

Código Documento: RNP/REL/0182A
Código Atividade: LA1/P1/SP1
Título Documento: Reunião Número Zero - GT de Engenharia de Redes Internet/BR
Versão: Preliminar
Autor: Gorgônio Araújo
Data: 16 de Maio de 1995

Local e data: Augusta Palace Hotel, São Paulo, 03 e 04/MAI/1995
Participantes: Adailton José dos Santos (RNP, Cps) <adailton@hq.rnp.br>
Alberto Gomide (FAPESP) <gomide@fosp.fapesp.br>
Alexandre Lopes Venziano (CR-SP) <alex@cr-sp.rnp.br>
Antonio Iyda Paganelli (CI-ONG) <iyda@ax.apc.org>
Antonio Pereira Lima Jr. (CNPq)
Carlos A. Campana Pinheiro (CR-DF) <carlos@cr-df.rnp.br>
Cybelle Suemi Oda (RNP, Cps) <cybelle@hq.rnp.br>
Demi Getschko (FAPESP) <demi@fosp.fapesp.br>
Edison Tadeu Lopes Melo (UFSC) <melo@npd.ufsc.br>
Elvis Melo Vieira (UFSC) <elvis@npd.ufsc.br>
Eratóstenes E. Ramalho Araújo (CNPq) <era@cnpq.br>
Eric Charles Anderson (CR-AM) <anderson@cr-am.rnp.br>
Ewerton Longoni Madruga (NC-RJ) <mumu@nc-rj.rnp.br>
Fabio Queda Bueno da Silva (UFPE) <fabio@di.ufpe.br>
Gorgônio Araújo (RNP, BA) <gorgonio@ufba.br>
Helder G. Costa (CR-CE)
Heraldo Madeira (UFPR) <heraldo@inf.ufpr.br>
João Galdino Melo de Souza (CR-MG) <galdino@dcc.ufmg.br>
Joel Weisz (FINEP)
José Arivaldo Frazão Jr. (CR-PE) <ari@cr-pe.rnp.br>
José Augusto Suruagy Monteiro (UFPE) <suruagy@di.ufpe.br>
José Geraldo Mill (UFES)
José Luis Ribeiro Filho (NC-RJ) <zeluiz@nc-rj.rnp.br>
Liane Tarouco (UFRGS) <liane@penta.ufrgs.br>
Marcal dos Santos (UNICAMP) <marcal@ccsun.unicamp.br>
Márcio Bunte de Carvalho (CR-MG) <mlbc@dcc.ufmg.br>
Marcio Calasans Rodrigues (CI-ONG) <calasans@ax.apc.org>
Marcio Pociotti (CR-SP) <pociott@cr-sp.rnp.br>
Marcos F. Bordin (RNP, Cps) <mbordin@hq.rnp.br>
Maria Ivete Lovato (UNICAMP) <ivete@ccsun@unicamp.br>
Pedro Sergio Nicolletti (UFPB) <peter@coepb.br>
Pedro Vazquez (UNICAMP) <vazquez@iqm.unicamp.br>
Rafael Pisco (NC-RJ) <rafael@nc-rj.rnp.br>
Renata Ciccilini (RNP, Cps) <renata@hq.rnp.br>
Ricardo Novais Pinto (CR-CE) <ricardo@lia.ufc.br>

Rodolfo Miguel Baccarelli (RNP, Cps) <rmbacca@hq.rnp.br>
Rossana Andrade (CR-CE) <rossana@lia.ufc.br>
Saliel Figueira Filho (CI-ONG) <saff@ax.apc.org>
Sandra Beatriz Tumelero Nunes (CR-DF) <sandra@cr-df.rnp.br>

RESUMO

Este relatório resume a reunião preparatória para a Reunião Nº 1 do GT de Engenharia de Redes Internet/BR. Realizada num momento de redefinições no plano político, na área de redes no país, essa reunião teve uma primeira parte política, conduzida pelo Dr. Ivan M. Campos (SEPIN/MCT), na tarde do primeiro dia; e um plenário técnico conduzido por Demi Getschko, no segundo dia. Aqui enfocaremos o plenário técnico, concluindo o trabalho com uma proposta preliminar para a 1ª Reunião do GT de Engenharia de Redes Internet/BR.

SITUAÇÃO ATUAL

A reunião foi realizada treze dias após a assinatura da portaria Nº 13 do Ministério das Comunicações, sobre "Condições para o acesso à Internet através da rede pública de telecomunicações", num momento de definições com relação ao provimento do chamado acesso comercial à Internet brasileira.

O PLENÁRIO TÉCNICO

Introdução

Demi iniciou a reunião lembrando que o propósito de realizá-la remonta a 1991, e que a expectativa é que ela passe agora a ser realizada periodicamente. A sua motivação básica é a operação do backbone para prestação de serviços. Foi resumido o funcionamento da IETF, lembrando que a idéia aqui não é a de reeditar o trabalho deste, mas sim gerar recomendações com o objetivo de manter a rede em operação estável, usando para isso, soluções e tecnologias já consagradas. Citou a existência de vários tópicos que devem ser discutidos, tais como segurança, protocolos de roteamento interno, estratégia de *upgrade* de linhas/velocidades, programas que devem ser preferencialmente adotados para alguns serviços, estratégia de distribuição de *news*. A introdução foi encerrada com uma rápida apresentação dos presentes.

Backbone

Foi apresentado o backbone atual, seus principais problemas e as soluções emergenciais encaminhadas.

Duas linhas de 9600 não estão funcionando, ou estão de modo precário, que são a linha Recife-Salvador e a linha Florianópolis-Porto Alegre, devido ao fato desses lugares terem 3 linhas cada um, quando o roteador alocado só possui 2 interfaces seriais. Estes roteadores serão trocados por outros existentes em estoque (4000 e AGS).

Serão postas em operação, emergencialmente, três linhas de 64 kbps entre SP-MG, SP-PE e RJ-SC.

As saídas para os EUA são:

- LNCC, 9600, tráfego NJE (BITNET);
- UFRJ: 64k, tráfego TCP/IP (Internet) servindo Rede Rio e ES;
- FAPESP: 256k, tráfego TCP/IP (Internet), e 128k, tráfego DECnet (HEPnet e transporte Bitnet), backup para TCP/IP.

Deve-se buscar uma maior eficiência no roteamento do backbone. Para facilitar essa tarefa é necessário que cada ponto do backbone seja composto apenas por um roteador, evitando que o tráfego passe por redes locais, ou pela rede regional. Foi citado o caso de dois POPs que funcionam como estrelas duplas: BA e RS. Na BA, devido ao fato do roteador do backbone só possuir duas interfaces seriais, a linha PE-BA está ligada a um 2º roteador o backbone da UFBA. Dois roteadores estão também sendo usados no RS para o backbone, com o agravante de serem separados por uma *bridge*.

Gomide falou aqui da necessidade de cada rede regional solicitar diretamente ao *Internic autonomous System Numbers*.

Demi discorreu sobre endereços IP's. Inicialmente não havia problemas com a solicitação de números ao Internic, mas de 93 para cá a falta de endereços passou a ser um problema, a ponto de ser extremamente difícil conseguir uma classe B hoje. Algumas soluções para a falta de endereços IP's foram levantadas na IETF o que levou a um reaproveitamento de endereços. A falta de classes B's levou a um outro problema: o tamanho das tabelas de roteamento dos backbones. A solução aqui foi o agrupamento de endereços classes C's em blocos.

Atualmente as classes C's de 200.128.0.0 até 200.255.0.0 estão alocadas para o Brasil. Na distribuição destas classes, tem-se buscado deixar cada rede regional em um bloco contínuo de endereços.

Swat

Gorgônio fez então a apresentação das atividades desenvolvidas pelo SWAT, descritas no (RNP/REL/0168). Aqui houve reclamações pelo fato do SWAT e seu trabalho não ser mais aberto e divulgado. Foi respondido que o SWAT era um grupo relativamente novo, voltado para prospecção tecnológica, e que a sua abertura já estava acontecendo, sendo essa reunião um sinal disso. Uma cópia do (RNP/REL/0168) ficou de ser enviada para cada um dos participantes dessa reunião.

Gerência de Rede

Cybelle apresentou as atividades na linha de Gerência de Rede capitaneadas por ela na RNP, fazendo um histórico que encerrou-se no estado atual da atividade (RNP/REL/0168, RNP/PRJ/0019, RNP/REL/0088, RNP/DOC/0034, RNP/DOC/0037, RNP/REL/0155). Demi enfatizou a importância de utilizar-se de um esquema de gerência de rede em regime permanente. Foi feita a sugestão de se analisar comparativamente os pacotes existentes no mercado, decidindo pela melhor opção e incluindo no pacote que será enviado para os POPs. Liane lembrou que as revistas especializadas têm apontado o HP-OpenView como melhor opção, e que o NetView, inicialmente baseado no HP-OpenView, na sua versão atual, já seria um produto novo, não mais baseado no OpenView.

Falou-se também em algumas soluções que funcionam hoje baseada em SWs públicos e em soluções caseiras. Na FAPESP hoje Demi usa um *software* da casa que permite apenas detectar quando algum nó do backbone não está acessível. Em SC, Elvis utiliza o NetView/6000 e, em pequena escala o OSIMIS. Os pedidos de licença para o OSIMIS-4.0 devem ser encaminhados para K.McCarthy@cs.ucl.ac.uk e o OSIMIS-3 pode ser obtido livremente pela rede, no RS Liane utiliza o SunNetManager e o snmpi (que vem com o ISODE) e Cybelle tem uma lista de *software* público que devem ser analisados.

Foi sugerido por Demi que, assim como o backbone nacional, cada backbone estadual fosse homogêneo, no que se refere à escolha dos roteadores. Usando, sempre que possível, roteadores de uma única marca, ou bastante compatíveis, a nível de interface e configuração, entre si.

Acesso Discado

Falou-se sobre acesso discado, descrevendo-se as várias experiências no assunto, uso e problemas de/com o TACACS para autenticação de usuários nos Cisco 500cs's e CS com melhor desempenho.

Demi recomendou o uso de protetores elétricos contra transientes em linhas.

Foi levantada a necessidade de uma política de manutenção e backup de equipamentos.

Pareceres sobre pacotes para acesso discado foram dados. Renata falou do trabalho feito em Campinas, onde além de testar pacotes comerciais e *shareware/freeware*, foram feitos contatos com os autores visando a customização dos pacotes para o Brasil. Saliel e Iyda falaram sobre o pacote do CI-ONG, que possui cerca de mil usuários com acesso discado SLIP/PPP. Tanto Renata como Saliel testemunharam que, em geral, os preços dos *software shareware* podem cair muito com o volume. O EUDORA foi escolhido para compor o kit básico no IBASE por ser mais fácil de operar do que o PMAIL. Foi levantado como furo do Eldora o fato de permitir que o endereço do remetente seja modificado pelo usuário, este problema foi contornado no CI-ONG fazendo modificações na configuração do sendmail no servidor. Foi argumentado também que a possibilidade de uso de falsos endereços de origem é algo possível com outros *software*, como o próprio *Mail* do Unix, sendo uma característica inerente do serviço.

Foram levantadas discussões com relação à segurança no acesso discado. A funcionalidade do BINA, do TACACS e de outros métodos de autenticação. O BINA funciona com restrições, dependendo das centrais telefônicas existentes entre o usuário e o provedor de acesso, conforme esclareceu Carlos. O seu uso deve ser acordado com a concessionária telefônica local. Alguns servidores de conexão permitem autenticação local, ou via TACACS, onde o registro pode ficar num servidor Unix. Outros servidores não permitem autenticação, sendo nesses casos utilizados para logar automaticamente em uma máquina que faça a autenticação.

Com a abertura para uso da rede, foi sugerido que haja normas de segurança para utilização do acesso discado. Este assunto foi abordado com mais detalhes a seguir.

News

Demi lembrou que a FAPESP tem todos os *newsgroups* e deve ser utilizada para repasse no país. Assim, os interessados deverão recorrer à FAPESP, que indicará quem é o *feeder* mais próximo. O *news* não deve ser puxado diretamente do exterior.

Segurança

A tarde do dia 04 começou debatendo-se segurança. Foram feitas sugestões no sentido de implementação de uma política de segurança em redes, foram comentados alguns casos de invasões ocorridas, foi levantado a necessidade de um respaldo legal para a questão.

Foi sugerida a criação de um esquadrão de segurança, que tivesse a possibilidade de inclusive, quando necessário, ser deslocado para agir quando violações à rede estivessem ocorrendo.

A criação de um kit de segurança, com recomendações, *check lists*, e ferramentas de auxílio foi sugerida: o *handbook* de segurança do administrador.

Foi sugerido que houvesse um responsável por segurança em cada site ligado à rede, que pudesse ser acessado via telefone, em caso de haver algum problema envolvendo o seu site.

Foi sugerida a criação de um curso de segurança, para ser repassado pelo país, onde assumiria-se que a audiência já teria um conhecimento básico sobre operação.

Alguns repositórios de *patches* para os sistemas mais utilizados serão mantidos no próprio país. Alguns voluntários são:

AIX: ftp://ftp.lia.ufc.br ([*a confirmar*])
ftp://ftp.ufsc.br
Solaris: ftp://ftp.coepb.br ([*a confirmar*])
SunOS: ftp://ftp.coepb.br ([*a confirmar*])

Foi sugerida a elaboração de normas contratuais (termo de adesão) para ligação à rede. Alguns temas deve ser debatidos, entre eles temos a privacidade de dados, a invasão de sistemas, prejuízos advindos de mau uso/administração da rede, danos/prejuízos causados via RNP/Internet, responsabilidades sobre acessos via outras instituições, anúncio de novas conexões.

Foi recomendado a criação de um grupo de ação corretiva especializado e juridicamente instrumentado, com apoio do SOFTEX e PROTEM.

Algumas sugestões técnicas foram dadas. Liane sugeriu restringir o uso dos comandos *r's* do Unix desativando os servidores *e/ou* removendo os *.rhosts*, lembrou também sobre a necessidade de desativação do *tftpd*, quando não utilizado. Ewerton sugeriu a utilização do *tcp-wrapper*. Carlos sugeriu o estudo sobre *Fire-walls*. Marçal testemunhou que em Cornell a conexão externa é centralizada, o que facilita o controle.

Alguns casos de violação foram rapidamente comentados. Carlos resumiu o problema ocorrido com autenticação via RENPAC. Adailton falou sobre os prováveis furos utilizados na recente invasão à EMBRAPA/UNICAMP.

Liane falou sobre a utilização do cron para acesso indevido no RS.

Atividades em Andamento

Bordin anunciou a abertura dos acesso *on line* para a documentação da RNP, o repositório institucional da RNP, para uma ou duas semanas, falando sobre o formato da documentação, as formas de acesso, e os mecanismos de busca.

Liane anunciou a existência de textos técnicos na área de rede em <ftp://penta.ufrgs.br/> e de um grande conjunto de *software* em <ftp://caracol.inf.ufrgs.br/>.

Nicolletti anunciou a existência de relatórios técnicos locais e de RFCs em <ftp://router.coepb.br/> ([*a confirmar*]).

Renata anunciou a disponibilização dos relatórios de análise de *softwares* coordenadas por ela via repositório institucional.

Iyda anunciou o local onde o kit de acesso discado do CI-ONG é distribuído: <ftp://ftp.ci-ong.rnp.br/pub/prgs/>.

Gorgônio falou sobre o uso de Unix's públicos (RNP/REL/0168). (a confirmar)

Carlos descreveu a tecnologia VSAT, exemplificando com a ligação CR-AM/PRODEMGE/CR-DF (RNP/REL/0168, RNP/REL/0120).

Ari falou sobre o levantamento feito de pesquisas com redes de alta velocidade no PROTEM e sobre o que é o PALOPS (RNP/REL/0168).

Marçal falou do convênio UNICAMP/EMBRATEL para testes de ATM. Está sendo feita uma ligação entre a UNICAMP, em Campinas, e a EMBRATEL, no Rio, utilizando-se um enlace STM-1 (155 Mbps) e equipamentos da Cabletron. Márcio Bunte falou sobre as experiências com ATM a serem feitas em Belo-Horizonte.

Gorgônio falou sobre os estudos feitos para ligação de pagers à rede (RNP/REL/0168). Foi comentado que serviços do gênero são utilizados pelo colégio Magnum, em São Paulo.

Demi comentou sobre as discussões comparativas entre o majordomo e o listserv, ocorridas no *swat-int*.

Correio Eletrônico

Heraldo levantou a questão do roteamento de correio eletrônico. Saliel e Gomide defenderam que é necessário apenas a figura do Relay Host dentro da instituição. O fisp.fapesp.br deve ser utilizado apenas como relay de BITNET, na falta de outro mais próximo.

SUGESTÕES

A proposta apresentada por Demi e a criação de uma lista provisória, com os presentes no evento. Sugestão: ENO-L (Engenharia e Operações (com antiácido incluído.. :-)). Seria uma lista fechada, mas candidatos a inscrição podiam ser aceitos pelo *owner* sem maiores consequências, desde que mostrassem que tem algo a ver com o assunto.

A idéia é evitar "curiosos" e "palpiteiros". Em paralelo, a REPTec seria reativada para assuntos exclusivos do backbone. *Swat-int* pode ser enriquecida pelos interessados, mas deve se manter em tópicos de prospecção, como é hoje.

Proposta para a Reunião Nº 1 do GT de Engenharia de Redes Internet/BR

- Gerência de Rede
- Pacotes comerciais
- Pacotes públicos
- Gerência do backbone
 - Gerência do backbone em função dos dados obtidos de gerência de rede, e da demanda.
- Normas
 - Especificação dos deveres da operação, sujeitos a auditoria externa, para os pontos internos da RNP e da redação do termo de adesão.
- O&M de Operação
 - Estabelecimento de procedimentos de operação.
- Prospecção Tecnológica
 - Estudos sobre novos serviços, ferramentas e tecnologias.
- Roteamento
 - Política de roteamento para o backbone.
- Segurança
 - Política de segurança. Definição de normas de segurança. Definição de procedimentos de segurança.
- Serviços
 - Preocupa-se desde o gerenciamento de serviços como o news, até a análise, discussão e recomendação de servidores e ferramentas.
- Archie
- Ftp anonymous
- Listas
- News
- Whois
- etc.