Núcleo de Computação Eletrônica - UFRJ
Position Paper - Abril de 1996

Carlos Eduardo Mendes de Azevedo

Caixa Postal 2324
Cidade Universitária - Ilha do Fundão
Rio de Janeiro - RJ
CEP 20001-970
e-mail: carlos@nce.ufrj.br

1. Introdução

O Núcleo de Computação Eletrônica é o centro de computação da Universidade Federal do Rio de Janeiro. Tem três áreas básicas de atuação: apoio a área acadêmica, definição e confecção de sistemas de informação e pesquisa na área de informática. Possui uma rede local cuja finalidade é o atendimento a pesquisadores, estudantes, professores e também a tarefas administrativas.

Esta rede é composta de estações de trabalho UNIX, de diferentes fabricantes, e de PC compatíveis. Também existem laboratórios públicos e outros específicos. Brevemente serão instalados novos equipamentos de rede utilizando tecnologia FDDI e ATM, permitindo um ambiente integrado para pesquisa, educação e administração, com o uso das mais novas e recentes aplicações distribuídas e multimídia.

Além disso, o NCE é o órgão da UFRJ responsável pela criação e manutencão do backbone da Universidade, bem como pelo apoio e suporte às demais unidades para permitir que elas se conectem e possam usufruir dos serviços em rede. O NCE tembém abriga o Centro de Operações da RedeRio, Rede Acadêmica Regional do Rio de Janeiro, que atualmente interliga mais de 40 instituições. O Centro de Operações é responsável pelo controle e gerência de toda a RedeRio.

2. Visão Geral da Rede NCE

A figura 1 mostra esquematicamente a rede local do NCE, com os clusters de workstations UNIX, laboratórios e microcomputadores pessoais. A rede existe desde 1990 e ainda é composta de equipamentos que não suportam SNMP, o que dificulta bastante o seu gerenciamento. No entanto, está prevista uma modificação de cabeamento e de equipamentos ainda no 1o. semestre de 1996.

O "backbone" da rede local NCE é atualmente baseada em cabo fino, e a este backbone se ligam as sub-redes dos laboratórios e dos "clusters" de estações de trabalho existentes. O cluster

“Pesquisa” suporta praticamente todos os serviços de rede, embora estejamos hoje procurando distribuir melhor estes serviços entre os demais.

Ligados ao backbone também estão aproximadamente 150 PCs, que se conectam a servidores Novell (3.12) e aos clusters UNIX. Na verdade, existem várias sub-redes IP em um mesmo cabo físico, implementado por um roteador Cisco. Isto leva a algumas ineficiencias de tráfego, mas foi a única solução encontrada na época da confecção da rede e com os equipamentos disponíveis.

Para o 1o. semestre de 96 está prevista a mudança de cabeamento para par trançado e o uso de switches para uma segmentação da rede. Além disso, mais servidores Novell também serão acrescentados e estes serão usados também como roteadores IP para permitir uma melhor segmentação interna.

Em termos de ambiente UNIX, os clusters são formados por Sun Sparcs e RISC/6000. Além da heterogeneidade de hardware, existe também a de software, com uma co-existencia de SunOS, Solaris, AIX 3 e AIX 4, bem como algumas máquinas com Linux.

A rede local do NCE atende cerca de 300 usuários fixos, do próprio NCE, e um número flutuante de usuários em torno de 1000, proveniente do uso dos laboratórios e dos clusters especializados.

Como dito anteriormente, a rede do NCE deve sofrer uma atualização para se tornar uma rede de alto desempenho ainda no primeiro semestre de 1996. Como pontos básicos, podemos destacar a mudança de cabeamento de cabo coaxial fino para par trançado, a substituição do backbone em cabo fino para um backbone colapsado em um switch Ethernet e a colocação de equipamentos que suportem SNMP e RMON, como hubs e roteadores profissionais. A tecnologia usada ainda será Ethernet, mas já no inicio do segundo semestre já teremos estações diretamente conectadas ao backbone FDDI da Universidade, bem como o possivel uso de ATM para o backbone interno do NCE e para alguns pontos especiais que exigirão altas velocidades de conexão, como por exemplo, no uso de videoconferencia e multimídia.

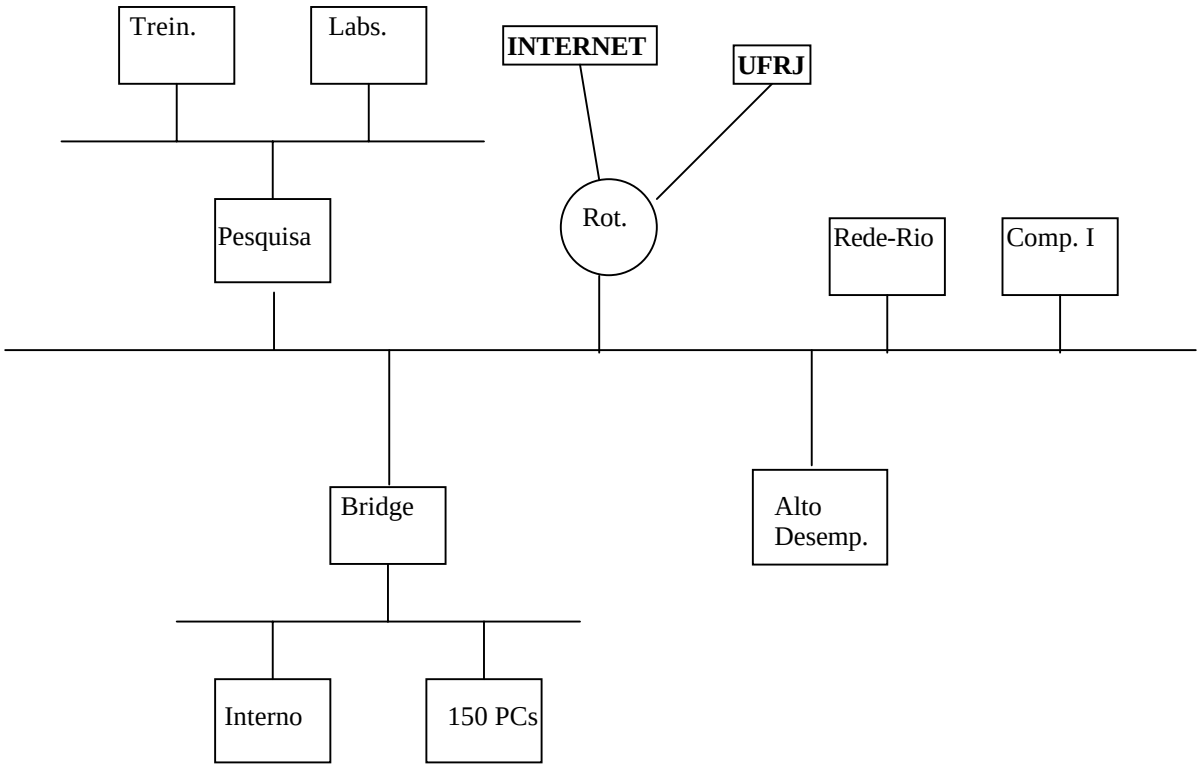

Figura 1

3. Serviços de Rede

Diversos serviços de rede estão disponíveis na rede, implementados em servidores UNIX na sua maioria.

a) Correio Eletrônico

Principal forma de comunicação entre os usuários, independente da plataforma. O serviço está basicamente distribuído nos ambientes servidores UNIX e Novell, sendo o primeiro usado por pessoas de caráter mais técnico e o segundo ambiente por pessoas de perfil mais administrativo. Como a plataforma PC é a mais utilizada, a interface mais comum é o Pegasus Mail, em ambiente DOS e Windows. Ambos os ambientes servidores suportam POP (Post Office Protocol), o que permite a leitura de correio remotamente, através do Eudora (mas que vem sendo substituído na preferencia dos usuários pelo WinPmail e Netscape v2.0). O endereço de todos usuários ainda não está unificado no domínio nce.ufrj.br, mas esta unificação está programada para ainda este semestre, juntamente com um alias (Primeiro-nome)_(Ultimo.nome)@nce.ufrj.br para todos os usuários. Com esta unificação, teremos um servidor de mail único, que receberá centralizadamente todos as mensagens e fará a distribuição para o servidor interno desejado por cada usuário individualmente.

b) Telnet

Usado para acesso aos servidores UNIX e ao mainframe Unisys, de uso administrativo.

c) News

Implementado em um servidor UNIX, com o software innd. A leitura dos artigos é feita geralmente pelo "tin" em ambiente UNIX e pelo Netscape e WinVN no ambiente Windows. Pelo fato de estarmos na ponta de um canal internacional para a Internet, recebemos o News diretamente do exterior e redistribuimos para a RedeRio, de modo a otimizar o tráfego internacional.

d) FTP

O serviço é oferecido em ambiente Novell e principalmente UNIX. Um repositório central, ftp.nce.ufrj.br, é o lugar usado para deixar disponível todos os softwares que são "recolhidos" na Internet, pacotes de aplicativos (shareware ou domínio público) de uso mais geral e documentos.

e) Servidores de listas

Atualmente estão operacionais dois servidores de listas: o listproc e o majordomo. Dependendo das características das listas e de seu tráfego, a lista é colocada no programa servidor mais apropriado para o gerenciamento da respectiva lista. Uma meta é unificar a interface com o usuário, ficando transparente se o servidor é o listproc ou o majordomo. Isso permitirá uma visão "unificada" das listas e até o uso de outros servidores no futuro, mas sem que o usuário perceba a alteração.

f) WWW

Obviamente, existe um servidor WWW, rodando em ambiente UNIX. Utilizamos o NCSA httpd 1.5 e estamos também testando uma modificação para o suporte a SSL, para transações com criptografia (uma aplicação de extrato bancário on-line vem sendo testado nesse ambiente). O serviço WWW no NCE é o ambiente de serviços que tem recebido mais atenção, pois além do uso tradicional de divulgação de informações e serviços através das páginas HTML, tem sido investigado o uso deste ambiente para computação cooperativa, com aplicações distribuídas orientadas a objeto, e como interface padrão para o usuário, em diferentes plataformas, para aplicações cliente-servidor. Uma meta a curto prazo é disponibilizar via WWW todos os procedimentos administrativos do NCE, bem como serviços hoje existentes apenas no mainframe, como acesso a biblioteca, acompanhamento de processos administrativos e sistema de registro de estudantes, entre outros. A gerência administrativa do NCE se dará a partir de um servidor WWW interno, ao qual não se terá acesso a partir de fora do NCE.

g) Nomes

O serviço de nomes utilizado é o DNS (Domain Name System). Em paralelo é utilizado também o NIS, mas apenas para acesso a máquinas dentro de um determinado cluster, não sendo o seu uso incentivado para acesso mais genérico. Todos os equipamentos, sejam PCs, estações de trabalho, servidores e roteadores, têm um nome cadastrado no DNS. O NCE também atua como servidor de nomes primário e secundário para muitas unidades da UFRJ e para muitas instituições da RedeRio.

h) Videoconferência

Um dos serviços que o NCE pretende oferecer em breve é o de videoconferencia. Há algum tempo já estão sendo realizados eventos experimentais, que passarão a ter um caráter mais permanente. A meta é que palestras e eventos realizados no NCE possam ser transmitidos por rede para o resto da UFRJ e para outras instituições. Eventos externos também poderão ser vistos no NCE em ambientes especiais que estão sendo preparados para tal fim, com equipamentos e recursos compatíveis com a demanda que esse tipo de serviço exige. Com o aumento da velocidade do canal internacional para 2Mbps, já criamos um túnel para o Mbone (serviço de videoconferência na Internet), reforçando as experiências que vêm sendo realizadas desde 1994, e estaremos disponibilizando este acesso para o restante da UFRJ e RedeRio.

i) Acesso Remoto

Existe um servidor de comunicações disponível (Cisco 2511) para acesso remoto, via slip ou PPP. O maior limitante deste serviço é a disponibilidade de linhas telefônicas na nossa instituição para esse serviço, o que vem sendo a principal barreira para uma maior expansão desse serviço.

4. Administração de Redes

A administração de redes envolve diversos fatores, cujo objetivo é dar ao usuário uma visão única e consistente dos sistemas e permitir que os serviços de rede funcionem sem problemas.

a) Contas

A política de contas ainda não está completamente implementada. Mas a idéia principal é ter um sistema de contas único, unindo UNIX, Novell e possivelmente Windows NT. Atualmente, no ambiente UNIX, todos os usuários que usam diferentes máquinas e clusters já tem o mesmo nome de conta e uid (<32000), ou seja, o “uid space” está unificado. Contas locais específicas de um sistema tem uid >32000. Ainda há grandes dificuldades na confecção de um sistema de gerenciamento único nos diversos sistemas operacionais. Estamos experimentando alguns sistemas para o gerenciamento no ambiente UNIX, em especial o SPM[1]. A integração dessas contas com o ambiente Novell é bastante importante, mas ainda não encontramos soluções técnicas adequadas, de domínio público. O padrão de diretórios dos usuários no ambiente UNIX tem a forma de /u/home<X>/<usuário>, onde <X> é um número que varia em função do perfil do usuário

b) Sistema de arquivos

É utilizado o NFS, juntamente com automount e NIS para a propagação de mapas (principalmente para passwd, hosts e arquivos de configuracao do automount). Devido aos problemas de segurança associado ao NIS, estamos estudando alternativas de propagação

dos arquivos de mapas. É também utilizado o conceito de mestre/escravo para a instalação e propagação de programas binários na rede, usando o software lfu[2]. Para cada versão de sistema operacional (Solaris, SunOs, AIX 3 etc.) existe uma máquina mestre, onde os originais dos binários são instalados. Periodicamente, sistemas escravos, que residem nos diferentes clusters, copiam do mestre correspondente estes binários, de modo a atuarem como servidor de arquivos dentro de cada cluster. Como regra geral, só há tráfego NFS dentro de cada cluster, tendo apenas como exceção o tráfego entre mestres e escravos. A estrutura de nomes é:

/master/local/<arch> - para os diretórios contendo os binários na máquina mestre

/slave/local/<arch> - para os diretórios contendo cópia dos binários na máquina escrava

e onde <arch> representa o sistema operacional (Solaris,SunOS, AIX, etc.)

Os sistemas dentro dos clusters mapeiam os diretórios usados pelos usuários como links para os diretórios montados via NFS. Por exemplo, um uma máquina rodando Solaris dentro de um cluster, /usr/local/bin é mapeado para /slave/local/solaris/local/bin, acessado via NFS.

Com a previsão de uso mais intenso de Windows NT e Win95, inicia-se também experiencias com o software SAMBA, de modo a permitir compartilhamento de sistemas de arquivos entre UNIX e Windows NT, e também de impressão entre esses ambientes.

c) Segurança

Este aspecto vem ganhando maior importancia a cada dia, em especial nos ambientes UNIX. Toda a rede local do NCE é separado da Internet por uma roteador, que atua como um filtro de pacotes IP, já fornecendo um grau de segurança mínimo. No entanto, como universidade, a demanda por acesso é muito grande e são grandes também as variações de localidades que podem acessar. A implantação de um firewall tradicional é dificil pelas limitações que imporia aos próprios usuários. A questão, portanto de segurança versus facilidade de uso vem sendo discutida bastante, e até o momento implantou-se apenas mecanismos básicos de segurança. Os servidores UNIX tem instalado um "wrapper" para controle de acesso aos principais serviços disponíveis. Apesar de todas as correções de software ainda não estarem instalados em todas as máquinas, optou-se primeiramente pelo aspecto de auditoria para saber pelo menos o que está acontecendo. Em breve, devemos estar testanto softwares que implementem criptografia na rede, como o uso de SSH[3], em substituição ao rlogin, e softwares que implementem OTP (One Time Password), em substituição ao uso tradicional de senhas.

d) Gerenciamento

Este é um dos aspectos que pretendemos dar mais destaque ao longo do ano. O perfil dos equipamentos atualmente instalado não permite o uso de SNMP, o que dificulta bastante o gerenciamento, não permitindo uma visão clara de como anda a rede e onde estão seus gargalos. A aquisição de novos equipamentos e o uso de RMON em pontos estratégicos permitirá a coleta de dados mais precisos. O trabalho atual vem sendo feito através de ferramentas mais simples, como etherfind, nfswatch, netstat, etc. Como meta, pretende-se

coletar estatísticas claras de uso da rede, nos diversos segmentos, como: protocolos usados, serviços IP usados, matriz de tráfego, maiores usuários, erros e colisões na rede física, etc.

e) Roteamento

O protocolo de roteamento utilizado é o RIP, pois é o denominador comum entre os protocolos existentes nos diferentes roteadores utilizados. Os roteadores profissionais, como os Ciscos, suportam vários protocolos de roteamento. No entanto, roteadores "improvisados" como um servidor Novell com duas ou mais placas de rede, ou softwares de domínio público, como KA9Q, suportam basicamente o protocolo RIP, e mesmo assim, nem sempre a implementação suporta todas as opções do protocolo. Como não será possível o uso de roteadores profissionais em toda a nossa rede a curto prazo, o protocolo RIP deverá continuar sendo o denominador comum por algum tempo. A sua troca também não é urgente, pois tem atendido a nossa demanda até o momento. Experimentos com OSPF e RIP-2 estão planejados tão logo a rede de alto desempenho esteja implantada e operacional.

Com o uso de videoconferência e Mbone, o roteamento multicast também passa a ter importância relevante. O uso de DVMRP é o que tem sido usado, por ser o protocolo utilizado no software mrouted. No entanto, experimentos com outros protocolos, como MOSPF e PIM, começam a ser iniciados, bem como sua interoperabilidade com o DVMRP.

f) Helpdesk

Como uma das atividades do NCE é o fornecimento de apoio e suporte aos usuários do NCE e da UFRJ, recebemos inúmeras solicitações de ajuda e consultoria por parte desses usuários. Com o crescimento da rede, cresceram também as solitações de auxílio. Cresceram tanto a ponto de, às vezes, inviabilizar o trabalho, pois ficávamos mais tempo atendendo telefonemas e em reuniões com os usuários do que propriamente na dedicação da solução dos problemas que eles solicitavam. Para tentar contornar o problema, basicamente atacamos em dois pontos: o uso de uma secretária para o atendimento de telefonemas e anotação de recados, e o desenvolvimento de um programa para que os usuários pudessem fazer os seus pedidos através de e-mail. O sistema de e-mail trouxe várias vantagens, tanto para nós quanto para os usuários. Do nosso ponto de vista, o nível de interrupção caiu bastante, os pedidos passaram a ficar registrados automaticamente, permitindo um atendimento mais programado e a distribuição dos pedidos passou a ser automatica, o que permitiu um nivelamento dos consultores, tanto de conhecimento quanto de trabalho. Do ponto de vista dos usuários, eles passaram a ter confirmação do recebimento do pedido (o sistema manda uma confirmação de recebimento automaticamente) e podem acompanhar como está a resolução do seu pedido, através de mensagens especiais. O sistema também trouxe algumas vantagens gerenciais, pois passou a ser possivel determinar quanto tempo está sendo gasto para a resolução das solicitações, evitando com isso que um pedido seja "esquecido", o que às vezes acontecia no sistema manual. Com o sucesso do sistema, pensa-se agora em expandi-lo para controlar também as tarefas internas do nosso grupo, tanto a nível coletivo quanto individual. Com isso,

conseguiríamos gerenciar não apenas as solicitações externas, mas também as nossas próprias pendências, tudo isso com apenas uma única interface.
Além disso, estamos trabalhando em cursos de nivelamento interno e para os adminstradores das redes das unidades, indicados formalmente pela direção de cada unidade/departamento. A idéia disso é que o usuário final procure sempre o seu administrador local, e que este entre em contato conosco no caso de problemas mais difíceis. Isso traria duas vantagens: maior diminuição de demanda para o nosso grupo, e a criacão e formação de pessoal mais envolvido com redes, o que é essencial dada a forte tendência de adminstração distribuída e descentralizada.

5. Referências

[1] Michael A. Cooper, “SPM: System for Password Management”, *Proceedings of LISA IX Conference, pp. 149-170, Usenix, 1995*

[2] Paul Anderson, “Managing Program Binaries in a heterogeneous UNIX Network”, *Proceedings of LISA V Conference, pp. 1-9, Usenix, 1991*

[3] SSH - Secure Shell - Disponível em http://www.cs.hut.fi/ssh