AP ROUTER NG (ÚLTIMA ATUALIZAÇÃO: 07/04/2006)

=>Versão 5

O IP DEFAULT DO EQUIPAMENTO ESTÁ CONFIGURADO COMO SENDO: 192.168.2.1

Recursos:

--> Suporte ao MESH (OLSR): http://www.olsr.org
--> SSH Cliente
--> Edição de Script pessoal /etc/script.sh via web
--> Edição do arquivo /etc/ethers via web
--> Controle de potência
--> Utilitário Iptraf
--> Utilitário tcpdump
--> Acesso remoto via SSH2
--> Suporte a agendamento de tarefas pelo Crond
--> Prende o MAC ao IP e fornece ip estaticamente baseado no MAC
--> Liberdade para escrever seus próprios scripts
--> Grupos de Controle de Banda, com rate mínimo garantido por membros do grupo
--> Watchdog por IP
--> Block Relay
--> PPPoE Relay
--> DHCP Relay
--> Assistente de configuração
--> Auto Discovery Tool
--> 3 Modos de Operação: WISP, Gateway e Bridge
--> Controle de banda por interface, por endereço IP ou MAC (por HTB)
--> Criptografia WEP
--> Autenticação 802.1x, WPA e Radius
--> Filtro de mac, ip, portas...
--> DMZ Host
--> PPPoE-Cliente em todas as interfaces
--> PPTP Protocol
--> DDNS Protocol
--> IAPP Protocol
--> "Esconde" o SSID evitando ser descoberto por scanners simples
--> Todo controle via WEB
--> Medidor de sinal
--> Watchdog de hardware
--> Opera como AP, Cliente, WDS+AP, WDS e Ad Hoc
--> Site Survey
--> Servidor DHCP
--> DHCP Cliente

--> Até 5 IP Alias em cada interface
--> Spanning Tree Protocol
--> Permite a troca da porta do Servidor WEB
--> Proteção contra gerenciamento via WAN
--> Proteção 802.11g
--> Clonagem de MAC (para somente um cliente)
--> Permite envio de comandos via interface WEB
--> Log do sistema (local e remoto)

=> PROCEDIMENTOS PARA CONFIGURAÇÃO

- Configure o ip do computador para 192.168.2.2 máscara 255.255.255.0.
- Entre via browser, no endereço 192.168.2.1.

=> NOTAS SOBRE O MODO DE OPERAÇÃO

- Existem 3 modos de operação no equipamento:

    GATEWAY
    BRIDGE
    CLIENTE ISP

-- Modo Gateway:
- Neste modo, as interfaces ETH0 + Wireless passam a ser o segmento LAN. A WAN ficará por conta da ETH1.

-- Modo Bridge:
- Neste modo, todas as interfaces (ETH1 + ETH1 + Wireless) serão pertencentes a br0, não havendo portanto, opções de roteamento e firewall.

-- Modo Cliente ISP:
- Neste modo, as interfaces ETH0 + ETH1 passam a ser o segmento LAN. A WAN ficará por conta da Wireless.

=> NOTAS DO MENU

--TCP/IP
- IP LAN: é o endereço IP do segmento LAN do rádio.
- IP WAN: é o endereço da WAN do equipamento (quando em modo GATEWAY ou Cliente ISP somente). Aqui você poderá configurar como sua porta WAN receberá o endereço IP, via PPPoE, DHCP, PPTP e estático.
- APELIDOS DE IP: são os apelidos de IP que você poderá configurar, tanto para LAN quanto para Wireless.

--FIREWALL
- As funções de firewall somente serão ativadas, quando o rádio não estiver operando em modo Bridge.
- Todas as funções de firewall via este menu, são de BLOQUEIO.

--LIMITAÇÃO DE BANDA
- POR INTERFACE: Possibilita o controle de velocidade na interface do rádio. Tanto LAN quanto Wireless.
- POR IP: Possibilita o controle de velocidade por endereço IP (até 40 endereços via WEB).
- POR MAC: Possibilita o controle de velocidade por endereço MAC (até 40 endereços via WEB). O NAT OU ROTEAMENTO DEVERÁ ESTAR ATIVADO PARA HAVER O CORRETO CONTROLE DE DOWNLOAD E UPLOAD POR MAC!!

=> COMO USAR O CONTROLE DE BANDA

O controle de banda é feito através do menu Controle de Banda, via interface WEB ou por edição do arquivo /etc/cbu.conf via terminal SSH. Para limitar todo e qualquer tráfego de dados, habilite o controle por Interface. Para controlar determinados endereços IPs, habilite o controle de banda por endereçamento IP.

Exemplos:

CASO 1:

Se você está instalando o equipamento em um cliente de Internet, que tenha uma velocidade máxima de Download de 256Kbits e uma velocidade máxima de Upload de 128kbits, entre no menu de Limitação de banda por interface, habilite o controle de banda e coloque os seguintes valores:

Saida da Interface LAN 256
Saida da Interface WAN 128

Visto que o sistema de controle de banda atua na SAÍDA DE DADOS da interface, o controle de Download do cliente será a saida do segmento LAN. A grande vantagem do controle de banda por interface, é o fato de controlar TODO E QUALQUER tráfego de dados, NÃO IMPORTANDO SE O NAT ESTÁ ATIVADO OU DESATIVADO!

CASO 2:

Se você está instalando o equipamento em um condomínio, e deseja controlar a velocidade de cada apartamento, entre no menu de Limitação de banda por IP, habilite o controle de banda e coloque o endereço IP do cliente a ser controlado bem como as velocidades máximas permitidas. Nesta situação, o DOWNLOAD dos clientes será limitado pela segmento LAN e o UPLOAD será limitado pela interface WAN. Para SOMENTE liberar o tráfego de dados para os ips/macs cadastrados na lista de controle de banda, habilite a opção de firewall neste mesmo menu. Neste caso, o firewall irá bloquear o tráfego de dados para os IPS que não estão na lista de controle. NOTE QUE O CONTROLE DE BANDA POR INTERFACE DEVE ESTAR DESATIVADO! PARA QUE O FIREWALL FUNCIONE É NESCESSÁRIO QUE O NAT OU ROTEAMENTO ESTEJA HABILITADO, ou seja, o equipamento deve estar operando em modo WISP ou GATEWAY!

CASO 3:

Se você está instalando o equipamento em modo ACCESS POINT, deseja controlar a banda de seus clientes, permitir que seus clientes recebam o endereço IP via DHCP e permitir que somente os MACs cadastrados naveguem na Internet, faça o seguinte: Habilite o controle de banda por MAC, cadastre os MACs dos clientes via rádio com sua devida velocidade de acesso, habilite o modo GATEWAY e habilite o Servidor DHCP do

equipamento. Somente os MACs cadastrados no controle de banda, poderão navegar na Internet e seus clientes receberão os IPs via DHCP.

=> COMO USAR O CONTROLE DE BANDA COM GRUPOS DE QoS

Grupos de QoS são usados para limitar um grupo de usuários a uma determinada velocidade máxima de acesso.

Exemplo:

Se você está instalando o equipamento em um condomínio, onde uma pessoa tem dois computadores em casa e deseja acessar a Internet, com seus dois computadores. Esta pessoa, possui um plano de acesso de 256Kbps. Neste mesmo condomínio, temos outros usuários que utilizam a Internet e tem seus planos de acesso distintos. Como fazer, para que a pessoa em questão, utilize seus dois computadores e limitar o acesso a uma velocidade máxima de 256Kbps? Fácil. Criando-se um GRUPO DE QOS.

Vá para o menu controle de banda e habilite a opção "Ativar Grupos de QoS". Entre com o ID do Grupo (valor numérico maior que 0 e menor do que 40) e coloque suas devidas velocidades de LAN/WAN.

No nosso caso:

ID do Grupo=1
Saída LAN=256
Saída WAN=256

Após, coloque no controle de banda por IP/MAC os dois endereços IP/MAC dos computadores pertencentes ao cliente em questão. No campo ID do Grupo, coloque o ID do grupo criado para estes dois computadores, no nosso exemplo 1.

Primeira Máquina do Cliente:

ID do Grupo=1 --> Grupo criado no exemplo
IP=xxx.xxx.xxx.xxx ou MAC=xxxxxxxxxxxx
Saída LAN= 0 --> QUANDO 0, SIGNIFICA IGUAL DIVISÃO DE BANDA DO GRUPO
Saída WAN= 0

Segunda Máquina do Cliente:

ID do Grupo=1 --> Grupo criado no exemplo
IP=xxx.xxx.xxx.xxx ou MAC=xxxxxxxxxxxx
Saída LAN= 0
Saída WAN= 0

Outr cliente qualquer:

ID do Grupo=0 --> Não pertence a um grupo específico
IP=xxx.xxx.xxx.xxx ou MAC=xxxxxxxxxxxx
Saída LAN= 256
Saída WAN= 256

Neste exemplo, criamos um Grupo com valocidade de 256Kbps, e colocamos nele, os endereços participantes desse grupo. Dessa forma, garantidos que os participantes desse

grupo, juntos, não passarão de 256Kbps. O valor de Saída LAN e saída WAN, quando "0", significa que os clientes irão dividir a banda do grupo igualmente.

Para garantir uma velocidade mínima para um membro do grupo, basta colocar o valor desejado na saída LAN e WAN.

Exemplo: Queremos que a primeira máquina do nosso cliente em questão, tenha no mínimo 200 kbit. No exemplo anterior, dividimos a banda do grupo (256 kbit) igualmente entre a máquina 1 e máquina 2. Agora, vamos garantir pelo menos 200 kbit para máquina 1 e o restante para máquina 2 (o restante será 56kbit). Ambos os valores de saída devem ser diferentes de 0 para a garantia de velocidade.

Primeira Máquina do Cliente:

ID do Grupo=1 --> Grupo criado no exemplo

IP=xxx.xxx.xxx.xxx ou MAC=xxxxxxxxxxxx

Saída LAN= 200 --> AQUI, ESTAMOS GARANTINDO UM MÍNIMO DE 200Kbit NA SAIDA LAN

Saída WAN= 200 --> AQUI, ESTAMOS GARANTINDO UM MÍNIMO DE 200kbit NA SAIDA WAN

Segunda Máquina do Cliente:

ID do Grupo=1 --> Grupo criado no exemplo

IP=xxx.xxx.xxx.xxx ou MAC=xxxxxxxxxxxx

Saída LAN= 0

Saída WAN= 0

NOTA: OS HARDWARES COM CHIPSET RTL8186 POSSUEM 2 INTERFACES DE REDE INDEPENDENTES, PORTANTO, PARA O CORRETO FUNCIONAMENTO DO SISTEMA EM GRUPOS, TODOS OS CLIENTES PERTENCENTES A UM MESMO GRUPO DEVEM ESTAR FISICAMENTE CONECTADOS NA MESMA INTERFACE DE REDE DO EQUIPAMENTO, POIS O CONTROLE DE BANDA ATUA NA SAIDA DE PACOTES DE CADA INTERFACE.

=> GARANTIR BANDA EM SISTEMA VOIP COM GRUPO DE QOS

Uma função muito interessante seria garantir uma quantidade de banda para um aparelho de Voip, por exemplo. Este efeito é facilmente alcançado utilizando o sistema de Grupos de QoS descrito acima!

Exemplo: Queremos que nosso equipamento Voip, que possui o IP 192.168.2.100 por exemplo, tenha pelo menos 64kbit de banda GARANTIDA. Suponhamos ainda, que tenhamos um link de 256kbit. Este link de internet alimenta toda uma rede de computadores, por exemplo de uma empresa ou residência.

Configurações do Grupo:

ID do Grupo = 1 --> ID do nosso grupo

Saída LAN = 256 --> nosso link de internet de 256kbit

Saída WAN = 256 --> nosso link de internet de 256kbit

Até agora, criamos um grupo com velocidade máxima a do nosso link, de 256kbit.

Configurações do controle de banda por IP:

ID do grupo=1	--> ID do grupo acima criado
IP = 192.168.2.100	--> IP do nosso Voip
Saída LAN = 64	--> Velocidade mínina garantida de 64kbit
Saída WAN = 64	--> Velocidade mínina garantida de 64kbit

Neste momento, reservamos uma banda de 64 kbit para nosso Voip, dos 256kbit disponíveis.

Continuação das configurações do controle de banda por IP:

ID do grupo=1	--> ID do grupo acima criado
IP = 0.0.0.0	--> 0.0.0.0 = Qualquer endereço IP
Saída LAN = 0	--> Banda restante calculada automaticamente
Saída WAN = 0	--> Banda restante calculada automaticamente

Agora, criamos uma regra dizendo para o sistema que qualquer outro enredeço IP estará pegando a banda restante. Como reservamos 64k para o Voip, temos então para o resto da rede 256 - 64 = 192kbit.

Importante notar o seguinte: Quando o voip não estiver sendo usado, a rede passará a usar toda banda disponível do grupo, que é de 256kbit. A partir do momento que o Voip entrar em ação, o QoS irá sempre garantir uma banda para o Voip e o resto da rede irá compartilhar o restante.

=> CONTROLE DE BANDA POR EDIÇÃO DE ARQUIVO

Esta versão permite um número ilimitado de clientes a serem controlados por IP e/ou MAC, através da edição do arquivo /etc/cbu.conf. Este arquivo possui a mesma sistemática adotada pelo controle de banda via WEB.

Após editar este arquivo com suas novas entradas, você deverá executar estes comandos, nesta ordem, para ativar e salvar as alterações:

```
# salvar
# /bin/cbu.sh
# /bin/firewall.sh
```

NOTA: LEMBRE-SE DE ATIVAR O CONTROLE DE BANDA VIA INTERFACE WEB.

=> INFORMAÇÕES SOBRE ACESSO VIA SSH

Este firmware permite o acesso via protocolo SSH2. O usuário para acesso SSH é root, com senha root por default.

Para alterar a senha de root, você deverá se conectar via SSH e digitar passwd. Após a alteração de senha, digite salvar para gravar a alteração da senha na flash do rádio.

Esta versão tem suporte ao SSH cliente. Através dele, você poderá se conectar a outro rádio ou computador via SSH, a partir do próprio equipamento com o firmware AP Router NG. Para executar o SSH cliente, digite:

```
# dbclient
```

=> LIBERDADE PARA EXECUÇÃO E CRIAÇÃO DE SCRIPTS VIA WEB

A partir da versão 5.1a, você poderá editar facilmente seu script pessoal a partir da interface WEB. Junto com o firmware já existe um arquivo modelo de script pessoal, contendo alguns comandos comuns e muito úteis.

Para executar seu script pessoal, basta entrar no menu Gerenciamento -> Editar Script Pessoal. Faça as alterações desejadas e clique em Salvar. A partir deste momento seu script será salvo e executado!

=> LIBERDADE PARA EXECUÇÃO E CRIAÇÃO DE SCRIPTS VIA TERMINAL SSH

Ao entrar no equipamento via SSH, como descrito acima, você estará apto a alterar qualquer arquivo e gerar seus próprios scripts, dentro do diretório /etc, utilizando o editor de texto "vi". Todos os arquivos alterados ou criados neste diretório, ficarão salvos na memória flash do equipamento, bastando digitar o comando "salvar". A estrutura de scripts de inicialização é parecida com a estrutura Debian. Dentro do /etc/init.d você encontrará arquivos nomeados da seguinte maneira:

Sxxnome_do_servico - xx= Um número decimal usado para dar prioridade de inicialização

Ex.: S10init

S20sshd - Neste caso, o serviço sshd irá ser executado após o init.

Se você quiser colocar um serviço ou script a ser iniciado com o equipamento, basta criar seu script dentro do /etc/init.d e renomeá-lo de acordo com sua prioridade de execução.

Lembre-se sempre de digitar o comando "salvar" após qualquer alteração na estrutura do diretório /etc.

NOTA: AO COLOCAR O SCRIPT A SER EXECUTADO PELO INIT.D, TODA VEZ QUE O RÁDIO SOFRER UMA PROGRAMAÇÃO VIA WEB, DEPENDENDO DAS REGRAS, ELAS SERÃO APAGADAS.

Para resolver o problema acima citado, basta criar seu script dentro do diretório /etc, e chamar ele através do script /etc/init.sh. O init.sh será executado quando você alterar algum parâmetro via interface WEB.
Para garantir que seu script sempre seja executado, coloque na última linha do /etc/init.sh a chamada para seu script.

Exemplo: Queremos criar uma regra específica, dizendo que um determinado IP da rede LAN não possa acessar a porta 21 por exemplo, de qualquer servidor FTP. Quero que esta regra seja sempre executada.

Primeiro passo, editar script: Vou chamar meu script de bloqueio.sh. Entro no rádio via SSH.

```
# cd /etc                 - Entro no diretório /etc ( pois somente o que estiver dentro dele será efetivamente salvo )
# vi bloqueio.sh          - Uso editor VI para criar o arquivo.
```

Conteúdo do arquivo bloqueio.sh:

```
#!/bin/sh
# IP 192.168.2.3 nao pode acessar a porta 21
iptables -t nat -I PREROUTING -p tcp -s 192.168.2.3 --dport 21 -j DROP
```

Salvo meu arquivo e torno ele um executável:

```
# chmod +x bloqueio.sh        - Torna o script executável
```

Agora, basta editar o arquivo /etc/init.sh e acrescentar na última linha:

```
/etc/bloqueio.sh
```

Salvo o arquivo, e digito "salvar" para gravar as alterações.
Pronto, este script será sempre executado quando o rádio iniciar ou quando alguma alteração for feita.

NOTA: CUIDADO AO EDITAR E MODIFICAR ARQUIVOS. PROCEDA COM CAUTELA, POIS REGRAS OU SCRIPTS MAL CONFIGURADOS PODERÃO FAZER COM QUE VOCÊ PERCA ACESSO AO EQUIPAMENTO OU AINDA, FAZENDO-O FICAR INOPERÁVEL.

=> PRENDENDO O IP AO MAC E OFERECENDO IP ESTÁTICO VIA DHCP (VIA TERMINAL SSH)

Com um único arquivo, você estará apto a "amarrar" o ip ao MAC, usando o aplicativo ARP e ao mesmo tempo oferecer o ip via DHCP de acordo com o mac do cliente. As

vantagens são claras: Segurança e facilidade de configuração, pois seu cliente terá um IP fixo, mas recebido através do DHCP.

Para usufruir deste novo recurso, basta editar o arquivo /etc/ethers e coloca o par mac ip de seu cliente da seguinte forma:

```
# Marcos da Silva
00:11:e0:4f:23:d1 192.168.2.100
# Paulo
00:34:df:e0:4a:5b 192.168.2.101
```

Após editar o arquivo, salve-o e digite "salvar" para gravar a alteração permanentemente. Para fazer com que as alterações entrem em funcionamento, digite: "init.sh gw all".

=> PRENDENDO O IP AO MAC E OFERECENDO IP ESTÁTICO VIA DHCP (VIA INTERFACE WEB)

Para editar o arquivo /etc/ethers via interface web, basta entrar no menu Gerenciamento - Editar Arquivo Ethers. O padrão do arquivo segue o modelo acima, composto pelo MAC IP. uma vez editado, clique no botão "salvar arquivo" e suas alterações serão salvas.

=> UTILIZANDO AGENDAMENTO DE TAREFAS (CROND)

Este firmware possui o serviço crond, que possibilita agendar tarefas a serem executadas automaticamente no sistema. O arquivo responsável pelo agendamento é: /etc/crontabs/root. O formato do arquivo segue:

```
minuto hora dia_do_mes mes dia_da_semana script_ou_comando_a_ser_executado
```

Ex.: Para executar um ping a cada 5 minutos.

```
*/5 * * * * ping -c 5 192.168.2.40
```

Altere o arquivo e digite "salvar". Reinicie ou digite "init.sh gw all".

=> SISTEMA MESH UTILIZANDO OLSRD

Esta versão tem suporte ao sistema MESH utilizando o programa OLSRD (**http://olsr.org**). O arquivo de configuração a ser editado é: /etc/olsrd.conf. Este arquivo já está pré-configurado por default.

Para se utilizar o sistema MESH, seu rádio deve estar configurado como CLIENTE AD-HOC.

Para maiores informações, consulte o link acima.