Quando o firmware padrão do roteador não consegue fazer tudo o que você quer, é possível substituí-lo por uma distribuição do Linux adequada às nossas necessidades – mas o esforço é enorme! Este artigo mostra como chegar lá.

Por Dirk von Suchodoletz, Arnim Wiezer, Mirko Dölle

credits of the image

Instalando o OpenWrt em roteadores Linksys

Mande seus dados pelos ares

Os *firmwares* originais oferecidos pelos fabricantes, ajustados individualmente a cada roteador, possuem um leque de funções muito limitado e são extremamente direcionados a um conjunto particular de objetivos. Entretanto, se usarmos o Linux como firmwa do roteador, aumentam as chances de se adicionar mais recursos no futuro. Além disso, você está usando um Software Livre como sistema operacional do roteador em vez do firmware original e proprietário.

Há muitos firmwares à disposição para os roteadores WRT54G(S), da Linksys, e similares: além do software original do fabricante, há também, por exemplo, as versões produzidas pela Sveasoft ou pela Portless Networks, com uma maior gama de funções. Entretanto, o firmware da Sveasoft exige que todos aqueles que desejem obter acesso aos fontes do programa se registrem junto à empresa, mediante pagamento, como desenvolvedor. Ao contrário deste, o OpenWrt é desenvolvido sob a GPL e constitui mais do que somente um firmware para roteadores com Linux embarcado: trata-se de uma mini-distribuição completa, inclusive com gerenciamento de pacotes, que pode ser ampliada quase que *à la carte*.

Tirando proveito dos bugs

Os autores do firmware original da Linksys não conseguiam instalar o OpenWrt como novo firmware por meio da função de atualização automática da interface web. Entretanto, para a utilização do método TFTP anônimo (TFTP Put), o gerenciador de boot do roteador precisa aguardar uma nova imagem do firmware após ser acionado, o que pode ser conseguido ao inserir a variável `boot_wait` na NVRAM (veja o **quadro Armazenando a configuração na NVRAM**) com o valor `on`.

Nesse caso, um erro de programação no front-end web pode ajudar: Por meio do formulário na página `ping.asp` você pode executar qualquer comando do Linux no roteador. Para isso, insira as seguintes linhas uma após a outra no campo do endereço IP. Lembre-se de enviar (dê *Submit*) o formulário a cada linha mostrada:

```
;cp${IFS}*/*/nvram${IFS}/tmp/n
;*/n${IFS}set${IFS}boot_wait=on
;*/n${IFS}commit
;*/n${IFS}show /tmp/ping.log
```

Recuperação de Falhas nos Roteadores da Linksys

Uma regra de firewall errada, uma variável mal aplicada de NVRAM ou uma atualização malfadada do firmware poderão impossibilitar o acesso ao roteador.

Basicamente deve-se ter muito cuidado nas alterações internas do roteador, inclusive com os scripts de início do OpenWrt, para que você não seja bloqueado por acidente. Entretanto, mesmo se todas as portas estiverem fechadas e você tiver desligado o `boot_wait`, ainda há esperança. Caso todas as tentativas de ressuscitação falhem, mesmo como o botão de *reset* e TFTP anônimo, o jeito é apelar para o circuito integrado da memória Flash, dentro do roteador.

Primeiro é necessário localizar o chip, que se encontra ao lado da conexão de rede, mais ou menos no meio da placa, facilmente reconhecível pela inscrição *Intel Flash*. Nos modelos WRT54G da Linksys é preciso fechar um curto-circuito entre os pinos 15 e 16 do soquete onde fica o chip da memória flash; no WRT54GS são os pinos 5 e 6. O pino 1 do chip é a primeira perna da esquerda, no lado com o "ponto" impresso no soquete.

O curto-circuito ocorre melhor com um fio de metal sólido (não trançado) e fino. Por segurança use fio encapado e só desencape a ponta que for usar. Coloque o fio entre os dois pinos indicados e prenda com fita adesiva. Também com a fita adesiva, isole a outra ponta do fio. Não esqueça de deixar o fio de uma maneira que possa ser facilmente retirado posteriormente. E *não use solda!*

A idéia por trás do truque é: por causa do curto-circuito das duas linhas de endereço, a flash não pode ser mais lida por completo. O gerenciador de boot, entretanto, verifica o firmware antes de iniciar o sistema; com o curto-circuito, a soma de verificação (*checksum*) não irá bater e o carregador permanecerá em modo TFTP.

O importante é desviar as duas linhas de endereço responsáveis pelo carregamento do firmware, mas não aquelas que fazem o gerenciador de boot iniciar. De outra forma, o gerenciador de boot não roda e o roteador não mostrará qualquer função até que o *jumper* de operação seja retirado – consulte o manual do roteador.

Enquanto o gerenciador de boot espera pelo firmware, o que se reconhece pelo LED *Power* piscando de modo intermitente ou pelas respostas aos pings, remova o *jumper* de operação e inicie o upload do firmware por TFTP. Após a conclusão da transferência de dados, o roteador é reiniciado (se tudo der certo) como de costume.

Após o envio da última linha, veja a lista de todas as variáveis na NVRAM no campo de log do formulário. Nela deverá constar `boot_wait=on`. Então, desligue o roteador.

Para começar, você deve baixar as imagens prontas de **[2]**. O pacote tar, que tem entre 7 a 8 MB, contém três variantes do firmware: `openwrt-g-code.bin` foi criado para o modelo WRT54G da Linksys, o `openwrt-gs-code.bin` para o roteador WRT54GS e, para os dispositivos compatíveis de outros fabricantes, você precisará da `openwrt-linux.trx`.

Troca de firmware via TFTP

Imediatamente após o roteador ser ligado, o gerenciador de boot é iniciado. Para ele, vale a variável `boot_wait=on`. A interface de rede é configurada com o endereço IP 192.168.1.1, a ser usado nas futuras atualizações do firmware. Os comandos para a conexão e transferência do firmware devem ser digitados com o roteador ainda desligado. Tecle ***[Enter]*** ao fim de cada linha:

```
linux:~# tftp 192.168.1.1
tftp> binary
tftp> rexmt 1
tftp> trace
Packet tracing on
tftp> put openwrt-gs-code.bin
.....
sent DATA <block=3003, 0 bytes>
received ACK <block=3003>
tftp>
```

Ligue o roteador somente após ter digitado o comando `put`. Após alguns segundos inicia-se a transferência, que idealmente deve ser concluída sem erros. Caso o programa exiba a mensagem *Code pattern is incorrect*, isso significa que o firmware transferido não é adequado ao seu modelo de roteador. Já a mensagem *Invalid Password* significa que você não foi rápido o suficiente, e o gerenciador de boot carregou o firmware original do roteador antes do início da transferência.

Enquanto o gerenciador de boot do roteador está rodando, o LED de *Power* (ligado) pisca. Somente quando os LEDs se estabilizarem, indicando um reinício completo do sistema operacional, a transferência estará concluída e o dispositivo pronto. Esse processo todo pode durar entre dois e três minutos.

Primeiros Passos no OpenWrt

Os pacotes de desenvolvimento (*snapshots*) do OpenWrt possuem somente um sistema Linux rudimentar que "levanta" a porta WLAN e lê os endereços de IP e configurações da NVRAM do roteador. Após a conversão para o OpenWrt seu roteador ainda utiliza os mesmos endereços que foram indicados anteriormente no firmware original. Além disso o OpenWrt ativa um firewall mínimo para bloquear, por exemplo, a porta Telnet na conexão WAN e, ao mesmo tempo, permite conexões Telnet na porta local.

As versões oficialmente lançadas do OpenWrt utilizam, em vez de um firewall e a conexão Telnet, um daemon SSH. Caso não seja possível conectar-se por Telnet após rodar o OpenWrt, tente o SSH.

A princípio o servidor Telnet no OpenWrt não exige senha para a conexão como root (**Figura 1**). O sistema de arquivos raiz é um JFFS2, como utiliza-

Figura 1: Para o primeiro login utilize o Telnet. O OpenWrt não solicita nenhuma senha de root, devido à conexão desprotegida.

Satisfação garantida ou seu velho firmware de volta

Caso o OpenWrt não atenda a suas expectativas, é possível voltar a qualquer momento para seu firmware original. Para tanto, primeiro baixe o firmware da seção de download do site do fabricante, como em [3] ou [4], para seu disco rígido e descompacte o arquivo zip.

No caso do Asus WL-500G, um firmware pronto pra usar é encontrado no arquivo zip. Baixe também o script `wl500g-recovery.sh` de [5]. Desligue o roteador e rode o script enquanto o LED indicador *Power* estiver piscando (ou seja, quando o gerenciador de boot estiver ativo). Como parâmetro, indique o nome do arquivo do firmware. Se tudo correr bem, logo depois o roteador Asus iniciará o firmware original.

Nos roteadores Linksys, salve o firmware com o nome `linux.bin` em seu computador. Depois você precisa inserir, no início do arquivo, 32 bytes nulos. O comando é:

```
dd bs=16 skip=2 if=linux.bin of=linux.trx
```

Na seqüência, copie o arquivo `linux.trx`, contendo o novo firmware, para o roteador Linksys em `/tmp`, seja por `wget` em um servidor Web ou por SCP, contanto que você tenha instalado o SSH no OpenWrt. O comando a seguir salva o novo firmware na Flash do roteador e reinicia o dispositivo, como mostrado na **figura 2**.

```
mtd write /tmp/linux.trx linux && reboot
```

Separe alguns minutos para esse processo e em hipótese alguma pressione *reset* durante o procedimento. O roteador reinicia-se após alguns instantes e então você pode trabalhar novamente com o firmware original.

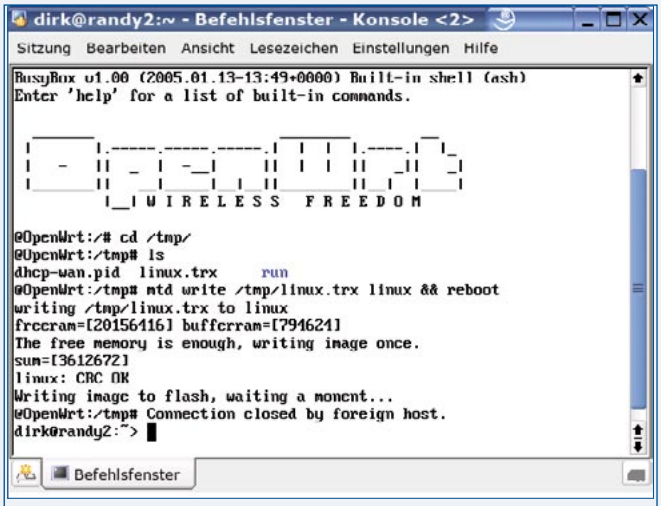

Figura 2: Volta às origens. Após copiar o arquivo com o firmware original para o roteador, utilize o comando `mtd` para gravá-lo na Flash ROM.

do, por exemplo, nos PDAs com Linux. Salvo exceções, a operação do OpenWrt quase não tem diferenças em relação a um sistema Linux "normal". Faltam ao snapshot padrão, entretanto, a maioria dos serviços e programas comumente encontrados em um Linux "de mesa".

O sistema de pacotes ipkg

Para a expansão do OpenWrt foi criado o sistema de pacotes *ipkg*, similar ao popular *apt*, que também pode ser utilizado nos PDAs Zaurus, da Sharp, e outros com o sistema Linux embarcado Opie. O comando `ipkg list` exibe todos os pacotes instalados e instaláveis; pode-se configurar as fontes de pacotes no arquivo `/etc/ipkg.conf`, como mostrado abaixo:

```
src openwrt http://openwrt.org/ipkg
src marc http://wrt54g.free.fr/openwrt/b4/ipkg
dest root /
dest ram /tmp
```

Porém, não é fácil lidar com os arquivos de configuração: por economia de espaço na partição JFFS2 na *Flash ROM* do roteador, os arquivos originais da distribuição são exibidos como links simbólicos no sistema de arquivos raiz. Antes de mexer no arquivo `/etc/ipkg.conf`, ou qualquer outro, é necessário primeiro recopiá-lo para o sistema de arquivos raiz:

```
OpenWrt:/etc# cp ipkg.conf ipkg.conf.new
OpenWrt:/etc# rm ipkg.conf
OpenWrt:/etc# mv ipkg.conf.new ipkg.conf
OpenWrt:/etc# vi ipkg.conf
```

O segundo comando remove o link simbólico da área de ROM do snapshot do OpenWrt e o terceiro renomeia a cópia do arquivo com o nome original.

O ipkg é muito semelhante ao APT do Debian (e de outras distribuições). Os comandos mais importantes são `ipkg update` para atualizar as listas de pacotes, `ipkg list` para listar todos os pacotes disponíveis e instaláveis e `ipkg install` *nome* e `ipkg remove` *nome* para instalação e remoção de pacotes, respectivamente.

Administração de VLANs

Os roteadores da família WRT54G da Linksys são equipados com um *switch* programável. Assim, a interface de rede do roteador é conectada fisicamente a uma das seis portas do *switch*. Entretanto, o OpenWrt pode configurar e controlar as cinco portas restantes com o programa *admcfg*.

Sem parâmetros definidos, o *admcfg* exibe as configurações atuais de todas as seis portas. A porta 0 indica a conexão WAN do roteador e as portas de 1 a 4 ficam disponíveis para as conexões de rede de números 1 a 4. A última porta indica a conexão interna à interface de rede *eth0*, implementada pelo hardware do switch.

O primeiro dos comandos a seguir desconecta a porta 1 do switch na VLAN e contém todos os pacotes de dados que entrarão por essa porta com a etiqueta (*tag*) 4 da VLAN. Com o segundo comando, todos os pacotes com a etiqueta 4 que entram por *eth0* são encaminhados para a interface de rede virtual *vlan4*:

```
admcfg   port1 PVID:4   vlan4
vconfig  add   eth0  4
```

A interface virtual *vlan4* reage como um dispositivo de rede tradicional. Logo após a instalação da VLANs, a *vlan4*, também conhecida como a primeira porta de rede do switch, traz o endereço MAC da interface mestre *eth0*. Esse processo pode ser ajustado por meio do comando `ifconfig vlan4 hw ether` *endereço MAC*.

Os dispositivos virtuais de Ethernet possibilitam, em princípio, uma priorização do tráfego de dados do protocolo IP. Entretanto, os autores não conseguiram configurá-lo com o `admcfg`. Nesse caso, o pacote *iproute2* ainda pode ajudar você – basta instalá-lo com o *ipkg*, da mesma forma que todos os outros programas e serviços que ainda faltem no firmware personalizado de seu roteador. ■

Armazenando as configurações na NVRAM

Os roteadores da família WRT54G armazenam seus dados de configuração no último bloco de armazenamento da Flash, a NVRAM (*Non-Volatile RAM*, ou RAM Não-volátil). Na atualização de firmware essa parte não é tocada, de forma que todas as configurações permanecem, como a senha de root, endereços IP e dados de configuração específicos do dispositivo.

Nesse caso, tratam-se das variáveis para as quais é alocado um valor, por exemplo, `boot_wait=on`. Sob o OpenWrt é possível ler o conteúdo da NVRAM simplesmente digitando o comando `nvram show`. Com `nvram set` *nome=valor*, define-se uma nova variável ou altera-se o valor de uma variável existente. O comando `nvram unset` *nome* remove uma variável da memória.

Todas as alterações ocorrem primeiro na RAM e não serão transferidas para a Flash. Essa transferência ocorre somente ao se executar pela primeira vez o comando `nvram commit`.

Informações

[1] Página Oficial do Projeto OpenWrt: www.openwrt.org

[2] Snapshots do firmware OpenWrt: www.openwrt.org/downloads/snapshots/

[3] Atualizações de firmware para roteadores da Família WRT54G da Linksys: www.linksys.com/download/firmware.asp

[4] Atualizações de firmware para o roteador Asus WL-500G: www.asus.com.tw/support/download/item.aspx?ModelName=WL-500g

[5] Script de recuperação para os roteadores WL-500G da Asus: ftp.linux-magazin.de/pub/listings/magazin/2005/04/Openwrt/wl500g-recovery.sh

[6] Cliente TFTP atftp: ftp.mamalinux.com/pub/atftp/