FACULDADE PITÁGORAS DE UBERLÂNDIA

Analise e desempenho de redes

Professor: Esp. Pedro Macedo Leite

E-mail: pedro.larva@gmail.com

Versão 1 Rev. 005

Uberlândia / MG

SUMÁRIO

1. Teoria

Cada um dos três séculos anteriores foi dominado por uma única tecnologia. O Século XVIII foi a época dos grandes sistemas mecânicos que acompanharam a Revolução Industrial. O Século XIX foi a era das máquinas a vapor. As principais conquistas tecnológicas do Século XX se deram no campo da aquisição, do processamento e da distribuição de informações. Entre outros desenvolvimentos, vimos a instalação das redes de telefonia em escala mundial, a invenção do rádio e da televisão, o nascimento e o crescimento sem precedentes da indústria de informática e o lançamento dos satélites de comunicação. TANENBAUM (2003)

Como resultado do rápido progresso tecnológico, essas áreas estão convergindo rapidamente e são cada vez menores as diferenças entre coleta, transporte, armazenamento e processamento de informações. Organizações com centenas de escritórios dispersos por uma extensa área geográfica podem, com um simples apertar de um botão, examinar o status atual de suas filiais mais remotas.

À medida que cresce nossa capacidade de colher, processar e distribuir informações, torna-se ainda maior a demanda por formas de processamento de informações ainda mais sofisticadas. TANENBAUM (2003)

A medida que estas redes residenciais, empresariais ou publicas crescem, também cresce a necessidade de analisar estas estruturas para entender como melhorar, mensurar e até dar maior performance e estabilidade para elas.

No decorrer desta apostila, falaremos de teoria, e boas praticas.

2. O que é rede

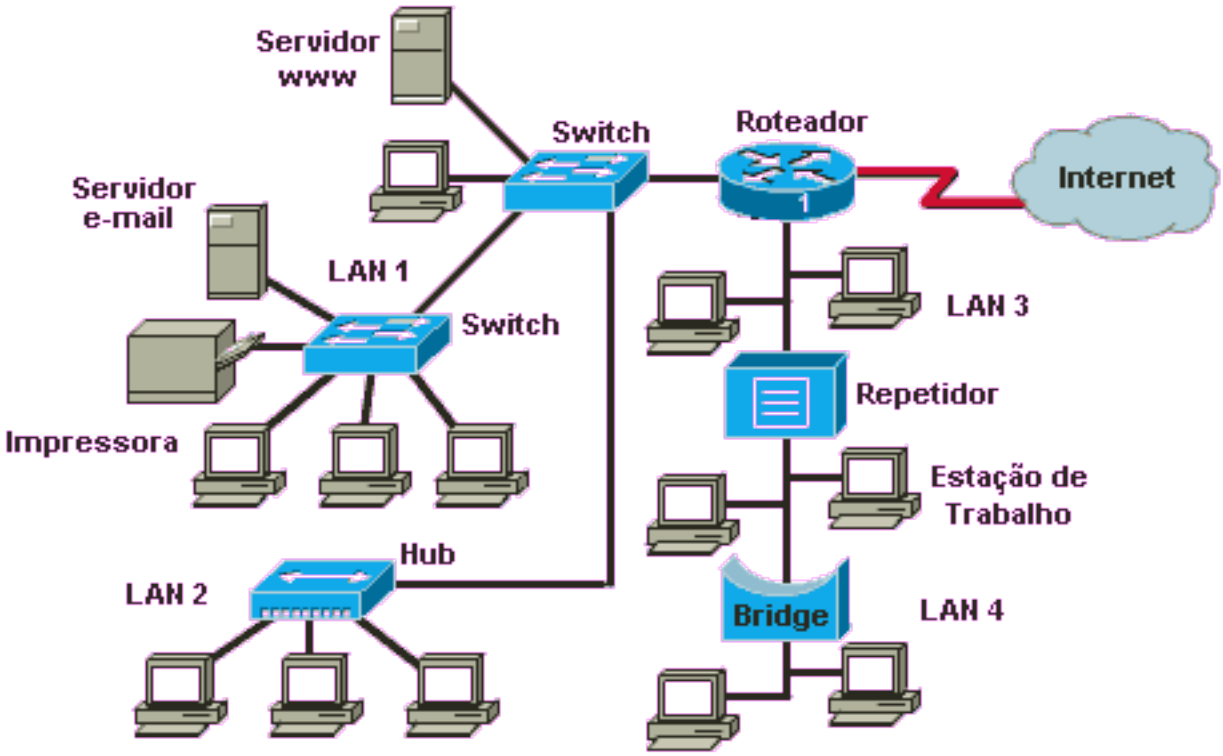
O conceito de redes de computadores é bem simples "***conjunto de computadores autônomos (independentes) interconectados (capazes de trocar informações)***".

3. Principais elementos

Hoje, temos diversos elementos que podem ser acoplados em uma rede, e falaremos de alguns que são mais comuns:

- Hubs: Equipamento que provê rede sem filtro.
- Switches de nível 2: Equipamento que fornece rede de maneira inteligente. Cada elemento da rede só vê o que deve.
- Switches de Nível 3: Tudo que o nível 2 oferece, mais algumas funções a nível de protocolo.
- Roteadores: Divisor de rede, prove interconexões.
- Firewalls: Agrega segurança a rede.
- Servidores: Provê informação.
- Consumidores: Consome informação.

Abaixo tem uma imagem que ilustra a maioria dos elementos:



4. Tipos de redes

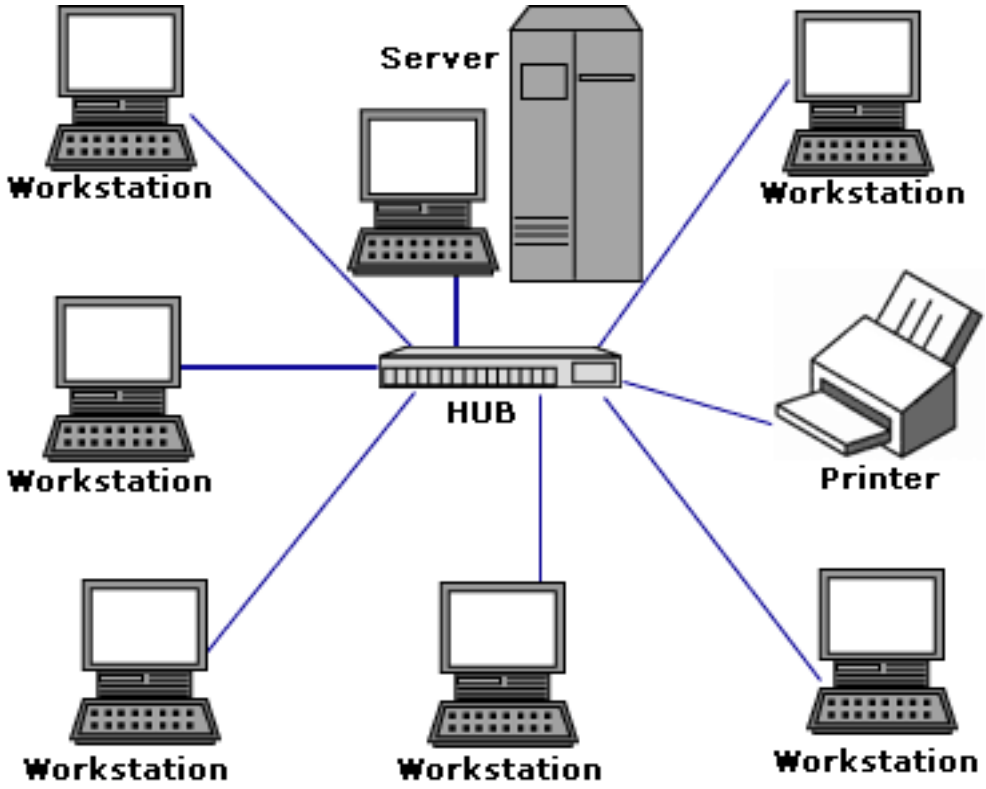
Considerando este conceito, onde tem interconexão de dados, é uma rede. Existem alguns tipos de redes:

- Local Area Network (LAN)
- Wireless Local Area Networks (WLAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)
- Storage Area Network (SAN)
- Personal Area Network (PAN)

Sendo que as redes que são constantemente faladas são as LAN, WLAN, WAN e SAN. Por isto, vamos exemplificar estas.

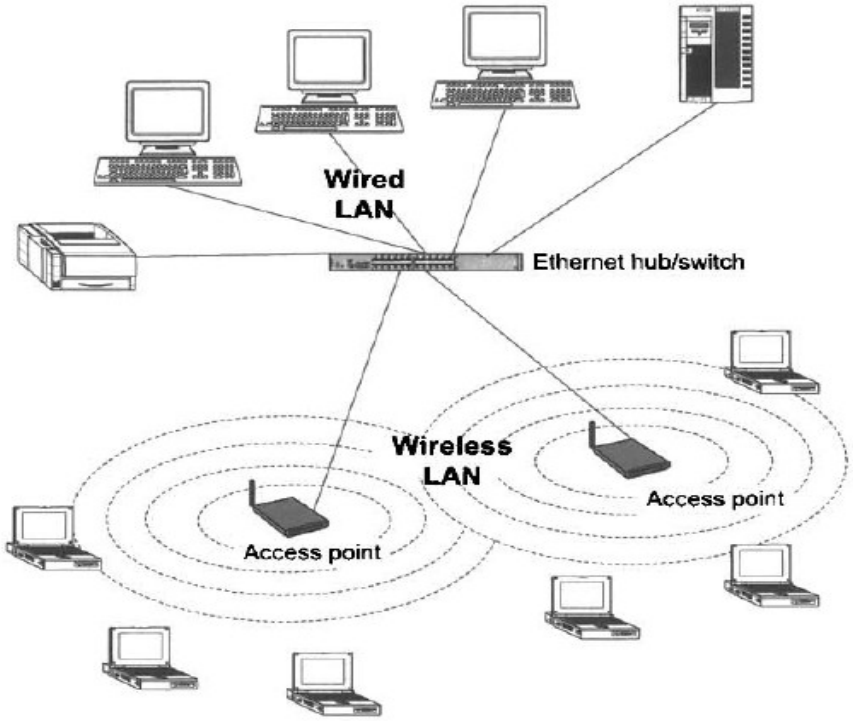
- **LAN**

Basicamente, é uma rede local, conforme ilustra a imagem abaixo:



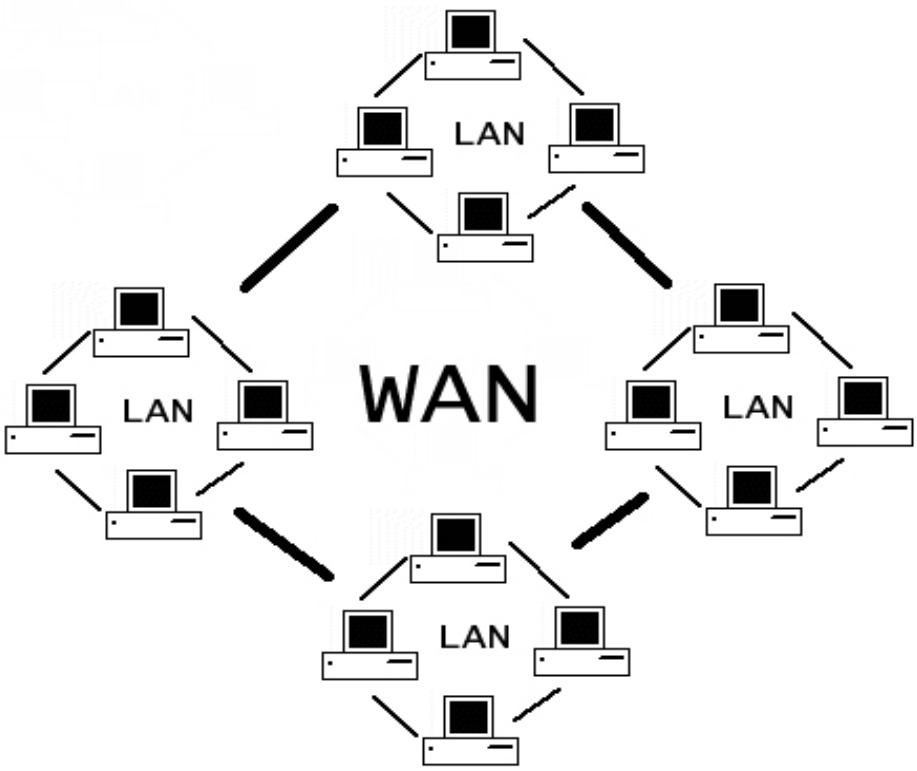
- **WLAN**

É a mesma rede LAN, porem sem fio. Normalmente, encontramos uma rede mista de WLAN com LAN. Como a imagem abaixo:



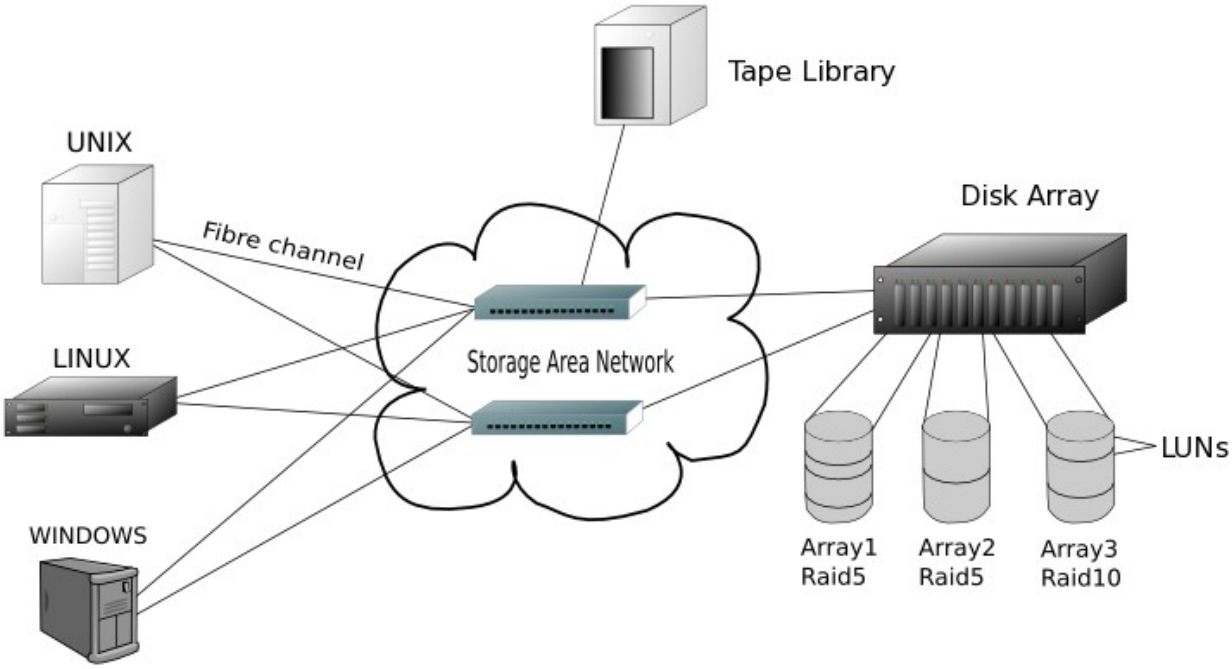
- **WAN**

Uma rede geograficamente distribuída, abrange uma grande área geográfica, com frequência um país ou continente.



- **SAN**

Uma rede especifica para dados, muito usada em redes de grande porte:

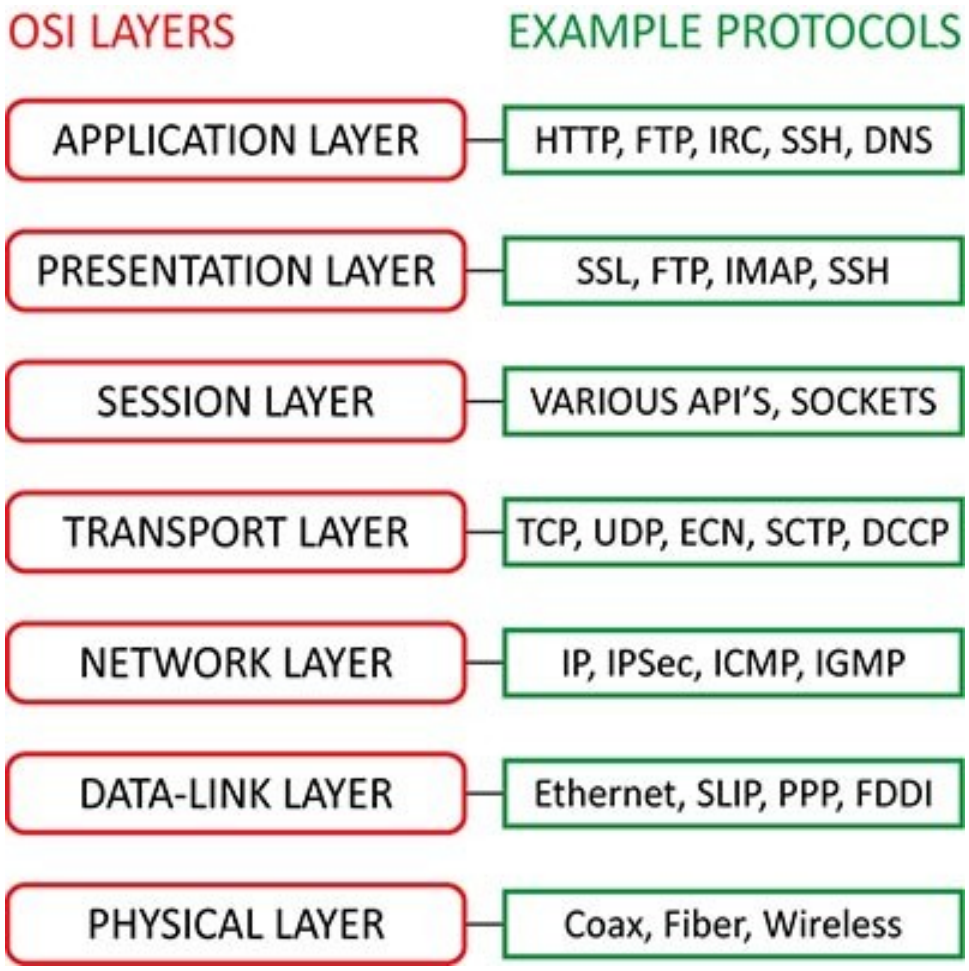


5. Protocolos

Um protocolo é uma convenção que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais.

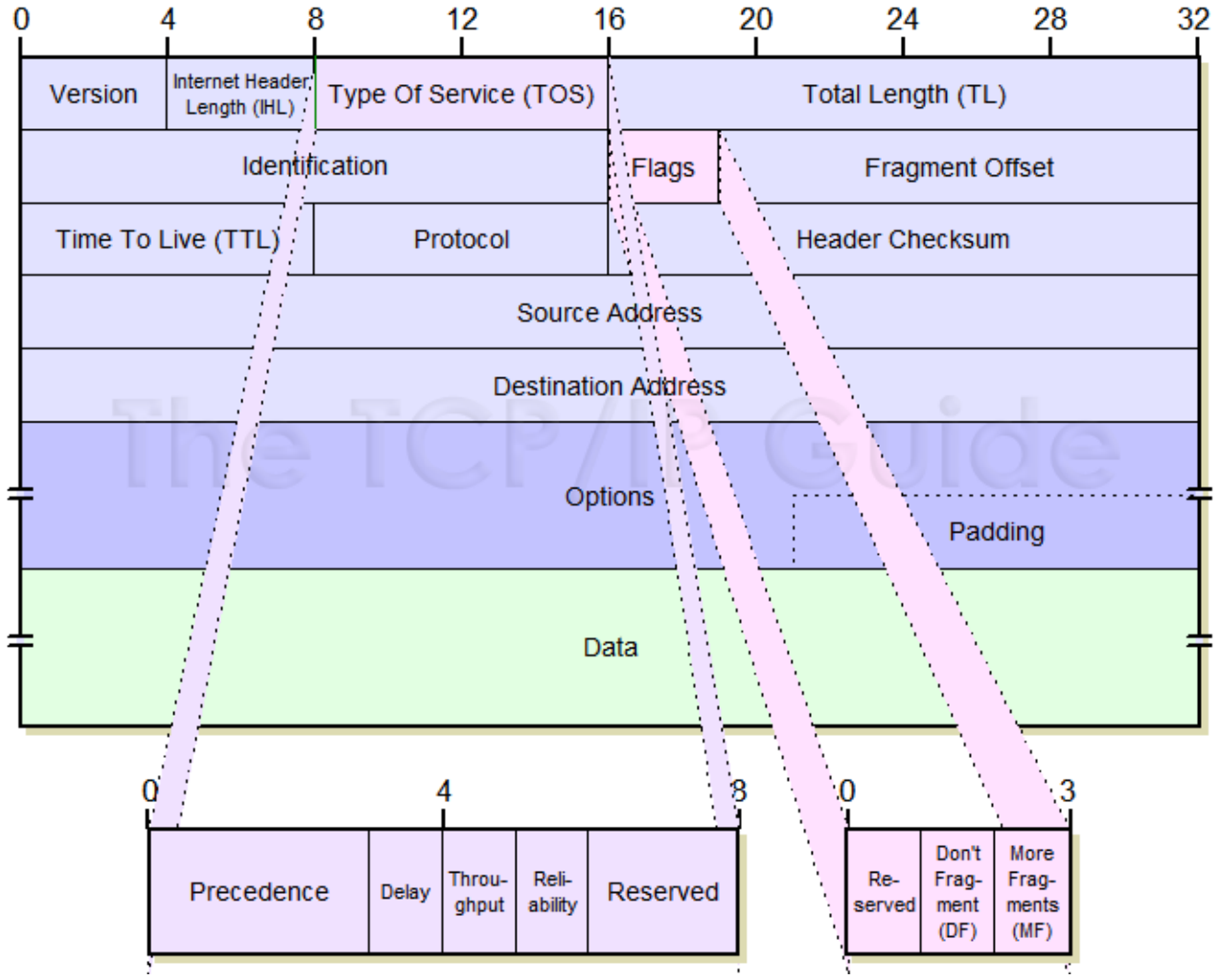
O Modelo OSI (Open Systems Interconnection) permite comunicação entre máquinas heterogêneas e define diretivas genéricas para a construção de redes de computadores (seja de curta, média ou longa distância) independente da tecnologia utilizada.

Abaixo uma imagem que explica o modelo OSI:



6. Endereçamento, mascara, segmentação, frames (jumbo)

Quando falamos das redes de computadores atuais, o principal protocolo de comunicação é o IP (internet Protocol). Este protocolo é explicado pelo desenho abaixo:

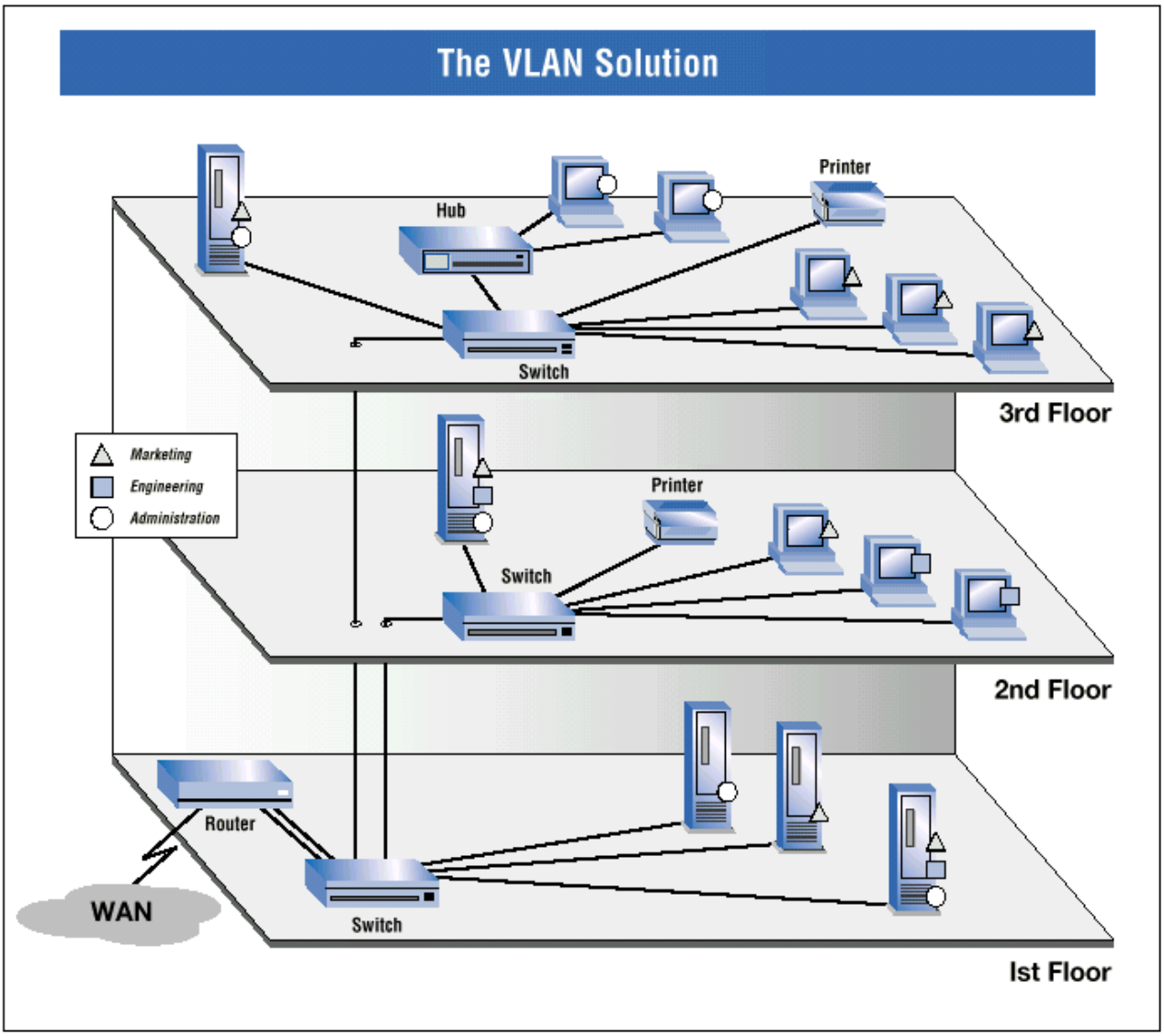


Neste desenho é possível ver o tamanho de cada campo, e a soma destes campos é popularmente conhecida como FRAME, e o tamanho máximo é conhecida como MTU (Maximum Transmission Unit), sendo que o cabeçalho pode ter de 20 bytes até 60 bytes. Exemplo, se o MTU é de 1500 bytes, e se o cabeçalho é de 20 bytes, então a sobra (1480 bytes) é a quantidade de dados trafegada em um pacote.

Existem técnicas de jumbo frames que podem aumentar consideravelmente este tamanho de pacote (ex. o jumbo frame mais utilizado é com um MTU de 8192 bytes)

O endereçamento do IPv4 é feito por quatro casas, cada uma contendo uma numeração de 0 a 255 (ex. 192.168.1.0), e o tamanho das redes é definida pela mascara. Um exemplo de mascara de IP é o /24, que oferece 254 Ips validos para utilização. Esta mascara é uma mascara bem comum nas redes empresariais.

Em uma rede de computadores é comum os elementos mandarem muitos broadcasts, e com isto, todos os computadores escutam. Fora os broadcasts, uma maquina com vírus pode mandar muito trafego para todas as redes. Para evitar este tipo de problema, é usual segmentar a rede. Ex.



Uma rede segmentada oferece maior segurança, maior performance, porem tem uma complexidade maior.

7. Pra que ADR?

As questões referentes ao desempenho são muito importantes nas redes de computadores. Quando centenas de milhares de computadores estão interconectados, são comuns interações complexas que trazem consequências imprevistas. Com frequência, essa complexidade resulta em um fraco desempenho, cujas razões todos desconhecem. TANENVAUM (2003).

Mesmo em empresas menores, o desempenho de rede é extremamente importante. É comum empresas com 50 ou mais elementos na rede experimentarem instabilidades na rede. E em empresas de pequeno porte, é incomum encontrar ferramentas de analises.

A analise e desempenho de redes deve identificar falhas de comunicação, performance, pontos de melhoria e consegue fornecer dados de crescimento da rede.

7.1. Parâmetros mais utilizados na ADR.

Existem algumas informações que são muito usadas na ADR, abaixo uma breve descrição:

- Bandwidth: É a largura de banda máxima que a estrutura pode suportar (ex. 10mbs, 100mbs, 1000mbs, etc)
- Throughput: Throughput de rede ou simplesmente taxa de transferência é a quantidade de dados transferidos de um lugar a outro, ou a quantidade de dados processados em um determinado espaço de tempo.
- Latency: É a quantidade de tempo entre o início de uma ação e seu término, ou seja, é o tempo que uma mensagem leva para atravessar de um ponto ao outro.
- Jitter: É a diferença da latência.
- Congestionamento: É quando tem um trafego maior de dados do que o elemento consegue trafegar, ai ele vai enfileirando os pacotes, similar a um engarrafamento de carros.
- Error rate: o número de bits errados, expressas em percentagem ou fracção do total enviado

7.2. Técnicas utilizadas para ADR

Existem varias técnicas de ADR, porem vamos falar apenas das três mais utilizadas.

a) Modelagem analítica

- Possibilita explorar um modelo sobre o qual se tem controle
- Modelos matemáticos simplificados geram resultados rapidamente
- Técnica barata: lápis, papel e cérebro
- Muitos pressupostos e abstrações são feitas
  - Pode-se perder o comportamento original
- Exemplo: sistemas de filas

b) Medição ou experimentação

- Realização de testes reais em uma rede
- Locais de experimentação:
  - Rede de produção como uma universidade ou a própria Internet
  - Rede específica para testes (testbed)
- Limitações de medição e experimentação:
  - Somente exploram redes e situações atuais
  - Nem sempre é possível ter acesso a uma rede
- Experimentação é uma técnica cara
- Técnica fundamental para a compreensão do comportamento de uma rede de computadores
- Aplicações:
  - Avaliar padrões e volume de tráfego

- Descobrir como os pacotes são roteados
- Avaliar a vazão e perda de pacotes em
- determinado roteador
- Identificar o atraso entre dois computadores
- Identificador locais e causas de congestionamento

c) Simulação

- Técnica para avaliação de sistemas:
  - Permite prever desempenho
  - Comparar alternativas
- Consiste na construção e execução de programas
- Simulação permite construir modelos mais complexos e representativos do mundo real
- Problemas:
  - Extrapolações indevidas
  - Pequenas variações modelo podem produzir resultados contraditórios
  - Pode esconder bugs nos programas

8. NMS - Network management system

Uma NMS (network management system) gerencia os elementos de rede, também chamados de dispositivos gerenciados.

O gerenciamento de rede possui cinco (5) áreas comuns conhecidas como FCAPS, desenvolvidas para o modelo de gerência OSI, contudo não deixa de ser compatível com o modelo SNMP:

1. F – “Fault Management” (Gerência de falhas): visa a detecção, localização e correção de problemas de hardware ou software em uma rede. Atualmente temos sistemas de gerência focando a pró-atividade na antecipação de falhas, onde rotinas de diagnóstico são executadas em períodos de tempo pré-definidos além de correlação de alarmes, thresoulds e syslog para diagnosticar a iminência de determinada falha.
2. C – “Configuration Mangement” (Gerência de configuração): esta relacionada com registros de inventário de hardware e software, histórico de modificação dos dispositivos (normalmente feito através de backups de configuração com registro de data, hora e responsável pela modificação), permitir a inicialização dos sistemas que compõem a rede (como o sistema operacional e a configuração de um roteador, serviço normalmente oferecido em um servidor que utiliza o protocolo TFTP também denominado como TFTPBoot), além de registros de topologia física, lógica e histórico de status dos dispositivos que compõe a rede.
3. A – “Accouting Management”(Gerência de registros, logs ou bilhetes): com a finalidade de registrar a utilização da rede para permitir contabilizar a utilização dos recursos da mesma, muito utilizado por provedores de acessos (ISPs) por motivos de tarifação de serviços, tais como: acesso discado, X.25, frame-relay, etc.
4. P – “Performance Management” (Gerência de performance): parte da perspectiva de como

saber ou definir que determinada rede está com um bom desempenho, uma vez que a rede pode ser vista de forma diferente por usuários de aplicações distintas; ou seja, enquanto ela pode ser considerada como rápida e eficaz para uma determinada aplicação também pode ser considerada extremamente lenta ou incompatível para outra. Através da gerência de performance os administradores de rede podem monitorar certas variáveis chaves como throughput, tempo de resposta, disponibilidade, permitindo definir como e onde o desempenho da rede pode ser melhorado.

5. S – "Security Management"(Gerência de segurança): visa regular e administrar o acesso aos recursos de rede e as determinadas informações, incluindo tarefas como: verificar o privilégio de acesso à rede dos usuários, detectar e registrar tentativas de acesso não autorizadas. Normalmente a autenticação, autorização e accounting de acesso a rede é feito de forma centralizada, e uma estrutura muito comum neste controle de acesso (principalmente para router e switchs) é a utilização de um servidor Tacacs.

A maioria das ferramentas de gerência utiliza a combinação de cinco (5) elementos distintos para a medição de desempenho de uma rede:

- Disponibilidade
- Tempo de resposta
- Utilização da rede
- Vasão (Throughput) da rede
- Capacidade de transmissão da rede

9. SNMP, clients

O protocolo SNMP (Simple Network Management Protocol) foi desenvolvido para permitir que dispositivos de rede que utilizam o protocolo IP (Internet Protocol) possam ser gerenciados remotamente, através de um conjunto de "simples" operações.

Ele usa o modelo manager/agent onde um servidor com a função de NMS ("manager", Network Management System) comunica-se com o agente de gerência de rede ("agent", instalado no dispositivo a ser gerenciado) através do protocolo de gerência.

O "manager" é responsável por polling (busca de informação no agente) ou por recebimento de traps (enviada pelo agente, sem necessidade de solicitação prévia, para informar alterações de status).

O "agent" é um software que roda no dispositivo gerenciado, podendo ser um programa separado (um "daemon", em um servidor Unix) ou incorporado (por exemplo, no Cisco IOS - Internetwork Operating System), para prover informações ao NMS.

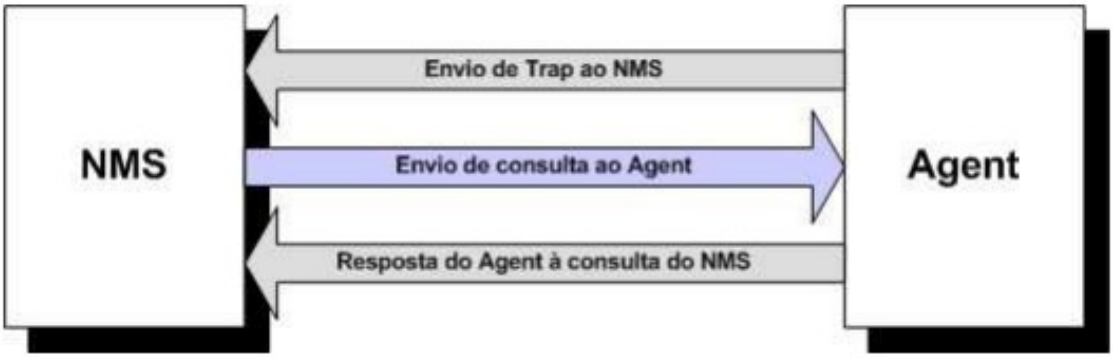


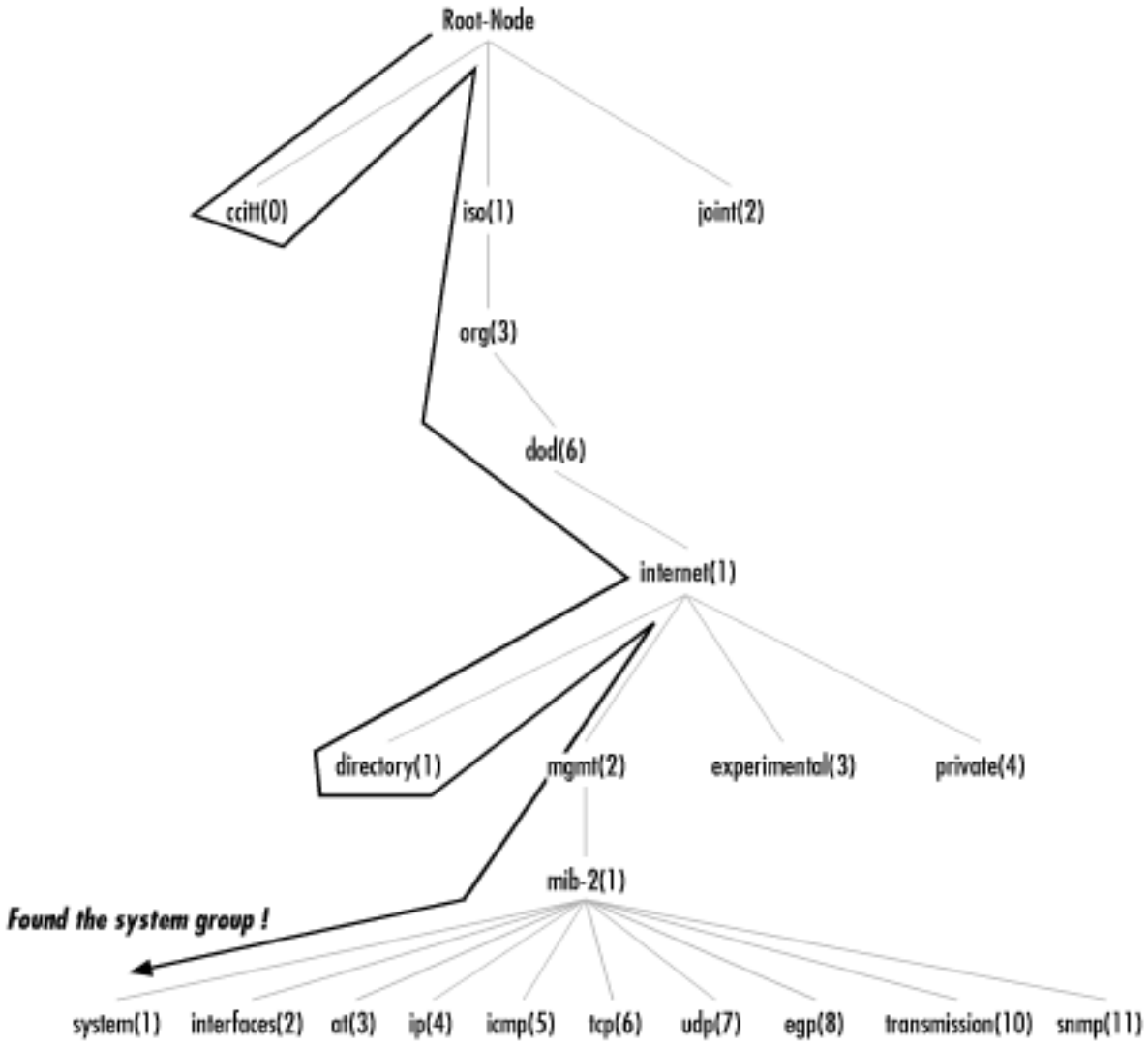
Figura 1. Relacionamento entre NMS e Agent

Dentro do SNMP, temos as MIB e as OID.

A MIB (Management Information Base) é o conjunto dos objetos gerenciados, que procura abranger todas as informações necessárias para a gerência da rede. Ou seja, é o comando do SNMP.

A OID é o endereço desta MIB. Imaginem o endereço Brasil, Minas Gerais, Uberlândia, bairro, rua, numero, apartamento, sala.

Seria similar ao endereço da MIB 1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3 ou ao endereço 1.3.6.1.2.1.1



Outros exemplos:

Load

1 minute Load: .1.3.6.1.4.1.2021.10.1.3.1
5 minute Load: .1.3.6.1.4.1.2021.10.1.3.2
15 minute Load: .1.3.6.1.4.1.2021.10.1.3.3

CPU

percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0
raw user cpu time: .1.3.6.1.4.1.2021.11.50.0
percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0
raw system cpu time: .1.3.6.1.4.1.2021.11.52.0
percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0
raw idle cpu time: .1.3.6.1.4.1.2021.11.53.0
raw nice cpu time: .1.3.6.1.4.1.2021.11.51.0

Memory Statistics

Total Swap Size: .1.3.6.1.4.1.2021.4.3.0
Available Swap Space: .1.3.6.1.4.1.2021.4.4.0
Total RAM in machine: .1.3.6.1.4.1.2021.4.5.0
Total RAM used: .1.3.6.1.4.1.2021.4.6.0
Total RAM Free: .1.3.6.1.4.1.2021.4.11.0
Total RAM Shared: .1.3.6.1.4.1.2021.4.13.0
Total RAM Buffered: .1.3.6.1.4.1.2021.4.14.0
Total Cached Memory: .1.3.6.1.4.1.2021.4.15.0

Disk Statistics

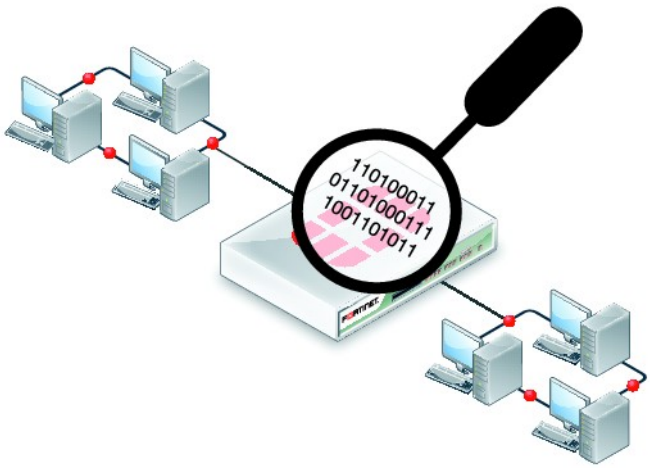
Path where the disk is mounted: .1.3.6.1.4.1.2021.9.1.2.1
Path of the device for the partition: .1.3.6.1.4.1.2021.9.1.3.1
Total size of the disk/partion (kBytes): .1.3.6.1.4.1.2021.9.1.6.1
Available space on the disk: .1.3.6.1.4.1.2021.9.1.7.1
Used space on the disk: .1.3.6.1.4.1.2021.9.1.8.1
Percentage of space used on disk: .1.3.6.1.4.1.2021.9.1.9.1
Percentage of inodes used on disk: .1.3.6.1.4.1.2021.9.1.10.1

Outros

System Uptime: .1.3.6.1.2.1.1.3.0

10. Sniffers

Um sniffer é um programa que consegue capturar o tráfego que passa em um elemento de uma rede para outro.



Das ferramentas disponíveis no mercado, como Wireshark, Sniffer Pró, TCP Dump, etc, todas realizam basicamente as mesmas tarefas básicas:

- Captura – capturar os dados binários que entram ou saem da placa de rede;
- Conversão – converter os dados binários da captura em informações legíveis;
- Análise – indicar problemas ou inconsistências relacionadas aos dados capturados.

Vamos a um exemplo prático de como o sniffer pode ser utilizado na resolução de um problema.

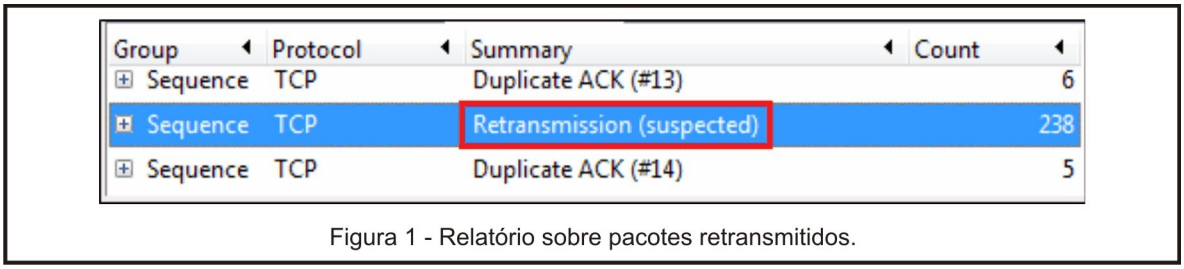
Cenário: Determinada aplicação apresenta lentidão durante a execução de algumas rotinas solicitadas pelos usuários. A aplicação em questão utiliza dois servidores localizados no mesmo CPD, sendo um servidor Web e um servidor de banco de dados.

Objetivo: Identificar se a causa de lentidão é algum problema de Hardware, Rede, ou dos Softwares envolvidos.

- **Retransmissão de pacotes**

Caso ocorra algum erro durante a transmissão dos pacotes de dados pela rede, o servidor precisará reenviar esta informação que foi perdida, isto se chama Retransmissão de pacotes TCP. Retransmissão de pacotes pode ser considerada “normal”, desde que mantenha uma proporção baixa, em relação ao montante de pacotes enviados.

Abaixo esta um exemplo desta detecção com o wireshark



Group	Protocol	Summary	Count
Sequence	TCP	Duplicate ACK (#13)	6
Sequence	TCP	Retransmission (suspected)	238
Sequence	TCP	Duplicate ACK (#14)	5

Figura 1 - Relatório sobre pacotes retransmitidos.

- **RTT elevado**

Round Trip Time (RTT) é o tempo gasto entre o envio do pacote e o recebimento da confirmação de que foi entregue, ou Acknowledge (ACK). O RTT é recalculado sempre que uma transmissão se fizer necessária, desta forma se tivermos um valor de RTT muito alto, significa que neste momento, estamos enfrentando um congestionamento de rede, indicando que não é problema na aplicação, e sim que temos pouca banda de rede disponível.

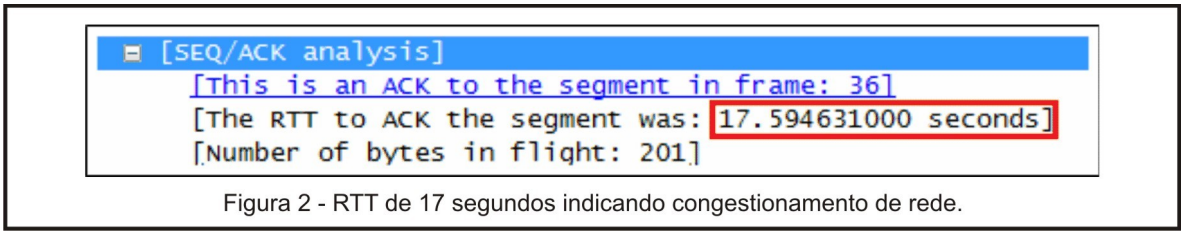


Figura 2 - RTT de 17 segundos indicando congestionamento de rede.

- **Lentidão no Banco de dados**

Um problema mais difícil de ser detectado é quando nos deparamos com erros que não são detectados pelo sniffer, porque não indicam erros de protocolo ou comunicação de rede, mas que devem ser analisados e interpretados pelo analista de rede.

No exemplo abaixo, não existem atrasos na entrega dos pacotes de rede, o que acontece é que após ter sido enviada uma solicitação do servidor de aplicação para o servidor Banco de Dados, o retorno com os resultados ocorre muito depois da aplicação já te retornado uma mensagem de erro para o usuário.

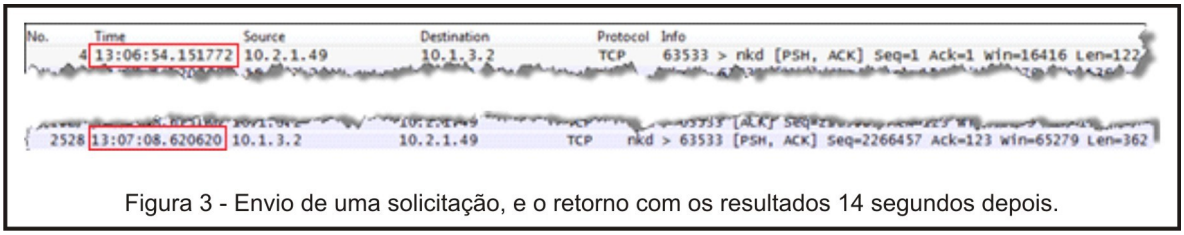


Figura 3 - Envio de uma solicitação, e o retorno com os resultados 14 segundos depois.

Alguns sniffers:

- wireshark
- tcpdump
- ettercap
- dsniff
- windump

- Microsoft Network Monitor
- Capsa Packet Sniffer
- NetworkMiner
- SniffPass

11. Simuladores

A utilização de ambientes de simulação vem aumentando de forma significativa uma vez que estes permitem o estudo e a avaliação de sistemas a custos reduzidos.

Os simuladores de rede desempenham um papel importante na tarefa de desenvolver, analisar e aperfeiçoar protocolos de comunicação. Destacam-se três importantes vantagens do uso de simulação: (Guedes, Conceição, Carvalho e Rodrigues, 2005).

- Permitem testar o comportamento dos protocolos em diversas redes e ambientes, cuja preparação num laboratório ou em uma empresa poderia ser impraticável, isso por questão de custos, ou em tempo de instalação, ou mesmo do ponto de vista administrativo;
- Facilitam a execução de testes em um ambiente controlado, onde é mais fácil fazer variar parâmetros de relevo mantendo os restantes parâmetros constantes;
- Facilitam a execução dos protocolos em múltiplos cenários de execução.

Infelizmente, na maioria dos casos, o ambiente de execução oferecido pelo simulador é bem diferente do ambiente de execução real. Por ambiente de execução entendem-se aspectos como interfaces a serviços, interface com os protocolos adjacentes, reserva de memória para armazenamento de mensagens, lançamento de alarmes, entre outros.

Existem diversos simuladores de tráfego IP disponíveis, os que mais se destacam comercial e academicamente são o **OPNET** (OPNET, 2006), o **GloMoSim** (Rochol, Souza, Sewald, Fernandes, Fernandes), o **NCTUns** e o **Network Simulator** (NETWORK SIMULATOR, 2006) (NS).

O NS é utilizado principalmente por pesquisadores, por ter distribuição gratuita e código aberto. Tal fato o torna adequado a situações onde é necessário desenvolver novas funcionalidades, como em teses e projetos de pesquisa aplicada. No entanto, a sua interface não é amigável ao usuário. A execução de um experimento de simulação no NS requer a elaboração de scripts em Tcl e grande trabalho adicional para obter e visualizar os resultados. Também é comum o usuário necessitar programar em C++ para que possa ter todas as funções do NS funcionando. Além disso, os protocolos e tecnologias no NS em geral são desenvolvidos para uso isolado, para resolução de problemas específicos.

O GloMoSim é uma plataforma moderna e atual de alto desempenho, baseada em processamento paralelo, com um enfoque específico para redes wireless e móveis sendo bem científico e matemático. O uso da biblioteca GloMoSim apresenta um elevado desempenho, contudo, sua maior desvantagem é o fato de ainda não ser totalmente difundida e exigir conhecimentos específicos de redes e de configuração. Como vantagem é muito robusto e escalável.

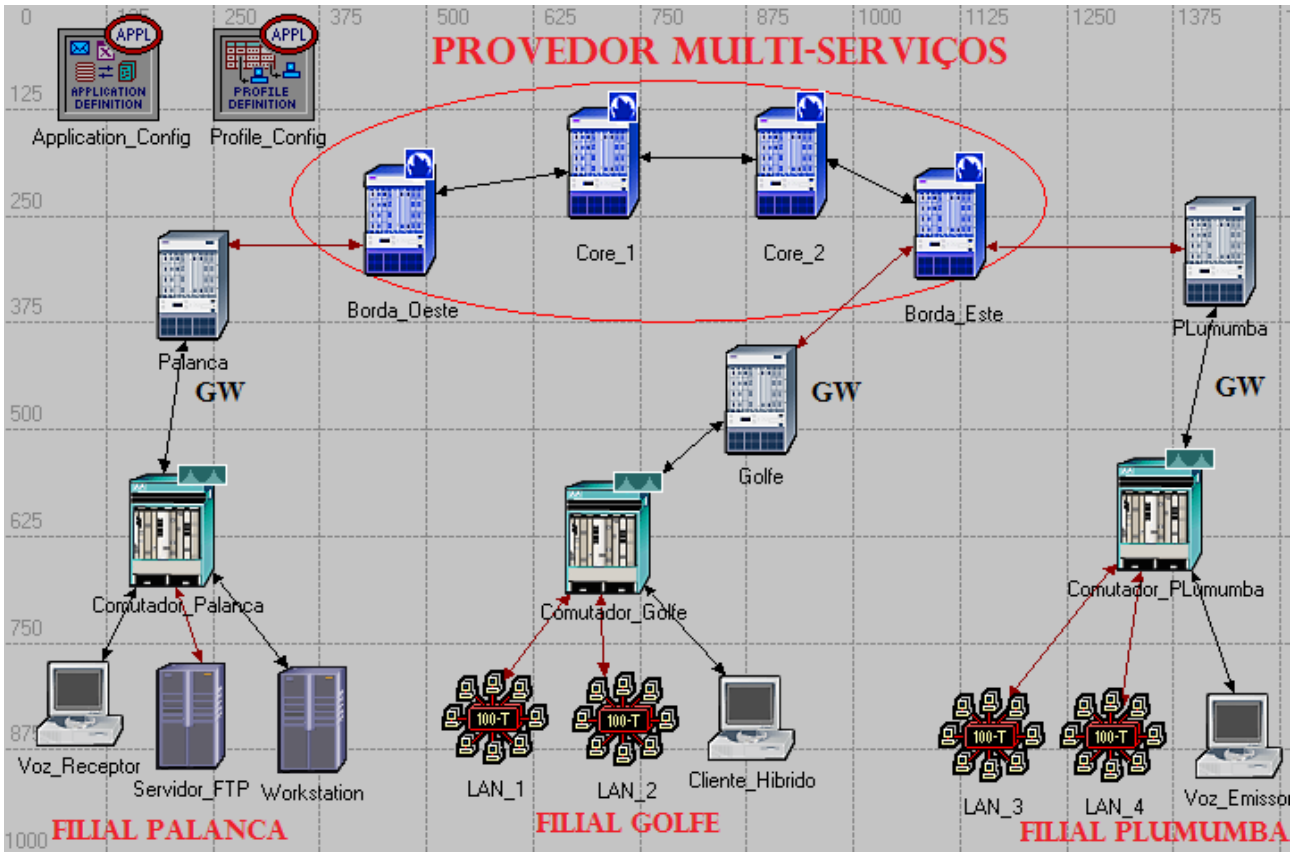
A plataforma NCTUns possui uma concepção moderna e inovadora, o que a torna interessante não só pelo seu alto desempenho mas também pelo seu aspecto pedagógico ou didático. Simula um conjunto amplo de protocolos, tanto para redes móveis como para redes fixas. Assim, a interface gráfica com o usuário é a sua grande vantagem. Como desvantagens é possível citar as dificuldades de implantação, bem como sua portabilidade para outros sistemas operacionais além do BSD. O cenário não pode crescer demais ficando limitado em poucas dezenas de estações na rede.

O OPNET é um simulador comercial largamente utilizado no âmbito corporativo, devido às

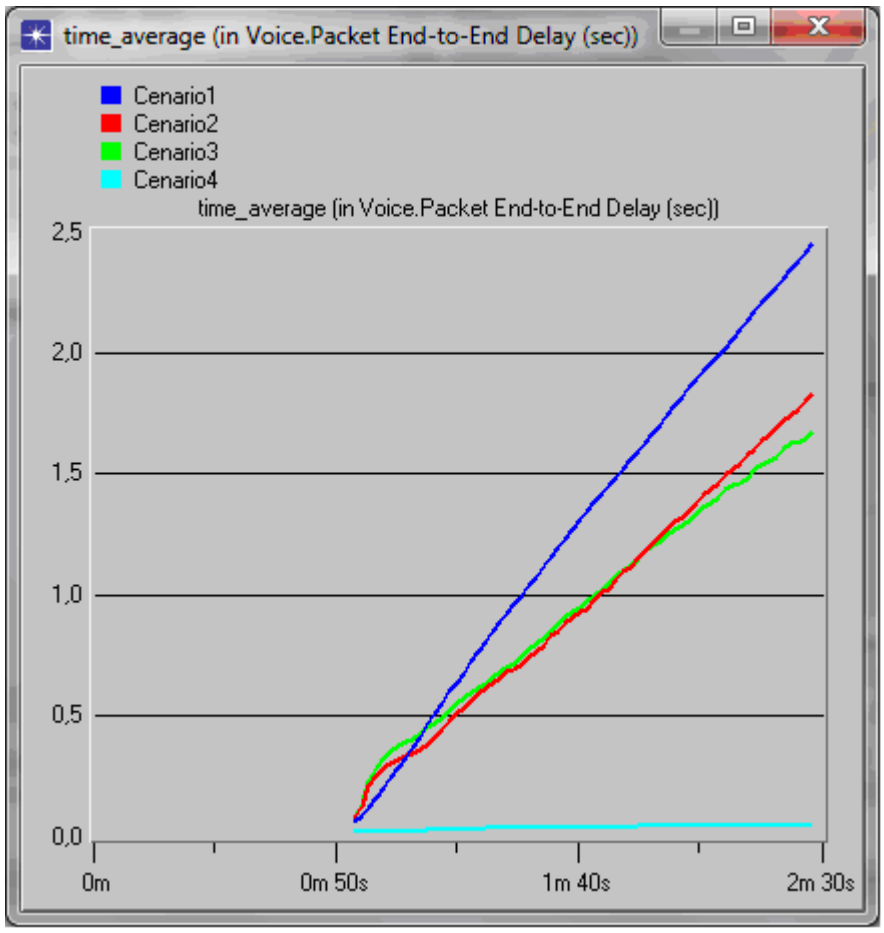
suas funcionalidades e precisão nos resultados. Ele é mais utilizado em grandes empresas e operadoras de telecomunicações, mas restrito em outros ambientes, principalmente devido ao seu alto custo. Uma de suas grandes vantagens é a sua interface gráfica fornecida ao usuário para configurar cenários e visualizar os resultados.

O OPNET tem uma versão acadêmica, o que possibilita o teste da ferramenta, e a aprendizagem.

Abaixo tem uma imagem demonstrando uma simulação de rede:



E uma outra imagem mostrando um relatório de performance comparando vários senários montados:



12. VLAN e QoS

Quando falamos de uma rede bem estruturada, temos dois aspectos que pode ajudar na segurança, na performance e na padronização da rede.

O primeiro é o QoS, que é definido:

- Qualidade de Serviço (QoS) é um requisito da(s) aplicação(ões) para a qual exige-se que determinados parâmetros (atrasos, vazão, perdas, ...) estejam dentro de limites bem definidos (valor mínimo, valor máximo).

O QoS é garantido pela rede, seus componentes e equipamentos utilizados.

Para entendermos melhor o QoS, precisamos falar de SLA (Service Level Agreement), que basicamente é quando a entidade A acorda com a entidade B alguns requisitos de qualidade, como tempo de entrega, largura de banda, etc.

Fazendo uma analogia, imaginem quando vocês contratam uma concessionaria de energia. Ela vai te oferecer uma quantidade suficiente para o seu uso, 24 horas por dia, 7 dias por semana. Isto é um SLA. O mesmo caso sem SLA, seria o mesmo que sem regras, a concessionaria poderia te entregar a energia apenas em alguns horários, ou dias, e apenas o suficiente para ligar uma lampada.

A SLA deve definir claramente quais requisitos devem ser garantidos para que as aplicações possam executar com qualidade. Um exemplo típico de SLA para uma aplicação de voz sobre IP (VoIP - Voice over IP) com algumas centenas de canais voz simultâneos numa rede IP WAN poderia ser:

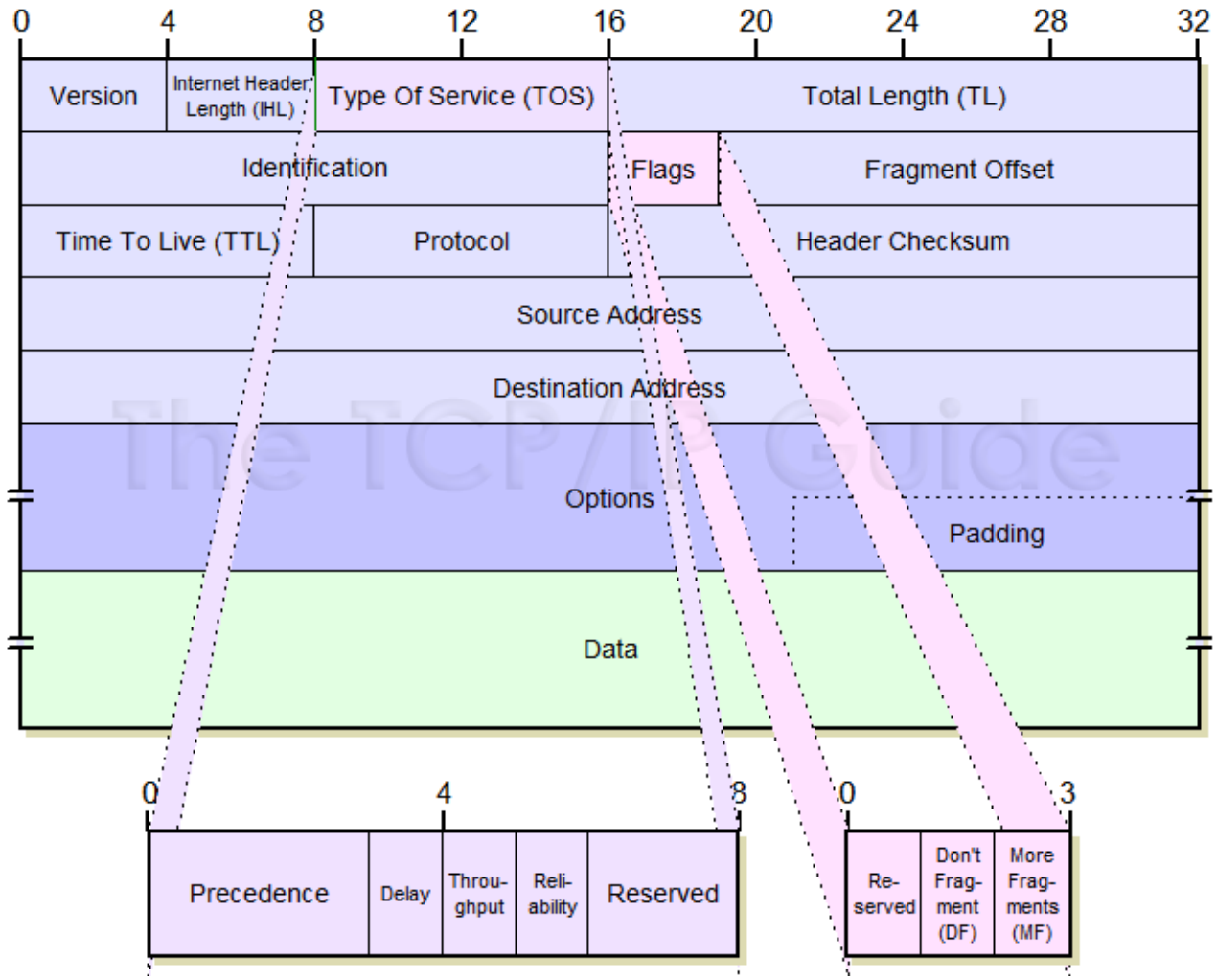
- Vazão ≥ 2 Mbps;
- Atraso ≤ 250 mseg

- Disponibilidade ≥ 99,5%

Os parâmetros mais utilizados para definição de um SLA é:

- Vazão (Banda)
- Atraso (Latência)
- Jitter
- Taxa de Perdas, Taxa de Erros, ...
- Disponibilidade

A implementação de um QoS é feita no campo “Type of service”. Abaixo uma imagem do pacote completo do IP.



E dentro do campo “type of service”, temos estas opções:

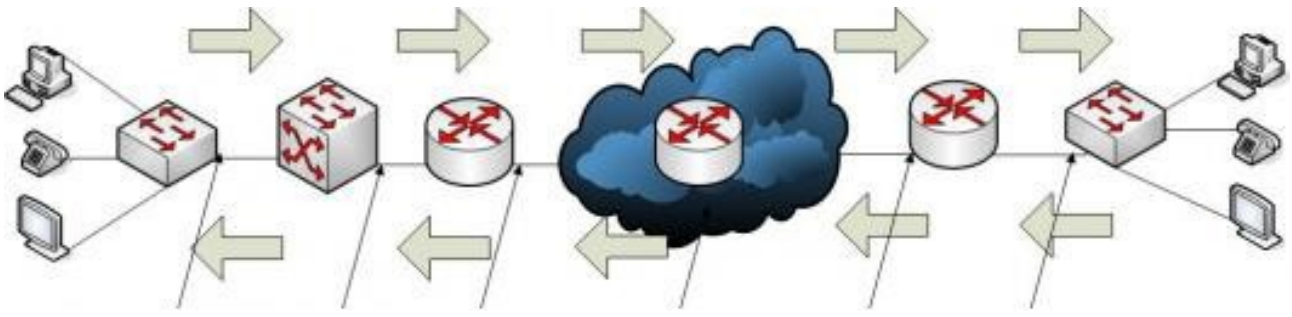
```
000 (0) - Route
001 (1) - Priority
010 (2) - Immediate
011 (3) - Flash
100 (4) - Flash Override
101 (5) - Critical
110 (6) - Internetwork Control
111 (7) - Network Control
```

```
   0     1     2     3     4     5     6     7
+-----+-----+-----+-----+-----+-----+-----+-----+
|                 |     |     |     |     |     |
|   PRIORIDADES   |  D  |  T  |  R  |  0  |  0  |
|                 |     |     |     |     |     |
+-----+-----+-----+-----+-----+-----+-----+-----+

Bit    3:  0 = Normal Delay,      1 = Low Delay.
Bits   4:  0 = Normal Throughput, 1 = High Throughput.
Bits   5:  0 = Normal Relibility, 1 = High Relibility.
Bit  6-7:  Reserved for Future Use.
```

Uma vez estes campos alimentados, o caminho completo da da rede deve estar configurado para aceitar o QoS, ou seja, do dispositivo de origem, aos roteadores, gateways, etc até chegar o dispositivo de destino.

No exemplo abaixo, mostra alguns elementos de rede interligando um computador, um telefone e uma televisão. Caso você queira colocar QoS no telefone, terá que configurar todos os elementos do meio para aceitar QoS.



13. Pratica

Vamos dividir a turma em três partes, todos devem pertencer a um grupo.

Todos os grupos deverão:

1. Montar uma rede com no minimo três elementos, o consumidor, o servidor, e o elemento de rede (ex. Servidor Web, hub e usuário acessando a pagina.

O grupo 1, deverá:

- Monitorar esta rede com um NMS.

O grupo 2, deverá:

- Verificar tipo de trafego na rede, verificar atrasos, tempo de resposta do servidor, se tem retransmissão e se tem QoS

O grupo 3, deverá:

- Simular a rede com um software, e propor melhorias.

E todos os grupos deverão apresentar os resultados (30 minutos) e entregar o relatório apresentando o que fez, porque fez, e como fez (de 10 a 15 paginas).

14. Bibliografia.

ABREU F R, PIRES H D. **Gerência de Redes**. Universidade Federal Fluminense (UFF-RJ) - Campus da Praia Vermelha, Escola de Engenharia

CAMPOS, A. L. P. S., MOREIRA R. C. O., ARAÚJO L. M.. **Análise de desempenho da tecnologia homeplug 1.0 em ambientes domésticos e não domésticos .** Holos, Ano 23, Vol. 2 – 2007

COSTA, G H., **Métricas para Avaliação de Desempenho em Redes QoS sobre IP**, Porto Alegre, dezembro de 2008.

DIAS B Z, JUNIOR N A, **Protocolo de Gerenciamento SNMP**. CBPF-NT-006/01

GIMENEZ, E J C, GARCIA A S. **Uma Metodologia Pragmática Para Avaliação De Desempenho E Planejamento De Capacidade Em Redes De Computadores**. March 19 - 22, 2006

GUEDES, S., CONCEIÇÃO, V., NUNO, C., RODRIGUES, L. **Plataforma de Desenvolvimento e Simulação de Protocolos**, 2005.

HUSTON, G. **"Quality of service". 1ª. Edição**. John Wiley & Sons, 1998.

LOPES S. **Troubleshoot de rede – Analisador de Pacotes (sniffer)**. Taskblog Agosto 2011.

LOPES, Raquel V. et al. **Melhores Práticas para Gerência de Redes de Computadores**. Rio de Janeiro:Campus, 2003. ISBN

MARTINS, R. **Qualidade de Serviço (QoS) em Redes IP Princípios Básicos, Parâmetros e Mecanismos**. Universidade Santa Cecília – Unisanta

MOQADI K A A. **Uso De Ferramentas De Gerência De Rede Para Análise De Desempenho De Uma Rede Local**. Ulbra Novembro de 2011

Network Simulator, "**Network Simulator Web Site**", http://www.isi.edu/nsnam/ns, acessado em 14.06.2006.

OPNET, "**OPNET Web Site**" ,http://www.opnet.com, acessado em 14.10.2013.

PRETE, L. R. **Análise e Desempenho de Redes de Acesso Sem Fio**. Ilha Solteira – SP, Abril de 2011

RAVAGNANI, G. S. **Simulação do Ip Móvel Via Network Simulator (Ns2): Uma Proposta de Rede Wireless.** 2008

TANENBAUM, Andrew S. **Redes de Computadores. 4.ed**. ed. Rio de Janeiro:Campus, 2003. ISBN

VASQUES, A.T., ESTEVES, R.P., ABELEM, A.J.G. . **Simulação de Redes de Computadores utilizando o Network Simulator**, 2004.

VERDI B S S, **implementação e análise de desempenho e segurança de uma rede wi-mesh ad-hoc em linux**. São José Dos Campos 2010