WiFi

Datum zpracování: 09. 01. 2024

Zpracovali: Kevin Daněk

Zadání

1. Zapojte lokální síť s DHCP.
2. Na routeru povolte WiFi rozhraní a nakonfigurujte primární SSID ve formátu **TUL-ledeXX** (XX je číslo routeru).
3. Nastavte zabezpečení na WPA2/PSK.
4. Připojte se k WiFi pomocí několika zařízení a pomocí programu **iperf3** porovnejte následující spojení:
    1. WiFi - WiFi,
    2. WiFi - kabel,
    3. kabel - kabel.
5. Nakonfigurujte alternativní WiFi se SSID **TUL-guestXX**, bez zabezpečení.
6. Na routeru oddělte pomocí bridge a odděleného IP rozsahu od zabezpečené WiFi a kabelové sítě.
7. Připojte se k WiFi pomocí několika zařízení a pomocí programu **iperf3** porovnejte rychlost mezi dvěma zařízeními s **nezabezpečenou** WiFi.
8. Nainstalujte balíček **luci-app-sqm** a omezte WiFi bez zabezpečení na rychlost 1 Mbps.
9. Ověřte nastavení pomocí **iperf3**.
10. V průběhu práce pořizujte screenshoty a záznamy použitých příkazů; použijte je v elaborátu a okomentujte postup.

Úlohu zpracovávejte ve 2 - 5 členných týmech.

Elaborát zpracujte do šablony v záhlaví kurzu, odevzdávejte ve formátu PDF.

Do abecedně seřazeného seznamu řešitelů na úvodním listu uveďte reálné složení týmu!

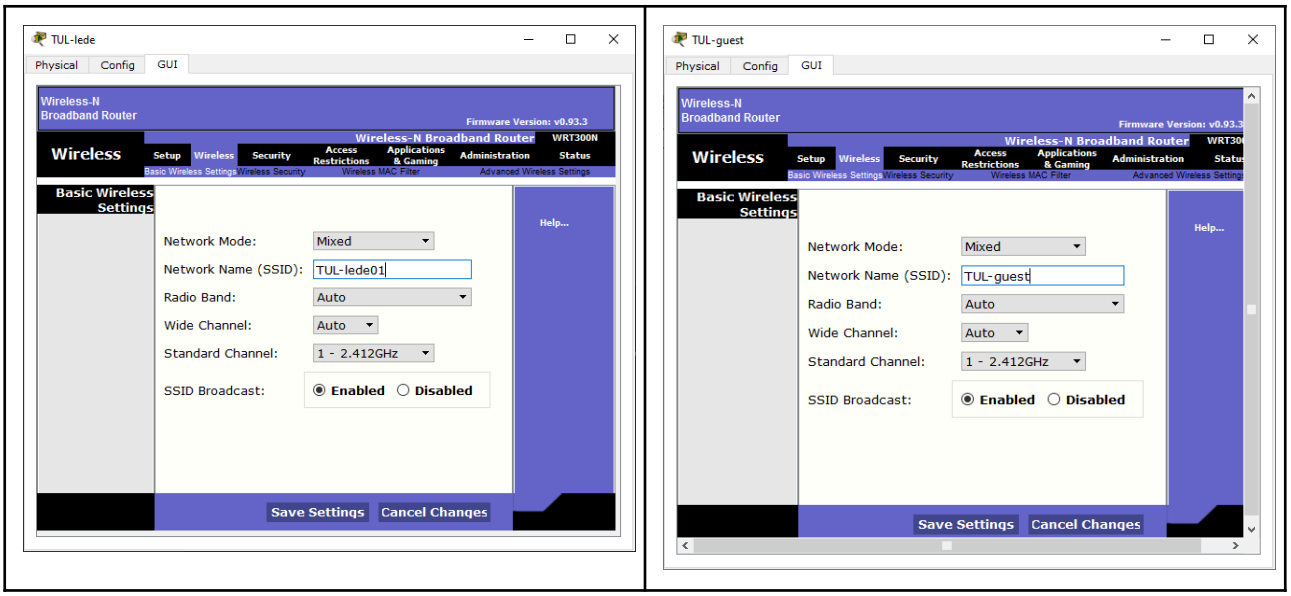
Příprava na cvičení

Stejně jako další cvičení, i tento elaborát není vypracován v laboratoři A305. Ačkoliv se některým mým kolegům podařilo elaboráty vypracovat (ať už s více či méně reálnými výsledky), když jsem se z trucu zkoušel přes ssh připojit do routeru v učebně A305 (192.168.1.1 již v SSH spojení do A0322), tak se mi nedařilo. Nebudu tedy pokoušet své štěstí a opět to vypracuji lokálně. Vzhledem k tomu, že potřebujeme simulovat WIFI, nemůžu použít Docker. K vypracování tedy využiji kombinaci simulátorů sítí (Cisco Packet Tracer Instructor 6) a reálného routeru Archer C6, a pokusím se pracovat "v duchu" zadání (ostatně jako u mých cvičeních v Dockeru).

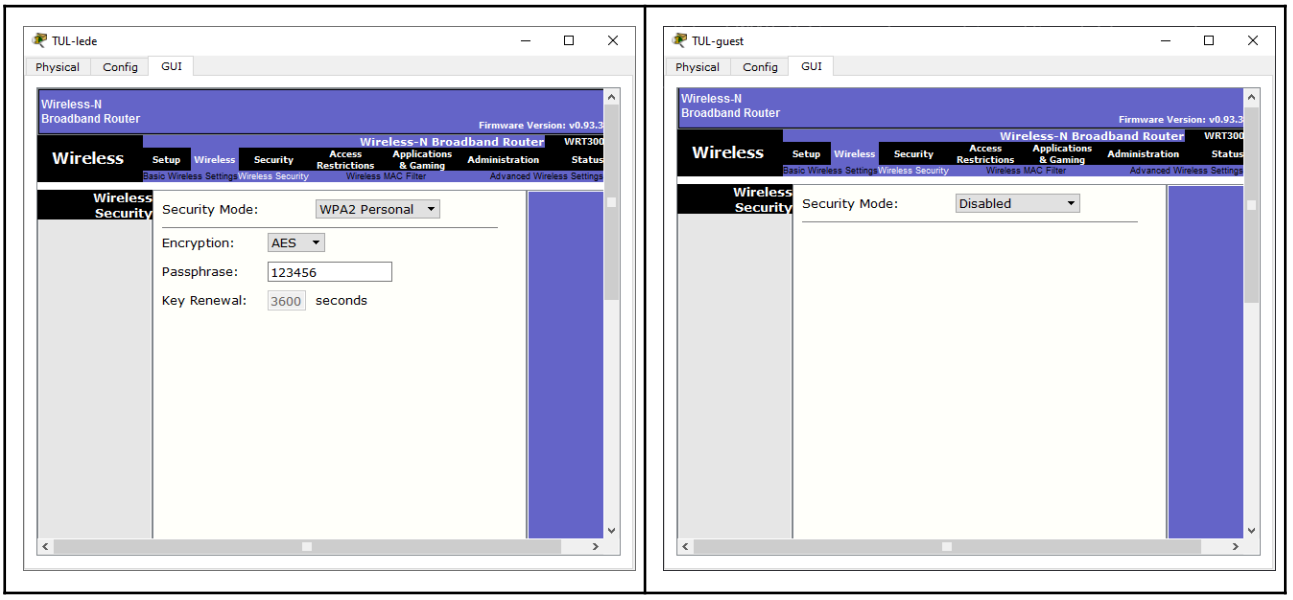
Nastavení dvou sítí s odděleným IP rozsahem

Abych to nemusel dlouhosáhle rozepisovat, nastavím jak síť **TUL-lede01** a **TUL-guest** rovnou nyní s tím, že ukážu jednotlivé odlišnosti v nastavení obou sítí. Obě sítě jsou pro jednodušší simulaci uvažovány jako samostatné routery, které si spravují své klienty. V praxi by šly použít VLANs na jednom routeru.

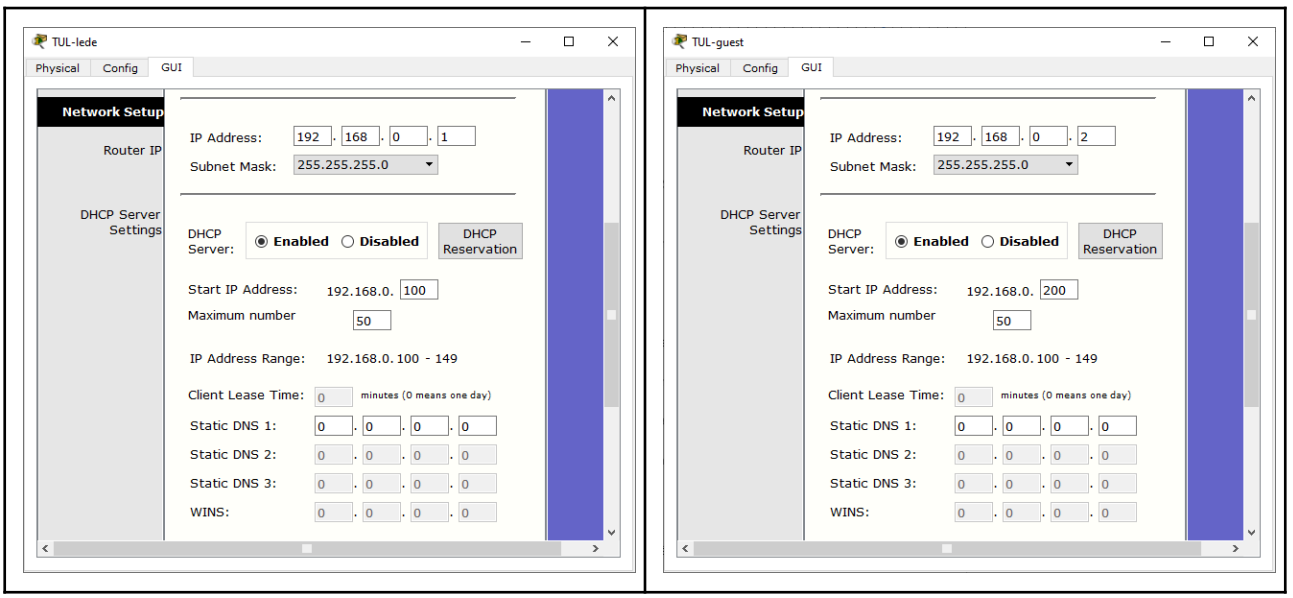
Začneme u nastavení SSID. Jedná se o jedinečný identifikátor nebo název, který se přiřazuje bezdrátovému síťovému rozhraní (například bezdrátovému routeru nebo přístupovému bodu). SSID slouží k identifikaci konkrétní bezdrátové sítě v rámci prostoru, kde může existovat více bezdrátových sítí.



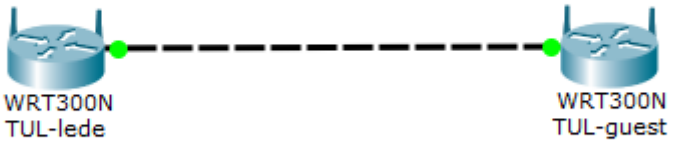
Dále jsou na řadě bezpečnostní režimy Wi-Fi. To jsou protokoly navržené pro zajištění bezpečné komunikace v bezdrátových sítích. Mezi nejčastěji používané patří WEP, i když již zastaralý a nebezpečný, následovaný vylepšenými verzemi WPA (WPA, WPA2 a nejnověji WPA3). WPA2 je momentálně považován za bezpečný standard. Existuje také bezpečnostní protokol WPS, ale kvůli bezpečnostním obavám se často nedoporučuje.



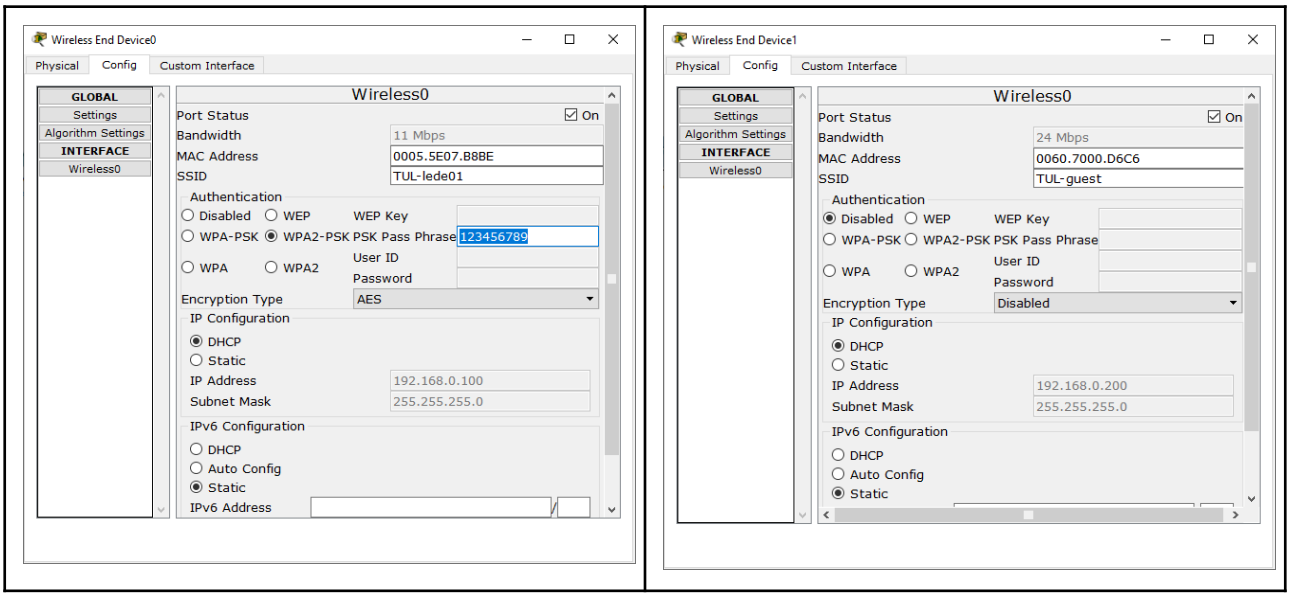
Síťový most slouží k propojení dvou oddělených sítí, umožňuje transparentní přenos dat mezi zařízeními v obou sítích a může být realizován buď fyzickým zařízením, jako je specializovaný síťový most, nebo virtuálně pomocí softwaru. Tato funkcionalita umožňuje segmentaci síťového provozu a integraci různých síťových segmentů s možností použití v různých scénářích, jako je spojování oddělených sítí nebo kombinování bezdrátových a kabelových sítí. Bezpečnostní úvahy jsou důležité při využívání síťového mostu mezi dvěma sítěmi.

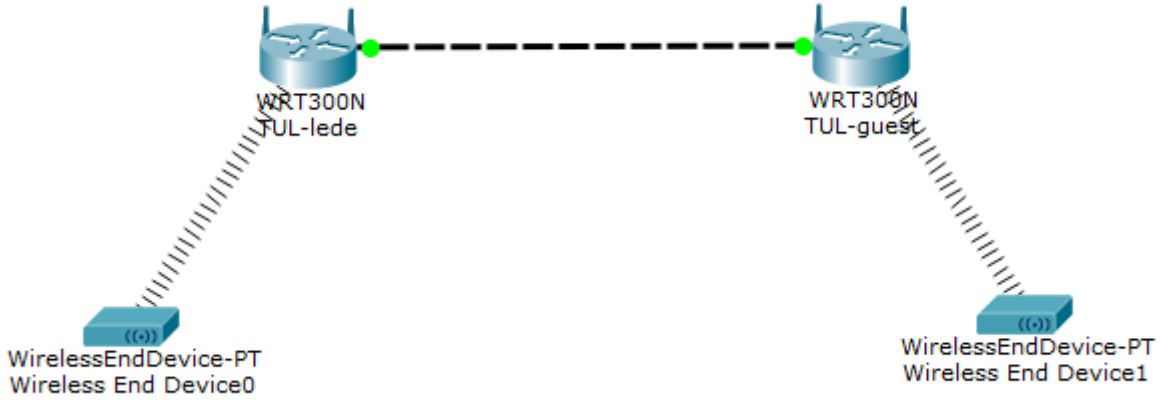


Síťový most lze vytvořit spojením dvou směrovačů pomocí propojení jejich LAN portů. Tento konfigurační krok umožňuje propojit dvě oddělené sítě a umožňuje datovým paketům volně cirkulovat mezi nimi. Propojení LAN portů obou směrovačů vytváří fyzický nebo virtuální most, který propojuje obě sítě a umožňuje zařízením připojeným k jednomu směrovači komunikovat s těmi připojenými k druhému. Tím se vytváří integrovaná síť, která umožňuje sdílení zdrojů a komunikaci mezi oběma sítěmi. Při tomto propojení je důležité konfigurovat směrovače tak, aby pracovaly v režimu mostu a aby byly dodrženy bezpečnostní opatření, zejména pokud jde o správu přístupu a šifrování dat, aby se minimalizovaly bezpečnostní rizika. Tímto způsobem může síťový most usnadnit propojení a integraci dvou samostatných sítí přes propojené LAN porty směrovačů.

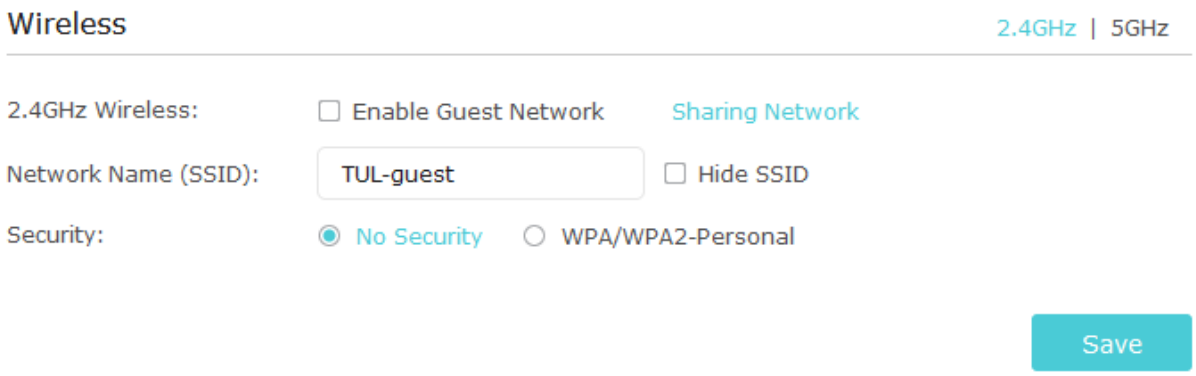


Připojení obecného bezdrátového zařízení k Wi-Fi se provádí pomocí SSID (Service Set Identifier), což je jedinečný název přiřazený bezdrátovému síťovému rozhraní. Uživatelé vybírají požadovanou bezdrátovou síť z dostupných sítí a zadávají případné heslo, pokud je síť zabezpečená.





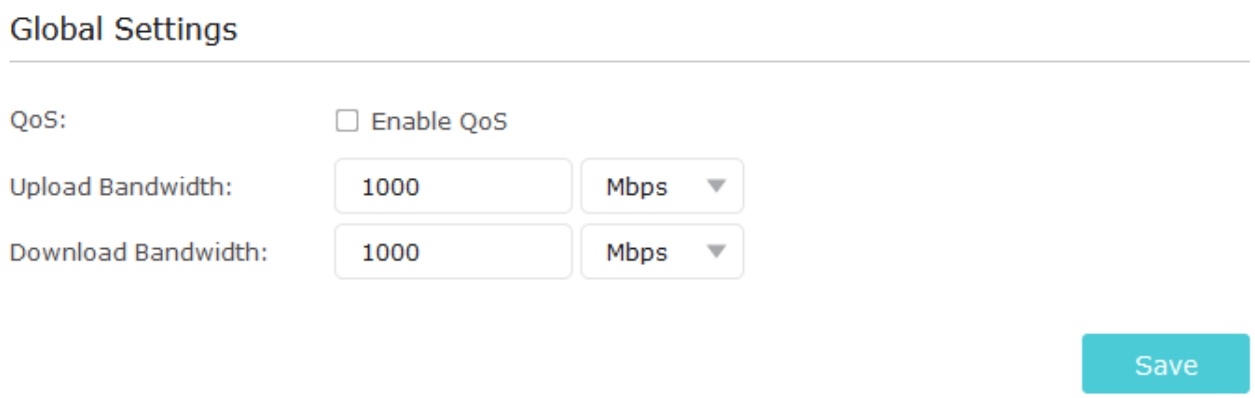
V komerčních routerech se můžeme již běžně setkat s možností WIFI pro hosty, která může mít nejen oddělený rozsah, ale i izolovat samotné klienty od sebe.



Omezení rychlosti WIFI

luci-app-sqm je balíček pro OpenWrt pro správu front v síťovém provozu přímo v rozhraní Luci. Jeho cílem je optimalizovat tok dat a minimalizovat zpoždění v síti, což může být zejména užitečné pro stabilizaci a optimalizaci připojení ve sdílených sítích nebo v případech, kdy je připojení zatíženo. luci-app-sqm může být použito k omezení šířky pásma (bandwidth) pro konkrétní síťové rozhraní, což může ovlivnit rychlost Wi-Fi, pokud je tato síťová rozhraní spojené s bezdrátovým přístupem.

Dnes lze šířku pásma omezit i na domácích routerech pomocí nastavení QoS (Quality of Service), které efektivně pracuje stejně jako SQM (Smart Queue Management) na OpenWrt routerech.



Závěr

Nastavení Wi-Fi sítí vyžaduje pečlivou pozornost k několika klíčovým aspektům. Jednou z důležitých úloh je zajištění jednoznačného a jedinečného identifikátoru sítě, známého jako SSID, který usnadňuje identifikaci sítě. Bezpečnostní opatření, jako je používání silného šifrování (například WPA3), jsou klíčová pro ochranu dat a zabránění neoprávněnému přístupu. Správa šířky pásma, kvality služeb (QoS) a další parametry jsou také důležité pro optimalizaci výkonu sítě. Aktualizace firmwaru zařízení a správná šifrování hesel pro přístup k síti přispívají k celkové bezpečnosti a úspěšnému provozu bezdrátové sítě.