MARCELO KAVAHASHI

UM ESTUDO SOBRE AS TECNOLOGIAS DE REDE MAIS REPRESENTATIVAS DA ATUALIDADE

Monografia apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título de MBA em Engenharia.

São Paulo

2002

MARCELO KAVAHASHI

UM ESTUDO SOBRE AS TECNOLOGIAS DE REDE MAIS REPRESENTATIVAS DA ATUALIDADE

Monografia apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do Título de MBA em Engenharia.

Área de Concentração:
Engenharia de Software

Orientador:
Prof. Kazutosi Takata

São Paulo
2002

Aos meus pais, que sempre me incentivaram

a perseguir os sonhos; com os nossos pensamentos,

realizamos o nosso mundo.

AGRADECIMENTOS

Ao amigo e orientador Prof. Kazutosi Takata, pelas preciosas recomendações e excelentes conselhos.

A todas as pessoas que colaboraram na realização deste trabalho.

RESUMO

O vertiginoso desenvolvimento da microeletrônica está resultando em uma otimização intensiva dos processos produtivos atuais. Surge então, a aurora da "sociedade do conhecimento", onde o suporte a essa comunidade tende a ser a infra-estrutura tecnológica. Atualmente, é um consenso que a convergência tecnológica será uma realidade inexonerável, trazendo benefícios altamente sinérgicos. A Integração de Sistemas está surgindo como uma alternativa bastante racional. O desenvolvimento tecnológico atual encontra um paralelo apenas na Revolução Industrial e um sólido entendimento dos elementos que compõem esse painel passa a ser de fundamental importância para que então seja possível corresponder às demandas da nova sociedade que se descortina.

ABSTRACT

The vertiginous development of microelectronics is resulting in an intense optimization of the current productive processes. It is the dawn of the information society, where the support to this community tends to be the technological infrastructure. Nowadays, it is a consensus that the technological convergence will be an inexonerable reality, bringing highly synergic benefits. The integration of the systems is surging as a very rational alternative. The current technological development has a parallel only in the Industrial Revolution and a solid understanding of the elements that compound this picture has a fundamental importance to match the demands of this new society.

SUMÁRIO

LISTA DE FIGURAS

1. INTRODUÇÃO

Este trabalho propõe-se a ser um breve histórico das tecnologias mais relevantes da informática, sendo que a parte de redes será bastante enfatizada, pois trata-se de um meio heterogêneo de interligar as diversas máquinas que atualmente exibem a tendência de convergir em plataformas pouco numerosas.

Além disso, trata-se de um amplo tema que é regido por uma evolução que freqüentemente foge às linearidades intrínsicas às ciências ditas exatas.

1. Divisões

O trabalho está dividido em três partes :

1) A inicial e também a de maior extensão : uma descrição das tecnologias de rede que atualmente formam a malha básica para a interconexão dos grupos existentes de computadores.

2) Um capítulo com as tendências que estão se delineando no campo da Tecnologia da Informação.

3) A parte final, contendo as conclusões do autor.

2. Comentários

É inegável a crescente necessidade de sistemas de informação por parte da sociedade, cujos equipamentos estão conectados por uma rede de computadores em que a confiabilidade associada deve estar em um patamar próximo das maiores quantidades possíveis de serem alcançadas por meio da tecnologia atual.

Além disso, tecer-se-á um histórico das tecnologias de software e hardware que mais impactaram o panorama atual da Tecnologia da Informação, segundo critérios

que enfatizaram mais a aceitação por parte dos inúmeros utilizadores, e não somente a estrita excelência técnica associada ao artefato considerado.

A motivação de elaborar uma monografia seguindo as diretrizes mencionadas é possibilitar a construção de uma base de conhecimentos que permita o envisionamento e a possível implementação de soluções sistêmicas, evitando repetições de erros que incontavelmente ocorreram na evolução tecnológica.

Os novos sistemas em desenvolvimento caracterizam-se por apresentar uma arquitetura freqüentemente baseada em camadas de abstração de hardware e software setorizado em componentes, facilitando em muito a localização de problemas e inconsistências no protótipo final.

Este manuscrito pode ser descrito como um resumo de algumas tecnologias de rede e de informática, tendo em vista o paradigma de desenvolvimento dos novos sistemas de informação, que certamente caracterizarão o alvorecer da sociedade do conhecimento.

2. AGRUPAMENTO DE COMPUTADORES

1. Introdução

A evolução dos processadores tem poucos paralelos na contemporaneidade, mas os intransponíveis limites físicos para a miniaturização dos chips estão a ser alcançados em alguns decênios.

No sentido de obter velocidades de processamento acima de alguns Teraflops, a utilização massiva de processadores emerge como uma das melhores soluções atuais.

Nesse contexto, os clusters "Beowulf" apresentam-se como uma alternativa a ser considerada.

2. Histórico

Os clusters Beowulf originaram-se na NASA (1994). A premissa básica é a existência de um nó central, incumbido de distribuir as tarefas entre os outros computadores ("escravos"), interligados através de uma rede de alta velocidade (Ethernet, tipicamente).

As vantagens são : alto desempenho e escalabilidade.

Com o protótipo, muitas hipóteses se confirmaram:

-A possibilidade de construir um sistema de computação paralelo a partir de componentes padronizados (hardware e software).

-Utilização bem-sucedida de ambientes paralelos (MPI/PVM) e software de código aberto (GNU/Linux).

-Possibilidade de rivalizar com outras arquiteturas (memória compartilhada e redes proprietárias).

A rápida adoção desta tecnologia está criando uma massa crítica, proporcionando uma base de ferramentas sólida o bastante para a formação de um novo padrão.

3. Tecnologia

Os computadores massivamente paralelos normalmente requerem redes de altíssima velocidade, não raro proprietárias, buscando a menor latência possível. Além disso, empregam milhares de processadores operando em paralelo.

Os clusters Beowulf situam-se entre os computadores massivamente paralelos e as redes de estações de trabalho, onde estes são utilizados durante os períodos de relativa inatividade dos usuários.

Este conceito dilui as fronteiras existentes entre os computadores extremamente interligados e os clusters distribuídos.

Isto ocorre devido ao conceito de confiabilidade existente atualmente nos sistemas paralelos, onde a mesma é obtida utilizando-se componentes redundantes e/ou dispositivos para detecção de falhas.

Basicamente, dois campos de utilização são bastante enfatizados : aplicações paralelas de alta performance e sistemas de alta produção de dados especializados.

Podemos distinguir os sistemas Beowulf de Redes de estações de trabalho através de detalhes mínimos :

A priori, os nós dos clusters tendem a ser exclusivos, facilitando a distribuição de carga a partir da baixa exposição a fatores externos ao sistema. Além disso, problemas relativos à latência inerente à arquitetura tendem a ser minimizados.

Existe também um ID global do processo, possibilitando a um nó encaminhar um sinal para outro nó a partir de um mesmo domínio.

Em workstations, parâmetros relativos ao desempenho da rede TCP/IP tendem a ser otimizados, enquanto nos clusters a vazão de dados é melhor enfatizada.

Em outras palavras, o cluster tem o seu funcionamento direcionado como uma única máquina, não como uma coleção de estações de trabalho.

4. Hardware

Atualmente, um sistema Beowulf é constituído de um servidor central, e vários nós conectados através de uma rede Ethernet. Normalmente, tais computadores utilizam o padrão PC, tendo como sistema operacional o GNU/Linux.

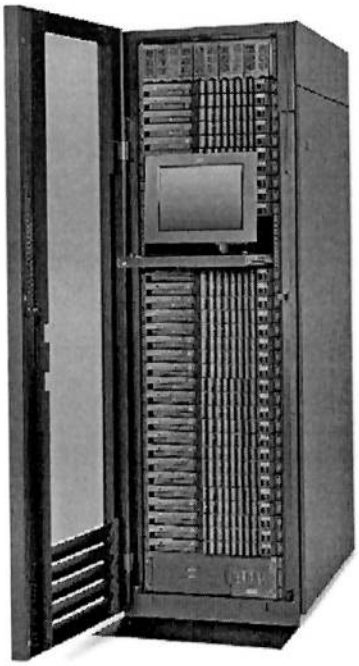

Figura 1 – Um sistema Beowulf compacto

O nó central coordena o cluster e transfere arquivos para os nós. Controla o console do sistema e atua como uma porta de entrada para o mundo exterior.

Tipicamente, os nós não têm teclados ou monitores, sendo acessados remotamente pelo nó central, via login remoto ou mesmo pela porta serial. Podem ser vistos como unidades de processamento e memória que são adicionados ao cluster como um todo, sendo reunidos para formar um computador virtual / paralelo.

Os nós não precisam ser homogêneos, mas devem executar o mesmo sistema operacional e software aplicativo.

Os computadores mais utilizados têm dois processadores por mainboard, com um barramento que suporta também memória compartilhada e apto a suportar as velocidades dos processadores atuais.

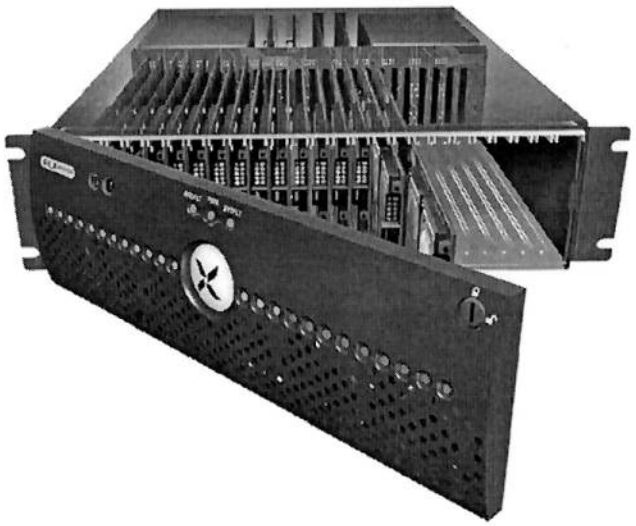

Figura 2 – Um Blade server em modo cluster

Em um projeto de cluster, a parte mais importante é a escolha da rede que será utilizada, pois determina o desempenho global do sistema.

Para o roteamento dos pacotes, uma linha de pesquisa propõe o projeto de um novo sistema para operar sobre ethernet, sem utilizar o protocolo IP.

Em se tratando de hardware, uma tecnologia passível de concorrer com o padrão ethernet é o "Myrinet", que em testes teve o melhor desempenho sustentado em 4Gbit/s, além das seguintes características:

-Baixa latência : 16 microssegundos para MPI

-Alta banda de passagem : 60 MB/segundo

Outro ponto importante é a escalabilidade da rede, que se torna mais significativo à medida que o número de nós do cluster aumenta. O objetivo principal é minimizar a queda na taxa de transferência entre as estações.

5. Software

Os softwares escritos para esta classe de máquinas devem conter algoritmos que contemplem a alta latência inerente a esta arquitetura, além de buscar um excelente balanceamento de carga. Além disso, estes programas não devem requerer sincronismo de altíssima resolução.

A latência mencionada torna-se um assunto de menor importância quando as aplicações requerem comunicações de baixa associação. Se os aplicativos tiverem pouca interdependência, um software de sincronização periódico pode coordenar os nós, resultando em baixo impacto no desempenho como um todo.

Para o intercâmbio de informações entre os nós, as mensagens são muito utilizadas. Sob um ponto de vista histórico, originaram-se a partir da arquitetura de memória local dos computadores paralelos primordiais.

Uma diferença entre as mensagens e as linhas de execução ("threads") é a necessidade de cópia das informações em questão.

Os fatores que limitam as bibliotecas de passagem de mensagens (PVM/MPI) são justamente a latência e a velocidade com que tais informações podem ser transmitidas aos nós de destino.

Essa metodologia tem um bom funcionamento em sistemas com processamento simétricos e clusters em geral.

A vantagem em se enfatizar a utilização de mensagens ao invés de linhas de execução é justamente a escalabilidade, adicionando-se máquinas no sistema para se obter um ganho proporcional.

Linhas de execução:

As linhas de execução foram implementadas nos sistemas operacionais para possibilitar o máximo desempenho das arquiteturas de memória compartilhada dos sistemas de multiprocessamento simétrico.

Tais arquiteturas garantiam comunicação e sincronização extremamente rápida entre os processadores do sistema.

Nesse caso, a cópia de informações torna-se desnecessária, devido ao compartilhamento de dados entre as linhas de execução.

Um problema inerente aos threads é a extrapolação dos limites físicos da máquina, além das dificuldades para manter a coerência das informações contidas nos caches associados aos processadores.

Uma possibilidade é a implementação de linhas de execução em associação com as mensagens, mas a eficiência geral é relativamente baixa.

Para desenvolver software tendo-se em mente o paralelismo, dois métodos são bastante utilizados:

1) Métodos implícitos:

São aqueles em que o programador transfere para o compilador alguns decisões sobre as paralelizações que serão executadas. Um exemplo é o Fortran 90.

Isso faz com que o usuário tenha de fornecer algumas informações sobre a natureza do software, para então o compilador decidir como irá executar tais concorrências em paralelo.

2) Métodos explícitos:

Nesta modalidade, o programador deve escrever código especial para um computador paralelo. Podemos citar as bibliotecas PVM ou MPI, além da possibilidade de inclusão de threads extras.

Assim, a dificuldade de implementar e depurar o código é maior, mas em contrapartida existem várias funções e bibliotecas prontas para implementar o paralelismo nas aplicações.

No passado, os programas escritos em Fortran eram muito utilizados para processamento numérico. Assim, existem muitas bibliotecas para sistemas paralelos. Atualmente, a linguagem C é a mais utilizada para esse tipo de programação.

6. Desempenho

Para mensurar o desempenho dos clusters Beowulf, um benchmark chamado "Linpack" é bastante utilizado. Inicialmente, consistia na solução de um sistema linear de cem linhas por cem colunas, usando a linguagem Fortran. É bastante preciso na avaliação de um nó do cluster.

Atualmente, utiliza-se o "Linpack escalável" ou "Linpack paralelo". A diferença básica reside no fato de não existir um limite na matriz do sistema linear já mencionado. O avaliador é instruído a dimensionar o problema de acordo com a capacidade da máquina, sendo que a memória instalada passa a ser o fator de maior importância.

Além disso, todos os recursos capazes de aumentar a performance da máquina são válidos, inclusive a otimização de bibliotecas com código assembler.

Uma desvantagem desta metodologia é arredondar superiormente a performance do sistema, em relação aos aplicativos utilizados normalmente. Isto ocorre porque os dados são densamente localizados, facilitando o armazenamento das informações em memórias de ordem superior.

A partir dos benchmarks existentes, é possível extrair vários parâmetros para avaliar a real performance da máquina:

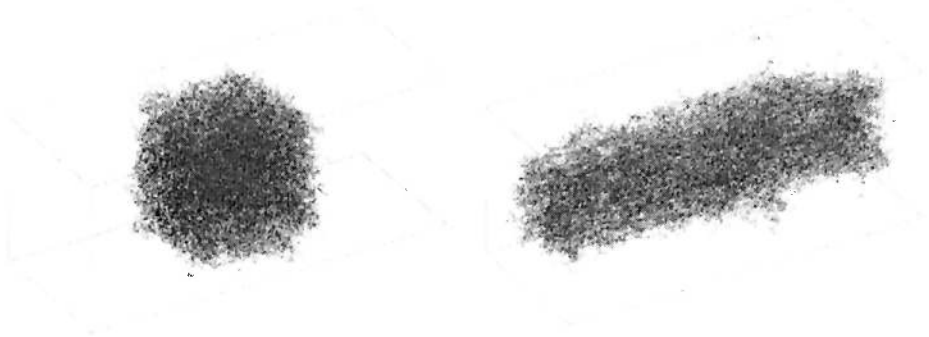

Figura 3 – Solução de problemas utilizando sistemas paralelos

1) Performance máxima teórica

Este número representa o desempenho máximo que está associado a um sistema, normalmente mensurado em Megaflops (milhões de operações em ponto flutuante por segundo) ou Gigaflops (bilhões de operações em ponto flutuante por segundo).

Quando as aplicações consideradas não são estritamente científicas, o desempenho do sistema em inteiros é também considerado.

A vantagem de utilizar este indicador é a facilidade com que pode ser obtido, normalmente não é objeto de muitas discussões e freqüentemente é publicado por meios especializados.

A desvantagem é a disparidade entre o número indicado e as aplicações reais, que pode ser bem relevante.

2) Utilização máxima (porcentagem)

Alguns benchmarks indicam também a carga de processamento dos processadores. É um indicador útil para verificar a demanda real de um aplicativo. Um número baixo significa um desalinhamento entre o sistema em questão e a carga real, necessitando de um melhor escalonamento dos recursos.

3) Utilização do sistema

Indica a carga média do cluster, em um tempo razoavelmente longo. Isto é válido para determinar problemas de competição nos sub-sistemas de entrada/saída, se existem deadlocks, etc.

4) Escalabilidade

É descrito como a razão entre a velocidade do cluster, utilizando "x" processadores e apenas um processador.

Quanto mais o número de aproximar de "x", melhor será a implementação adotada para o paralelismo em questão. A qualidade também será tanto melhor quanto mais linear for a melhoria de desempenho, em relação aos processadores adicionais.

É útil também para determinar a demanda real de processamento por um aplicativo.

5) Latência e banda de passagem

É um dos parâmetros mais úteis para determinar a velocidade real de um cluster, pois a interconexão entre os processadores é determinante para o desempenho do sistema.

O cálculo é relativamente simples, mas quando uma rede está altamente carregada, o desempenho da mesma altera-se substancialmente, muitas vezes de um modo não-linear.

6) Desempenho da aplicação

Mede o comportamento real do sistema em questão, e é usualmente fornecido em Megaflops. Obviamente, é mais significativo do que os cálculos teóricos que são expressos nas mesmas unidades.

Entretanto, é uma medida bem mais difícil de se obter, porque a aplicação tem de ser transposta para o cluster, o que pode ser um trabalho considerável.

Além disso, é preciso obter o processamento real que está sendo produzido. Dúvidas sobre a qualidade dos algoritmos empregados poderão surgir.

Outro ponto seria a otimização do código para o sistema em questão, o que pode levar a enganos na interpretação dos números.

Entretanto, se bem executado, é um dos indicadores mais úteis desta lista.

7) Tempo de execução da aplicação

É simplesmente a medição do tempo gasto pelo cluster para a execução de um determinado aplicativo. A vantagem é a não-necessidade de contar as operações realizadas.

Também evita as distorções acarretadas pela utilização de um algoritmo não muito eficiente. Pode ser considerado um dos melhores métodos de avaliação, pois avalia globalmente o sistema como um todo.

O problema surge na comparação entre dois clusters, pois há a necessidade de carregar exatamente os mesmos aplicativos, o mesmo ambiente operacional, etc.

8) Eficiência do paralelismo

É a razão entre o desempenho global pelo número de processadores. Quanto mais se aproximar de 1, melhor será o sistema.

Conforme relatado, existem vários tipos de benchmark, alguns carregando um sentido mais figurativo. Em suma, pode-se afirmar que o tempo de execução do aplicativo é o mais representativo dentre os indicadores apresentados.

A desvantagem é a necessidade de o sistema existir fisicamente, dificultando projeções teóricas.

7. Tipos de aplicações

É importante distinguir dois conceitos associados aos softwares para clusters : concorrente e paralelo.

-Partes concorrentes de um software podem ser executadas independentemente.

-Partes paralelas são aquelas cujas partes concorrentes são executadas em processadores separados ao mesmo tempo.

Execução paralela deveria resultar em um desempenho melhor. O fator limitante é a velocidade de comunicação e a latência entre os nós. Idealmente todas as partes concorrentes poderiam ser executadas em paralelo.

Para dois computadores paralelos que utilizem processadores que implementem a mesma arquitetura, o que tiver processadores mais lentos será melhor empregado em aplicações que utilizem uma alta taxa de entrada/saída.

Nessa situação, a menor velocidade dos dispositivos de I/O (discos, fitas) limitará o desempenho global da máquina.

É importante determinar se o fator limitante da aplicação é o processador (cálculos intensivos) ou o subsistema de entrada/saída.

Em suma, em ambientes paralelos é importante verificar a adequação de uma máquina à sua aplicação: é necessário avaliar vários itens, tais como: CPU, compilador, bibliotecas, rede, etc.

Verificar apenas a demanda computacional não é suficiente, é preciso também validar se a rede suporta o tráfego existente entre os nós do cluster.

8. Desvantagens

O padrão Ethernet apresenta algumas limitações em latência e banda de passagem, mas é suficiente para a grande maioria das aplicações.

Para tanto, placas especializadas desviam o processamento que seria realizado no processador, atingindo velocidades próximas aos dos supercomputadores proprietários.

A arquitetura sofre do overhead existente no protocolo padrão TCP/IP, aumentando a latência entre as mensagens. Uma solução é utilizar o protocolo UDP, para um desempenho melhor.

O aumento no número de estações reduz o MTBF do sistema como um todo. Isso faz com que o software tenha de ser projetado para isolar tais ocorrências. Assim, servidores tolerantes a falhas constituem um campo de pesquisa em ascensão.

Na área de software, a grande maioria dos programas utiliza a linguagem C, e a existência de ponteiros pode fazer com que a localização real das dependências de dados fique um tanto difícil de ser determinada. Uma solução seria utilizar uma análise automática de ponteiros.

9. Vantagens

Existem muitas vantagens na arquitetura descrita, podendo-se enumerar as principais:

-Subsistemas de entrada/saída distribuídos, melhorando a banda de passagem e latência globais.

-Armazenamento paralelo e distribuído.

-Utilização de componentes de uso disseminado, facilitando a construção de máquinas conforme a aplicação a ser utilizada.

-Melhorias no desenvolvimento de sistemas mais confiáveis.

Aplicações previstas:

-Realidade virtual, simulações de alta precisão, etc.

10. Conclusão

Tal arquitetura representa uma tecnologia que descreve uma tendência no sentido de obter maiores velocidades, com a utilização de uma quantidade relativamente baixa de dispositivos físicos (hardware).

A velocidade de 100 Teraflops é considerada um marco, pois representa a fronteira necessária para ocorrer a emulação da maioria dos eventos comumente observáveis, para muitos especialistas em processamento paralelo.

3. 802.11

O sucesso do padrão Ethernet para a comunicação de dados entre computadores resultou na difusão da tecnologia para os sistemas "wireless", possibilitando o intercâmbio de informações sem a necessidade da utilização de cabos físicos.

Espera-se que as wireless LAN (WLAN) sejam o padrão para o acesso móvel às redes IP.

1. Topologia

Uma WLAN é um sistema de comunicação que provê acesso sem fio peer-to-peer (equipamento-a-equipamento) e também conectividade ponto-a-ponto (LAN-a-LAN), com a utilização de ondas eletromagnéticas.

A topologia mais simples de uma rede 802.11 é composta de pelo menos dois nós mutuamente já reconhecidos, comunicando-se entre si através de um modo peer-to-peer, em uma determinada área de alcance.

Tais topologias freqüentemente contém um AP (Access Point). A função desse dispositivo é agir como transmissor e receptor, formando uma conexão entre a rede LAN e a rede wireless.

É similar a uma estação rádio-base das redes celulares. Quando existe um AP, as estações não mais se comunicam no modo peer-to-peer, mas sim em um modo denominado infraestrutura.

Os AP's não são móveis, e fazem parte da infraestrutura da rede LAN.

2. Características principais

O padrão 802.11 tem as seguintes características:

-Opera na faixa de freqüência de 2.4 GHz.

-Suporta uma banda passante de 11 Mbps, com um alcance de 50 metros. A velocidade diminui com o aumento da distância entre o receptor e o transmissor, em passos de 5.5 Mbps, 2 Mbps e 1 Mbps.

-As velocidades mais baixas são também utilizadas para a compatibilidade com os sistemas WLAN legados.

-O padrão IEEE 802.11b prevê a existência de 11 canais de acesso, sendo que três não podem compartilhar a mesma cobertura de sinalização.

-O sistema 802.11g, mais recente, utiliza a modulação OFDM (Orthogonal frequency-division multiplexing), mais eficiente, podendo atingir até 54 Mbps.

-As transmissões usam 100 milliwatts de potência.

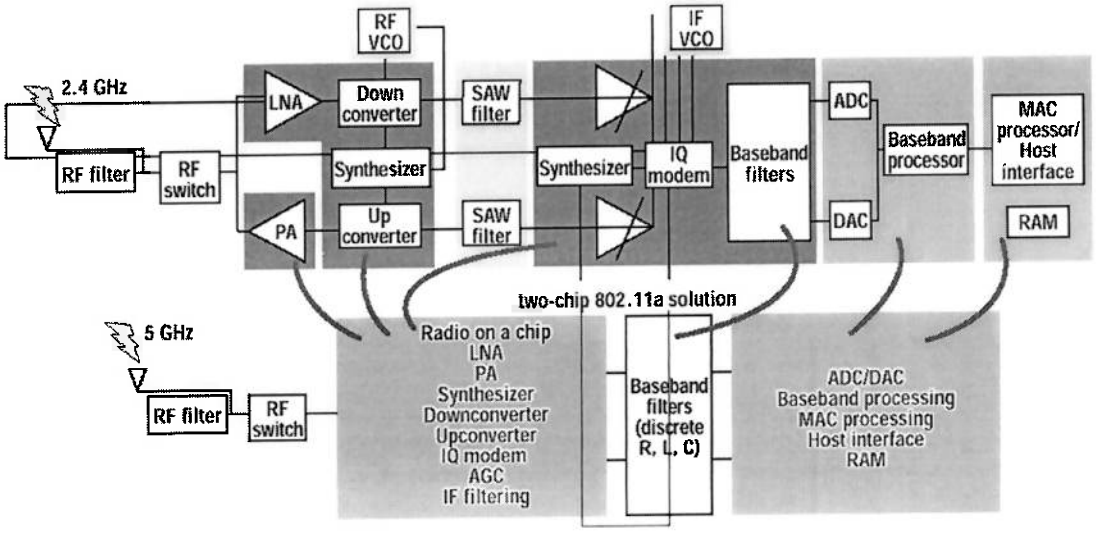

Figura 4 – Um projeto 802.11a

3. Roaming

O padrão permite também o roaming entre vários pontos de acesso, que podem estar operando em canais diferentes.

As estações móveis utilizam o sinal periódico enviado pelos AP para avaliar a existência de conexão, além de mensurar a potência do sinal incidido. Se o sinal for demasiado fraco, a estação pode selecionar outro AP.

O padrão identifica as mensagens básicas para o suporte ao roaming, e um protocolo específico para tal foi criado: o IAPP (Inter-Access Point Protocol).

4. PHY

A camada física (PHY) usa a tecnologia CCK (Complementary Code Keying), suportando três interfaces :

1) DSSS
2) FHSS
3) Infravermelho (IR)

A camada MAC é comum aos 3 PHYs. A modulação usada é o QPSK/BPSK.

5. Tecnologia

As implementações podem ser baseadas em rádio-freqüência, mas utilizando o DSSS (Direct Sequence Spread Spectrum) ou o FHSS (Frequency Hopping Spread Spectrum).

Ambos foram projetados para operar em um modo 2.4 GHz ISM, uma faixa de freqüência mundialmente alocada para operação sem licenças.

O FHSS normalmente opera em 1 Mbps, podendo atingir 2 Mbps em condições favoráveis.

Com o FHSS, a transmissão e a recepção são sincronizadas por canais, utilizando uma seqüência pré-determinada que é conhecida somente pelas estações.

O IEEE 802.11 especifica 78 seqüências e 79 canais. Se um canal não está em condições de operar, os dados são retransmitidos quando um novo canal é utilizado.

6. Wi-Fi

A finalidade do "Wireless Ethernet Compatibility Alliance" é desenvolver normas e padrões para a LAN wireless, além de prover certificações de conformidade.

Para tanto, reconheceu-se a sigla Wi-Fi (wireless fidelity), para que seja possível identificar os sistemas aprovados em testes de interoperabilidade criados pela instituição acima mencionada.

7. Direct Sequence Spread Spectrum

As implementações normalmente utilizam o DSSS, porque essa nova especificação possibilita taxas de transmissão de até 11 Mbps, mas assegurando a co-existência com o padrão anterior.

A camada física DSSS especifica um máximo de 2 Mbps, podendo cair até a 1 Mbps em caso de um ambiente altamente ruidoso.

Os sistemas DSSS usam uma tecnologia similar aos satélites GPS.

Cada bit de informação é combinado com uma função "xor" com uma seqüência PN (Pseudo-random Numerical).

O resultado é um fluxo de alta velocidade que é modulado na freqüência de operação usando o DPSK (Differential Phase Shift Keying).

A estação que recebe o sinal utiliza um filtro de correlação que remove a seqüência PN e recupera a informação original.

8. Direct Sequence Spread Spectrum - canais

A faixa de freqüência de 2.4 GHz contém 80 MHz de espectro, podendo acomodar até três canais DSSS de banda equivalente sem sobreposição.

Cada canal DSSS tipicamente ocupa 22 MHz de banda passante e é necessário um mínimo de 25 MHz para minimizar interferências entre os canais.

Isso permite que até três AP (Access Point) possam ser ativados simultaneamente, cada um programado para ocupar um dos três canais que podem ser alocados na mesma área de cobertura.

Cada bit que é transmitido é codificado com um padrão redundante, conhecido apenas pelos enviadores e receptores das estações envolvidas, dificultando a decifração dos dados codificados.

O padrão redundante permite a recuperação dos dados sem retransmissão, se um dos bits for perdido ou danificado durante a transmissão.

9. MAC

O MAC (Media Access Control) é bastante resiliente a erros, incluindo controle de seqüência e possibilitando várias tentativas de acesso. Além disso, pode interoperar com o padrão Ethernet normal, através de pontos de acesso (AP).

As funções principais do MAC são:

1. CSMA/CA

A tarefa básica do MAC é prover acesso à mídia aérea e evitar colisões de dados. Duas funções de acesso são definidas : DCF (Distributed Coordination Function) e PCF (Point Coordination Function).

O CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) significa que os rádios devem verificar se o meio não contém nenhuma transmissão em progresso, antes de encaminhar os próprios pacotes.

2. Controle de potência

As estações podem entrar em modo de espera por longos períodos, sem perda de informação. As estações periodicamente são ativadas, para receber uma sinalização notificando se existem pacotes armazenados no AP.

3. Autenticação

Aumenta a segurança de uma rede wireless, controlando o acesso. Antes do estabelecimento de uma conexão, é necessário realizar a autenticação.

Há dois tipos de autenticação: chave compartilhada e sistema aberto.

4. Segurança

É definido para proteger as informações, usando um algoritmo para assegurar a confidencialidade dos dados transmitidos.

O algoritmo de encriptação é o RC4, com uma chave de 64 bits.

5. Associação e reassociação

Cada estação deve associar-se com um AP antes de encaminhar informações através de um sistema de distribuição. A reassociação provê roaming e balanceamento de carga.

6. Tipos de Frame

-Frames de supervisão (manter a comunicação entre as estações e os APs)
-Frames de controle

Em um sistema wireless, a chance de que uma mensagem não seja recebida na estação de destino é maior do que a LAN normal.

Para minimizar este problema, o sinal ACK (Acknowledge) foi adicionado no MAC, para que o receptor envie ao transmissor um sinal indicando que a mensagem foi recebida com sucesso.

Se o enviador não receber esse sinal, o mesmo retransmitirá a mensagem.

10. Sincronismo

Para o gerenciamento da potência, são utilizados recursos que podem maximizar a duração da bateria, mas também podem trazer problemas porque tipicamente determinam a inatividade do sistema, após um certo período de tempo.

Isso pode fazer com que transmissões críticas sejam perdidas. Para resolver esse problema, os pontos de acesso (AP) contam com buffers para armazenar as mensagens.

Os terminais remotos são trazidos à atividade e então recuperam as informações que seriam descartadas.

Os relógios das estações são ajustados através da transmissão periódica de um sinal de sincronismo, gerados pelo AP, que controla o relógio central.

A sincronização é mantida ao redor de 4 microssegundos, mais o atraso de propagação. As informações emitidas incluem : indicação de tráfego, taxas de transmissão suportadas, etc.

11. Segurança

Em um sistema IEEE 802.11, a segurança é obtida através de autenticação e encriptação.

É o meio de verificar a autorização de comunicação com uma estação ou com um AP, que pode ser de dois modos:

a) Sistema aberto: nesta opção, qualquer estação pode requisitar uma autenticação, que pode ser aceita o usuário se estiver em uma lista de acesso.

b) Chave compartilhada : somente estações que tenham uma chave secreta criptografada podem ser autenticadas.

Além disso, existe o mecanismo chamado WEP (Wired Equivalent Privacy), baseado no algoritmo RC4 de encriptação, estando localizado no MAC.

Se o WEP estiver habilitado, então todas as informações transmitidas através da rede wireless são encriptadas. Adicionalmente, o suporte à seqüencia de controle e campos de fragmentação permitem a operação mesmo em caso de atenuação de sinal.

12. CCK

O CCK (Complimentary Code Keying) é o formato básico de modulação para os sistemas IEEE 802.11b.

Todos os dados são transmitidos e modulados através de uma simples portadora. É capaz de atingir velocidades de 11 Mbps e 5.5 Mbps.

Cada pacote pode ser decomposto em :

1) Preâmbulo/Cabeçalho : indica o início de uma transmissão de dados.

2) Carga útil : contém os dados a serem encaminhados para o receptor. Pode variar de 64 bytes a 1500 bytes.

Na modulação CCK, o preâmbulo/cabeçalho e a carga útil são transmitidos em seqüência.

13. OFDM

O OFDM (Orthogonal Frequency Division Multiplexing) foi desenvolvido para atingir maiores velocidades de transferência, acima de 20 Mbps.

É um sistema de modulação com múltiplas portadoras. Os dados são divididos entre várias subportadoras, proporcionado uma operação confiável mesmo em ambientes com um alto grau de distorção de sinal.

Nesta tecnologia, o preâmbulo passa a ter um comprimento menor, passando de 72 ms para 16 ms, evitando um overhead excessivo.

14. CCK/OFDM

É uma modulação híbrida, sendo que o CCK é usado para transmitir o preâmbulo/cabeçalho e o OFDM é utilizado para transferir a carga útil.

A combinação CCK/OFDM pode atingir até 54 Mbps, sendo parte do IEEE 802.11g.

O preâmbulo CCK alerta todos os dispositivos Wi-Fi que uma transmissão está se iniciando, informando também a duração da transferência.

15. PBCC

O PBCC (Packet Binary Convolutional Coding) é um sistema de portadora simples, usando também o CCK para transmitir o prâmbulo/cabeçalho e o PBCC para transferir a carga útil.

Pode atingir a velocidade de 33 Mbps e emprega uma complexa constelação de sinais (8-PSK). Entretanto, os picos de transferência são menores do que o CCK/OFDM.

É considerado um elemento opcional do IEEE 802.11b.

16. Conclusão

Provavelmente, uma solução adequada seria a utilização de sistemas 2.5G/3G em ambientes mais distantes das áreas que contam com infra-estrutura adequada, enquanto o padrão IEEE 802.11 seria melhor aproveitado dentro das construções prediais que caracterizam as áreas urbanizadas.

4. VOIP

1. Introdução

A rede telefônica pública (PSTN) tem como base primordial a comutação de circuitos, evoluindo gradativamente até culminar nos sistemas CCN7 atuais. A tecnologia VoIP propõe a migração para a comutação de pacotes, mas agravantes técnicos fazem com que a disseminação seja realizada em um ritmo relativamente lento.

Tecnicamente, VoIP é a possibilidade de realizar chamadas telefônicas sobre uma rede de dados baseada no protocolo IP, com uma qualidade de serviço (QoS) aceitável.

2. Histórico

Primordialmente, as redes de dados e de voz eram mantidas separadamente, porque os requerimentos que as regiam eram diferentes, sendo que alguns requisitos estavam no limite da contradição.

Atualmente, os avanços tecnológicos subseqüentes (Fast Ethernet, Gigabit Ethernet) possibilitaram a convergência de ambas as redes. Isso possibilitou o desenvolvimento de aplicações avançadas, integrando voz e dados.

A rede IP em questão pode ser tão minúscula quanto dois dispositivos interconectados ou tão grande quanto a Internet.

As conversações são convertidas para um fluxo de pacotes IP, mas novas formas de conversão podem aparecer no futuro.

Os requisitos técnicos e as expectativas do usuários direcionam as pesquisas sobre a qualidade de serviço (QoS).

Os usuários estão acostumados com a alta qualidade proporcionada pelo sistema telefônico atual, baseado na comutação de circuitos e orientado à conexão. Isso ocorre porque cada chamada tem uma banda de passagem previamente reservada.

Uma chamada via PSTN requer cerca de 64 Kbps de banda de passagem. Utilizando compressores e DSPs (Digital Signal Processors), é possível reduzir substancialmente esse requisito.

3. Tecnologia

Um dos pontos-chaves em um projeto VoIP é construir uma infra-estrutura baseada em IP capaz de alcançar os requisitos de qualidade atingidos pelas redes telefônicas convencionais.

Quando uma solução VoIP é adotada, as chamadas são encaminhadas para um ISP (Internet Service Provider). Basicamente, há três arquiteturas dominantes : cartões dedicados, novos PBXs e gateways.

Há dois grupos determinando os padrões que serão utilizados : o ITU-T (International Telecommunication Union) e o IETF (Internet Engineering Task Force). Há uma grande discrepância no tratamento da elaboração das especificações, sendo que o ITU-T preza em maior grau o formalismo técnico.

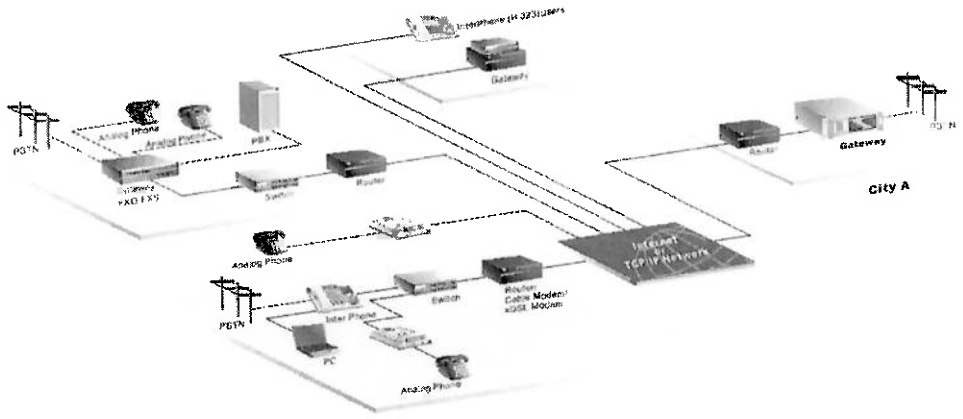

Figura 5 – Diagrama em blocos de um sistema VoIP

4. Compressão da voz digitalizada

A partir da digitalização da voz, a banda de passagem pode requerer de 32 Kbps até 64 Kbps. Alguns métodos podem atingir até 8 Kbps, caso do G.729. O desafio é manter essa banda, sem depender da utilização da rede.

1. Codecs

Existem três codecs (codificadores/decodificadores) principais, a saber:

G.711, G.729 e G.723.

Eles diferem nas técnicas de codificação e na taxa de transmissão dos fluxos de dados. As técnicas mais utilizadas são o PCM (Pulse Code Modulation) e o ADPCM (Adaptive differential PCM).

O principal problema relatado aos mesmos é a delay (atrasos) que os mesmos proporcionam, durante a compressão da voz.

Existem três tipos de delay:

1) Atraso de processamento : o tempo necessário para formar um quadro.
2) Atraso por antecipação : o tempo para verificar o próximo quadro, enquanto o atual está sendo processado.
3) Atraso do quadro : o tempo necessário para transmitir um frame.

Os três codecs citados adicionam os seguintes atrasos:

1) G.711: não há compressão (64 Kbps) e o atraso é imperceptível. A voz está no correto formato para ser encaminhado ao sistema telefônico público (PSTN).
2) G.729: existe a compressão para 8Kbps e o atraso é de 25ms.
3) G.723: comprime a 6.4 Kbps ou 5.3 Kbps, com um delay de 67ms. Produz quadros com predição linear, utilizando o MP-MLQ ou o ACELP, respectivamente.

São implementados com a utilização de chips DSP (Digital Signal Processing).

Os algoritmos de compressão baseiam-se nos padrões repetitivos encontrados na fala humana. Os frames contém normalmente de 10 a 30 bytes, sendo que normalmente não são encaminhados durante as pausas existentes nas conversações.

A avaliação da voz digitalizada e compactada segue princípios subjetivos, sendo utilizado mais freqüentemente o MOS (mean opinion score), que varia de 1 (ruim) a 5 (excelente).

Normalmente, as avaliações dos codecs mencionados são:
G.711: 4.4 e G.723: 3.5

2. H.323

O primeiro padrão VoIP a atingir níveis consideráveis de aceitação por parte de especialistas e usuários foi o H.323, sendo que uma das implementações baseadas em software denomina-se "Netmeeting".

É um padrão global cuja qualidade é comparável à proporcionada pela rede pública, se o tráfego existente na rede IP associada for relativamente baixo.

Baseia-se em uma complexa pilha de protocolos, a partir do modelo OSI e da codificação ASN.1. O H.323 determina os protocolos que os terminais devem utilizar, para que ocorra a comunicação entre os mesmos. Define também os formatos utilizados pelos gatekeepers e gateways. A compatibilidade dos codecs utilizados é essencial para a interoperabilidade.

Os terminais devem suportar pelo menos o padrão G.711, sendo este o denominador comum.

O H.323 contempla os seguintes elementos de rede:

1) Terminais
2) Gateways
3) Gatekeepers
4) Unidades de controle multiponto

Cada equipamento realiza uma tarefa específica. Alguns podem estar reunidos em um mesmo sistema físico, ou distribuídos através de uma rede IP.

1) Terminais

O terminal suporta comunicações audíveis e pode suportar vídeo-conferência, opcionalmente. Existem implementações em hardware, mas a situação mais comum é a utilização de um PC mais o software Netmeeting.

O sistema deve realizar a codificação/decodificação da voz para o hardware de áudio, conectado por sua vez a transdutores sonoros. Uma câmera de vídeo pode também estar associada ao sistema.

A comunicação é realizada utilizando o H.245 e o Q.931 para o controle da chamada.

2) Gateways

Provêem a interconexão das redes IP com a rede PSTN, permitindo o intercâmbio de sinais entre os dois domínios.

Traduz os diferentes formatos de transmissão, codecs de áudio e procedimentos de comunicação.

Obviamente, o sistema tem interfaces LAN e POTS, podendo manipular sinais T1/E1, ISDN e CCN7.

Pode ser decomposto em três sub-sistemas:

a) Media Gateway : traduz o tráfego IP codificado em G.723 para um canal T1/E1 ou ISDN H.320 para equipamentos de vídeo.

Um requisito básico é a alta disponibilidade deste equipamento, para evitar descontinuidades no serviço prestado. Além disso, contém componentes para o controle de QoS, gerenciando o atraso, cancelação de eco e jitter.

b) Controlador : mantém um banco de dados para traduzir os endereços IP para o plano de numeração correspondente.

c) Sinalização : traduz os sinais CCN7 para a sinalização equivalente H.323.

3) Gatekeepers

Controlam a chamada em si, proporcionando funções que incluem : bilhetagem, roteamento, reserva de banda, tradução de endereço, etc.

4) Unidades de controle multiponto

Um banco de dados é o núcleo deste subsistema, devendo ter características de alta disponibilidade.

É um componente que possibilita a ampliação dos serviços de VoIP, podendo-se citar a conferência/videoconferência. Proporciona a capacidade de interligar três ou mais terminais. É ativado pelo Gatekeeper.

O sistema mescla os dados de áudio e/ou vídeo provenientes das estações, através do protocolo H.245.

Protocolos de sinalização :

É utilizado o H.225, para que ocorra o registro e a admissão no Gatekeeper, além do intercâmbio de informações sobre as propriedades dos terminais. Situa-se entre o Gateway e o Gatekeeper.

3. SIP

O protocolo SIP, proposto pelo IETF, utiliza uma metodologia diferente da adotada pelo H.323. Pode ser descrito como uma série de recomendações, não um complexo conjunto de protocolos interligados.

É bem mais simples do que o H.323, utilizando mensagens codificadas como texto, semelhantes aos padrões do HTTP, aumentando a extensibilidade do protocolo.

O SIP não requer outros protocolos, mas normalmente é utilizado com sistemas que garantem a qualidade do áudio, a exemplo do RSVP (Resource Reservation Protocol), que prioriza os pacotes VoIP.

Para relatar os codecs que serão empregados, o SDP (Session Description Protocol) enumera os parâmetros mais importantes, além de informar a banda passante, o nome da sessão, a mídia (vídeo/áudio) e o sistema de transporte (RTP / Universal Data Protocol).

É composto de dois elementos básicos : o "user agent" e o servidor. O "user agent" inicia a chamada e o servidor decodifica as mensagens-texto. Há três tipos de servidores:

a) Registro : mantém o endereço dos usuários.

b) Proxy : encaminha as requisições para o servidor que controla o "user agent" correspondente.

c) Redirect : retorna o endereço do servidor ao invés de encaminhar as requisições.

Para seqüenciar os pacotes de áudio/vídeo, o RTCP (Real-Time Control Protocol) e o RTTP são empregados, adicionando informações de sincronismo e de feedback da qualidade de serviço.

A conexão é estabilizada com o RTP (Real-Time Protocol), para transportar informações sensíveis à passagem do tempo, mesmo com a utilização do UDP. O TCP solicitaria o reenvio dos pacotes mal formados, tornando errático o fluxo da conversação.

4. Outros protocolos

Um protocolo comum ao H.323 e ao SIP é o MGCP (Media Gateway Control Protocol). Controla a sinalização entre os "call agents" e o gateways de telefonia, através de um conjunto de oito comandos.

Os protocolos são baseados no H.254, Q.931 e CCN7.

5. Qualidade de serviço

É um dos tópicos mais importantes da telefonia IP, que incluem áudio e confiabilidade da chamada. A chamada deve ter baixa latência, baixo jitter e mínima perda de pacotes.

Sendo um processo de tempo real, a rede IP deve suportar o fluxo de pacotes entre os dois pontos de comunicação, com uma latência ao redor de 150 ms. A partir de 300 ms, a cadência da conversação torna-se difícil.

Para solucionar esta questão, os pacotes VoIP devem ter uma prioridade maior do que os outros tipos de tráfego. As tecnologias a respeito são :

-Diffserv : informa ao roteador como tratar os pacotes, a partir de um campo IP.

-MPLS (Multi-Protocol Label Switching)

-IPv6 : contém bits de prioridade de fluxo

-RSVP : reserva uma banda de passagem

A seguir, serão listados os principais parâmetros sobre QoS:

1) Atraso (delay)

É um dos parâmetros mais importantes, pois o comunicação por áudio é um processo de tempo real. Se o atraso for considerável, a fala tornar-se-á irreconhecível.

É um fator inerente à tecnologia e é causado por diversos fatores. Um atraso aceitável é de 200 ms.

Há dois tipos de atraso:

a) Propagação : é causado pelas características do meio de transporte, normalmente baseado em fibra óptica ou cabos de cobre.

b) Processamento : tem como origem os dispositivos eletrônicos que codificam a voz propriamente dita, e normalmente o impacto destes é maior. Cada elemento constitui um fator de atraso : DSP (~10/20 ms), roteadores, gateway, etc.

Mesmo os codecs contribuem para este fator : o G.711 e o G.726 atrasam cerca de 5ms, e o G.729, devido à maior compressão, cerca de 10ms.

2) Jitter

Representa a variação da latência, à medida que o tempo passa, causando uma descontinuidade no fluxo de pacotes. Os mesmos não são transmitidos de uma maneira determinística.

Com um jitter muito elevado, a conversação pode conter saltos de modulação. Uma solução é um buffer de armazenamento temporário de pacotes, de modo a não aumentar a latência demasiadamente.

3) Cancelamento de eco

É possível que exista um eco, a escuta da própria voz no terminal, devido a uma circulação ocasional dos sons que transitam entre o alto-falante e o microfone do equipamento VoIP.

Se a diferença entre o som emitido e o percebido exceder 25ms, é possível perceber tal situação. É necessário eliminar este fenôneno, não apenas por causa do tráfego extra que é produzido, mas também devido ao desconforto que é gerado.

Existe um algoritmo que elimina este problema, o G.168, operante a partir dos codecs dos DSP's.

4) Perda de pacotes

Em caso de um congestionamento temporário da rede, pacotes podem ser descartados e a conseqüente queda da qualidade da voz pode ser percebida.

5) Fluxo de dados

Os canais que constituem a ligação exigem uma banda de passagem pré-definida. Se a rede não puder suportar tal requisito, em casos extremos, a ligação pode ser derrubada.

6) Disponibilidade da rede

Uma rede IP contemplando o serviço de voz deve ser operacional, sempre que possível, atingindo as expectativas que são proporcionadas pela rede comutada normal.

7) Qualidade da sinalização

No estabelecimento de uma chamada, é importante que os sinais de controle fechem os circuitos virtuais de voz no menor tempo possível, evitando esperas demasiadas por parte dos usuários.

6. Desvantagens

A menos que um software de encriptação seja utilizado, torna-se possível captar o tráfego de voz.

Além disso:

-A dependência em relação à Internet para a realização de comunicações com o mundo exterior aumenta.

-A qualidade de voz pode variar bastante, de acordo com a utilização geral da rede.

-Os equipamentos de rede podem requerer atualizações.

-A compressão dos sinais pode resultar em distorções.

7. Vantagens

A principal vantagem de utilizar o VoIP é a possibilidade de realizar chamadas de longa distância a um custo muito baixo.

É possível também citar a transmissão opcional (e simultânea) de imagens, além da integração de caixas de correio eletrônicas.

O link com a Internet é melhor aproveitado e também simplifica o gerenciamento das comunicações.

8. Conclusão

Apesar dos problemas relatados, é possível afirmar que a tecnologia VoIP pode representar o futuro das comunicações bidirecionais e audíveis, devido à crescente interoperabilidade dos sistemas e padronização dos equipamentos de rede, projetados para alcançar um QoS aceitável.

5. 3G

1. Introdução

O vertiginoso desenvolvimento tecnológico se aplicou também aos sistemas "wireless", onde os protótipos primordiais eram transportados em veículos automotores, até os terminais atuais, que possibilitam também o acesso a redes de pacotes.

A tecnologia 3G representa uma convergência de vários sistemas wireless 2G em um único sistema que envisa tanto a parte terrestre quanto o acesso via satélite.

Os sistemas 3G são baseados em comutação de pacotes, com várias extensões para o suporte de múltiplos serviços de voz, dados e imagem, enfatizando a qualidade de serviço para o suporte de altas taxas de transmissão.

O maior benefício será a obtenção de maiores capacidades e taxas de transmissão do que as atuais (2.5G). Será possível a construção de serviços que restringirão as fronteiras existentes entre a computação móvel e as estações de trabalho, possibilitando a interoperabilidade de ambos os domínios.

2. Tecnologia

Atualmente, existem três interfaces aéreas : wideband CDMA, UWC-136 (Universal Wireless Communication) e CDMA2000, podendo alcançar de 144 Kbps até 2 Mbps.

O ITU (International Telecommunication Union) denomina o sistema como IMT-2000 (International Mobile Telecommunication), que engloba os padrões já mencionados, além de assegurar a compatibilidade com os padrões legados que existem (por exemplo, AMPS).

O ETSI (European Telecommunications Standards Institute) nomeia tal tecnologia como sendo UMTS.

Há um esforço internacional para criar um padrão único, denominado 3GPP (Third Generation Partnership Project). Nessa situação, a interface escolhida é o wideband CDMA (WCDMA).

Os princípios do sistema incluem controle de potência, handoff, receptores, processamento de chamadas e serviço de dados.

3. Sistemas 2G

Poucas gerações tecnológicas transversaram a comunicação móvel, partindo de sistemas baseados em comutação de circuitos (2G - GSM, IS-136, DAMPS, IS-95) até a comutação de pacotes em baixa velocidade (2.5G).

Basicamente, pode-se descrever um sistema de comunicação móvel como sendo composto por dois blocos principais:

-Uma rede de acesso por rádio, que verifica a interface aérea.

-Um núcleo que realiza as funções de comutação e interfaces externas, a exemplo da Internet e da rede PSTN.

Com as tecnologias 2G, é impossível não existir a exaustão das freqüências de rádio, devido à alta demanda de dados, principalmente das aplicações que envolvem vídeo.

Para lidar com o alto volume de transferências de dados, é necessário implementar novos protocolos para a evolução das comunicações móveis, podendo-se citar o protocolo IP, QoS e as novas tecnologias de rádio.

4. Sistemas 3G

O 3G é baseado em pacotes, podendo ser usado para transmitir texto, digitalização de voz e imagem, a uma velocidade de até 2 Mbps em um terminal sem fio.

Utilizando os protocolos adotados pela Internet, isso significa que o sistema estará sempre conectado à rede IP.

A migração não é só baseada nas melhorias da rede e das interfaces de rádio, mas sim na evolução de várias tecnologias (EDGE, GPRS, IS-136, etc).

A médio prazo, o XML proverá um padrão para acessar o conteúdo da Internet.

Uma rede 3G pode ter até três interfaces aéreas, suportando também o GSM e o IS-41.

5. CDMA

A tecnologia CDMA é baseada em um padrão denominado IS-95, que difere dos sistemas anteriores por usar técnicas de espalhamento de espectro para a transmissão de informações por vias aéreas.

Ao invés de dividir o espectro de rádio em canais separados por freqüência ou tempo, o CDMA separa os usuários através de códigos dentro do mesmo espectro.

As vantagens incluem:
-Alta capacidade para acomodar muitos usuários
-Imunidade à interferências de outros sinais

Em cada fluxo de voz, é atribuída uma seqüência que direciona a resposta apropriada ao usuário correspondente.

O terminal extrai o sinal usando o código apropriado. O áudio resultante conterá somente a conversação, eliminando os ruídos de fundo.

Isso permite a reutilização das freqüências, ocupando o mesmo espaço no canal de comunicação e aumentando o número de usuários simultâneos.

Os problemas são:
-Qualidade da recepção
-Alteração da voz transmitida

Para resolvê-los, as operadoras usam vocoders de 13 Kbps.

Outra vantagem é a simplificação na expansão do sistema, pois todos os transmissores usam a mesma freqüência.

O padrão CMDA2000 provê a migração dos sistemas 2G atuais, sendo atualmente composto de uma interface aérea e de uma rede central, sendo compatível com o padrão cdmaOne e com o IS-95.

6. WCDMA

O WCDMA (Wideband CDMA) é uma das interfaces aéreas de múltiplo acesso mais apropriadas para os sistemas de terceira geração, tendo um canal com largura de faixa de 5 MHz ou 10 MHz, além de ser compatível com o GSM.

O WCDMA original utilizava uma taxa de 4.096 Mcps (Megachips por segundo), mas atualmente uma taxa de 3.84 Mcps é implementada, para o suporte simultâneo do CDMA2000.

O WCDMA também utilizará um controle de potência de transmissão e recepção, a uma taxa de 1600 vezes por segundo.

Outro aspecto importante é o que especifica uma operação assíncrona da estação-base, diferentemente do CMDA2000.

A interface aérea focará em redes assíncronas e síncronas. Em uma rede síncrona, a atualização ocorrerá a cada poucos microssegundos.

Em redes assíncronas, as estações-base não estarão em sintonia, eliminando o uso do GPS (Global Positioning System) e facilitando a expansão das instalações do WCDMA.

A camada física proverá dois tipos de pacotes, para canais randômicos ou dedicados.

O acesso randômico é utilizado em comunicações com freqüência ocasional, podendo carregar informações de controle e/ou dados a partir do terminal para a estação-base. O canal não é mantido entre as comunicações, resultando em um overhead menor.

Um canal dedicado é para as comunicações mais freqüentes, tanto para o upload ou o download de informações.

O espectro do WCDMA também incorpora informações de vídeo que são enviadas em pacotes.

7. Estrutura

As redes 3G têm uma estrutura em camadas, sendo que a primeira é a camada de conectividade, provendo suporte para voz e dados. Consiste em equipamentos de rede: roteadores, switches ATM e sistemas de transmissão.

A seguir, está a camada de controle, composta por servidores de HLR, etc.

A próxima camada refere-se a aplicações, permitindo o desenvolvimento de serviços (m-commerce, GPS, etc.)

Há muitos grupos desenvolvendo padrões para a estrutura 3G, e o grupo principal denomina-se 3GPP (Third Generation Partnership Project).

8. Infraestrutura

A partir da perspectiva do usuário, o 3G é somente uma tecnologia de RF.

Entretanto, a operadora tem de instalar uma considerável infraestrutura de rede cabeada (terrestre) para tanto.

O RAN (Radio Access Network) é uma denominação coletiva dos componentes de infraestrutura interligados por cabos, suportando acessos sem fio, independentemente da tecnologia do núcleo da rede.

É responsável pelo gerenciamento das sessões, conectividade com o PSTN (Public Switched Telephone Network) e com a Internet.

Os elementos básicos que compõem o RAN são :

1) Equipamento do usuário

Também chamado de estação móvel, inclui o celular 3G, o PDA (Personal Digital Assistants) e modems conectados a PCs.

2) Nó B

Também chamado de BSC (Base Station Controller), provê a interface entre o handset e o RNC (Radio Network Controller) e está envolvido nas decisões de handover, a partir do sinal RF da estação móvel.

3) RNC (Radio Network Controller)

Coordena as estações-base e controla as atividades de handover das chamadas entre as estações.

4) Core Network Interface

Também chamado de MSC (Mobile Switching Center), denota a infraestrutura de rede ligada ao RAN (Radio Access Network). Exemplo : Internet, PSTN.

9. ATM

O grupo 3GPP define uma série de protocolos entre o RAN WCDMA:

Os serviços 3G operam a partir de infraestrutura ATM, projetada para interoperar com redes públicas orientadas à conexão ou por pacotes. Exemplos : multiplexação de voz e dados, QoS, estabelecimento da conexão através das camadas de adaptação AAL-2 e AAL-5, além dos protocolos de sinalização UNI e NNI.

A interconexão dos elementos de rede da RAN e o núcleo da rede é desenvolvida através das interfaces Iub, Iur and Iu da camada 2 do ATM:

a) A interface Iu divide-se em duas partes: orientado a circuito e a pacote. A interface Iu é baseada no tráfego de voz em circuitos virtuais usando AAL2 e IP sobre ATM usando a tecnologia AAL5. É a comunicação entre o RNC e a rede central.

b) A interface Iub é a conexão entre o Nó B e a RNC.

c) O Iur é a interface de comunicação entre RNCs adjacentes.

Os protocolos específicos incluem o procedimento de conexão entre a parte de RF e os sistemas terrestres da rede, além de suportar recursos específicos (handover). É uma complexa operação que demanda coordernação entre o sinal de RF recebido e as multi-conexões da infraestrutura de rede.

10. Arquitetura detalhada

Em uma rede 3G, é possível detalhar a arquitetura em várias partes:

1) GMM (Global Mobility Management)

O protocolo define funções de conexões, segurança e roteamento.

2) NBAP (Node B Application Part)

Provê procedimentos para broadcast, supervisionamento de recursos lógicos ou dedicados e distribuição de informações de paging.

3) PDCP (Packet Data Convergence Protocol)

Mapeia características de alto nível em características da interface de rádio, além de prover a transparência para protocolos de nível mais alto.

4) RLC (Radio Link Control)

Provê o controle das ligações lógicas da interface de rádio.

5) MAC (Medium Access Control)

Controla os procedimentos de acesso para o canal de rádio.

6) RRC (Radio resource Control)

Supervisiona a alocação e a manutenção de canais de comunicação por rádio.

7) RANAP (Radio Access Network Application Protocol)

Encapsula a sinalização de camadas mais altas. Supervisiona a sinalização entre o RNC e as conexões orientadas a circuito do MSC.

8) RNSAP (Radio Network Service Application Part)

Provê a comunicação entre RNCs.

9) GTP (GPRS Tunnel Protocol)

Provê o tunelamento através da rede IP, adicionando informações de roteamento. Opera acima do TCP/UDP.

10) MAP (Mobile Application Part)

Suporta a sinalização entre o HLR (Home Location Register) e o SGSN (Serving GPRS Support Node).

11) Sinalização AAL2

Protocolos utilizados para transferência de voz sobre uma infraestrutura ATM usando a camada de adaptação 2.

12) Sigtran

Protocolos para transferir sinalização SCN (Switched Circuit Network) em uma rede IP.

11. Desvantagens

As desvantagens incluem:

-Instabilidade da rede

-Cobertura incompleta

-Qualidade sonora

-Maior consumo de energia, devido à grande complexidade dos circuitos eletrônicos.

12. Vantagens

As vantagens são:

-Maior segurança nos serviços disponíveis.

-Conexão permanente à Internet.

-Capacidades de posicionamento global (GPS)

13. Conclusão

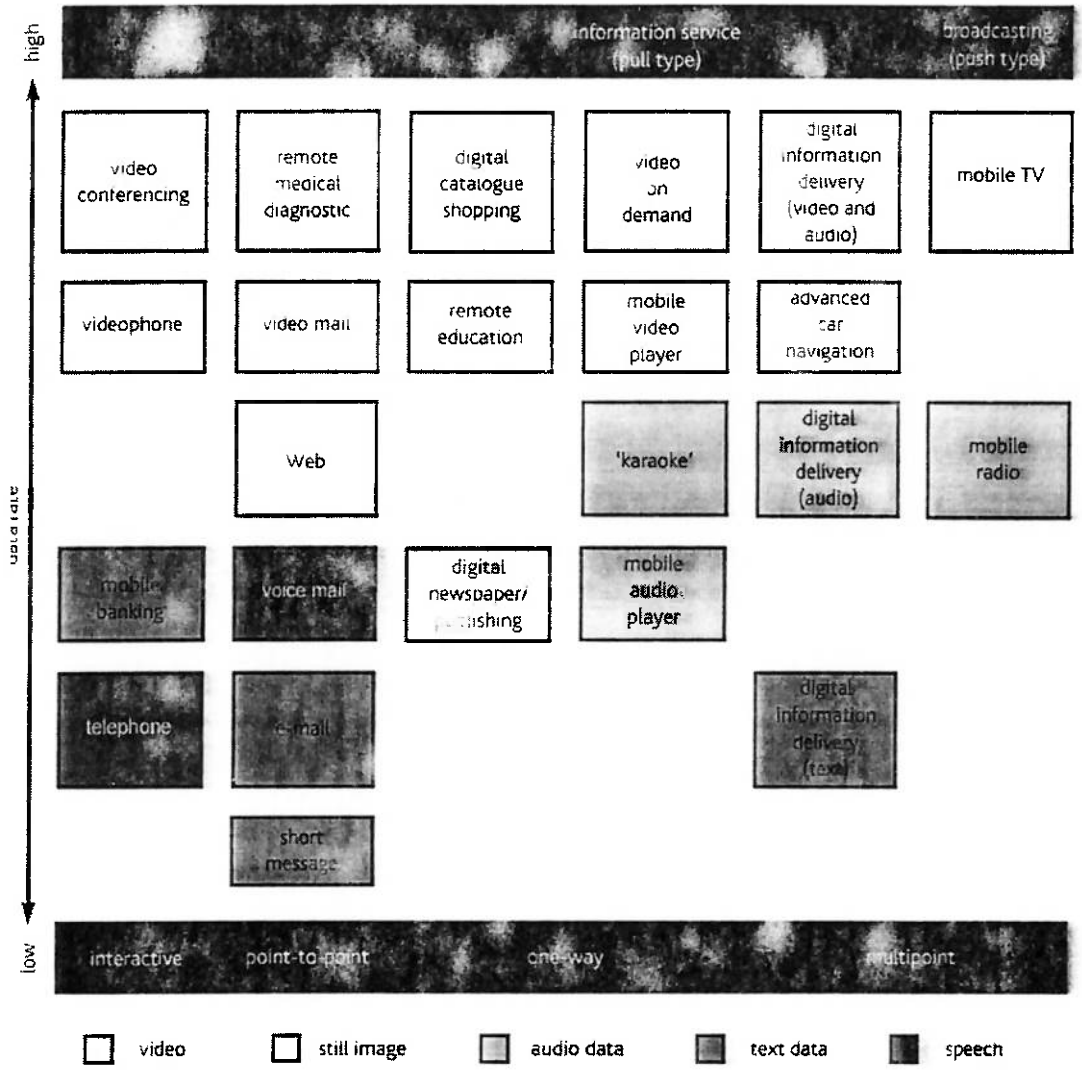

Figura 6 – Aplicações 3G

Atualmente, sistemas 3G estão sendo utilizados em poucos países, devido ao alto custo em ampliar toda a infra-estrutura já existente.

No entanto, é a tecnologia que representará o maior avanço tecnológico nas comunicações móveis, pois converge dois domínios (voz e dados) em uma única entidade.

6. VPN

1. Introdução

A necessidade de segurança na permutação de informações consideradas valiosas resultou no desenvolvimento de sofisticados algoritmos de encriptação em tempo real, possibilitando a criação de redes virtuais.

Uma VPN transmite informações utilizando redes de computadores, mas encriptando os dados para garantir a segurança dos usuários.

Uma analogia é visualizar a VPN como sendo a emulação de um circuito fechado em uma rede particular.

Em outras palavras, é uma tecnologia que permite a criação de uma conexão (ou túnel) virtual segura mesmo utilizando estações interligadas por uma rede pública.

É um ambiente cujo acesso é restrito a um conjunto de estações, tendo como denominador comum um meio de comunicação não-exclusivo.

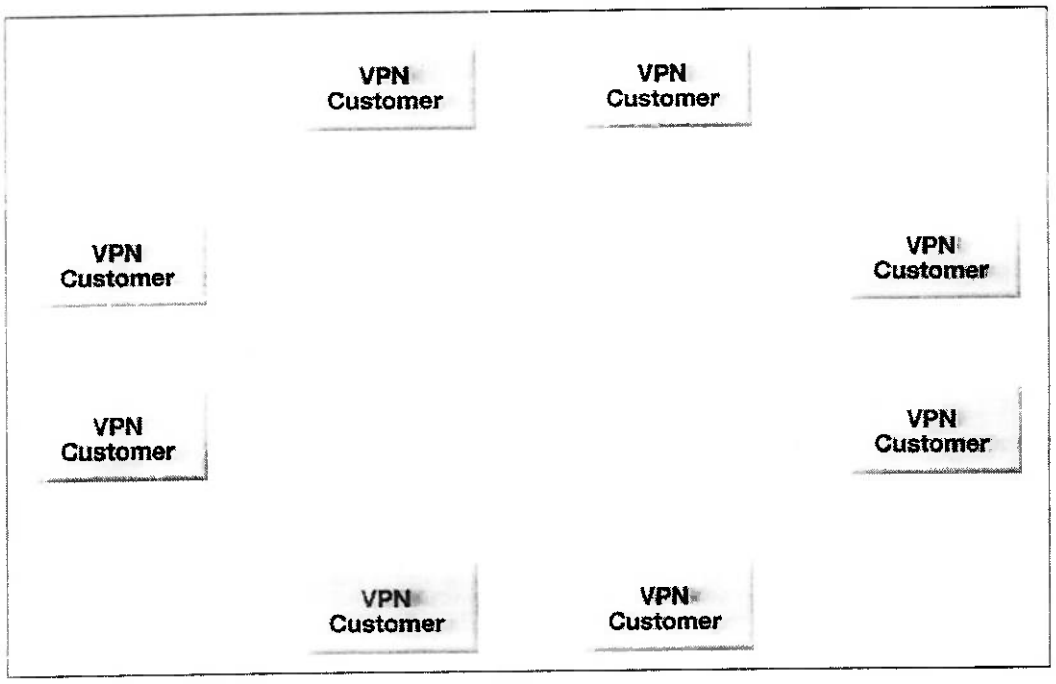

Figura 7 – Uma topologia VPN típica

2. Tecnologia

As VPNs podem existir entre uma máquina individual e uma rede privativa. Os recursos de segurança incluem encriptação, autenticação forte e mecanismos de mascaramento de informações.

Normalmente, engloba três componentes:

1) Controle do acesso : determina quais usuários poderão acessar a VPN. Sem este recurso, os dados estarão protegidos, mas a rede em si provavelmente não.

2) Controle do tráfego : o protocolo aumenta o tráfego, existindo um risco de afetar o desempenho da rede como um todo. Uma solução VPN deve contemplar o compartilhamento adequado da mídia, de acordo com a importância da informação que é transportada pela mesma.

3) Gerenciamento da complexidade : à medida que se expande a infraestrutura, a complexidade da mesma tende a crescer. O crescimento ordenado é um fator de grande importância, na medida em que pode ser controlado de modo similar aos outros dispositivos de segurança da empresa.

Duas funções básicas são desempenhadas:

1) Encriptação : os dados a serem transmitidos são codificados de modo a proteger a confidencialidade dos mesmos. Uma alternativa é a utilização do IPSec (IP Security).

2) Tunelamento : as informações são encapsuladas dentro de pacotes TCP/IP para que seja possível o transporte através da Internet. Há muitos tipos de tunelamento que podem ser utilizados.

3. Estrutura

Elementos básicos de uma rede VPN : servidor VPN, cliente VPN e protocolos de tunelamento.

A seguir, são descritos tais elementos:

Servidor de VPN : é um computador central que aceita conexões VPN a partir dos clientes remotos. Normalmente, contém um acesso à Internet de alta velocidade (E1/T1, Frame Relay, xDSL, etc).

Cliente VPN : inicia uma conexão segura ao servidor. Pode ser um computador comum ou um roteador, para obter uma conexão roteador-a-roteador.

Protocolos de tunelamento : padrões de comunicação para gerenciar os túneis e encapsulamento e encriptação de dados.

Uma solução VPN deve prover, pelo menos, as seguintes funções:

1) Autenticação do usuário : o sistema deve verificar a identidade do usuário e restringir o acesso aos usuários autorizados.

Além disso, deve registrar a hora do acesso e o tipo da informação acessada.

2) Gerenciamento dos endereços : a solução deve designar um endereço para a estação do usuário, sem fornecer os endereços reservados.

3) Encriptação de dados : os dados porventura extraídos a partir da rede pública devem ser ininteligíveis para tais acessos não-autorizados.

4) Controle das chaves : o sistema deve gerar chaves para o cliente e o servidor.

5) Suporte a vários protocolos : a solução deve ser capaz de ler informações a partir dos protocolos de rede mais utilizados. Exemplos: o IP e o IPX (Internet Packet Exchange), embora o último seja de uso mais restrito.

VPNs também suportam vários métodos de autenticação, podendo-se citar o Radius, o SecureID e certificados digitais.

4. Implementações

Para a implementação de uma VPN, existem três categorias principais:

1) Baseada em hardware

Muitos VPNs baseados em hardware são roteadores com funções de encriptação. Estes equipamentos maximizam as capacidades do hardware disponível e normalmente têm a melhor vazão de dados dentre todos os sistemas VPN.

O problema é a baixa flexibilidade destes sistemas, sendo que os mais antigos não permitem a atualização do software residente.

2) Baseada em firewall

Estes equipamentos utilizam os recursos dos mecanismos de segurança inerentes a um firewall, podendo também fazer a tradução de endereços e alarmes em tempo real. As proteções existentes nos sistemas operacionais provêem grande segurança.

A desvantagem é o alto overhead proveniente dos vários softwares específicos que são executados em paralelo.

3) Baseada em aplicações

VPNs baseados em aplicações têm grande flexibilidade no gerenciamento do tráfego associado, podendo criar túneis de acordo com endereços, protocolos, etc.

Entretanto, são mais difíceis de gerenciar, pois exigem proeficiência no sistema operacional utilizado, no pacote de software específico, dentre outros fatores.

As distinções existentes entre as três implementações estão lentamente tornando-se cada vez menos definíveis.

5. Tunelamento

Um túnel é uma combinação de encriptação, autenticação e outros esquemas de segurança, permitindo a operação de uma VPN em uma rede insegura.

Em caso de ocorrer vários acessos remotos, deve existir um túnel para cada conexão.

O tunelamento encapsula os frames originais, adicionando ainda um cabeçalho, que provê informações de roteamento para atravessar o caminho lógico formado pela rede intermediária.

Pode ser descrito como encapsulação, transmissão e extração de pacotes.

Exemplos antigos incluem o SNA (System Network Architecture) sobre IP, encapsulado em um pacote UDP. Acontece um evento similar em redes IPX, a partir de um servidor NetWare.

Tecnologias recentes incluem o PPTP, L2TP e o IPSec.

Tipos de túneis:

1) Túneis voluntários : um cliente pode emitir uma requisição de VPN para criar um túnel voluntário. Neste caso, o computador do usuário age como um terminante do túnel.

2) Túneis compulsórios : um servidor habilitado para VPN cria um túnel compulsório, em caso de acesso por linha discada.

6. Camadas 2/3

Obviamente, para que um túnel seja estabelecido, o servidor e o cliente devem utilizar o mesmo protocolo de tunelamento, que pode estar na camada 2 ou 3, de acordo com o modelo OSI (Open Systems Interconnection).

Os protocolos que operam na camada 2 (enlace) usam frames como a unidade de intercâmbio.

O PPTP, o L2TP e o L2F são protocolos de tunelamento que operam na camada 2, encapsulando as informações em um frame PPP (Point-to-Point Protocol). Uma solução VPN que os utilize atinge os requisitos básicos. Outras soluções, tal como o IPSec, alcança alguns dos requisitos necessários.

Os protocolos que atuam na camada 3 assumem que todos os problemas de configuração foram solucionados e não há a fase de manutenção do túnel. Após a formação do túnel, os dados podem ser transmitidos.

7. PPP/L2SEC

1) PPTP : O PPTP (Point-to-Point Tunneling Protocol) é uma extensão do protocolo PPP (Point-to-Point Protocol) que permite a encapsulação de quadros PPP em datagramas IP.

O sistema utiliza uma conexão TCP para manter o túnel, com dados comprimidos e encriptados.

2) L2TP : O L2TP (Layer 2 Tunneling Protocol)

Na teoria, o L2TP encapsula os frames PPP para as redes IP, X.25, Frame Relay e ATM. Na prática, é utilizado o L2TP sobre IP, utilizando o UDP e uma série de mensagens para manter o túnel.

Os protocolos de tunelamento que operam na camada 2 usam o EAP (Extensible Authentication Protocol) e suportam uma grande variedade de métodos de autenticação, incluindo senhas, criptografadores e cartões inteligentes.

Além disso, têm os seguintes recursos:

1) Desígnio dinâmico de endereço : baseado no mecanismo de negociação NCP (Network Control Protocol).

2) Compressão e encriptação de dados

3) Gerenciamento de chaves

4) Suporte a multi-protocolos

8. IPSec

O IPSec (Internet Protocol Security), definido pelo IEEE, é o mecanismo mais utilizado para garantir a segurança de um tráfego percorrendo uma VPN.

Pode utilizar o DES, 3DES e outros algoritmos para criptografar dados, algoritmos de hash (HMAC, MD5) para autenticar pacotes e certificados digitais para validar chaves públicas.

O protocolo inclui três elementos de segurança principais:

1) Autenticação do cabeçalho

Provê a integridade adicionando informações de autenticação no datagrama IP, assegurando que os dados não estarão disponíveis para uma estação não-autorizada.

2) Segurança no encapsulamento

Pode prover integridade e autenticação, de acordo com o algoritmo utilizado. Parte do cabeçalho e todos os dados do datagrama são encriptados.

3) Alteração da chave

É um protocolo para gerenciar as chaves utilizadas nos itens anteriores. Provê uma solução muito escalável.

9. Chaves

Distribuição de chaves : é um dos principais pontos de verificação a ser verificado, pois isso determina o acesso ao sistema.

A chave é um código usado pelo algoritmo de encriptação para criar uma versão normalmente ininteligível das informações a serem protegidas.

Existem dois tipos de chaves : simétricas e assimétricas.

Quando a mesma chave é usada para decriptar e encriptar as informações, as chaves são simétricas e as extremidades da rede compartilham as mesmas chaves.

É crucial distribuir as chaves simétricas com alta segurança, utilizando pelo menos o SSL/TLS, SFTP ou SCP.

Outra solução é criptografar os dados com uma chave e descodificar com outra, que não podem ser intercambiadas. São as chaves assimétricas, e são compostas de uma chave pública e uma chave privada.

A chave pública pode ser transmitida de um modo não secreto. Entretanto, a chave pública não pode ser inteceptada e modificada, pois isso possibilitaria um ataque que derrotaria a proteção proporcionada pela VPN.

A chave secreta não pode ser transmitida e é utilizada para decifrar as mensagens recebidas. As chaves assimétricas são tipicamente longas – de 1024 a 2048 bits, requerendo uma carga considerável de poder de processamento.

A segurança depende muito do comprimento das chaves. Uma chave com 16 bits provê apenas 65.536 combinações.

10. DES

Um dos melhores métodos de encriptação é o DES (Data Encryption Standard), existindo as variações 3DES (Triple DES) e o Triple-Pass DES.

O DES utiliza uma chave de 56 bits para codificar informações em blocos de 64 bits. Entretanto, devido ao tamanho da chave, é possível percorrer todas as

combinações em pouco tempo, utilizando hardware especialmente projetado para tanto.

Assim, o Triple-Pass DES aumenta a segurança encriptando a informação múltiplas vezes: os dados são codificados usando uma chave de 56 bits. O resultado é decriptado com outra chave de 56 bits. Finalmente, é encriptado novamente usando a primeira chave.

O resultado é uma chave de 112 bits.

O 3DES utiliza o mesmo algoritmo, mas o executa com três chaves diferentes, obtendo-se um código de 168 bits.

11. Assinaturas digitais

A tecnologia de autenticação garante :

1) A identidade dos participantes

2) A integridade da informação recebida

Há muitos tipos de autenticação, sendo que o mais comum é simplesmente o nome de login e a senha.

Um corolário é a necessidade de utilizar nomes e senhas não muito extensas. Mesmo assim, podem existir problemas de segurança neste quesito.

Existe uma tecnologia denominada certificação digital que permite a autenticação sem a necessidade de utilizar logins e senhas.

Um certificado digital é um registro que inclui informações tais como o nome da pessoa, endereço, chave pública e a validade do certificado.

Em uma VPN, o certificado é utilizado de modo análogo a um passaporte, no sentido de identificar o usuário que está tentando conectar-se a uma rede.

Para verificar que a informação recebida é autêntica, é utilizada uma tecnologia chamada assinatura digital, que garante a integridade e a origem do certificado.

A criação segue dois passos:

1) A mensagem transmitida é processada utilizando-se um algoritmo chamado função de hash, que transforma uma seqüência de dados em um número de comprimento fixo.

O número que é criado é chamado de sinopse da mensagem. Alterando-se a mensagem, a sinopse altera-se também.

As funções de hash incluem o SHA (Secure Hash Algorithm) e o MD5 (Message Digest 5).

2) A sinopse é criptografada usando a chave não pública, gerando a assinatura digital.

Para garantir a autenticidade de uma mensagem, deve-se criar uma assinatura digital e incluí-la na resposta.

O cliente testa a autenticidade da seguinte forma:

1) Descriptando a assinatura usando a chave pública.
2) Recalculando a sinopse usando a função de hash.
3) Comparando os dois resultados.

Se forem idênticos, é possível afirmar que a mensagem é autêntica e não foi alterada.

Um CA (Certificate Authority) aceita chaves públicas com uma prova de identificação e gera certificados digitais. Manter um CA é uma tarefa não trivial.

Um PKI (Public Key Infrastructure) é um conjunto de serviços de segurança para gerenciar chaves e certificados digitais e provê coordenação entre múltiplos CAs.

Os certificados digitais provavelmente são a melhor forma de autenticação atual.

12. Conclusão

A combinação de encriptação, assinaturas digitais, chaves, tunelamento e autenticação possibilita a criação de conexões seguras, mesmo utilizando a Internet.

Os sistemas de hardware e software que implementam uma VPN utilizam uma variação destes padrões de segurança.

A profusão de serviços digitais delinham a tendência a ser seguida no futuro, sendo que a autenticação emerge como um dos elementos principais de um sistema que utilize a Internet.

7. CONTINGÊNCIA

1. Introdução

A crescente dependência da sociedade moderna por sistemas de informação resultou na necessidade de máquinas resilientes, onde a disponibilidade ininterrupta passa a ser uma característica primária.

No passado, apenas o acesso aos mainframes era considerado um aplicativo de missão crítica.

Atualmente, arquiteturas cliente/servidor e sistemas de múltiplas camadas tornaram-se cruciais para a operação eficiente da maioria dos processos automatizados.

A disponibilidade dos servidores das redes em questão tornou-se um requisito obrigatório.

E a demanda por redes HA (High Availability) tornou-se ainda maior, com a convergência de redes de voz e dados em uma estrutura IP comum, além dos novos aplicativos com alta demanda de QoS, armazenamento remoto de dados, redes multisserviço e vídeo em demanda.

Assim, a tendência é que os sistemas de rede tenham como um critério básico a possibilidade de evolução para alta disponibilidade.

2. Redes de alta disponiblidade

A existência de camadas passou a ser um imperativo nos domínios da informática e das telecomunicações, em equipamentos e/ou software.

Isso facilita a detecção e correção de problemas, solucionando-os com substituições e/ou reparos dos elementos que compõem as camadas.

Além disso, essa metodologia possibilita um projeto modular, existindo também implementações proprietárias.

Para a construção de redes tolerantes a falhas, três camadas são necessárias:

1) Camada de acesso : onde as estações se conectam à rede em questão.

2) Camada de distribuição : um ponto de concentração das camadas de acesso

3) Núcleo : conecta todas as camadas de distribuição, contendo vários roteadores capazes de suportar o tráfego da rede.

3. Camada de acesso

Normalmente, os dispositivos que implementam esta camada são concentradores (hubs), unidades de acesso ou armários especiais que ficam situados em cada andar de um edifício.

Os cabos que são conectados nos equipamentos dos usuários geralmente terminam em um dos elementos anteriormente citados.

Para que ocorra a separação de broadcasts, normalmente redes virtuais podem ser programadas nesta camada.

Utilizando tal metodologia, em caso de falha, os usuários que fazem uso desta camada serão afetados, mas o restante poderá continuar a utilizar a rede.

Dependendo dos requisitos do projeto, a utilização de UPS (uninterruptible power supply) pode vir a ser uma necessidade.

A maioria do trabalho de administração de rede é realizada nesta camada, pois os dispositivos de rede estão na camada de acesso, podendo também conter switches e roteadores.

A quantidade de equipamentos a utilizar será determinada pelo tráfego da rede, além do número de usuários.

4. Camada de distribuição

A função da camada de distribuição é permitir que a camada de acesso tenha comunicação com o núcleo.

O projeto é desenvolvido de um modo que os dispositivos da camada de acesso tenham intercâmbio de pacotes entre si, além de permitir a transferência de informação para o núcleo.

Os seguintes aparatos podem ser encontrados:

-Firewalls
-Roteamento entre redes
-Listas de acesso
-Filtragem de pacotes
-Políticas de segurança, etc.

Sendo que as camadas de acesso serão interligadas pela camada de Distribuição, é importante assegurar que os dispositivos que a constituem sejam capazes de suportar altos volumes de tráfego.

Muitas funções desta camada exigem o uso de roteadores. assim é relevante afirmar que tais equipamentos devem ter a capacidade de desempenhar muitas funções previstas na camada 3 do modelo OSI.

Pode-se citar : translação de segurança, concentração de pontos de acesso, etc.

5. Redundância

Para aumentar a confiabilidade da rede, a redundância é um importante recurso existente na camada de distribuição, pois falhas neste subsistema devem ser evitadas.

Normalmente, os dispositivos da camada de distribuição são duplicados, com uma interconexão de rede entre os mesmos. Além disso, contém fontes de energia redundantes e utilizam no mínimo dois links para a camada de acesso.

Softwares de gerência são usados para monitorar tal rede, denominada de alta disponibilidade (HA).

Para suportar o tráfego da rede e os protocolos de segurança, a velocidade dos processadores dos roteadores e a quantidade de memória RAM não podem ser subdimensionadas.

6. Núcleo

Um núcleo conecta duas ou mais redes de distribuição, sendo que a ênfase deve ser a velocidade do sistema, evitando congestionamentos nos pontos de comunicação entre as redes.

Assim, não é possível implementar políticas de segurança, filtros e firewalls, pois isso diminuiria a eficiência global. Essa tarefa é delegada à camada de Distribuição.

Não existe um projeto já definido nesta camada, isso dependerá mais dos requisitos iniciais.

Existem argumentos para que somente a camada 2 OSI seja utilizada, para a obtenção de maiores velocidades.

Alguns sistemas também usam a camada 3, devido aos protocolos de roteamento, convergência rápida e capacidades de redundância.

7. Redes HA

O projeto de uma rede HA requer uma combinação de tecnologias de rede e procedimentos operacionais complementares, tendo-se em vista as seguintes considerações:

1) Objetivos

Uma rede HA deve conter parâmetros mensuráveis, tendo como um dos indicadores principais o MTBF da rede.

2) Diagnóstico e procedimentos em caso de falha

É importante no sentido de evitar a recorrência dos problemas já surgidos no passado. Pode incluir a existência de instrumentos de precisão com capacidade de correlacionar eventos.

3) Confiabilidade dos equipamentos

A qualidade do hardware a utilizar deve estar associada à camada de operação do dispositivo, além do impacto resultante em caso de um problema no equipamento.

Um sistema em produção no núcleo deve ser redundante e/ou tolerante a falhas.

4) Práticas operacionais

Os problemas que não dependem do hardware da rede podem ser reduzidos mediante a adoção dos procedimentos operacionais mais utilizados.

8. Dispositivos tolerantes a falha

Um caminho para a construção de redes de alta disponibilidade é a utilização de equipamentos com tolerância a falha.

Isto é obtido com o uso de sistemas backup para os componentes-chave, por exemplo: fontes redundantes, processadores extras, duplicação de mainboards, etc.

Além disso, tais sistemas devem suportar ao menos duas conexões com a rede.

É possível obter um MTBF (Mean Time Between Failure) de milhares de horas, teoricamente, atingindo a disponibilidade de 99.999%.

Entretanto, existem algumas desvantagens em um projeto orientado a tais equipamentos:

1) Os recursos para a aquisição desses dispositivos normalmente têm de ser multiplicados por dois.

2) O princípio de funcionamento é o "hot stand-by", significando que uma parte do equipamento não contribuirá para o aumento de performance do sistema como um todo.

3) O foco em apenas alguns dispositivos pode acarretar em uma negligência em outros fatores também importantes. Exemplos : problemas de software, controle do ambiente de operação, que podem diminuir a confiabilidade da rede.

Entretanto, é um enfoque válido se o sistema não tiver simples pontos de falha e for completamente redundante, podendo-se observar então altos níveis de disponibilidade da rede.

9. Fatores importantes

Os principais fatores que influem no MTBF de uma rede são:

1) Adoção de uma série de práticas para gerenciamento das falhas
2) Controle de configuração de equipamentos de rede
3) Privilégios de acesso e segurança
4) Controle de versão de software
5) Qualidade do cabeamento
6) Manutenção da rede

Considera-se que a verificação apurada desses requisitos pode fazer com que a duplicação total da rede não seja tão benéfica para a qualidade geral do sistema.

10. Balanceamento de carga

Redes baseadas em OSPF ou EIGRP podem proporcionar balanceamento de carga entre vários links.

Em caso de falha em um circuito, são capazes de reestabelecer a comunicação entre tais redes em poucos segundos (10s ou menos).

Com um ajuste nos relógios de controle, torna-se possível obter altos índices de disponibilidade da rede.

11. Topologias redundantes

Uma outra tecnologia para construir redes HA é justamente obter a maior parte da confiabilidade com uma topologia redundante, ao invés de enfatizar somente a confiabilidade dos equipamentos de rede em questão.

Por exemplo, em um sistema de missão crítica, é possível duplicar as conexões de rede existentes entre o computador central (servidor) e os clientes que acessam tal equipamento.

Existem algumas vantagens nesta tecnologia:

1) Os elementos que provêm a redundância não precisam estar localizados nos equipamentos de rede, diminuindo a ocorrência global de problemas.

2) Os problemas de software podem ser corrigidos na rede primária, enquanto a rede secundária continua a interligar os sistemas que compõem o ambiente em questão.

Isso reduz os problemas que não envolvem o hardware da rede.

3) Com a redundância da rede, cada dispositivo não precisa ser especialmente configurado, com a exceção dos equipamentos que operam no núcleo, que precisam conter sistemas de tolerância a falha.

4) A distribuição do tráfego pode ser melhor balanceada com redes redundantes, aumentando o desempenho da rede duplicada.

5) As redes redundantes podem ser configuradas para isolar automaticamente a parte que apresentar problemas, e o tempo de interrupção do serviço se resume à demora da comutação propriamente dita, que pode durar apenas alguns segundos.

12. Outras tecnologias

1) Fast Spanning Tree

Esse protocolo foi desenvolvido para superar as limitações lógicas das três camadas já descritas e permitir uma rápida convergência, reduzindo o tempo de comutação das redes redundantes.

Se uma das conexões entre as duas camadas superiores deixar de operar, o protocolo tentará encontrar um caminho alternativo.

2) PVST

O Per-VLAN Spanning Tree permite que o tráfego existente entre a camada de distribuição de acesso seja dividido entre as conexões redundantes.

3) ISL

O protocolo Interswitch link também opera em linhas de comunicação redundantes.

Em caso de queda de um link, o protocolo procurará o link mais adequado para substituí-lo.

4) VIP

A função do "Virtual IP Address / Interface Redundancy" é obter endereços IP que possam ser usados em duas ou mais conexões físicas.

Os endereços MAC e IP são compartilhados, e não podem ser alterados em caso do link reserva ser ativado.

13. Conclusão

Para sistemas de HA, provavelmente a melhor solução é uma combinação de topologias que combinem a redundância de equipamentos com a duplicação do cabeamento das redes.

Com a correta sincronização dos relógios e protocolos existentes nesses sistemas, é possível conseguir tempos de indisponibilidade da ordem de dezenas de segundos.

A convergência tecnológica provavelmente fará com que as redes HA sejam absolutamente necessárias, resultando na diminuição das interrupções observadas, até que estejam em par com os padrões alcançados pelos serviços de voz atuais.

8. GIGABIT ETHERNET

1. Introdução

A revolução tecnológica estendeu-se também ao campo das redes de computadores, onde a capacidade inicial do padrão mais disseminado (Ethernet) evoluiu de 10Mbps para mais de 10Gbps, resultando no padrão de fato na citada área.

A maior vantagem deste padrão é a possibilidade de utilizar aplicativos que demandam alta vazão de dados, acompanhando a evolução dos processadores e mantendo a infraestrutura já instalada.

2. Histórico

A Ethernet (IEEE 802.3) é o padrão de fato em uma rede CSMA/CD, cujas especificações foram publicadas em 1985. É baseada em uma tecnologia antiga, denominada ALOHA. A velocidade era de 2.9 Mbps, conectando cem máquinas em um cabo de 1 Km de extensão. O protótipo teve sucesso, sendo expandido rapidamente para 10 Mbps.

Basicamente, CSMA/CD designa uma tecnologia de compartilhamento de mídia, disciplinando o uso da mesma.

Antes de encaminhar um pacote, a estação deve perscultar a mídia. Se não há informações transitando na mídia, é possível transmitir os dados do pacote.

Se dois computadores emitirem informações ao mesmo tempo, uma colisão ocorrerá. Um lapso de tempo deve ser respeitado, antes de reenviar os mesmos pacotes.

Em 1995, o padrão Fast Ethernet foi anunciado, tendo uma velocidade de 100 Mbps. Recursos adicionais eram : a possibilidade de transmissão full-duplex e auto-negociação.

Operando nessa velocidade, as colisões tendem a ocorrer mais freqüentemente.

Por essa razão, as redes 100 Base-T usam hubs para separar as redes em domínios elétricos diferentes, além de switches para criar um caminho único entre as estações.

Obviamente, o próximo passo da evolução é o Gigabit Ethernet, denominado IEEE 802.3z.

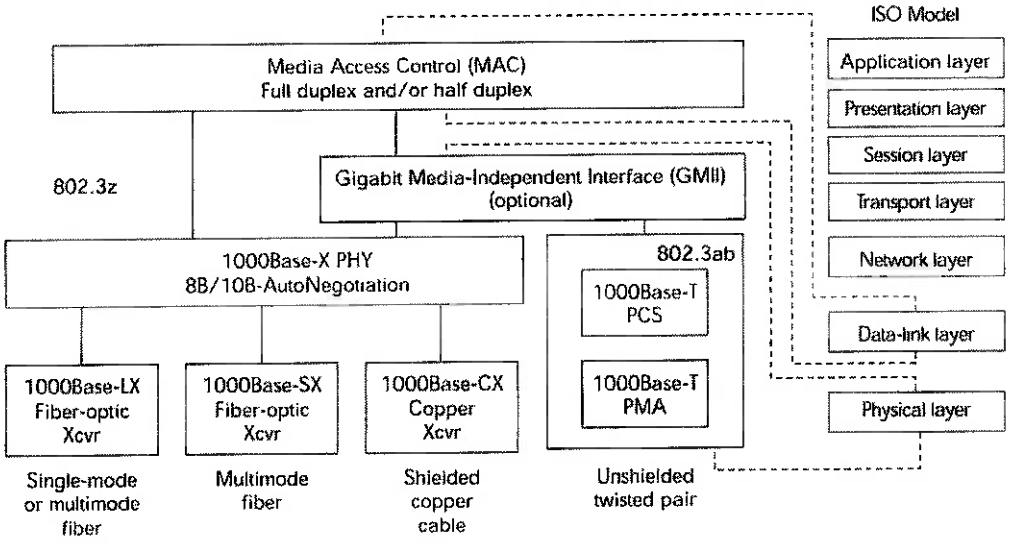

Figura 8 – Representação gráfica da tecnologia Gigabit Ethernet

3. Cabeamento

Há o suporte tanto para half-duplex (CSMA/CD) como para full duplex, além de controle de fluxo e gerenciamento de objetos. É possível operar em par trançado (UTP/150 ohms) categoria 5, fibra óptica multi-modo (MMF) e também em modo simples (SMF):

A padronização 1000 Base-CX (coax) define os requisitos para Gigabit Ethernet em um cabo especial, balanceado e blindado, até uma distância de 25 m. É utilizado principalmente para interligar equipamentos de rede (hubs, servidores e switches) que estão normalmente localizados em uma sala.

A utilização universal dos cabos categoria 5 resultou em um novo padrão, 1000 Base-T, publicado em 1999. O comprimento do mesmo pode atingir até 100 m e um cabo categoria 5 deve conter 4 pares trançados sem blindagem. O padrão 1000 Base-T requer todos os oito fios e deve seguir os requisitos descritos no padrão TIA (Telecommunications Industry Association) 568-A.

Recentes melhorias incluem a utilização de fibra óptica na camada física. O padrão 1000 Base-SX (short wavelength) utiliza um par dual para conectar os equipamentos. O cabo pode atingir até 275m, usando uma fibra multimodo de 62 micrômetros.

No caso da fibra ser de 50 micrômetros, a distância pode alcançar até 550m.

Outro padrão é o 1000 Base-LX (long wavelength), que pode atingir até 5 quilômetros, utilizando um par de fibras de 10 micrômetros.

4. Tecnologia

Gigabit Ethernet estende os padrões IEEE 802.3, que determina as velocidades de 10 e 100 Mbps, sendo que tais especificações foram publicadas em 1998. Teoricamente, pode alcançar 1000 Mbps (1 Gbps).

Em modo half-duplex, Gigabit Ethernet utiliza o sistema CSMA/CD para resolver o acesso à mídia compartilhada.

Em modo full-duplex, todas as conexões são ponto-a-ponto, e múltiplas sessões podem existir na rede sem colisões.

O tamanho mínimo do quadro é de 64 bytes, para diminuir a possibilidade de colisões.

É melhor utilizado em tráfego de rajadas ("bursty"), onde a latência torna-se mais crítica do que a largura de banda propriamente dita.

É um protocolo não orientado à conexão, e cada frame Ethernet deve carregar o endereço de destino que será encaminhado via rede.

5. Mídia

A camada MAC (Media Access Control) define o formato do quadro Ethernet, e o mecanismo para acessar o meio físico.

O LLC (Logical Link Control) situa-se no topo da camada MAC, servindo como uma interface para a camada de rede.

GMII (Gigabit Media Independent Interface)

O GMII é a interface entre a camada MAC e a camada física.

É uma extensão do MII (Media Independent Interface) utilizado no Fast Ethernet, inclusive usando a mesma interface de gerenciamento.

Suporta taxas de transmissão de 10, 100 e 1000 Mbps. Provê caminhos de dados de oito bits, suportando tanto o modo full-duplex como o half-duplex.

O GMII provê dois sinais de estado:

a) indicação da presença do sinal de transporte
b) não-ocorrência de colisões

A camada RS mapeia estes sinais para as primitivas PLS (Physical Signalling), entendidas pela camada MAC.

Com o GMII, é possível conectar vários tipos de mídia, podendo-se citar o par trançado blindado ou não, fibras ópticas de modo simples e múltiplo, com o mesmo controlador MAC.

O GMII é subdividido em três camadas: PMD, PCS e PMA.

1) PCS (Physical Coding Sublayer)

É a camada que provê uma interface entre a camada RS e a mídia física.

Utiliza a codificação 8B/10B, onde conjuntos de 8 bits são representados por grupos de código de 10 bits.

Alguns grupos representam caracteres de 8 bits, outros são símbolos de controle.

Esta camada indica a detecção de colisões e o sensoreamento da transportadora, com a gerência do processo de auto-negociação da NIC (Network Interface) e a determinação da velocidade da rede (10, 100 ou 1000 Mbps), além do modo de operação (half-duplex ou full-duplex).

2) PMD (Physical Medium Dependent)

Esta camada mapeia o sistema físico para o PCS, definindo o padrão de sinalização usado para as várias mídias. O MDI (Medium Dependent Interface) é a real interface física.

Esta camada define a conexão física, a exemplo dos conectores para os diferentes tipos de mídia.

3) PMA (Physical Medium Attachment)

Esta camada provê o suporte não dependente da mídia, serializando os grupos de código para transmissão e também extraindo os bits recebidos em forma de código de grupos.

O serializador é responsável também pelo suporte de múltiplos esquemas de codificação para as camadas superiores.

6. Hardware

O GBIC (Gigabit interface converter) permite a configuração de cada porta gigabit, para interfaces de fios de cobre (CX) ou não (LX, SX e LH).

Os GBICs LH estendem a distância das fibras de modo simples para 10 Km. Normalmente, seria de 5 Km.

A especificação do PMD (Physical Medium Dependent) permite 1.062 Gigabaud em full-duplex. Gigabit Ethernet aumentará esta velocidade para 1.25 Gbps.

O conector normalmente utilizado é o SC, com suporte para fibras multimodo e modo simples.

7. Mídia

Os lasers que utilizam fibra óptica têm a vantagem da variação da atenuação em uma cabo. Em diferentes comprimentos de onda, a atenuação pode alterar-se significativamente.

Por essa razão, o cabo é iluminado com muitas freqüências distintas. Os lasers com um longo comprimento de onda podem percorrer distâncias maiores.

A tecnologia que pode atravessar grandes distâncias utiliza fibra de modo simples, com um núcleo de 9 mícrons e um laser de 1300 nanômetros, apresentando um baixo ruído.

O conector utilizado no 1000 BaseCX é o DB-9, sendo prevista uma melhoria para o HSSDC. A perda é limitada em 20 dB para minimizar distorções nas transmissões.

Para minimizar interferências devido a diferenças de voltagem, os transmissores e os receptores devem utilizar um fio terra compartilhado.

8. 1000 Base-T

O padrão 1000 Base-T foi projetado para transmissão em cabos de categoria 5, similar ao Fast Ethernet.

Isso foi possível devido aos métodos de sinalização e codificação/decodificação que mantém a integridade do sinal transmitido.

A padrão 1000 Base-T transmite a 125 Mbaud, a mesma velocidade do padrão 100 Base-T.

Bauds por segundo são freqüentemente associados com bits por segundo. Entretanto, o baud rate significa o número de transições de um sinal por segundo em uma onda senoidal.

Bits por segundo medem exatamente a quantidade de informação que está sendo transferida em uma linha.

A método de codificação PAM 5 permite mais do que dobrar a quantidade de informação que é transmitida pelo padrão 100 BaseT, permitindo a transferência de

250 Mbps em cada par de fios. Utilizando os 4 pares, é possível transmitir 1000 Mbps.

O padrão 100 BaseT usa a codificação 4B/5B. Devido a esse motivo, o transporte de 125 Mbps faz com que a taxa real seja equivalente a 100 Mbps, onde quatro bits de dados são convertidos em símbolos de 5 bits. A banda restante é usada para a detecção de erros.

O PAM 5 usa quatro níveis de voltagem para gerar 2 bits por ciclo. O transmissor pode emitir quatro combinações de 2 bits e o receptor decifra o nível de voltagem na combinação correspondente.

É possível comprovar que um sinal de 4 voltagens transmitido a 125 Mbaud produz uma taxa de 250 Mbps.

O quinto nível existente no esquema de codificação PAM 5 permite símbolos redundantes, para correção de erros.

Para maior resistência aos ruídos externos, a decodificação Viterbi e a codificação Trellis são utilizados, proporcionando a existência de sinais com baixa correlação no fluxo de dados. Para corrigir problemas de atenuação, equalizadores adaptivos são também usados.

9. Codificação 8B/10B

A camada FC-1 (Fiber Channel) define o protocolo de transmissão, incluindo a codificação e decodificação serial, controle de erros e caracteres especiais.

É similar à codificação 4B/5B, que não foi adotado no Gigabit Ethernet (laser) por falta de um balanceamento DC, que pode resultar em um aquecimento dos lasers devido à dependência da informação transmitida.

A codificação dos dados provê algumas vantagens:

-Limita as características de transmissão (exemplo: excesso de transmissão de um único padrão de bits).

-Possibilidade de detectar e corrigir erros de transmissão e/ou recepção.

-Distinção entre bits de controle e de dados.

A camada FC-1 recebe dados a partir da interface física e os codifica de 8 para 10 bits, adicionando variáveis de controle para integrar os dados com a informação de relógio requerida pelas técnicas de transmissão serial.

10. Melhorias

-Distribuidor

Para manter a compatibilidade com os padrões anteriores, a operação em half-duplex é ainda suportada.

Um novo dispositivo foi considerado, para prover as funcionalidades de um hub em modo full-duplex:

Um distribuidor contendo várias portas, com repetidores capazes de realizar transmissões em full-duplex.

Cada porta contém uma fila de entrada e de saída. Um quadro que incida em uma porta é repetido para as demais, exceto para a porta de entrada. O distribuidor realiza o arbítrio CSMA/CD, antes de encaminhar os dados para as respectivas saídas.

Assim, as colisões não podem mais ocorrer nos links, diminuindo os requisitos quanto à distância das estações. Nesse sentido, as propriedades dos meios físicos ganham mais relevância.

11. TSB-95

Devido ao fato do padrão 1000 Base T utilizar todos os quatro pares de fios do cabo categoria 5, com transmissões bi-direcionais, sistemas adicionais para a prevenção de distúrbios devem ser considerados.

Novos padrões de testes foram adicionados:

Os novos requisitos foram reunidos em um documento chamado TSB-95, sendo integrado no informativo TIA/EIA 568-B.1, anexos D e N.

O ruído que acontece nos quatro receptores em um dispositivo 1000 BaseT consiste em :

1) Ruído do ambiente

2) Distúrbios locais

3) Distúrbios distantes

4) Eco

Além disso, os parâmetros relativos ao cabeamento também devem ser considerados:

a) Comprimento

O cabo instalado não deveria exceder noventa metros, mas é permitida a existência de uma margem adicional de dez metros.

b) Atenuação

Uma medida do sinal recebido em comparação com o sinal transmitido, mensurado em decibéis (dB).

c) Mapeamento dos cabos

Um teste de continuidade. Assegura que os fios individuais estão propriamente conectados em toda a extensão do cabo, sem quebras, curto-circuitos ou instalação incorreta.

d) Perda de retorno

A medida do sinal que é refletido para o transmissor, devido a mudanças na impedância do cabeamento.

12. Vantagens

-Confiabilidade

Em uma rede, a confiabilidade é um dos requisitos mais importantes. Gigabit Ethernet é uma evolução das tecnologias 100 BaseX e 10 BaseX, que têm um histórico de décadas.

-Ferramentas

Há numerosas ferramentas que foram desenvolvidas ao longo dos anos, para localizar os problemas existentes na rede.

-Alto nível de desempenho

-Alta escalabilidade

-Compatibilidade : muitos equipamentos de rede Gigabit Ethernet (hubs, switches) podem automaticamente detectar a presença de dispositivos mais antigos e escolher uma velocidade menor, se necessário.

13. Conclusão

O crescente poder dos computadores provavelmente fará com que os aplicativos também exijam uma alta demanda por parte das redes locais, tornando indispensável a melhoria da banda passante associada.

Em um futuro próximo, a aquisição de sistemas Fast Ethernet não será mais compensadora, sendo que os terminais Gigabit Ethernet provavelmente serão os sistemas mais difundidos no campo da tecnologia da informação.

9. SNMP

1. Introdução

A disseminação de redes de interligação resultou na necessidade de um protocolo para gerenciar os elementos que formam tal sistema e verificar em tempo real os eventos que nele ocorrem.

Atualmente, o SNMP (Simple Network Management Protocol) é o mais utilizado para monitorar os diversos equipamentos existentes, sendo um protocolo relativamente simples.

O SNMP especifica uma infraestrutura para que possa ocorrer o intercâmbio de informações entre os elementos que compõem uma rede, facilitando a localização dos problemas que possam ocorrer na mesma.

Os administradores da rede podem encaminar comandos para um sistema que implemente o protocolo mencionado.

Além disso, é possível consultar a MIB (Management Information Base) associada, que contém diversas variáveis informando o estado do equipamento em questão.

2. Tecnologia

O SNMP utiliza o modelo cliente-servidor. Os equipamentos gerenciados podem ser: roteadores, PCs, servidores, impressoras de rede, etc. Um servidor (agente) é instalado nesses dispositivos.

O agente, normalmente implementado com a utilização de softwares específicos, disponibiliza as informações coletadas ao sistema de gerenciamento, que periodicamente lê os dados através do rede, utilizando o SNMP.

O agente pode também responder a mensagens da estação gerenciada, através de traps.

A MIB é uma estrutura de dados contendo diversas variáveis que podem ser modificadas pelo sistema de gerenciamento, representadas através do ASN.1 (Abstract Syntax Notation).

O SNMP pode ser visto através de três diferentes pontos de vista:

1) Um padrão de variáveis : um protocolo que especifica o formato de uma mensagem que utiliza o UDP.

2) Um padrão sobre objetos gerenciados : cada objeto é identificado através de um nome, além de um identificador expresso em notação de pontos.

3) Um padrão sobre expansão de objetos : um padrão para aumentar a quantidade de objetos controlados.

3. Histórico

Primordialmente, o ICMP era utilizado para a obtenção de informações básicas sobre o estado dos equipamentos de rede (ping, etc.). Em 1987, surge o SGMP (Simple Gateway Management Protocol), desenvolvido para gerenciar pilhas OSI.

Um complexo protocolo chamado CMIP foi criado para a mesma finalidade. Houve uma adaptação para o TCP/IP, na forma de um sistema denominado CMOT. Sendo relativamente complexo, desde então o SNMP começou a ser mais utilizado.

SNMP Versão 1.0:

Nessa versão, os agentes são modulos de software que rodam nos dispositivos que estão sendo gerenciados. Eles coletam informações que são disponibilizadas aos sistemas de gerenciamento através do protocolo SNMP 1.0.

Presumindo-se que tais dispositivos tenham baixa capacidade de processamento e armazenamento, o NMS (Network Management System) deveria utilizar os padrões mais comuns, que pouco impactavam no desempenho dos objetos gerenciados.

Normalmente, o NMS consistia em uma estação de trabalho possuindo um grande poder de processamento, além de dispositivos de armazenamento de massa contendo uma grande capacidade. Basicamente, executava o software de gerenciamento da rede, exibindo as informações ao usuário através de uma interface gráfica.

O padrão contemplava que os dispositivos gerenciados deveriam fornecer dados substanciais ao NMS, por exemplo:

-Pacotes recebidos e encaminhados
-Estado das interfaces de rede
-Número de bytes enviados
-Mensagens de erro

Tipos de comando

Se o NMS precisar gerenciar um determinado equipamento, é necessário encaminhar uma mensagem para o mesmo, solicitando a alteração dos valores das variáveis associadas. Existem quatro classes de comandos:

1) Leituras – para verificar os valores das variáveis mantidas pelos objetos gerenciados
2) Escritas – alterar o conteúdo das varíaveis dos objetos gerenciados

3) Consultas – para saber quais são as variáveis suportadas pelos objetos.
4) "Traps" – para reportar determinados eventos para o NMS, de um modo assíncrono.

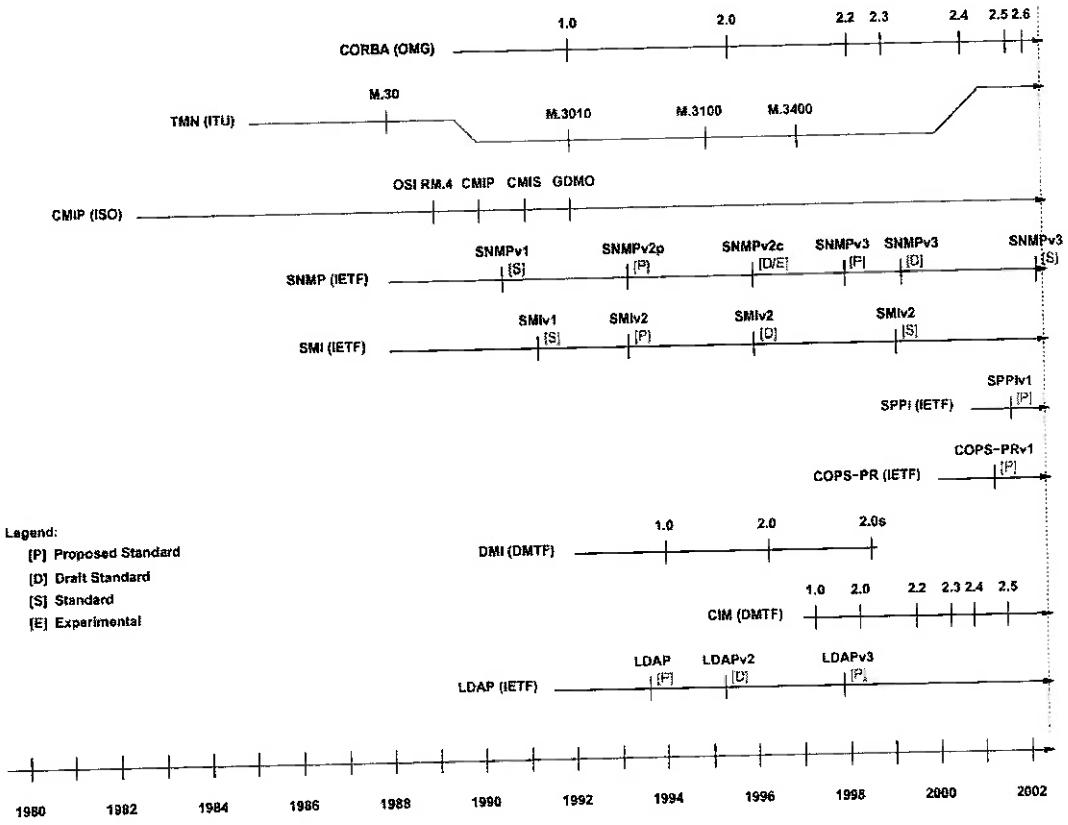

Figura 9 – Evolução do sistema SNMP

4. SNMP Versão 2.0

É uma evolução do protocolo anteriormente descrito, visando mais segurança.

O "SNMP seguro" (Secure SNMP - SMP) definiu novos recursos de segurança, sob pena de incompatibilidades com a versão v.1. Entretanto, havia mais flexibilidade nos recursos gerenciados e um maior número de ambientes a operar.

A evolução do SMP acarretou no surgimento do padrão v.2, em 1993. Inclui melhorias na arquitetura de gerenciamento e na segurança. Houve o suporte a novos

tipos de dados e uma nova convenção para criar linhas conceituais em uma tabela. Os contadores foram ampliados para 64 bits, além da criação de tipos sem sinal.

O protocolo definido no SNMP v.2 usa o mesmo formato dos PDUs no caso de informação de operações, mas permite a obtenção de resultados parciais, ao invés de operar em um modo absoluto (toda a informação ou nenhuma)

Criou-se o conceito de módulo de informação, especificando um grupo com características semelhantes:

1) Módulos MIB : definições de objetos gerenciados.
2) Condições de compatibilidade : descreve o grupo de objetos gerenciados que deve ser obrigatoriamente implementado.
3) Condições de capacidade : descreve o nível de suporte de um agente a uma determinada MIB.

Várias operações são suportadas:

1) Get : obtém uma instância de um agente. Muitos valores podem ser obtidos sem a necessidade de login no dispositivo controlado.
2) Get-next : obtém a próxima instância a partir de uma tabela, a partir de um agente. Percorre os valores SNMP de um agente.
3) Set : determina uma instância em um agente.
4) Trap : informa de um modo assíncrono a ocorrência de um evento.
5) Inform : permite a um gerenciador encaminhar informações a respeito de um trap, para um outro gerenciador.
6) Get-bulk : permite a um gerenciador obter grandes blocos de informação, ao invés de solicitar vários trechos menores de dados.

Essas mensagens são codificadas em PDUs (Protocol Data Unit), que são intercambiados entre dispositivos SNMP.

Existem também melhorias para os seguintes problemas de segurança:

-Mascaramento, que significa a tentativa de executar operações de gerenciamento assumindo a identidade de uma entidade autorizada.

-Modificação da informação : uma entidade pode alterar uma mensagem enviada por uma entidade autorizada, resultando em operações não-autorizadas.

-Seqüência da mensagem : o SNMP v.1 opera em um meio de transporte sem conexão, podendo uma entidade copiar, reordenar e gerar novamente uma mensagem SNMP v.1.

-Descobertas : uma entidade pode capturar os valores de objetos gerenciados, monitorando as variáveis transmitidas de um gerenciador para um agente.

5. RMON

O RMON (Remote Monitoring Standard) foi desenvolvido para coletar dados de tráfego de rede, para uso estatístico.

As informações são coletadas através da utilização de agentes SNMP especiais, chamados de RMON.

As variáveis requeridas são definidas nas RMON MIBs, estendendo as funcionalidades do protocolo SNMP v.2 original. Os recursos básicos são:

-Tabela de dados : contém estatísticas, logs, etc.

-Tabela de controle : contém os parâmetros que devem ser monitorados e com que freqüência.

-Outros : sondas compartilhadas, tabela de concorrência de acesso, propriedade das tabelas.

6. Formato da mensagem

Para simplificar a decodificação da mensagem, todas as operações usam o mesmo formato, exceto a instrução "get-bulk", tendo os seguintes campos:

-Tipo da PDU : get, set, get-next, trap, response

-ID da requisição : associa requisições com respostas

-Estado do erro : indica a ocorrência de um erro

-Index do erro : associa o erro com uma variável particular

-Associação de variáveis, com o valor corrente.

O "get-bulk" tem o seguinte formato:

-Tipo da PDU, ID da requisição, associação de variáveis : têm as mesmas funções em relação às instruções "get, get-next, set, response e trap".

-Não-repetidores : especifica o número de variáveis que será retornado.

-Repetições máximas : especifica o número restante de variáveis que será retornado.

Os campos de uma mensagem SNMP v.2 têm o seguinte formato:

-Destino : identifica o receptor, este campo aparece duas vezes: no início da mensagem e na parte da mensagem que pode ser criptografada.

-Fonte : identifica quem encaminhou a mensagem

-Contexto : identifica a coleção de objetos gerenciados acessíveis por uma entidade.

-PDU : identifica o operação de gerenciamento

-Resultado : contém o valor resultante do algoritmo do cálculo da mensagem.

-Horário do destino : o valor que o enviador presume para o relógio do receptor.

-Horário de envio : contém a valor do relógio do enviador.

O SNMP v.2 tem três tipos de mensagens:

-Não seguras : sem nenhum dispositivo de segurança do SNMP v.2

-Autenticação sem privacidade : o SNMP v.2 utiliza um valor conhecido pelo enviador e pelo receptor, para autenticação da origem.

-Autenticação com privacidade : as mensagens são autenticadas e criptografadas.

7. SNMP Versão 3.0

É uma implementação da arquitetura proposta na RFC 2271, sendo uma extensão para melhorar a segurança. Um objetivo é possibilitar uma maior facilidade de expansão.

Nesta versão, os agentes e os objetos gerenciados são denominados entidades, sendo compostos de duas partes: o gerador e as aplicações.

1) O gerador

a) Distribuidor

O distribuidor encaminha e recebe mensagens. Quando uma mensagem é recebida, tenta verificar a versão da mensagem e o encaminha para o decodificador apropriado. Se ocorrer um erro neste procedimento, a mensagem é descartada.

O distribuidor também encaminha PDUs para as aplicações.

b) Subsistema de processamento de mensagens

Este módulo prepara as mensagens para o encaminhamento e também extrai informações das notificações recebidas. O subsistema de segurança é ativado para decodificar as informações e também verificar a autenticação.

c) Subsistema de segurança

Esta parte provê os seguintes serviços : autenticação e decriptação das informações. Há o suporte do padrão de comunidades, para a compatibilização com os padrões SNMP v.1 e SNMP v.2.

O padrão baseado em segurança do usuário define o uso do MD5 ou DES, podendo ser expandido.

d) Subsistema de controle de acesso

Determina quais objetos podem ser gerenciados. É possível controlar os usuários e as operações que podem ser executadas.

8. Estrutura

Um dos motivos para que o SNMP seja de utilização geral é a propriedade de expandir o conjunto de objetos, com novos valores. Este processo denomina-se compilação da MIB.

As definições são descritas no formato ASN.1 (Abstract Syntax Notation One). Os valores são definidos na RFC 1213.

Cada valor é associado a um nome oficial ou em notação de pontos. A tendência é a utilização do texto em si, de um modo análogo à tradução dos endereços IP nas respectivas URLs.

Os objetos gerenciados representam um conjunto de variáveis que pode ser monitorado. Podem ser escalares (há somente uma instância) ou tabulares (várias instâncias).

A MIB é representada por uma árvore. Os objetos principais são designados pela ISO/IEC (International Organization for Standardization/International Electrotechnical Commission). Os objetos de nível mais baixo são alocados pelas organizações associadas. Além disso, é possível definir ramificações próprias.

Um documento chamado SMO (Structure of Management Information) define a estrutura da MIB e como defini-las, por exemplo:

-Contadores
-Medidores : retém o máximo valor alcançado.
-Tempo : centésimos de segundo desde um evento determinado.

As tabelas são um tipo especial de objetos SNMP, permitindo matrizes de informação. Podem ser expandidas sem limites.

No total, existem vários tipos primitivos:

1) Texto : até 256 caracteres.
2) Contadores : pode ser incrementado
3) Medidores : pode ser incrementado ou decrementado
4) Tipos inteiros : valores positivos ou negativos
5) Enumerações : associa um texto a um valor numérico
6) Tempo : centésimos de segundo após um evento
7) Objetos : identificador de outro objeto SNMP
8) Endereços IP : expresso em notação de pontos.
9) Endereço físico : o endereço MAC de um dispositivo de rede
10) Tabelas : matrizes de informação

9. Vantagens

A principal vantagem é a depuração remota, sendo que a estação-alvo pode estar a milhares de quilômetros do sistema de gerenciamento.

10. Desvantagens

O SNMP tem alguns problemas endêmicos ao protocolo propriamente dito:

1) Problemas de segurança : Não há um padrão de encriptação. Os nomes comunitários (que servem para limitar o acesso a um agente) são encapsulados em cada mensagem SNMP, podendo ser extraídos com um software específico.

2) Problemas de latência : É um protocolo de requisição e resposta, significando que existe um atraso entre a emissão da mensagem e a recepção da resposta. O problema torna-se maior quanto mais estações intermediárias existirem entre o NMS e o agente, e quanto mais informação for extraída do dispositivo.

11. Conclusão

O SNMP representa o padrão de fato para gerenciar os equipamentos conectados em uma rede que utilize o protocolo IP. Além de não causar um grande overhead no processamento do software dos agentes, permite a expansão dos parâmetros que podem ser monitorados remotamente.

Apesar dos problemas de segurança e latência já comentados, tais questões serão provavelmente resolvidas ou minimizadas nas próximas versões do SNMP, que atualmente está na versão 3.

10. ATM

1. Introdução

A comutação de pacotes permite o compartilhamento de um mesmo canal físico. Entretanto, essa mesma característica pode resultar em uma série de colisões entre os pacotes transmitidos, degradando a vazão (throughput) da rede considerada. Para minimizar o problema, a comutação de células tem como foco principal a qualidade de serviço (QoS).

O ATM (Asynchronous Transmisson Mode) é uma tecnologia orientada à conexão, que utiliza a comutação de células para o intercâmbio de informações.

2. Histórico

A priori, as maiores limitações para o transporte de informações eram : as distâncias a serem percorridas pelos sinais elétricos e o tempo de roteamento. A distância física não pode ser alterada substancialmente, mas é possível aumentar a banda de passagem.

Para tanto, foram desenvolvidas rotas que utilizam fibras ópticas, por exemplo o SONET (Synchronous Optical Network). Há várias velocidades: o OC-1 (51.84 Mbps), o OC-2 (103.68 Mbps), o OC-3 (3 vezes a velocidade do OC-1) e assim sucessivamente.

O mesmo sinal óptico, quando convertido para sinais elétricos, denomina-se STS (Synchronous Transport Signal). A menor velocidade é de 51.84 Mbps, a mesma do OC-1. Atualmente, o OC-192 atinge a velocidade de 9.95 Gbps.

O ATM pode suportar redes que utilizem o T1/E1 e o T3/E3.

Em 1993, o ATM Fórum determinou as especificações para as implementações futuras dessa tecnologia, ressaltando-se o formato das células.

Historicamente, é uma evolução do frame relay e também do padrão STM (Synchronous Transfer Mode), inicialmente desenvolvido para o transporte de voz e dados com o uso de multiplexação por tempo. A desvantagem era a necessidade de um circuito dedicado, similar ao sistema telefônico tradicional.

As primeiras implementações tinham opções limitadas: era possível apenas reservar uma banda para cada conexão baseado no fluxo máximo de dados do emissor.

Atualmente, é possível selecionar combinações de tráfego e parâmetros de desempenho específicos.

A pilha de protocolos ATM é composta, basicamente, de três camadas:

1) Camada física

2) Camada ATM : provê o roteamento dos pacotes ATM, dependendo dos rótulos VCI (Virtual Channel Identifiers) e VPI (Virtual Path Identifiers). Também realiza a extração e a geração dos headers das células ATM.

3) Camada de adaptação : mapeia os vários tipos de tráfego existentes em um conteúdo correspondente nas células ATM.

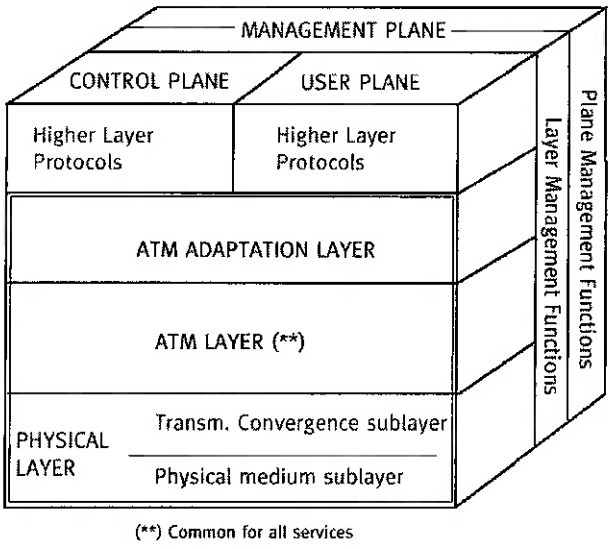

Figura 10 – Camadas representativas da tecnologia ATM

3. Tecnologia

Para evitar a ocupação de um circuito, várias modificações foram realizadas:

-Estabelecimento de uma célula de tamanho fixo (53 bytes), evitando processamento adicional para lidar com células de tamanho variável e podendo existir comutação diretamente em hardware.

-Desenvolvimento de roteadores de alta velocidade, possibilitando a escolha dinâmica de rotas no tempo requerido.

O ATM assume que a mídia seja de alta qualidade, fazendo com que os protocolos de nível superior verifiquem se as informações transmitidas contém erros. Isso possibilita atingir altas velocidades de transferência.

4. QoS

Um outro problema acontece quando o delay entre o envio de um pacote e a sua recepção ultrapassa 200 ms. Em um circuito telefônico, o tempo mencionado passa a ser perceptível.

Para resolver tal problema, o CES (Circuit Emulation Service) foi desenvolvido para permitir taxas consistentes de transferência.

Com um circuito emulado de alta velocidade e canceladores de eco, a qualidade da voz sobre ATM torna-se aceitável.

5. Célula

As células ATM têm um comprimento de 53 bytes.

Os primeiros cinco bytes são reservados para a informação do cabeçalho, incluindo bits para priorização de pacotes, dependendo do tipo da mídia (dados, voz ou vídeo).

Bytes adicionais são usados para origem, destino, roteamento, informação de seqüenciamento de células e detecção de erros.

Os 48 bytes restantes são a carga útil e contém os dados propriamente ditos. Não só a eficiência do sistema foi considerada, mas também o atraso de empacotamento, que é o tempo necessário para preencher uma célula a partir de um fluxo de dados de 64 Kbps. A célula é preenchida a partir das informações provenientes das AALs (ATM Adaptation Layer).

6. Tecnologia

O ATM é uma tecnologia de comutação de células.

Isso significa que o primeiro pacote proveniente de uma transmissão faz com que o endereço seja analisado por hardware e uma rota seja escolhida.

Todos os pacotes com o mesmo endereço de destino serão encaminhados utilizando a mesma rota virtual.

Entretanto, o ATM não transmite as células assincronamente. As células de tamanho fixo são transmitidas de um modo síncrono, mas continuamente.

Quanto não existem dados a encaminhar, as células são preenchidas com um padrão de bits que indica uma célula vazia.

7. VCC

Um VCC (Virtual Channel Connection) pode ser descrito como um caminho entre qualquer origem e qualquer destino, em uma rede ATM. Fundamentalmente, o ATM é uma tecnologia orientada à conexão, e os circuitos virtuais podem ser estabelecidos permanentemente (PVC) ou em demanda (SVC).

A comutação ATM é desenvolvida com o roteamento de pares VPI/VCI de entrada para diferentes VPI/VCI de saída, normalmente utilizando uma tabela baseada em hardware.

As células incidentes têm o VPI/VCI modificado com novos valores e então são encaminhadas para a porta apropriada. Portanto, o par VPI/VCI tem significância apenas local, alterando-se em cada ponto do switch ATM.

8. IP over ATM

Historicamente, existiram tentativas no sentido do protocolo IP atuar sob SDH ou SONET. Mas o ATM provê maiores recursos para o gerenciamento da rede, especialmente para redes públicas.

Tecnicamente, para que seja possível transportar o tráfego IP usando o ATM, o endereço IP precisa ser traduzido para um par VPI/ VCI, sendo que, no destino, essa mesma informação deve ser extraída.

As aplicações VoIP são sensíveis ao jitter (variação da latência) e os sistemas ATM são também projetados para minimizar a variação do tempo de trânsito das células.

9. AAL

O AAL (ATM Adaptation Layer) situa-se acima da PHY (Physical Layer) e provê funções para as camadas superiores. É responsável por seccionar as informações em pacotes e então reconstruí-las após a transmissão dos mesmos.

Muitos dos requisitos de uma aplicação podem ser atingidos através da escolha de um AAL (ATM Adaptation Layer) adequado.

É dividido em subcamadas CS (Convergence Sublayer) e SAR (Segmentation And Reassembly). A camada PHY subdivide-se em TC (Transmission Convergence) e PM (Physical Medium).

Há diferentes tipos de AALs, que suportam vários requisitos de tráfego:

a) AAL1 – Suporta o tráfego CBR (Constant Bit Rate) – exemplos : vídeo em tempo real, emulação de circuitos.

O protocolo básico contempla um header que precede 47 bytes de informação. O header contém o número de seqüência das células.

b) AAL2 – Projetado para o tráfego VBR (Variable Bit Rate) - exemplos : vídeo MPEG, onde o fluxo de dados é variável.

c) AAL3/4 – Também suporta o tráfego VBR, podendo ou não ser orientado à conexão.

É um complexo protocolo usado para dados que não necessitem ser transferidos em tempo real, por exemplo : cópia de arquivos, backup de dados, etc.

d) AAL5 – É uma versão simplificada do AAL3/4, podendo também suportar tráfego orientado ou não à conexão.

Algumas mensagens foram removidas, aumentando a eficiência do protocolo.

10. Controles

Em um switch ATM, existem vários sistemas para controlar a qualidade do serviço (QoS):

1) Header Error Control (HEC) : o cabeçalho de cada célula tem um campo de oito bits, que armazena o checksum dos quatro bytes restantes do header, proporcionando uma alta probabilidade de encontrar erros no mesmo.

O HEC não verifica se a carga útil contém erros. Essa função é normalmente atribuída à camada de transporte.

2) Controle genérico do fluxo : esse campo existe nas células UNI (User Network Interface), proporcionando indicadores sobre os dados incidentes em uma rede ATM.

3) Cell Loss Priority : é a reação de um switch ATM aos congestionamentos que podem ocorrer na rede. O comportamento a essa situação é flexível : vídeo de alta prioridade pode reservar células específicas. Normalmente, as células que excedem o CIR (Committed Information Rate) são descartadas, se necessário.

11. Categorias de serviço

1) UBR (Unspecified Bit Rate)

Essa categoria é destinada às aplicações mais simples, que não requerem tempo real. Exemplos: transferência de arquivos, correio eletrônico.

O tráfego é representado por fluxos não-contínuos de células. Essa categoria não especifica serviços de garantia de tráfego.

2) ABR (Available Bit Rate)

É uma categoria onde as características da camada de transferência da rede podem ser alteradas, depois do estabelecimento da conexão. Um mecanismo de controle de fluxo é especificado, apto a responder às mudanças dessas características.

É esperado que as estações adaptem-se ao fluxo de tráfego, visando a obtenção de uma parte da banda passante disponível de acordo com a perda de pacotes.

Esta categoria, a priori, não suporta sistemas de tempo real. Uma aplicação típica é a interconexão de redes.

3) CBR (Constant Bit Rate)

É utilizado para conexões que necessitem de um banda passante estática, tendo um PCR (Peak Cell Rate) garantido durante o tempo de conexão à rede ATM.

Esta categoria foi projetada para suportar aplicações de tempo real, com baixa latência e "jitter" reduzido.

A característica básica é a manutenção do QoS previamente negociado, durante o tempo de conexão. Células que são recebidas acima do valor especificado pelo CTD (Cell Transfer Delay) podem ter baixo significado para a aplicação.

É apropriado para sistemas multimídia e para a emulação de circuitos.

4) VBR (Variable Bit Rate)

A categoria VBR é útil para as aplicações que requerem multiplexação estatística, com a emissão de informações a uma taxa variável e que tenham tolerância a pequenas perdas.

O VBR pode ou não ter a característica de tempo real.

O rt-VBR (real-time VBR) é apropriado para aplicações de voz e vídeo, com variações na taxa de transmissão. É mais eficiente na utilização dos recursos da rede ATM, com baixa perda de desempenho.

O nrt-VBR (non-real time VBR) é melhor utilizado em sistemas que tenham picos de tráfego ("bursty"), podendo suportar multiplexação estatística de conexões. Pode ser usado em aplicações de transferência de dados, mesmo com requisitos de um tempo de resposta crítico.

12. UNI

O gerenciamento das redes ATM é uma requisição crucial, para monitorar o estado e o comportamento do sistema. Para tanto, o sistema UNI (User to Network Interface) foi desenvolvido.

As informações que a MIB ATM UNI terá são : camada física, camada ATM, conexões virtuais (VP/VC), etc.

O header da célula UNI (User to Network Interface) também provê informações de endereçamento, um fluxo de controle e verificação de erros no header.

13. ATC

O ATC (ATM Transfer Capabilities) descreve as características gerais de uma conexão, além de parâmetros e procedimentos da camada ATM.

O ITU-T especificou alguns ATCs:

1) DBR (Deterministic Bit Rate) : garante que um fluxo máximo de células será disponibilizado continuamente. É bastante utilizado com as aplicações CBR, enquanto as aplicações VBR podem ou não requisitar este parâmetro.

2) SBR (Statistical Bit Rate) : garante um fluxo médio de informações, permitindo picos de tráfego limitados.

14. Conclusão

Um dos pontos principais do protocolo ATM é a ênfase no aspecto QoS, possibilitando o transporte de informações que representam vídeo e sinais audíveis. Isso é possível devido ao fato da utilização de células de tamanho fixo.

É possível criar um circuito virtual com diferentes níveis de serviço, permitindo otimizar as capacidades da rede.

11. PROTOCOLOS DE ROTEAMENTO

1. Introdução

Um fator determinante para mensurar o desempenho de uma rede é avaliar o protocolo de roteamento que a mesma emprega.

A característica básica é o deslocamento de informações entre as estações de uma determinada rede.

Se o protocolo mencionado emprega mais de um equipamento, é comum referir-se como sendo um processo coletivo de comunicação.

O roteamento não significa apenas a escolha correta do caminho a ser percorrido, mas envolve também o cálculo da menor distância possível entre os pontos da conexão propriamente dita.

Além disso, o protocolo deve considerar que os equipamentos de rede não são completamente à prova de falhas e erros, e um novo caminho deve ser escolhido assim que um problema na rota seja detectado.

Após a solução do problema, ou após a adição de novos equipamentos, o sistema deve avaliar os caminhos existentes na rede e comunicar as novas rotas para os roteadores adjacentes.

2. Tipos de protocolos

Existem três tipos básicos:

1) Compartilhamento de árvores multicast

2) Estado dos links

Mantém a topologia da rede na memória do equipamento, ou pelo menos a área associada ao sistema.

3) Avaliação da distância

Os protocolos DV (Distance Vector) avaliam a distância até um determinado endereço IP e encaminham a tabela de roteamento aos sistemas adjacentes, a intervalos regulares.

Se a rede tornar-se muito extensa, as tabelas de roteamento podem consumir um tempo considerável, existindo a possibilidade de formação de rotas circulares durante a atualização da topologia da rede.

Existem muitos protocolos de roteamento, sendo que alguns serão citados :

3. RIP

Em meados da década de 1980, o protocolo de roteamento mais utilizado era o RIP (Routing Information Protocol).

Embora fosse útil para redes homogêneas que não fossem gigantescas, o crescimento da Internet resultou no aparecimento dos limites desta metodologia.

A simplicidade excessiva do algoritmo (contagem de estações intermediárias) e o baixo limite de hops (16) fizeram com que caísse rapidamente em desuso.

4. OSPF

O OSPF (Open Shortest Path First) é um protocolo orientado ao estado dos links, cujo princípio básico é a identificação de cada circuito existente em uma rede.

Cada roteador mantém uma tabela contendo o estado de todos os circuitos, possibilitando o cálculo da topologia da rede.

Quando o estado de um link é alterado, essa informação é emitida para todos os roteadores.

Este protocolo converge rapidamente, sem a formação de caminhos circulares, mas surgem problemas conforme o crescimento da rede, diminuindo a estabilidade da mesma.

Para resolver essas questões, há uma hierarquia de roteamento, em áreas distintas. As informações contendo os estados dos links são transmitidas a todos os roteadores de uma determinada área.

Para os sistemas externos à área, é repassada a possibilidade de roteamento, e não o estado dos circuitos.

O objetivo é restringir o controle da topologia às áreas propriamente ditas.

5. IGRP

O IGRP (Interior Gateway Routing Protocol) foi desenvolvido em meados dos anos 80, tendo como principal objetivo a robustez, dentro de um sistema autônomo.

Mantém internamente vários temporizadores e variáveis monitorando os intervalos de tempo, a citar:

-Temporização de atualização (90 segundos)

-Temporização para invalidação : determina o tempo que o equipamento deve esperar para invalidar uma rota já estabelecida, por falta de atualização.

-Tempo de espera.

-Tempo de sincronismo : quanto tempo esperar até que a rota seja finalmente descartada da tabela de roteamento.

Características principais do IGRP:

Os protocolos de roteamento orientados à distância fazem com que as tabelas de roteamento dos equipamentos adjacentes sejam intercambiadas a intervalos regulares. Com isso, torna-se possível o cálculo das distâncias entre os nós de uma rede.

Os protocolos de roteamento orientados à distância contrastam com os protocolos orientados ao estado dos links, que encaminham o estado das conexões a todos os nós da rede.

O IGRP utiliza uma combinação de métricas, considerando a confiabilidade, carga, banda de passagem e carregamento para a decisão das rotas.

O peso dos fatores pode ser definido pelo administrador da rede em questão.

Além disso, o IGRP permite o roteamento com múltiplas conexões, por exemplo: em uma rota com vários circuitos, o protocolo pode selecionar automaticamente a conexão com o melhor desempenho.

Para aumentar a estabilidade, vários recursos são utilizados, a exemplo do Hold-down, que inibe temporariamente a mudança de rotas se um problema em um equipamento da rede for detectado.

6. Enhanced IGRP

O Enhanced IGRP foi desenvolvido no início dos anos 90, para aumentar a eficiência do protocolo IGRP.

Uma característica de um sistema que use o Enhanced IGRP é o armazenamento de todas as tabelas de roteamento dos equipamentos adjacentes, possibilitando a rápida localização de rotas alternativas.

Se não existe uma rota apropriada, o Enhanced IGRP consulta os roteadores interconectados para que seja possível descobrir um caminho apropriado. Estas consultas são propagadas, até a descoberta de uma rota adequada.

O Enhanced IGRP é compatível com o IGRP, através de mecanismos de redistribuição automática e métricas que são traduzíveis entre si.

7. Recursos do EIGRP

As características principais do protocolo são:

1) Máscaras de subrede variáveis

2) Atualizações parciais

O Enhanced IGRP não realiza atualizações periódicas, mas somente quando a métrica de uma rota é alterada.

Somente os roteadores que utilizam tal rota são informados dessa mudança, consumindo uma quantidade de banda de passagem menor do que o IGRP.

3) Suporte a múltiplas camadas de rede (Novell, IP, Appletalk, etc.)

Além disso, novas tecnologias foram incorporadas ao Enhanced IGRP:

1) Detecção de sistemas adjacentes

É usado pelos roteadores para descobrir novos roteadores na rede em questão, além de detectar a inoperância de alguns equipamentos de rede.

2) RTP (Reliable Transport Protocol)

Este protocolo garante que todos os pacotes EIGRP alcançarão o destino, sendo unicast ou não.

8. Tipos de pacotes

Os pacotes EIGRP são:

1) Hello

São pacotes multicast encaminhados para detectar novos sistemas adjacentes. Um sinal ACK (Acknowledgment) não é necessário.

2) Update

Informam se uma rede é alcançável, resultando na atualização das tabelas de roteamento dos equipamentos adjacentes.

3) Query

Encaminhados quando o roteador em questão não registra sucessores em um destino. O pacote "reply" indica à origem que não é necessário recalcular a rota em questão.

4) Request

Usados para obter informações específicas dos roteadores próximos à origem.

9. Multicast

A transmissão da mesma informação a um conjunto de usuários com a utilização do unicast normalmente resulta em um consumo excessivo de banda de passagem, aumentando proporcionalmente ao número de estações a serem contactadas.

Assim, o multicast foi desenvolvido para reduzir a banda de passagem necessária para tanto.

Obviamente, para que tais pacotes sejam transportados, pelo menos um protocolo de roteamento multicast deve existir na rede IP.

Eles podem ser caracterizados pela distribuição dos nós, que podem estar densamente localizados ou não.

Os protocolos de roteamento multicast mais utilizados são:

10. DVMRP

O DVMRP (Distance-Vector Multicast Routing Protocol) foi definido na RFC1075 e é a base do MBONE (Multicast Backbone).

A algoritmo baseia-se no "path-flooding", que encaminha uma cópia do pacote para todos os caminhos possíveis, exceto a interface de origem.

Problemas de escalabilidade podem aparecer, devido ao tráfego em excesso.

O protocolo aceita um máximo de 15 hops nas tabelas de roteamento, além de armazenar o estado das rotas.

11. MOSPF

O MOSPF (Multicast Open Shortest Path First) é uma extensão do OSPF, de acordo com a RFC1584.

Um roteador MOSPF calcula as rotas para cada fonte/grupo multicast quando o equipamento recebe tráfego para esse par, através das informações de multicast obtidas das conexões OSPF.

Há algumas vantagens nesse protocolo:

1) não há limites de hops na tabela de roteamento.

2) converge mais rápido do que o DVMRP.

3) Não é preciso encaminhar pacotes para todas as interfaces porque o protocolo armazena a rota para cada grupo.

4) O conceito de áreas pode ser aplicado, reduzindo o tempo de convergência.

Entretanto, o MOSPF é compatível somente com redes que usam OSPF, e tem desempenho melhor em ambientes com poucas fontes de tráfego multicast.

12. PIM-DM

. O PIM-DM (Protocol Independent Multicast-Dense Mode) é similar ao DVMRP, mas utiliza o sistema unicast da rede em questão.

Isso permite que qualquer protocolo de roteamento possa ser usado com o PIM-DM.

Este sistema também encaminha pacotes para todas as interfaces (excetuando-se a da origem).

13. PIM-SM

O PIM-SM (Protocol Independent Multicast-Sparse Mode) é otimizado para muitas fontes streams e poucas LANs, conforme a RFC2117.

É definido um ponto Rendezvous (RP), que concentra os fluxos de dados. O RP é utilizado pelo receptor e pelo emissor de pacotes multicast, sem hops desnecessários.

Isso melhora a distribuição de tráfego multicast, sem existir a necessidade de emitir pacotes para todas as interfaces de rede.

A desvantagem é que as rotas das fontes para os destinos freqüentemente não são otimizadas, além de existir um ponto de convergência de pacotes, podendo resultar em altas latências.

14. Conclusão

A complexidade aumenta consideravelmente se a estação de destino for móvel (celular, satélite, etc).

Com o crescimento da Internet, novos protocolos terão de ser desenvolvidos, especialmente para as aplicações que exigem baixa latência e alta capilaridade, a exemplo dos sistemas wireless, que se caracterizam pela alta dinamicidade da topologia de rede.

12. BGP

1. Introdução

O BGP 4 (Border Gateway Protocol version 4) é o padrão mais utilizado no roteamento entre domínios da Internet.

Sendo um protocolo de roteamento para um sistema autônomo, é utilizado para determinar as rotas para destinos que estão fora do AS. É um contraste com o OSPF, que seleciona rotas para destinos que estão dentro do AS.

É usado nos maiores pontos de acessos à rede (NAP), onde os grandes provedores de Internet se conectam para que ocorra o intercâmbio de tráfego.

Os ISPs têm múltiplas conexões entre si, e tal protocolo de roteamento foi desenvolvido para selecionar o melhor ponto para o intercâmbio de tráfego.

2. Tecnologia

A rigor, o BGP é considerado também um Exterior Gateway Protocol, desenhado para selecionar rotas entre domínios.

Os roteadores usam o EGP para controlar o acesso a outros sistemas autônomos, servindo também para seccionar uma rede gigantesca em partes menores.

Um sistema autônomo (AS) pode ser definido como um grupo de redes e roteadores que estão sob domínio de uma mesma entidade administrativa.

A Internet é uma coleção de vários AS, e o objetivo do BGP é reduzir o tráfego de um sistema autônomo, com a utilização opcional do roteamento baseado em políticas, que é determinado pelos administradores de rede.

3. Histórico

O desenvolvimento do BGP iniciou-se com a publicação da RFC 1771. A versão atual é a RFC 1654.

O primeiro protocolo de roteamento externo de maior relevância denominava-se EGP. Entretanto, existiam diversos problemas, salientando-se o fato de que se tratava mais de um protocolo de possibilidade de conexão a um sistema de roteamento.

O BGP foi então desenvolvido para solucionar tais problemas. Assim, uma das características mais importantes é a possibilidade de detecção de roteamentos circulares (loops), além de um escalamento mais eficiente.

O roteamento divide-se em duas atividades básicas: selecionar a melhor rota entre dois pontos e o transporte propriamente dito dos pacotes, que são duas atividades de complexidades opostas.

Os protocolos anteriores de roteamento não eram capazes de suportar o gigantesco número de rotas existentes na Internet. Por exemplo, o RIP encaminhava periodicamente uma listagem de todas as redes conhecidas, podendo facilmente congestionar o sistema.

4. Características

-Transporte confiável : o BGP usa o protocolo TCP como uma mídia de transporte confiável, encaminhando periodicamente as atualizações das rotas.

-Next-Hop : o BGP informa as distâncias (em hops) para cada destino.

-Autenticação : é permitido a um receptor a autenticação de mensagens.

-Informação de caminho : as mensagens BGP incluem os caminhos alcançáveis e também as informações que permitem a um receptor saber os AS existentes até o destino.

-Endereçamento sem classes : O BGP possibilita o uso do CIDR (Classless Inter-Domain Routing), um sistema para obter mais endereços do que o permitido pelo IP.

-Agrupamento de rotas : o BGP melhora a eficiência da rede permitindo que as informações das rotas sejam agrupadas e enviadas em um conjunto representando múltiplos destinos.

-Políticas : o administrador pode implementar políticas locais, podendo configurar os roteadores BGP para que haja a distinção das rotas usadas pelas estações de um AS.

Em resumo, o sistema foi projetado para gerenciar uma tabela gigantesca de roteamento, a exemplo da Internet, que se caracteriza por ser um ambiente heterogêneo que não é controlado por uma organização.

5. Operações básicas

A função de um sistema utilizando o BGP é trocar dados que indiquem a possibilidade de conexão com outros sistemas BGP. Tais informações podem incluir uma lista de sistemas autônomos (AS) e as rotas para alcançá-los.

Assim, os sistemas BGP mantém tabelas de roteamento, transmitem atualizações de rotas, etc.

É importante salientar que o BGP não seleciona a rota tendo como base diminuir sua métrica, como assim fazem alguns protocolos (exemplos: OSPF e RIP).

As características BGP de cada link são obtidas a partir de vários fatores, por exemplo: estabilidade, velocidade e atraso. Essas características resultam em um valor, que é utilizado para determinar a melhor rota para um destino.

Quando um roteador é conectado a uma rede, as tabelas de roteamento são obtidas. Depois, as atualizações de roteamento são intercambiadas com a recepção de mensagens "updates".

O BGP não necessita de uma atualização periódica da tabela de roteamento. Apesar de manter informações contendo todas as rotas possíveis em uma rede, o BGP apenas anuncia as rotas primárias nas mensagens.

6. Funções

As atividades principais são:

1) Recepção e filtragem de rotas

Um sistema BGP irá receber anúncios de rotas a partir de outros roteadores, mas tais informações podem ser filtradas (exemplo: rotas circulares).

2) Seleção de rotas

Um roteador pode receber vários anuncios para um mesmo AS, mas deve escolher o melhor caminho, e então adicionar o mesmo na própria tabela de roteamento.

Normalmente irá escolher o caminho mais curto, mas as políticas de decisão orientarão a escolha.

3) Envio de mensagens

Um roteador BGP recebe várias mensagens, mas o protocolo também determina o envio de informações para os roteadores adjacentes. As políticas de decisão, novamente, contribuirão para o envio de rotas por parte de um sistema BGP.

7. Tipos de roteamento BGP

Cada roteador BGP mantém uma tabela de roteamento que lista todos os caminhos para uma rede particular.

Existem três tipos de roteamento:

1) Roteamento inter-autônomo

É o encaminhamento de pacotes entre dois roteadores BGP em diferentes AS, para manter uma consistente imagem da topologia da rede.

A Internet utiliza este tipo de roteamento, pois é composta de vários domínios administrativos, com rotas otimizadas para interligar os vários AS.

2) Roteamento intra-autônomo

Isso ocorre entre dois ou mais roteadores BGP localizados dentro de um mesmo AS.

Qualquer organização pode usar o BGP para localizar as melhores rotas dentro de um mesmo domínio administrativo.

3) Roteamento de passagem

Ocorre quando o tráfego entre dois roteadores BGP passa por um sistema que não usa o protocolo mencionado.

O BGP deve interagir com esse protocolo, para que o tráfego seja transportado com sucesso dentro do sistema autônomo.

8. Políticas de roteamento

As políticas de roteamento não são parte do protocolo, mas determinam critérios para escolher as rotas, dentre múltiplas alternativas.

O fluxo de informação pode ser descrito em cinco passos:

-Recebimento das rotas a partir de outros sistemas
-Política de entrada, para filtrar as rotas ou alterar tais atributos
-Processo de decisão
-Política de saída, para modificar tais atributos
-Anúncio das rotas escolhidas pelo roteador BGP

Os roteadores BGP trocam informações detalhadas sobre as rotas, além da distância entre os domínios.

9. Operação do BGP

O BGP usa um conjunto de critérios para selecionar as rotas que farão parte da tabela de roteamento.

-Selecionar a rota com o maior significado administrativo

Cada rota consiste em um número de rede, uma lista de sistemas autônomos pelas quais a informação deve passar, e atributos da rota.

Estas informações podem ser usadas para construir um gráfico de conectividade entre sistemas autônomos, evitando rotas circulares e enfatizando as rotas que são passíveis de definição em uma política de roteamento.

10. Formato

1) Header

As mensagens BGP usam um cabeçalho básico. Enquanto a mensagem keep-alive carrega somente o header, as outras têm campos adicionais.

O header é composto por 4 campos:

1) Marcador : contém um indicador de autenticação
2) Comprimento : quantos bytes de informação a mensagem contém
3) Tipo : indica uma das quatro categorias existentes de mensagens.
4) Dados : campo opcional, pode carregar informações provenientes das camadas superiores.

11. Mensagens

1) Open

Quando um sistema BGP precisa estabelecer uma conexão com um outro roteador BGP, uma mensagem 'Open' é encaminhada, permitindo a identificação e a autenticação do mesmo.

Se a requisição for aceita, uma mensagem 'Keepalive' é retornada. Assim, é possível intercambiar informações através de 'updates' e notificações.

Há seis campos nesta mensagem: versão, sistema autônomo, tempo de espera, identificador do BGP, comprimento dos parâmetros opcionais e parâmetros opcionais.

2) Update

Uma mensagem 'Update' é utilizada para anunciar uma rota para um destino. Pode ser usada também para cancelar uma rota já informada.

A mensagem contém cinco campos: comprimento das rotas canceladas, rotas removidas, comprimento dos parâmetros da rota, parâmetros da rota e informação sobre a camada de rede.

3) Notification

Esta mensagem indica a ocorrência de um erro (de uma mensagem ou o fechamento da sessão).

Há três campos :

-Código do Erro

-Subcódigo do erro

-Informações sobre o erro

4) Keepalive

Indica que um sistema BGP está em operação, mas não existe informação a ser emitida. A mensagem não contém campos adicionais.

12. Atributos

Atualmente, cinco atributos são definidos:

1) Origem

Pode assumir um dos três valores : EGP, IGP ou incompleto.

O IGP significa que a rede é parte de um AS.

O IGP tem prioridade, pois as rotas EGP podem falhar em caso de roteamentos circulares. O incompleto significa que outros protocolos foram utilizados.

2) Caminho do AS

Contém a lista dos AS existentes até o destino.

3) Próximo salto

Indica o endereço do roteador que deve ser usado para as redes indicadas na mensagem "update".

4) Inalcançável

Indica que a rota não é mais possível de ser atingida.

5) Métrica inter-autônoma

É uma informação usada pelos roteadores externos ao AS para escolher a melhor rota até uma estação no sistema autônomo.

13. Desvantagens

Em um sistema relativamente simples, é melhor usar uma rota padrão a utilizar o BGP, especialmente se há apenas uma conexão à Internet.

Caso contrário, haverá um aumento de tráfego considerável apenas para obter a tabela de roteamento, além das notificações das mudanças.

14. Conclusão

O padrão BGP continua a evoluir. Uma versão futura do BGP possibilitará o agrupamento de rotas similares em apenas uma única rota.

Apesar da relativa simplicidade do protocolo, pode-se atestar a grande eficácia do mesmo, possibilitando a operação das rotas que compõem as milhares de redes que são conectadas via Internet.

13. FRAME RELAY

1. Introdução

A confiabilidade inegável do padrão X.25 resulta também em um efeito não propriamente ignorável : uma quantidade relativamente alta de overhead nos dados transmitidos, justificável nos primórdios da comunicação de dados, onde a taxa de erros era considerável.

Apesar de ser considerado uma evolução do padrão X.25, o Frame Relay difere quanto ao formato dos pacotes e à funcionalidade. É um protocolo com menos informações de controle, sendo mais eficiente e com um maior desempenho.

É considerado bom para as aplicações que requerem picos de transmissão, mesmo em redes dispersas, existindo ainda interoperabilidade entre as diversas implementações.

O Frame Relay proporciona capacidades de roteamento de pacotes, usadas para interligar equipamentos de destino (DTE). Entre os mesmos, os equipamentos de rede são descritos como sendo DCE (Data Circuit Equipment).

Características básicas :

-Orientado a circuito.

-Verificação limitada de erros, evitando um overhead excessivo.

-Pode prover circuitos virtuais múltiplos, a partir de uma interface física.

-Conexão através de circuitos síncronos.

2. Vantagens

-Altas velocidades (até 44.7 Mbps)

-Conectividade múltipla : qualquer dispositivo conectado em um Frame Relay pode comunicar-se com um outro equipamento da mesma rede, através da programação de um PVC.

-Baixo atraso

-Alta vazão de dados

-Gerenciamento simplificado da rede

-Transparência de protocolos

-CNM : permite a obtenção de informações de gerenciamento através de consultas via SNMP (falhas, configuração e desempenho).

-Combina as vantagens das linhas privativas com o transporte de pacotes e circuitos.

-O Frame Relay provê uma alta banda de passagem, através de sistemas digitais de transmissão.

-As rotas de comunicação entre dois pontos da rede são alteradas dinamicamente, de acordo com o tráfego.

-A multiplexação estatística do Frame Relay faz com que seja possível a utilização do mesmo em canais TDM (Time-Division-Multiplexing).

3. Histórico

Originalmente, foi desenvolvido para ser utilizado entre sistemas ISDN. Em 1984, projetos iniciais foram submetidos à apreciação do ITU-T (International Telecommunication Union Telecommunication Standardization Sector).

Em 1990, existiram grandes avanços no padrão, devido ao ANSI (American National Standards Institute). As melhorias ocorreram basicamente no espectro das capacidades de operação em ambientes complexos.

Usualmente, uma conexão utilizava uma linha digital com uma banda passante de 56 Kbps ou 64 Kbps. Algumas instalações usavam até os 30 canais disponíveis em uma linha E1.

O Frame Relay assume que a rede de transporte é relativamente confiável e que os erros serão corrigidos pelas camadas superiores dos protocolos de rede, além do controle de fluxo. Assim, é bem mais simples do que o X.25 e pode atingir maiores velocidades de conexão, até 44.7 Mbps.

Historicamente, o frame relay pode ser descrito também como sendo um tipo primitivo de VPN, devido ao particionamento lógico de tráfego na camada 2.

4. Tecnologia

Um sistema frame relay é composto por vários módulos, a saber:

1) A rede : Frame relay utiliza PVCs (Permanent Virtual Connection) para estabelecer a comunicação entre dois pontos.

Um PVC pode ser descrito como um canal lógico de uma porta do serviço para outra porta, sendo orientado à conexão.

É possível selecionar um CIR (Committed Information Rates) para cada PVC, e significa uma banda de passagem garantida.

2) O link de acesso : provê um meio de acessar a rede, conectando os equipamentos do usuário à porta do sistema propriamente dito.

3) Portas : são pontos físicos de acesso para os PVCs e possibilitam a alocação de banda de passagem para as aplicações.

4) DLCI (Data Link Connection Identifier): para cada extremidade de um PVC é designado um DLCI, que identifica o DTE associado (roteador, multiplexador, etc.)

5. Formato do quadro

No Frame Relay, o quadro é delimitado pelos campos denominados "flags".

A seguir, dois bytes informam um endereço. Dez bits destes dois bytes indicam o DLCI (Data Link Connection Identifier), a conexão lógica que é multiplexada no canal físico.

No fim de cada DLCI, está o bit de EA (Extended Address). Se for 1, o byte corrente é o último do DLCI. O bit C/R não é atualmente mais usado.

Três bits do DLCI proporcionam o controle de congestionamento.

O campo FECN (Forward Explicit Congestion Notification) tem o valor 1, se houve congestionamento no transporte do quadro, a partir da origem para o destino.

O BECN (Backward Explicit Congestion Notification) também tem o valor 1, se acontecer problemas de congestionamento no sentido do destino para o origem.

O bit DE (Descard Eligibility) é ativado se o quadro tem uma importância relativamente baixa, podendo ser até descartado pela rede.

6. DLC

Um fluxo de dados individual é conhecido como DLC (Data Link Connection), tendo em vista uma conexão entre dois pontos.

Em redes maiores, vários links podem conectar dois roteadores, para aumentar a redundância entre os mesmos.

Mas cada roteador deve ter uma linha DLC especial, para conexão com a rede frame relay em si. Esta conexão é chamada de LMI (Local Management Interface).

7. Tratamento de problemas

O Frame Relay inclui um algoritmo CRC (Cyclic Redundancy Check) para detecção de erros, mas não inclui qualquer mecanismo para corrigi-los.

O quadro com problemas (CRC, DLCI inválido, etc.) é simplesmente descartado.

Outra diferença para o X.25 é a ausência de controles de fluxo por circuito, essa tarefa é repassada para as camadas de ordem superior.

O Frame Relay contém um mecanismo relativamente simples para notificação de congestionamentos, que podem ser causados quando os usuários excedem o CIR (Committed Information Rate) ou quando as operações de roteamento dinâmico são executadas.

8. Parâmetros principais

O Frame Relay suporta PVCs e SVCs, utilizando as seguintes primitivas :

1) Procedimento de chamada
2) Conexão
3) Estabelecimento da chamada
4) Desconexão
5) Término da conexão

Para cada PVC, é associado um nível de serviço específico. Os parâmetros utilizados para mensurar a qualidade de serviço prestado por cada PVC incluem:

1) CIR : Committed Information Rate (banda passante garantida, que a rede deve suportar)
2) Tc : tempo de observação
3) Bc : Bits a serem transmitidos no tempo de observação (máximo)
4) Be : número de bits a serem transmitidos no tempo de observação (em excesso ao parâmetro Bc).

Além disso, um SLA (Service Level Agreements) pode estar envolvido, resultando na verificação dos seguintes parâmetros :

5) FTD (Frame Transfer Delay) : o tempo necessário para encaminhar um quadro entre dois pontos de um PVC.

6) FDR (Frame Delivery Ratio) : indica a razão entre os pacotes recebidos com sucesso e as tentativas de envio de pacotes.

7) DDR (Data Delivery Ratio) : é a razão entre os dados recebidos com sucesso e as tentativas de transmissão de dados.

8) MTBF (Mean Time Between Failures) e o MTTR (Mean Time To Repair)

9. LMI

As extensões realizadas no padrão Frame Relay original são denominadas coletivamente sob a sigla LMI (Local Management Interface). Inclui extensões para facilitar o gerenciamento de redes complexas e grandes, podendo estar interligadas.

Por exemplo, as quedas dos enlaces Frame Relay podem ser indicadas através de procedimentos LMI ou pelos alarmes transportados através do SNMP (Simple Network Management Protocol).

Nestas condições, a rede pode ser reprogramada para desviar o tráfego para um outro link através de um roteamento dinâmico, no caso do SVC, ou estático (PVC).

Existem as extensões LMI comuns, que são adotadas por todos os implementadores, e também as opcionais. São utilizadas para as seguintes funções:

1) Mensagens sobre o estado dos circuitos virtuais

Provê a sincronização entre o usuário e a rede, indicando em tempos regulares a adição e a exclusão de PVCs, além de informar a integridade dos circuitos.

2) Multicasting

Permite a um enviador encaminhar um único quadro à rede, que será recebido por múltiplas estações.

3) Endereçamento global

Isto faz com que uma conexão tenha identificadores globais, ao invés de possuir significância apenas local, podendo ser localizado em uma rede Frame Relay.

4) Controle de fluxo simples

Provê um mecanismo de controle de fluxo tipo Xon/Xoff a uma interface específica. É indicado para os protocolos de comunicação cujas camadas de controle não podem usar os bits de notificação de congestionamento.

10. Multicasting

O multicasting é um recurso opcional do LMI. Grupos são designados por uma série de valores DLCI reservados.

Os quadros usam um valor reservado que são replicados pelo sistema, até atingir todas as extremidades da rede.

As mensagens LMI para multicasting também notificam os usuários da alteração dos grupos.

O multicasting DLCI é útil em uma rede com roteamento dinâmico, pois as informações sobre as rotas podem ser distribuídas para vários roteadores, ou apenas para um grupo deles.

É utilizado também para os procedimentos de resolução de endereço, que podem ser encaminhados para várias estações de um modo simultâneo.

11. Endereçamento global

As especificações básicas do Frame Relay suportam apenas valores no campo DLCI que identificam PVCs locais.

Não há endereços que identifiquem interfaces de rede, ou nós conectados a estas interfaces. Assim, não podem ser descobertos por técnicas de resolução de endereço.

Isso significa que mapas estáticos devem ser criados, para indicar quais DLCIs devem ser empregados para encontrar um dispositivo remoto.

O endereçamento global permite a identificação de nós, e os valores existentes nos DLCIs passam a ter significado de endereçamento.

Isto permite um roteamento adaptativo em redes complexas.

12. Formato da mensagem LMI

As mensagens LMI são enviadas em quadros contendo DLCIs específicos.

O cabeçalho é o mesmo existente nos quadros normais. A mensagem inicia-se com quatro bytes obrigatórios e um número váriável de IEs (Information Elements).

Cada IE consiste em um identificador de um único byte, o comprimento do campo e os bytes representando a informação em si.

Há dois tipos de mensagens :

Mensagens de estado e mensagens de solicitação de estado (exemplos : "keepalives" e estado de PVCs)

Estas informações são críticas em um ambiente com roteamento dinâmico, pois os algoritmos decidem as rotas com base na integridade dos links.

13. Conclusão

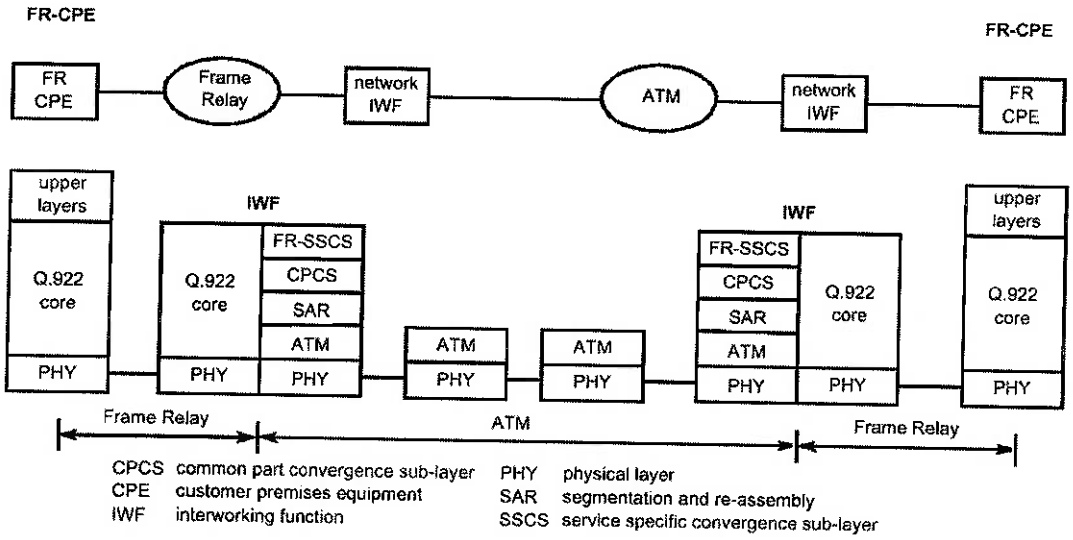

Figura 11 – Interoperabilidade entre o Frame Relay e o ATM

Historicamente, o Frame Relay pode ser descrito como uma tecnologia de transição para o ATM, que tem maiores recursos de gerenciamento, qualidade de serviço (QoS) e flexibilidade de operação.

14. ANÁLISE DAS TENDÊNCIAS FUTURAS

No universo da Tecnologia da Informação, pode-se claramente envisionar três grupos distintos:

1) Software
2) Hardware
3) Redes

Nas próximas partes, um breve histórico desses grupos será apresentado, além de projetar uma visão a respeito dessas tecnologias, à luz das diretrizes atuais.

1. Software

O software pode ser descrito, de uma forma genérica, como uma sucessão de dígitos binários produzidos por um compilador, se a linguagem for de alto nível, ou um montador, no caso de código assembler, cujos resultados são interpretados pelo conjunto de instruções implementado no processador em questão.

A linguagem C se destacou rapidamente, devido à eficiência do código gerado pelos compiladores. O surgimento da linguagem C++ representou um grande avanço em termos de linguagens de programação, combinando uma eficiência relativamente alta com a possibilidade de desacoplamento dos módulos que representam os objetos do sistema.

Outras linguagens importantes incluem : Java e Pascal.

Na parte dos sistemas operacionais, um marco foi a criação do Unix, em meados dos anos 1970, existindo muitas variações até o surgimento do Linux, em 1992.

O desenvolvimento do Windows XP trouxe mais estabilidade a uma classe de software muito popular.

Os bancos de dados ganharam uma contribuição muito determinante, com a desenvolvimento da linguagem SQL.

Entretanto, a Internet pode ser considerada uma das maiores invenções da História, sendo mais utilizada a partir de 1995.

2. Software para dispositivos portáteis

No campo dos dispositivos portáteis, não existe ainda uma predominância clara quanto às tendências deste campo, mas há três forças atuantes neste cenário:

a) PalmOS

Este sistema pioneiro combina uma facilidade de uso com aplicativos de uso geral, pavimentando a trilha dos computadores portáteis.

b) Symbian

Representa um esforço conjunto para criar uma sistema operacional para os telefones celulares, e atualmente encontra-se em um estágio de desenvolvimento.

c) Outras tecnologias

O Pocket PC foi otimizado para o processador ARM, apresentando muitos recursos relacionados a aplicações multimídia e também extensões de aplicativos de produtividade.

Provavelmente, devido à grande flexibilidade proporcionada pelas ferramentas de programação disponíveis, deve representar o futuro dos dispositivos portáteis pelos próximos anos.

3. Software de simulação

Uma classe de software está recebendo uma grande ênfase nas pesquisas, que são os sistemas de realidade virtual.

Normalmente, o processo para a renderização desses ambientes simulados segue os seguintes passos:

1) O ambiente 3-D a ser emulado é dividido em partes atômicas (espaços tridimensionais cujas superfícies podem ser renderizadas sem que se leve em consideração o cálculo de outras superfícies oclusivas ao espaço de visão do observador virtual).

2) As partes atômicas são representadas como sendo os nós de uma árvore BSP (Binary Space Partitioned), que indica a correta ordem de renderização das superfícies que compõem o ambiente a ser simulado.

3) De acordo com a posição espacial do observador, a árvore é percorrida transversalmente, podendo-se criar tais simulações com a utilização de bibliotecas gráficas, a exemplo do OpenGL (Open Graphics Library).

Esse algoritmo é adequado para a construção de ambientes estáticos, pois a árvore BSP deve ser construída por um outro processo em separado, antes do tempo de execução.

Para se criar uma ilusão da realidade, o processo acima mencionado deve ocorrer a pelo menos 60 vezes por segundo, diferentemente dos 30 fps (frames per second) que normalmente se atribuem aos sistemas de vídeo NTSC.

4. Previsões

As tecnologias Linux, .NET e Web services estão guiando a maioria dos novos projetos de software da atualidade, juntamente com os sistemas de e-learning.

O UML está se consolidando como o principal meio de informar aos desenvolvedores de programas de computador a estrutura do software em questão, sendo que as extensões para tempo real possibilitam também a modelagem de sistemas críticos à passagem temporal.

Com o desenvolvimento de sistemas neurais e agrupamentos de computadores com uma capacidade que já ultrapassa dezenas de Teraflops, somada a uma evolução exponencial, torna-se possível a geração automática de código, a partir dos diagramas UML.

Provavelmente, a evolução do software seguirá um caminho rumo à automação, sendo que não é impossível que no limite uma fração da construção de sistemas possa se resumir na correta escolha de componentes de software pré-programados.

5. Hardware

Nesta parte, o avanço tende a ser o mais previsível dentre os três grupos principais: a "Lei de Moore" rege a evolução dos microprocessadores há muitos anos, atualmente significando que a quantidade de transistores em um processador dobra a cada dezoito meses.

6. Microprocessadores

Pode-se afirmar que o ponto inicial e simbólico para a microinformática foi a invenção do microprocessador, pela Intel.

O processador 4004 continha cerca de 2300 transistores, a um clock de 740 KHz.

A série 8080/Z80/8085 praticamente formou uma geração de engenheiros, combinando um ISA eficiente com uma alta velocidade.

Os processadores 6502 e a série 68000 também contribuíram para muitas classes de máquinas extremamente bem construídas.

Nesse ínterim, surgiram grandes arquiteturas de microprocessadores : o SPARC, o PowerPC, a série Alpha e o MIPS, que permaneceram mais no segmento dos servidores em geral.

Entretanto, a criação do processador Pentium representou um marco na história da tecnologia da informação, com novos sucessores que praticamente dominam o cenário da informática desde então.

A arquitetura atual alcança nos tempos atuais uma freqüência de clock de 3.0 GHz, com a possibilidade de virtualização de um processador extra.

Isso mantém os pipelines do processador mais ocupados, aumentando o fluxo de informações. Em especificações técnicas, tal arquitetura possibilita o aumento da freqüência do relógio central até cerca de 10 GHz.

Assim, é possível afirmar que a necessidade de um maior poder de processamento não é mais uma grande prioridade, com a exceção de aplicações que demandam uma quantidade altíssima de cálculos de simulação, a saber: realidade virtual, sistemas multimídia com o cálculo de milhões de polígonos texturalmente renderizados, etc.

Os discos rígidos atingem cerca de 160 GB por dispositivo, sendo que no futuro capacidades na ordem de Terabytes serão comuns.

O grande desafio será a construção de sistemas de memória RAM com baixas latências, sendo que a DDR 400 tem a maior velocidade atual.

Os sistemas de vídeo estão tornando-se tão complexos quanto a própria CPU, sendo que o subsistema de maior desempenho atinge cerca de 300 milhões de polígonos por segundo.

Pode-se afirmar que a tendência atual é a construção de sistemas massivamente paralelos, com milhares de processadores, provendo serviços de alcance global, por meio da Internet.

7. Hardware para dispositivos portáteis

No início, os computadores portáteis continham processadores com versões especiais para não consumir energia elétrica em demasia, em comparação com os sistemas desktop.

No campo da arquitetura x86, foi anunciado um processador que apresentava um baixo consumo de energia, com tecnologia VLIW, mas o desempenho não foi considerado excepcional.

Várias arquiteturas existiam nos primórdios desse segmento da tecnologia da informação, a saber: a série SH, o ARM e o MIPS.

Atualmente, a arquitetura ARM apresenta a melhor razão entre o desempenho e o consumo de potência, sendo que provavelmente será o microprocessador mais utilizado para tais equipamentos.

8. Previsões

Não se descarta a possibilidade de um sistema portátil vir a ser o dispositivo a ser rotineiramente utilizado nas atividades mais comuns dos trabalhadores do conhecimento, visto que a barreira dos 500 MHz representa a quantidade de processamento que torna a operação das ferramentas de produtividade um tanto quanto suficiente.

Atualmente, o processador mais rápido para dispositivos portáteis atinge cerca de 400 MHz, normalmente equipado com 128 MB de RAM.

Uma alternativa é a utilização da plataforma Tablet PC, que se caracteriza pelo uso de uma caneta especial para a entrada primária de informações.

9. Redes

O desenvolvimento deste setor segue um padrão menos regular do que a evolução dos processadores, mas provavelmente os links ópticos terão uma capacidade de dezenas de Terabits por segundo.

Os telefones celulares terão capacidade multimídia, sendo uma versão reduzida dos computadores portáteis atuais, com uma ênfase maior nos aplicativos de interatividade remota.

Se os problemas de capilaridade e QoS forem definitivamente solucionados, não é impossível que o sistema CATV entre em declínio, sendo então utilizado o protocolo IP.

Em um futuro muito distante, os sistemas VoIP provavelmente substituirão a rede PSTN, fazendo com que as chamadas de longa distância possam ser realizadas sem maiores restrições quanto ao tempo de conversação em si.

15. CONCLUSÃO

1. Objetivos

O objetivo deste trabalho foi descrever as principais partes que formam as tecnologias de rede atuais, para auxiliar no desenvolvimento de uma visão geral das formas de comunicação digital mais comumente utilizadas.

Ou seja, este trabalho procurou descrever, em linhas gerais, a evolução ocorrida nos grandes grupos que formam a Tecnologia da Informação, com a óbvia ênfase à parte relativa às redes de computadores.

Em última instância, o conhecimento das bases tecnológicas torna-se um fator importante para a criação de sofisticadas soluções sistêmicas, que provavelmente permearão a maioria das atividades humanas do futuro.

2. Extrapolações

Ray Kurzweil, notório cientista famoso por prever com relativa precisão certos eventos relacionados com o progresso dos computadores, conseguiu envisionar, com um ano de erro, a vitória de um supercomputador (Deep Blue, da IBM) sobre um oponente humano, mas que é considerado um dos maiores mestres de xadrez de todos os tempos : Garry Kasparov.

Essa previsão, por si só, seria aliviadora se se circundasse apenas nesse evento isolado; entretanto, o mesmo cientista previu uma série de acontecimentos baseados na evolução do poder de processamento dos computadores.

3. Modelamento matemático

O cérebro contém cerca de 100 bilhões de neurônios, em média contendo 1000 conexões com neurônios adjacentes. Cada neurônio é capaz de executar cerca de 200

cálculos por segundo. Com 100 trilhões de conexões a 200 comutações a cada segundo, é possível conseguir 20 milhões de bilhões de cálculos por segundo.

Atualmente, o sistema mais rápido existente (o Earth Simulator) consegue atingir uma velocidade de 35 Teraflops.

A previsão é que os mais potentes supercomputadores do mundo consigam atingir a velocidade de 20 milhões de bilhões de cálculos por segundo em 2010.

Segundo a Lei de Moore, os computadores pessoais atingirão tal velocidade uma década depois.

4. Teste de Turing

O teste de Turing é atribuído a um matemático inglês, que por volta de 1950 criou um método subjetivo para avaliar a "inteligência" dos computadores, que consiste em um operador humano interagir, por meio de um terminal, com uma máquina.

Se a operador for iludido a ponto de concluir que o interlocutor é um outro humano, então não haveria como negar a inteligência da máquina. Um interessante corolário a respeito desse teste é a capacidade do sistema emitir falsos julgamentos, para no mínimo evitar as óbvias perguntas a despeito da natureza física da entidade sendo então avaliada.

O teste de Turing provavelmente será atingido por volta de 2029, com o compartilhamento massivo de gigantescos bancos de dados.

Se esse exame for vencido, não é impossível que a inteligência dos supercomputadores, devido à sua evolução exponencial, possa superar o raciocínio humano.

5. Análise final

Em um futuro muito distante, e espera-se que isso não aconteça, os computadores provavelmente estarão em todos os lugares que tenham a presença humana, e muitos poucos eventos deixarão de ter seus rastros armazenados em algum sistema.

Se os computadores quânticos se desenvolverem, cerca de 1000 qu-bits proporcionarão cerca de 10^{342} cálculos por segundo.

No limite teórico e improvável, será possível reconstruir quase que na integridade os atos e as experiências cometidas por um humano em particular, não sendo impossível extrair as diretrizes que regem tais comportamentos, podendo-se calcular, com base nas leis dos grandes números, os prováveis atos futuros associados aos mesmos.

Apesar de algumas previsões catastrofistas a despeito da evolução da Tecnologia da Informação, o autor não compartilha de tais previsões, tendo uma visão muito mais complementista das atividades humanas, e não um ponto de vista estritamente concorrencial.

LISTA DE REFERÊNCIAS

[1] "BEOWULF: A Parallel Workstation for Scientific Computation", Donald J. Becker et al, Proc International Conference on Parallel Processing, 95.

[2] "Communication Overhead for Space Science Applications on the Beowulf Parallel Workstation", Donald J. Becker et al. Proc High Performance and Distributed Computing, 1995.

[3] "A Design Study of Alternative Network Topologies for the Beowulf Parallel Workstation", Chance Reschke et al, Proc High Performance and Distributed Computing, 1996.

[4] "Beowulf Supercomputer Howto Draft", J. Radajewski, 1998.

[5] Ralph D T and Shephard C G: 'Services via mobility portals', BT Technology J, 19, No 1, pp 88—99 (January 2001).

[6] Haardt M. and Mohr W., "The Complete Solution for Third-Generation Wireless"

[7] "Evolution of Mobile Cellular Communication Systems", Dr.Monira A.Abu El-Ata ,17th National Radio Science Conference, NRSC'2000

[8] "The MD5 Message-Digest Algorithm", IETF RFC 1321, Apr,1992.

[9] G. Banavar et al., "Challenges: An Application Model for Pervasive Computing," in Proc. MobiCom'2000, August 2000

[10] OMG, UML Specification. OMG document formal/2000-03-01, March 2000.

[11] Smith, Clint & Collins, Daniel. (2001). 3G Wireless Networks Tata McGraw-Hill TELECOM.

[12] Telcordia Technologies (2001). (Online Paper). Wireless Network Migration from 2G to 3G Technology.

[13] Maarouf, M. (2001). Wireless LAN: The Next Killer Application (Research Brief). Gartner,Inc.

[14] Geier, J. (1999), Wireless LANS: Implementing Interoperable Networks (Macmillan Technical Publishing, Indianapolis, IN).

[15] LAN MAN Standards Committee of the IEEE Computer Society, High-Speed Physical Layer Extension in the 2.4 GHz Band, ANSI/IEEE Std 802.11b, 1999.

[16] Oren Eliezer, Evaluation of Coexistence Performance, IEEE 802.15-01/091, January 2001.

[17] Wireless LAN Security White Paper

[18] Bluetooth White paper, "Bluetooth Security Architecture," Version 1.0.

[19] IEEE Standards Board, "802 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications."

[20] Multi–Protocol Over ATM — Version 1.0, ATM Forum, July 1997.

[21] "Cisco Documentation", 2000.

[22] J Moy, OSPF version 2, April 1998, Internet Engineering Task Force, RFC2328.

[23] M Laubach and J Halpern, Classical IP and ARP over ATM, April 1998, Internet Engineering Task Force, RFC2225.

[24] ITU-T Recommendation I.356, "B-ISDN ATM layer cell transfer performance," 1993.

[25] General DataComm, "A Management Briefing on Adapting Voice For ATM Networks: An AAL2 Tutorial"

[26] ITU-T Recommendation I.361 - B-ISDN ATM Layer specification.

[27] C. Partridge. Gigabit Networking. Addison Wesley, October 1993.

[28] Internet sources : search engine results (2002)

[29] Brown T S et al: 'Broadband transport — the synchronous digital hierarchy', BT Technol J, 16, (January 1998).

[30] ITU-T Recommendation I.555: 'Frame Relay Bearer Service Interworking', Com 13 R2-E (July 1994).

[31] Frame Relay Forum: 'Frame Relay/ATM PVC Network Interworking Implementation Agreement, FRF.5', (20 December 1994).

[32] IEEE Std 802.3z-1998, "Media Access Control (MAC) Parameters, Physical Layer, Repeater and Management Parameters for 1000 Mbps Operation,"

[33] R. Perlman. Fault-Tolerant Broadcast of Routing Information. Computer Networks

[34] Ray Kurzweil. The Age of Spiritual Machines. Penguin Books.