacidade será definido se a infraestrutura de rede é apta a suportar todos os serviços que o negócio do cliente necessita para funcionar. Capacidade está diretamente ligada à demanda, ou seja, a quantidade de recursos que

utilizam e que fazem parte da rede é o que vai determinar se os meios disponíveis estão aptos a suportar uma determinada carga de tráfego de dados.

Disponibilidade refere-se à acessibilidade de um recurso em tempo específico quando necessita ser utilizado. É um quesito crítico para o gerenciamento e que transparece para o cliente a execução de um serviço como todo e não em partes.

Em termos gerais o cálculo da disponibilidade se dá pela seguinte razão [2]:

$$\frac{TSA - Downtime}{TSA} x100\%$$

TSA é o Tempo de Serviço Acordado, isto é, o tempo em que o provedor garante a disponibilidade do serviço. O *Downtime* indica a quantidade de tempo em que o serviço ficou indisponível.

A avaliação do desempenho não é um item específico da normas, mas é encontrada no gerenciamento de continuidade e no gerenciamento de níveis de serviços. Gerenciar o desempenho diz respeito a controlar se a forma como os recursos atuam na execução de uma determinada atividade é eficaz ou não. Em rede de computadores, o desempenho estará mais voltado à velocidade e facilidade com que os ativos operam as transações que lhes são requisitadas.

F. *Modelo de ANS*

A Fig. 3 é uma proposta de modelo de ANS utilizada para o desenvolvimento do trabalho.

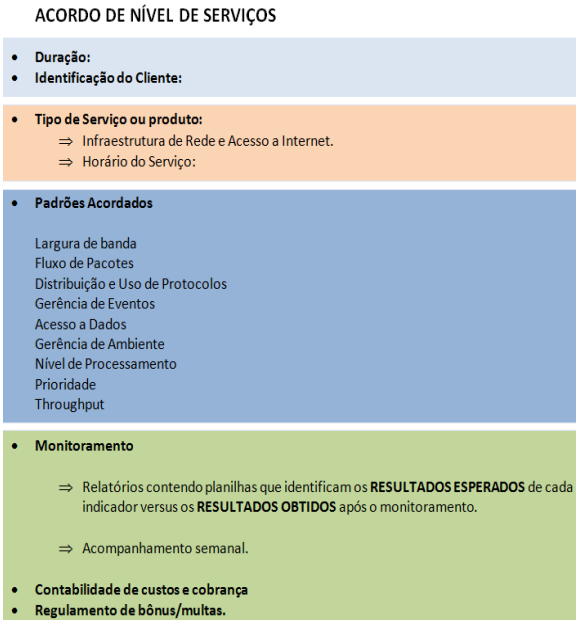


Fig. 3. Modelo Básico de Acordo de nível de Serviço [3].

III. ANÁLISE DE FLUXO DE TRÁFEGO

O uso de técnicas para diagnosticar os ativos de rede sempre foi um fator essencial para a garantia de um bom gerenciamento de redes e desempenho de serviços. Este monitoramento pode estar aplicado tanto para os equipamentos quanto para os dados que trafegam na rede em diversos níveis.

Em [2] é concluido que o fornecedor do serviço deve contar com uma infraestrutura de rede confiável, planejada e mantida segundo critérios e métodos bem definidos. É preciso monitorar partes envolvidas, segundo critérios de desempenho de rede, e devem existir mecanismos de verificação da qualidade e monitoração do ponto de demarcação (ponto de acesso do cliente ao serviço).

A. *Tipos de Monitoramento*

Calyam [15] define dois métodos de monitoramento de infraestrutura de redes: o monitoramento ativo e o passivo.

No método ativo ocorre a inserção de pacotes na rede para efetuar a medição, por exemplo, medir o tempo que um pacote leva para ir de uma extremidade a outra. Ao passo que esses pacotes são inseridos, o tráfego existente é alterado, podendo causar congestionamento e perda de pacotes, sendo importante controlar o volume de pacotes inseridos e a largura de banda disponível. O comando *ping*, usado para medir o tempo de tráfego dos pacotes *Internet Control Message Protocol* (ICMP), é uma das ferramentas para medição ativa.

O modo passivo mede a rede sem criar ou modificar nenhum tráfego. Monitorar a rede passivamente provê um conjunto detalhado de informações sobre um determinado ponto da rede, como a quantidade de tráfego, grupos de protocolos e taxas de bits. As aplicações de rede também podem ser monitoradas por meio da visualização do conteúdo dos pacotes emitidos, fornecendo ao administrador da rede a capacidade de analisar se a estrutura de rede é suficiente para suportar a quantidade de tráfego gerado por elas.

B. *Protocolos, Ferramentas e Técnicas de gerenciamento.*

As informações de gerenciamento obtidas através de sistemas de monitoramento de redes podem ser definidas como um grupo de ferramentas integradas. Tais ferramentas utilizam basicamente dois tipos de abordagem para a coleta destas informações, denominadas *polling* e *event-reporting*.

A técnica de *polling* consiste em uma interação do tipo requisição/resposta entre um gerente e um agente. O gerente pode solicitar a um agente autorizado o envio de valores de diversos elementos de informação. O agente responde com os valores constantes em sua estação de gerenciamento (MIB – *Management Information Base*) [16].

O protocolo da camada de aplicação *Simple Network Managenment Protocol* (SNMP) segue esta estrutura, facilitando o intercâmbio da comunicação entre dispositivos. Criado pela *Internet Engineering*

Task Force (IETF), no início da década de 80, tem como definição dos recursos reais do sistema o conceito de objetos gerenciados, que podem ser lidos ou alterados de acordo com as devidas permissões. Estas leituras representam o estado real dos recursos e o conjunto de objetos gerenciados constitui a MIB, de organização hierárquica, contendo em sua estrutura lógica o identificador e o nome de cada objeto. A Fig. 4 ilustra a estrutura de funcionamento do SNMP.

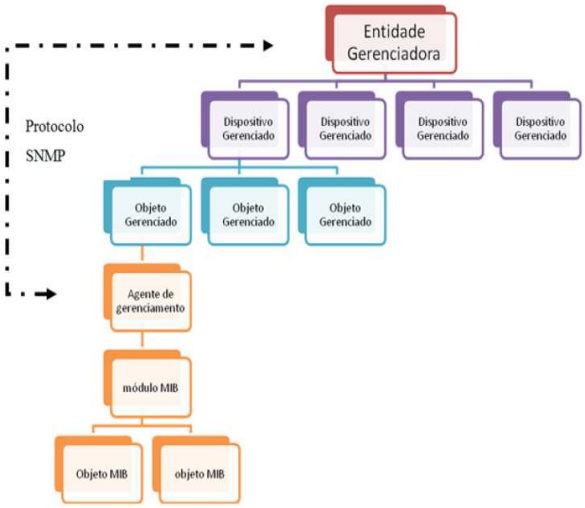


Fig. 4. Estrutura de funcionamento do SNMP [17].

Na técnica de *event-reporting* o gerente monitora a rede através da escuta do tráfego que passa por ela, aguardando sempre as informações que são enviadas pelo agente. Um agente pode enviar relatórios periódicos, contudo os eventos específicos e não usuais constituem a característica básica deste mecanismo.

Ferramentas e protocolos deste tipo atuam, em geral, para o controle do fluxo de tráfego, diferente dos modelos baseados em polling que focam apenas no gerenciamento dos estados dos recursos e equipamentos; dentre elas encontram-se os protocolos *Netflow* e IPFIX (*IP Flow Information Export*) que serão descritos na próxima seção.

Em [18] é salientado que as técnicas de *event-reporting* são mais eficientes que o *polling*, especialmente para o monitoramento de objetos cujos valores mudam de forma inconstante, e que a escolha de uma das técnicas depende de alguns fatores como a quantidade de tráfego gerado, a capacidade de processamento dos equipamentos, e as aplicações de monitoramento suportadas.

C. *Monitoramento passivo em captura de Pacotes*

O monitoramento baseado em análise de pacotes é definido como um aplicativo analisador de pacotes que frequentemente pode ser denominado como coletor de pacotes (*packet sniffing*) ou analisador de protocolo (*protocol analysis*) [19].

Analisadores de pacotes podem ser utilizados para diversos fins, considerando que permitem a monitoração da rede de forma transparente e não interferem na transmissão. A função característica de um *sniffer* é a captura de pacotes, isto é, o armazenamento de todos os sinais que saem e que chegam pela interface habilitada. Os processos utilizados pelos analisadores de pacotes se constituem na captura de todos os pacotes, que se dá pela modificação da interface do dispositivo para o modo promíscuo em redes cabeadas, ou modo monitor para interfaces sem fio. Em seguida, há o processo de conversão os dados binários para formato legível. Esta conversão depende exclusivamente de uma biblioteca ou uma Interface de Programação de Aplicativos (API – *Application Programming Interface*), sendo mais utilizadas as de código aberto.

O processo de análise é a ultima etapa do monitoramento baseado em pacotes. Em [17] é caracterizado as ferramentas de análise de pacotes em cinco parâmetros: Suporte a sistemas operacionais; Suporte ao aplicativo; Custo; Interface amigável de gerenciamento; e Suporte a protocolos. A interface e o suporte a protocolos são características fundamentais que irão diferir entre os analisadores de pacotes disponíveis de acordo com as plataformas e sistemas operacionais que os suportam.

Atualmente, as ferramentas *open source* mais utilizadas para a análise de pacotes são o *Tcpdump* e o *Wireshark*, sendo a primeira funcional apenas para sistemas Linux ou Freebsd e a segunda além destas, funciona também em sistemas Windows, através da biblioteca *Winpcap*.

D. *Monitoramento de fluxo de tráfego*

O fluxo de tráfego de uma rede é uma cadeia de dados IP (*Internet Protocol*)– qualquer conexão TCP é um fluxo, por exemplo. A maioria dos sistemas de monitoramento registra o endereço lP, protocolo, portas e volume de dados transitados [20].

A ideia de monitoramento de fluxo foi inicialmente concebida pela empresa Cisco Systems através de seu protocolo denominado *Netflow* e devido a seu uso amplo tornou-se um modelo padrão para os dispositivos de diversos fornecedores. Este conceito, bem como todas as definições do protocolo *Netflow*, foi seguido e está sendo aprimorado pelo protocolo aberto intitulado Protocolo de Exportação de Informações da Internet (IPFIX) [21].

Diferente da captura de pacotes, um registro de fluxo é um resumo de informação sobre uma conexão, que grava qual *host* comunicou com outros *hosts*, quando esta comunicação ocorreu, como o tráfego foi transmitido, e outras informações básicas sobre a conversação na rede, na forma de metadados. Registros de fluxo resumem cada conexão na rede, desta forma, registro de fluxos são bem menores e inferem um custo menor no seu armazenamento [8].

E. *Estrutura*

A padronização básica do sistema de monitoramento de fluxo com os protocolos *Netflow* e

IPFIX é fundamentada através de três componentes: sensores, coletores e geradores de relatórios. Sendo o primeiro e o segundo partes insubstituíveis de qualquer ambiente de monitoramento de fluxo.

O sensor é o dispositivo ou programa que captura dados de fluxo da rede e encaminha para o coletor. Sensores de fluxo é, possivelmente, a parte mais difícil de gerenciar em um sistema de monitoramento de fluxo, inclusive em redes extensas [8].

Por se tratar de uma sonda, deve-se priorizar a sua localização estratégica, ou seja, o sensor precisa estar alocado em um ponto onde é possível capturar todos os dados de interesse.

Em geral, todos os *switches* e roteadores Cisco são capazes de capturar fluxo de dados que passam por suas interfaces, desde que possuam a versão 12 ou superior do sistema operacional. Outros fabricantes como 3COM e *Juniper* também possuem equipamentos capazes de capturar fluxos. Sensores também podem ser implementados via software pela instalação de pacotes como o *SoftFlow*, preferencialmente em plataformas UNIX.

Os pacotes capturados pelo sensor são enviados para coletores que assim como os sensores estarão situados em locais de fácil acesso ao administrador de rede. No coletor os dados são armazenados de forma persistente, em discos, possibilitando que um gerador de relatórios relacione estes dados em informações consistentes que serão exibidas em formas de tabelas ou gráficos.

F. Composição do fluxo

De acordo com [8], um fluxo é uma série de pacotes que compartilham a mesma fonte e endereços IP de destino, origem e destino portos, e do protocolo IP. A palavra fluxo às vezes também é usada para significar um conjunto de fluxos individuais. A seguir são descritas as operações de fluxo dos protocolos mais conhecidos, que são ICMP, UDP e TCP.

Fluxos ICMP identificam o propósito geral do pacote com formatos, tipos e código próprios, ou seja, não utiliza mecanismos de flags ou endereçamento de porta como TCP e UDP. Portanto cada requisição de cliente e também as respostas como em chamadas echo-request e echo-response constituirão um fluxo cada.

Os fluxos de pacotes via UDP incluem o número de porta em sua identificação. Em uma operação usual de UDP a um serviço básico como DNS (*Domain Name System*), a requisição do IP de um site será feita em duas vias simples, sendo que, o servidor irá utilizar uma porta conhecida, neste caso a porta 53 do serviço e o cliente uma porta arbitrária. Este processo define o terceiro e o quarto fluxo da mesma conexão.

Os fluxos TCP utilizam além do número de porta, *flags* que indicam o estado da conexão, que é a operação básica do TCP. Em um primeiro momento o cliente envia uma mensagem requisitando a sincronização com o servidor (*Synchronization packet*), com porta de origem arbitrária e porta de destino 80, constituindo o quinto fluxo. A resposta de estado do servidor (*Acknowledgement packet*) é um fluxo diferente, visto que o número de porta e IP de destino serão do cliente.

IV. TRABALHOS RELACIONADOS

Dentre as demais pesquisas referentes à análise de fluxos de tráfego em redes feitas recentemente, destacam-se:

"Uma estratégia de Monitoramento do Tráfego de Redes baseada em *Netflow*/IPFIX" por Raphael Ruiz, como defesa de tese em mestrado em Engenharia de Telecomunicações na Universidade Federal Fluminense no ano de 2010. Na qual é apresentado um estudo de caso do monitoramento de redes da Universidade, demonstrando como podem ser obtidas informações a partir do monitoramento de fluxos e sua importância para a garantia da segurança em redes.

Outro trabalho de relevância é o descrito por André Couto em defesa de mestrado na Universidade de Brasília no ano 2012, que tem como título: "Uma Abordagem de Gerenciamento de Redes Baseado no Monitoramento de Fluxos de Tráfego *Netflow* com o Suporte de Técnicas de *Business Intelligence*", no qual apresenta um estudo sobre a abordagem de monitoramento passivo de redes com *Netflow*, visando o suporte à decisão e integrando os fluxos obtidos pelo protocolo como soluções de *Business Intelligence* para fornecimento de consultas.

Ambos os trabalhos abrangem o monitoramento de redes WAN e utilizam basicamente as mesmas ferramentas e técnicas, ainda que tenham finalidades diferentes, devido à ampla aplicação do protocolo *NetFlow*. O diferencial da abordagem que será proposta neste artigo em relação aos trabalhos supracitados é realizar o monitoramento de fluxos eu um ambiente mais restrito e voltado a gerar relatórios específicos para atender os requisitos de um ANS.

V. MATERIAIS E MÉTODOS

Os serviços de rede analisados estão contidos em três áreas de gerenciamento determinadas como capacidade, disponibilidade e desempenho. No gerenciamento de capacidade será definido se a infraestrutura de rede é apta a suportar todos os serviços que o negócio do cliente necessita para funcionar. Capacidade está diretamente ligada à demanda, ou seja, a quantidade de recursos que utilizam e que fazem parte da rede é o que vai determinar se os meios disponíveis estão aptos a suportar uma determinada carga de tráfego de dados.

Disponibilidade refere-se à acessibilidade de um recurso em tempo específico quando necessita ser utilizado. É um quesito crítico para o gerenciamento e que transparece para o cliente a execução de um serviço como todo e não em partes. A avaliação do

desempenho diz respeito a controlar se a forma como os recursos atuam na execução de uma determinada atividade é eficaz ou não. Em rede de computadores, o desempenho estará mais voltado à velocidade e facilidade com que os ativos operam as transações que lhes são requisitadas.

Para alinhar o processo de captura de fluxos a indicadores específicos o estudo aborda o caráter caráter quanti-qualitativo, quantificando os resultados da medição com os limites e métricas dispostos no ANS e qualificando através de um MAPA de ANS a eficácia dos indicadores, isto é, se as especificações foram atendidas ou não. A obtenção desses resultados segue as seguintes etapas:

- Definir métricas específicas a cada indicador.
- Capturar fluxos de tráfego via *Netflow*
- Comparar a obtenção desses fluxos com os resultados esperados, de acordo com os níveis de serviços especificados em um modelo.
- Gerar um Mapa de ANS com base nestas comparações.

A. *Descrição do Cenário*

O ambiente de estudo trata-se do Provedor de Internet Aerolink Telecom, com sede no município de Feira de Santana-BA, o qual presta serviços de conexão com a Internet e suporte a redes privadas, nessa e demais cidades circunvizinhas. Os clientes dos serviços são tanto usuários finais, que solicitam apenas acesso a Internet, como entidades e instituições privadas, que pagam pelo suporte e infraestrutura de rede completa.

B. *Indicadores e Métricas*

Antes da etapa de configuração do ambiente de monitoramento, identificaram-se os indicadores relativos ao serviço prestado pelo provedor. Esses indicadores são as principais variáveis que devem ser monitoradas para embasar o ANS.

Quanto às métricas, para o ambiente de trabalho, o mais viável foi compor fórmulas distintas para cada variável coletada na análise de fluxo, de forma que fornecesse maior alinhamento com os níveis de gerenciamento em capacidade, desempenho e disponibilidade, de acordo com Paschke [13]. A Tabela II descreve os indicadores e métricas utilizadas.

TABELA II. INDICADORES E MÉTRICAS PARA GERENCIAMENTO DE CAPACIDADE, DISPONIBILIDADE E DESEMPENHO

	INDICADORES	DESCRIÇÃO	MÉTRICAS
CAPACIDADE	Largura de Banda	Retornar capacidade de tráfego em cada link de rede secundário e do link principal.	**$L = \frac{(L_1 + L_2 + \ldots L_n)}{n}$** L = Média geral da largura de banda da rede
	Média de Unidade Máxima de Transmissão (MTU)	Informar a média de tamanho máximo das unidades que passam pela rede	$M = \sum_{t}^{x}$ M = Médias de MTU x = Média de grupos de unidades t = Total de pacotes
	Distribuição do Tráfego	Verificar e separar o uso da rede por tipos de tráfego.	$Dr = \frac{C}{Ch}$ Dr = Distribuição Trafego C= Categoria de tráfego (IP normal, IP fragmentado, ou Não-IP) Ch = Carga da rede
DISPONIBILIDADE	Link de rede	Indicar o comportamento dos eventos queda, retorno, pausas dos meios de transmissão.	**D = (TS – d)/TSx100** D = Disponibilidade do link TS = tempo de serviço acordado d = tempo de indisponibilidade
	Aplicações	Indicar o comportamento dos eventos queda, retorno, pausas das aplicações.	**A = (TA – d)/TAx100** A = Disponibilidade das Aplicações TS = tempo de serviço acordado d = tempo de indisponibilidade
	Dispositivos	Indicar o comportamento dos eventos queda, retorno, pausas dos dispositivos.	**E = (TE – d)/TEx100** E = Disponibilidade dos Dispositivos TE = tempo de serviço acordado d = tempo de indisponibilidade
DESEMPENHO	Carga da Rede	Mostrar a carga de processamento suportada pelos ativos de rede	**P = Pc/f x 100** Pc = quantidade de pacotes f = Tempo em segundos.
	Distribuição dos protocolos	Utilização do link de acordo com os principais protocolos	**$Dp = \frac{P}{tp} * 100$** Dp = Porcentagem do uso do protocolo P = protocolos (TCP, UPD, ICMP). tp = quantidade total de pacotes.
	Throughput	Carga de tráfego real da rede.	**Th = Cr/L *100** Cr = carga L = largura de banda

C. *Captura dos Fluxos*

O modelo para a captura de fluxo de dados teve como suporte o protocolo *Netfow* versão cinco. Baseou-se, portanto, no espelhamento de dados através de uma das interfaces do roteador Cisco 3800, configurada para o encaminhamento de tráfego à rede interna, a um computador designado a ser o coletor dos fluxos, como mostra a Fig. 5. A máquina responsável pela coleta de dados funcionou também como o gerador de relatórios, através das saídas emitidas pelas ferramentas *flow-tools* e *Ntop*.

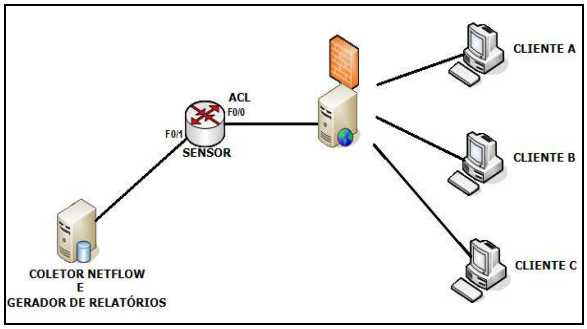


Fig. 5. Organização do ambiente de monitoramento.

Com os equipamentos devidamente configurados, iniciou-se a captura dos fluxos, que totalizou, para efeito deste trabalho, 30 dias consecutivos.

A validação do funcionamento da plataforma de monitoramento *Netflow*, pôde ser confirmada pela verificação de arquivos salvos periodicamente a cada 15 minutos no diretório do coletor, através primitiva *flow-capture*, conforme a Fig. 6.

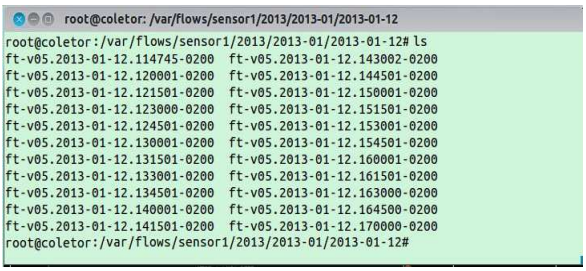


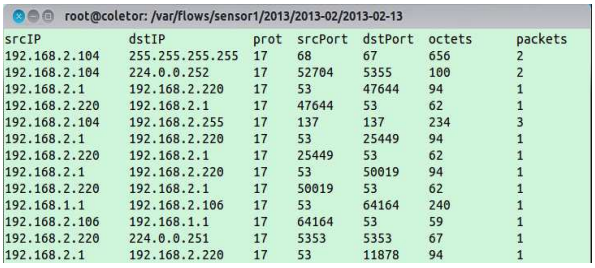
Fig. 6. Armazenamento de arquivo *Netflow* com *flow-capture*.

Após a captura, cada fluxo foi armazenado e categorizado segundo critérios relativos à origem e destino, tipo de protocolo utilizado e quantidade de fluxos por direção.

Em seguida, a análise e tratamento dos fluxos procederam de duas formas: por console e através de gráficos e tabelas.Na primeira, os fluxos foram filtrados através da primitiva *flow-nfilter*. Tal primitiva possibilitou alinhar os filtros, os indicadores e as métricas estipuladas para o ANS. É possível observar a saída dos fluxos específicos UDP (*User Datagram Protocol*) e TCP (*Transmission Control Protocol*) filtrados nas Fig. 7 e Fig. 8, respectivamente.

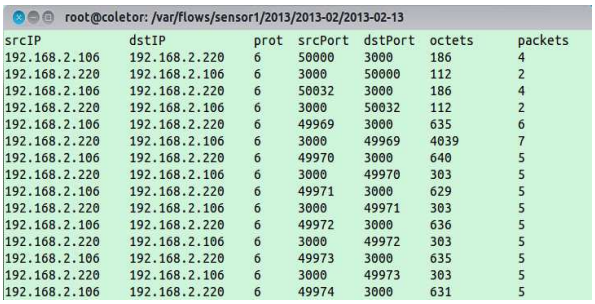
Para o tratamento e análise dos fluxos em forma gráfica, utilizou-se o *Ntop*, que é um software livre criado por Luca Deri, de fácil instalação e manutenção. Além da possibilidade da geração de gráfico por análise da interface do servidor, o *Ntop* possui *plugins* específicos para a captura de dados *Netflow*, o que o torna uma ferramenta para a geração de relatórios e bastante flexível. Para a plotagem das informações em forma de gráfico, foram instaladas também as ferramentas *RRDtools*, *Perl*, *Xmap* e a linguagem de marcação *EXtensible Markup Language* (XML) possibilitou exportar as descrições de fluxo. O acesso ao programa foi realizado via *web browser*, através do protocolo HTTP (*Hypertext Transfer Protocol*) com número IP e porta pré-configurados. A Fig. 9 exibe a tela inicial do *Ntop*.

Em seguida, procedeu-se, à comparação entre a quantidade de fluxos obtidos e esperados para cada indicador de acordo com a Tabela III.



srcIP	dstIP	prot	srcPort	dstPort	octets	packets
192.168.2.104	255.255.255.255	17	68	67	656	2
192.168.2.104	224.0.0.252	17	52704	5355	100	2
192.168.2.1	192.168.2.220	17	53	47644	94	1
192.168.2.220	192.168.2.1	17	47644	53	62	1
192.168.2.104	192.168.2.255	17	137	137	234	3
192.168.2.1	192.168.2.220	17	53	25449	94	1
192.168.2.220	192.168.2.1	17	25449	53	62	1
192.168.2.1	192.168.2.220	17	53	50019	94	1
192.168.2.220	192.168.2.1	17	50019	53	62	1
192.168.1.1	192.168.2.106	17	53	64164	240	1
192.168.2.106	192.168.1.1	17	64164	53	59	1
192.168.2.220	224.0.0.251	17	5353	5353	67	1
192.168.2.1	192.168.2.220	17	53	11878	94	1

Fig. 7. Filtragem de fluxo *Neflow* por protocolo UDP (17).



srcIP	dstIP	prot	srcPort	dstPort	octets	packets
192.168.2.106	192.168.2.220	6	50000	3000	186	4
192.168.2.220	192.168.2.106	6	3000	50000	112	2
192.168.2.106	192.168.2.220	6	50032	3000	186	4
192.168.2.220	192.168.2.106	6	3000	50032	112	2
192.168.2.106	192.168.2.220	6	49969	3000	635	6
192.168.2.220	192.168.2.106	6	3000	49969	4039	7
192.168.2.106	192.168.2.220	6	49970	3000	640	5
192.168.2.220	192.168.2.106	6	3000	49970	303	5
192.168.2.106	192.168.2.220	6	49971	3000	629	5
192.168.2.220	192.168.2.106	6	3000	49971	303	5
192.168.2.106	192.168.2.220	6	49972	3000	636	5
192.168.2.220	192.168.2.106	6	3000	49972	303	5
192.168.2.106	192.168.2.220	6	49973	3000	635	5
192.168.2.220	192.168.2.106	6	3000	49973	303	5
192.168.2.106	192.168.2.220	6	49974	3000	631	5

Fig. 8. Filtragem de fluxo *Neflow* por protocolo TCP (6).

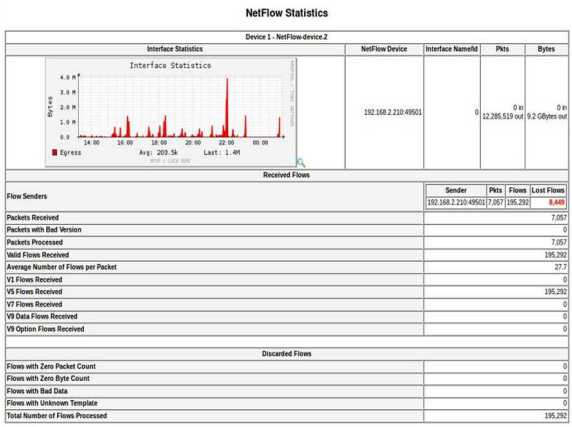


Fig. 9. Estatística *Netflow* Sensor 1.

VI. RESULTADOS

A estabilidade do ambiente de monitoramento possibilitou o desenvolvimento da pesquisa sem maiores dificuldades, graças à disponibilidade de hardware para a exportação de fluxo. Outra questão que vale destacar é a consistência das aplicações utilizadas para a geração de relatórios, neste caso o pacote *flow-tools* e o *Ntop*, que se mostraram eficientes para concluir as tarefas requisitadas.

A aquisição dos fluxos proporcionou a obtenção de informações precisas para preencher o ANS, conforme os indicadores levantados. A Tabela III exibe os resultados obtidos em contrapartida aos resultados esperados baseados no modelo do ANS e consoante os requisitos de cada indicador para um cliente.

TABELA III. RESULTADO DOS INDICADORES

CAPACIDADE		RESULTADOS ESPERADOS	RESULTADOS OBTIDOS
Largura de Banda		2.0 Mbps	1,8 Mbps
Unidade Máxima de Transmissão (MTU)	0 < 64	15%	32,2%
	64 < 1024	25%	17%
	1024 < 1518	60%	50,8%
Distribuição do tráfego	IP completo	97%	96,88%
	IP fragmentado	0%	0,12%
	Não-IP	3%	3%

DISPONIBILIDADE			
Link de Rede	Link de Rede	99%	98,8%
Aplicações	Aplicações	99%	98,8%
Dispositivos	Dispositivos	99,9%	99%

DESEMPENHO			
Carga da Rede (pacotes por segundo)		82	68
Uso dos Protocolos	TCP	74%	71,3%
	UDP	25%	27,8%
	ICMP	1%	0,9%
Throughput		2 Mbps	1,56 Mbps

A partir destes resultados e com conhecimento prévio do comportamento padrão da rede, pôde-se notar que os serviços de rede medidos conseguiram atingir as metas estipuladas. A flexibilidade do protocolo *Netflow* possibilitou formatar a filtragem dos fluxos de pacotes e mensurar cada indicador levantado de forma eficaz, tornando o ANS um documento de maior valor agregado ao demonstrar em que nível as especificações foram atendidas, confirmando, portanto que embasar acordos de níveis de serviço com análise de fluxos é uma estratégia válida. Além de alcançar o escopo do trabalho, o estudo possibilitou constatar outras vantagens como:

- Maior rapidez em identificar a causa de divergência de um indicador.
- Inferir se problemas que afetam o desempenho da rede estavam relacionados com a dispersão de indicadores, reduzindo tempo de diagnóstico.
- Documentação da rede de forma mais dinâmica, criando bases para comparação futura e com o mínimo espaço de armazenamento necessário.

Com os resultados obtidos, observou-se também que a partir das análise de fluxo de tráfego, foi possível embasar documentos e contratos sem a necessidade de recorrer a diversas ferramentas ou aplicativos de monitoramento.

O processo adotado possui duas grandes vantagens quando comparada com a captura de pacotes. A primeira consiste na abrangência em relacionar qualquer tipo de tráfego para análise diferentemente de outras ferramentas de medição como o *Multi Router Traffic Grapher* (MRTG), que apenas vêem o estado da rede de acordo com o funcionamento dos dispositivos.

O segundo benefício é o baixo custo de armazenamento dos dados coletados, visto que, em experimento realizado no mesmo ambiente, a captura de pacotes via *Wireshark* em um período de cinco minutos necessita de 64,2 Mb de espaço em disco, enquanto o mesmo período em medição de fluxo consomem apenas 5,73 Kb.

Em suma, a obtenção destes resultados propicia a confecção de um Mapa de Acordo de Nível de Serviço, o qual pode ser elaborado mensalmente e exibe os níveis de atendimento a cada especificação, criando uma forma efetiva de preencher o ANS, como exibe a Fig. 10.

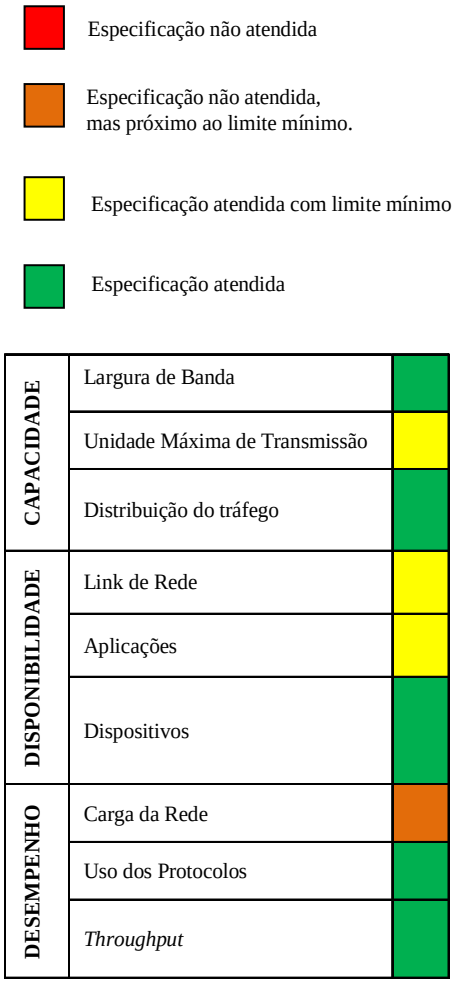


Fig. 10. Mapa de Acordo de Nível de Serviços.

VII. CONCLUSÃO

Depreende-se que o trabalho desenvolvido, justifica tanto o uso de ANS para embasar serviços de rede, quanto a adoção apropriada de mecanismos para categorizar indicadores e medi-los com eficiência, contribuindo, dessa forma, para a evolução na prestação de serviços em TI.

O estudo das técnicas de monitoramento e do protocolo *Netflow* para a entrega de resultados é eficiente, pois não acarreta cargas de tráfego extra à infraestrutura, e reduz a gama de materiais e métodos

utilizados na busca de solução de problemas. A identificação e medição de indicadores de serviços propiciam economia de tempo, recursos e auxiliam na manutenção de acordos entre provedor e usuário de serviços.

REFERÊNCIAS

[1] S. B. Gomes, R. A. Falbo, e C. S. Menezes, "Um modelo para acordo de nível de serviço em TI", Simpósio Brasileiro de Qualidade de Software 4 (2005): 377-391.

[2] G. Muncinelli, "Acordo de Níveis de Serviço", RTI: Redes Telecom e Instalações, São Paulo, vol. único, nº 141, fev. 2012. Disponível em <http://www.arandanet.com.br/midiaonline/rti/2012/fevereiro/index.html>. Acesso em: 29 de março de 2014.

[3] OGC: ITIL – The key of Managing IT Services, Service Delivery, Stationery Office for OGC, 2009.

[4] A. Sahai, *et al*, "Automated SLA Monitoring for Web Services", Workshop on Distributed Systems: Operations and Management, 2002.

[5] D. Ingram, "Information Technology for Business Success", Disponível em: <http://smallbusiness.chron.com/information-technology-business-success-4019.html>. Acesso em: 30 de Maio de 2014.

[6] A. S. Tanenbaum e D. J. Wetherall, "Redes de Computadores". 5. ed. Rio de Janeiro: Pearson, 2011.

[7] B. K. Atrostic E S. Nguyen, "How Businesses Use Information Technology: Insights For Measuring Capital And Productivity", SSHRC International Conference on Index Number Theory and the Measurement of Prices and Productivity. Vancouver, 2004.

[8] M. W. Lucas, "Network Flow Analysis". 2. ed. San Francisco: No Starch Press, 2010.

[9] C. C. Barths, "Os Usos das Tecnologias na Comunicação e Organizacional Interna". São Leopoldo – RS. 2009.

[10] S. Godbolt, "Why service level Agreements: An overview of Their origins And best practice", IFHM Inform. Ohio, vol. 13, nº 03. jun. 2003.

[11] L. Wu, R. Buyya, "Service Level Agreement (SLA) in Utility Computing Systems". Tech. Rep. CLOUDS-TR-2010-5, Cloud Computing and Distributed Systems Laboratory, The University of Melbourne, Australia (September 2010).

[12] H. Marquis, "Secrets to Successful Service Level Management", itSM Solutions. LOCAL, vol. 5, nº 13. abr. 2009. Disponível em: http://www.itsmsolutions.com/newsletters/DITYvol5iss13.htm. Acesso em: 30 de maio de 2014.

[13] A. Paschke, e E. Schnappinger-Gerull, "A Categorization Scheme for SLA Metrics", Service Oriented Electronic Commerce, v. 80, p. 25-40, 2006.

[14] J. Sauvé, et al, "SLA Design from a Business Perspective", Proceedings of the 16th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management, Springer Berlin/Heidelberg, 2005, pp. 72–83.

[15] P. Calyam "Active and Passive Measurements on Campus regional and National Network Backbone Plath"*. IEEE, 2005.

[16] E. S. Specialski, "Gerência de Redes de Computadores e de Telecomunicações". Material de estudo – Apostila . Florianópolis: UFSC, 2000.

[17] A. V. Couto, "Uma abordagem de Gerenciamento de Redes baseado no Monitoramento de Fluxos de Tráfego Netflow com o suporte de Técnicas de Business Intelligence", Dissertação de Mestrado, Publicação PPGENE.DM – 107/2012, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 116. 2012.

[18] M. Subramanian, "Network Management: Principles and Practice", 1st edition, Addison-Wesley Lognman, 2000.

[19] C. Sanders, "Practical Packet Analysis". EUA: No Starch Press, Inc. 2007.

[20] R. Spenneberg, "De Olho no Tráfego". Linux Magazine, São Paulo, vol. 1, nº 29, abr. 2007. Disponível em http://www.linuxnewmedia.com.br/issue/lm_29_bloqueando_intrusos. Acesso em: 30 de Março de 2014.

[21] B. Claise, "RFC 5101. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information". MAC: Keyed-Hashing for Message Authentication, 2008, Disponível em: <http://tools.ietf.org/html/rfc5101>. Acesso em 30 de Março de 2014.