Instalace NixOS na Turris routery

Installfest 2024

Karel Kočí

16.03.2024

Instalace na Turris Mox

Příprava SD karty

```
~$ sudo parted /dev/mmcblk1
(parted) mktable gpt
(parted) mkpart NixTurris 0% 100%
(parted) set 1 boot on
(parted) quit
~$ sudo mkfs.btrfs /dev/mmcblk1p1
~$ mount /dev/mmcblk1p1 /mnt
~$ tar -xf nixos-system-aarch64-linux.tar.xz -C /mnt
~$ umount /mnt
```

U-Boot

Nutné aktualizovat U-Boot:

```
~# opkg update
~# opkg install turris-nor-update
~# nor-update
```

První boot

```
U-Boot 2022.07 (Aug 15 2022 - 12:25:08 +0000)
...
Hit any key to stop autoboot:  0
=> setenv ramdisk_addr_r 0x9000000
=> saveenv
Saving Environment to SPIFlash... Erasing SPI flash...Writing
to SPI flash...done
OK
=> boot
```

Instalace na Turris Omnia

Příprava USB flash disku

```
~$ sudo parted /dev/sdx
(parted) mktable gpt
(parted) mkpart NixTurris 0% 100%
(parted) set 1 boot on
(parted) quit
  ~$ sudo mkfs.btrfs /dev/sdx1
~$ mount /dev/sdx /mnt
~$ tar -xf nixos-system-armv7l-linux.tar.xz -C /mnt
~$ umount /mnt
```

U-Boot

Nutné aktualizovat U-Boot:

```
~# opkg update
~# opkg install turris-nor-update
~# nor-update
```

První boot

```
U-Boot 2022.10-rc4-OpenWrt-r16653+119-44ce70f0e2
...
Hit any key to stop autoboot:  0
=> setenv boot_targets usb0 mmc0 nvme0 scsi0 pxe dhcp
=> saveenv
Saving Environment to SPIFlash... Erasing SPI flash...Writing
to SPI flash...done
OK
=> boot
```

Aktualizace

```
nix flake init -t gitlab:cynerd/nixturris
nix build .#tarball
```

Nasazení

```
nix build .#toplevel
nix copy --to root@192.168.1.142 $(readlink -f result)
readlink -f result

ssh root@192.168.1.142:

nix-env -p /nix/var/nix/profiles/system --set /nix/store/...
/nix/var/nix/profiles/system/bin/switch-to-configuration switch
```

Intermezzo

Výhody

- Je to server nebo router? Aktualizuje se to stejně..
- Nastavení systému nebo monitoring všude stejné
- Plošné nasazení konfigurace a její aktualizace
- Spousta připraveného softwaru a jednotné balení pro Nix
- Aktualizace je skoro to samé jako čistá instalace
- ...

Není to růžové

- Ne vše co je v Nixpkgs jde cross-zkompilovat
- Armv7l není oficiálně podporovaná platforma
- Turris Omnia aktuálně jen Linux kernel 6.1

NixDeploy

Nasazení na běžící systémy přes SSH z vývojářského PC s podporou cross-kompilace.

```
nix flake init -t gitlab:cynerd/nixdeploy
nix run . -- --help
nix run . laptop
```

SystemD-NetworkD

```
networking = {
  useNetworkd = true;
  useDHCP = false;
};
systemd.network = {};
```

Switch

```
systemd.network = {
  netdevs = {
    "brlan".netdevConfig = {Kind = "bridge"; Name = "brlan";};
  };
  networks = {
    "brlan" = {
      matchConfig.Name = "brlan";
      networkConfig = {DHCP = "yes"; IPv6AcceptRA = "yes";};
    };
    "lan-brlan" = {
      matchConfig.Name = "lan* end0"; networkConfig.Bridge = "brlan";
    };
  };
};
```

Router

```
systemd.network = {
  netdevs."brlan".netdevConfig = {
    Kind = "bridge";
    Name = "brlan";
  };
  networks."lan-brlan" = {
    matchConfig.Name = "lan*";
    networkConfig.Bridge = "brlan";
  };
  wait-online.anyInterface = true;
};
```

Router (end2 jako wan)

```
systemd.network.networks = {
  "end2" = {
    matchConfig.Name = "end2";
    networkConfig = {
      DHCP = "yes";
      IPv6AcceptRA = "yes"; DHCPPrefixDelegation = "yes";
    };
    dhcpV6Config.PrefixDelegationHint = "::/56";
    dhcpPrefixDelegationConfig = {
      UplinkInterface = ":self";
      Announce = "no";
    };
    linkConfig.RequiredForOnline = "routable";
  };
```

Router (brlan network)

```
systemd.network.networks"brlan" = {
  matchConfig.Name = "brlan";
  networkConfig = {
    Address = "192.168.4.1/24";
    IPForward = "yes";
    DHCPServer = "yes";
    DHCPPrefixDelegation = "yes";
    IPv6SendRA = "yes";
    IPv6AcceptRA = "no";
  };
};
```

Router (DHCP)

```
systemd.network.networks"brlan" = {
  dhcpServerConfig = {
    UplinkInterface = "end2";
    PoolOffset = 100; PoolSize = 100;
    EmitDNS = "yes"; DNS = "192.168.4.1";
  };
  dhcpServerStaticLeases = [
    { dhcpServerStaticLeaseConfig =
      { MACAddress = "a8:a1:59:10:32:c4"; Address = "192.168.4.20"; };
    }
  ];
  dhcpPrefixDelegationConfig = {UplinkInterface = "end2"; Announce = "yes"; };
};
```

Router (DNS, Firewall)

```
services.resolved = {
  enable = true;
  fallbackDns = ["1.1.1.1" "8.8.8.8"];
  extraConfig = ''
    DNSStubListenerExtra=192.168.4.1
  '';
};
networking = {
  firewall = {
    interfaces."brlan" = {allowedUDPPorts = [53 67 68];};
    filterForward = true;
  };
  nat = { enable = true; externalInterface = "end2"; internalInterfaces = ["brlan"]; };
};
```

Hostapd (Wi-Fi access point)

AR9287

```
services.hostapd = { enable = true;
  radios = {
    "wlp3s0" = {
      channel = 7; countryCode = "CZ";
      wifi4 = { enable = true;
        inherit (lib.hostapd.qualcomAtherosAR9287.wifi4) capabilities;
      };
      networks."wlp3s0" = {
        ssid = "NixOSInstallFest";
        authentication = {
          mode = "wpa2-sha256"; wpaPassword = "InstallFest2024";
}; }; }; }; };
systemd.network.networks = {
  "lan-wlp3s0" = { matchConfig.Name = "wlp3s0"; networkConfig.Bridge = "brlan"; };
};
```

QCA988x (Wi-Fi 5)

```
nixpkgs.config.allowUnfree = true;
hardware.enableAllFirmware = true;
services.hostapd.radios."wlp2s0" = {
  channel = 36; band = "5g"; countryCode = "CZ";
  wifi4 = { enable = true; inherit (lib.hostapd.qualcomAtherosQCA988x.wifi4) capabilities; };
  wifi5 = { enable = true; inherit (lib.hostapd.qualcomAtherosQCA988x.wifi5) capabilities; };
  networks."wlp2s0" = {
    ssid = "NixOSInstallFest5";
    authentication = { mode = "wpa2-sha256"; wpaPassword = "InstallFest2024"; };
  };
};
systemd.network.networks = {
  "lan-wlp2s0" = { matchConfig.Name = "wlp2s0"; networkConfig.Bridge = "brlan"; };
};
```

Síť pro hosty

VLANy (brlan)

```
systemd.network.netdevs = {
  "brlan" = { netdevConfig = { Kind = "bridge"; Name = "brlan"; };
    extraConfig = ''
      [Bridge]
      DefaultPVID=none
      VLANFiltering=yes
    ''; };
  "home" = { netdevConfig = { Kind = "vlan"; Name = "home"; }; vlanConfig.Id = 1; };
  "guest" = { netdevConfig = { Kind = "vlan"; Name = "guest"; }; vlanConfig.Id = 2; };
};
systemd.network.networks."brlan" = {
  matchConfig.Name = "brlan";
  networkConfig.VLAN = ["home" "guest"];
  bridgeVLANs = [ {bridgeVLANConfig.VLAN = 1;} {bridgeVLANConfig.VLAN = 2;} ];
};
```

VLANy (brlan)

```
systemd.network.networks."lan-brlan" = {
  matchConfig.Name = "lan*";
  networkConfig.Bridge = "brlan";
  bridgeVLANs = [
    {
      bridgeVLANConfig = {
        EgressUntagged = 1;
        PVID = 1;
      };
    }
    {bridgeVLANConfig.VLAN = 2;}
  ];
};
```

VLANy (home a guest)

```
systemd.network.networks = {
  "home" = {
    matchConfig.Name = "home";
    networkConfig = {
      Address = "192.168.4.1/24";
      IPForward = "yes";
      DHCPServer = "yes";
...
  "guest" = {
    matchConfig.Name = "guest";
    networkConfig = {
      Address = "192.168.5.1/24";
      IPForward = "yes";
...
};
```

VLANy (Wi-Fi)

```
services.hostapd.raios."wlp3s0".networks = {
  "wlp3s0" = {
    ssid = "Home"; bssid = "12:f0:21:23:2b:00";
    authentication = { mode = "wpa2-sha256"; wpaPassword = "InstallFest2024"; }; };
  "wlp3s0.guest" = {
    ssid = "Guest"; bssid = "12:f0:21:23:2b:01"; authentication.mode = "none"; };
};
systemd.network.networks = {
  "lan-wlp3s0" = {
    matchConfig.Name = "wlp3s0"; networkConfig.Bridge = "brlan";
    bridgeVLANs = [ { bridgeVLANConfig = { EgressUntagged = 1; PVID = 1; }; } ]; };
  "lan-wlp3s0.guest" = {
    matchConfig.Name = "wlp3s0.guest"; networkConfig.Bridge = "brlan";
    bridgeVLANs = [ { bridgeVLANConfig = { EgressUntagged = 2; PVID = 2; }; } ]; };
};
```

Další tipy

PPPoE

```
services.pppd = { enable = true; peers."wan".config = ''
  plugin pppoe.so end2
  ifname pppoe-wan
  lcp-echo-interval 1
  lcp-echo-failure 5
  lcp-echo-adaptive
  +ipv6
  defaultroute
  defaultroute6
  usepeerdns
  maxfail 1
  user O2
  password 02
''; };
systemd.services."pppd-wan".after = ["sys-subsystem-net-devices-end2.device"];
```

PPPoE (network)

```
systemd.network.networks."pppoe-wan" = {
  matchConfig.Name = "pppoe-wan";
  networkConfig = {
    BindCarrier = "end2";
    DHCP = "ipv6";
    IPv6AcceptRA = "no";
    DHCPPrefixDelegation = "yes";
  };
  ...
};
networking.firewall.extraForwardRules = ''
  tcp flags syn tcp option maxseg size set rt mtu comment "MSS clamping"
'';
```

PPPoE na VLANě

```
systemd.network = {
   netdevs = {
     "end2.848" = {
       netdevConfig = { Kind = "vlan"; Name = "end2.848"; };
       vlanConfig.Id = 848;
   }; };
   networks = {
     "end2" = { matchConfig.Name = "end2"; networkConfig.VLAN = ["end2.848"]; };
     "end2.848" = {
       matchConfig.Name = "end2.848";
       networkConfig.BindCarrier = "end2";
   }; };
```

Routable VPN - home

```
networking.firewall = {
  nftables.enable = true;
  extraForwardRules = ''
    iifname {"home", "vpn"} oifname {"home", "vpn"} accept
  '';
};
```

Wi-Fi (problémy s připojením klientů

```
services.hostapd.radios."wlp3s0".networks."wlp3s0".settings =
{
  wpa_key_mgmt = mkForce "WPA-PSK"; # force use without
sha256
  ieee80211w = 0;
};
```

Firewall: Reject spam

```
networking.firewall.logRefusedConnections = false;
```

Omezení velikosti logů

```
services.journald.extraConfig = ''
  SystemMaxUse=512M
'';
```

Co dál?

- Dokumentace nastavení routeru na NixOS Wiki
- systemd-resolved a DNSSEC do sítě
- Podpora Turris Sentinel
- Šifrovaný root disk (atsha a mox-otp)
- Snazší nastavení pro routery

Děkuji za pozornost

Karel Kočí

https://gitlab.com/cynerd/nixturris

https://git.cynerd.cz https://gitlab.com/cynerd