
© Copyright 2005 Compex Systems Pte Ltd

Všechna práva vyhrazena

Tento dokument obsahuje informace, které jsou chráněny autorským zákonem. Reprodukce, úprava nebo překlad bez předchozího povolení je zakázáno. Možné je to akorát v případech, které uvádí autorský zákon.

Informace o obchodních značkách

Compex®, ReadyLINK® a MicroHub® jsou registrované obchodní značky firmy Compex, Inc. Microsoft Windows a logo Windows jsou obchodní značky firmy Microsoft, Corp. NetWare je registrovaná obchodní značka firmy Novell, Inc. Všechny další značky a názvy produktů jsou obchodními značkami nebo registrovanými obchodními značkami příslušných vlastníků.

Poznámka: Autorská práva © 2005 Compexu, Inc. Všechna práva vyhrazena. Reprodukce, úprava nebo překlad bez předchozího povolení firmy Compex je zakázáno. Možné je to akorát v případech, které uvádí autorský zákon.

Revize manuálu : Ann

Číslo manuálu: U-0478-V1.1C Verze 1.1 Listopad 2005

Odvolání

Compex, Inc. poskytuje tento manuál bez jakékoliv záruky, a není tedy možné se na něj odvolávat. Compex, Inc. si vymezuje možnost provedení změn a/nebo vylepšení produktu a/nebo jeho norem popsaných v tomto manuálu bez předchozího oznámení. Compex, Inc. nebude zodpovědný za žádné technické nepřesnosti nebo typografické chyby v tomto manuálu. Změny jsou průběžně uváděny v informační příloze a budou začleněny do novější verze manuálu. Obsažené informace se mění bez předešlého oznámení.

Vaše reakce

Oceníme vaše reakce. V případě, že v tomto uživatelském manuálu naleznete chyby, nebo budete mít návrhy na jeho zlepšení, budeme rádi, když nás o nich informujete. Prosíme kontaktujte nás na:

Fax: (65) 62809947

Email: feedback@compex.com.sg

FCC PRAVIDLA

Toto zařízení bylo testováno a vyrobeno společností s vymezením pro třídu B digitálních zařízení ve shodě s částí 15 FCC směrnic. Tato vymezení jsou navržena pro poskytování dostupné ochrany proti škodlivým vlivům při montáži v obytných zónách. Toto zařízení generuje, užívá a může vyzařovat energii rádiových vln a pokud nebude instalováno a užíváno v souladu s instrukcemi, může mít škodlivý vliv na radiokomunikaci. Není zde však zaručeno, že se tyto vlivy nevyskytnou při jednotlivých instalacích. Pokud bude toto zařízení příčinou rušení rádiových nebo televizních signálů, je třeba zkusit odstranit rušení jedním z následujících způsobů:

- Přeorientovat nebo přemístit přijímací anténu .
- Zapojit počítač do jiné zástrčky než na stávajícím místě .
- Zvětšit vzdálenost mezi počítačem a přijímačem.
- Konsultovat problém s dealerem nebo zkušeným rádiovým či televizním technikem .

Varování: Jakékoliv neautorizované změny v zařízení mohou zrušit záruky a správnou funkčnost zařízení.

FCC Sdělení o shodě: Toto zařízení vyhovuje části 15 FCC směrnic. Provoz musí splňovat dvě následující podmínky:

1. Toto zařízení by nemělo být příčinou rušení
2. Toto zařízení musí respektovat jakékoliv vlivy přijaté, včetně vlivů, které mohou být příčinou nežádoucí operace

Produkty obsahující rádiový vysílač jsou označeny FCC ID a mohou také nést FCC logo.

Varování: Vystavení záření radiofrekvence.

Pro vyhovění požadavkům FCC RF je nutné splnit tyto zásady instalace antény a ovládání zařízení:

- a) Pro konfiguraci používající integrovanou anténu, musí být vzdálenost mezi anténou a lidským tělem (včetně rukou, zápěstí, chodidel a kotníků) nejméně 2,5cm (1 palec).
- b) Pro konfiguraci používající externí anténu, musí být vzdálenost mezi anténou a lidským tělem (včetně rukou, zápěstí, chodidel a kotníků) nejméně 20cm (8 palců).

Vysílač by neměl být spojen s jinými vysílači či anténami.

Ustanovení ICES 003

Tato třída B digitálních přístrojů vyhovuje kanadské normě ICES-003.

Prohlášení o shodě

Compex, Inc. prohlašuje následující:

Název produktu: Compex Wireless-G 54Mbps XR™ Access Point

Číslo modelu: Compex WP11B+ se řídí následujícími standardy produktu:

Toto zařízení vyhovuje směrnici elektrinagnetické kompatibility (89/336/EEC), která byla vydaná komisí Evropského společenství. Dodržení této směrnice znamená přizpůsobit se následujícím evropským normám (v závorkách jsou ekvivalentní mezinárodní normy)

Electromagnetické vlivy (přenos a záření): EN 55022 (CISPR 22)

Electromagnetická odolnost: EN 55024 (IEC61000-4-2,3,4,5,6,8,11)

Směrnice nízkého napětí: EN 60 950: 1992+A1: 1993+A2: 1993+A3: 1995+A4: 1996+A11:1997.

Tento produkt je ve shodě s následujícími regionálními normami: FCC třída B : zastupující FCC část 15 směrnici; **CE certifikát** : zastupující EC směrnici.

Compex, Inc. Také prohlašuje, že:

Bezdrátová karta v tomto produktu je ve shodě se směrnicí R&TTE (1999/5/EC) vydaná komisí Evropského společenství. Dodržení této směrnice znamená přizpůsobit se následujícímu:

EMC normy: FCC: 47 CFR část 15, odstavec B, 47 CFR část 15, odstavec C (sekce15.247); CE: EN 300 328-2, EN 300 826 (EN 301 489-17)







Tento produkt je ve shodě s následujícími regionálními normami: FCC třída B : zastupující FCC část 15 směrnici; **CE certifikát** : zastupující EC směrnici.

Informace technické podpory

Informace o záruce a registrační formulář můžete najít v Rychlém průvodci instalací.

Pro technickou podporu můžete kontaktovat Compex nebo jeho zastoupení. Pro vaše pohodlí můžete také vyhledat technickou asistenci vašeho místního distributora nebo autorizovaného dealera, od kterého jste si produkt zakoupili. Můžete dále využít technické podpory po internetu pomocí našeho mailu support@compex.com.sg.

V tabulce naleznete odkaz na nejbližší centrum technické podpory:

Centra technické podpory	
Kontaktujte centrum technické podpory, které se nachází v oblasti, kde žijete.	
U.S.A., Kanada, Latinská Amerika and Jižní Amerika	
 Pište	Compex, Inc. 840 Columbia Street, Suite B Brea, CA 92821, USA
 Volejte	Tel: +1 (714) 482-0333 (8 a.m.-5 p.m. Pacific time) Tel: +1 (800) 279-8891 (Ext.122 Technical Support)
 Faxujte	Fax: +1 (714) 482-0332
Asie, Austrálie, Nový Zéland, Sřřední východ a zbytek světa	
 Pište	Compex Systems Pte Ltd 135, Joo Seng Road #08-01, PM Industrial Building Singapore 368363
 Volejte	Tel: (65) 6286-1805 (od 8 do 17 místního času)
 Faxujte	Tel: (65) 6286-2086 (linka 199 technická podpora) Fax: (65) 6283-8337
Internet	E-mail: support@compex.com.sg FTPsite: ftp.compex.com.sg
Website:	http://www.cpx.com or http://www.compex.com.sg

O tomto dokumentu

Produkt, popsáný v tomto dokumentu, Compex Wireless-AG 54Mbps XR™ Managed Access Point, Compex WP54AG je licencovaný produkt firmy Compex Systems Pte Ltd. Tento dokument obsahuje instrukce pro instalaci, konfiguraci a používání Access pointu. Dává také celkový pohled ke klíčovým aplikacím a síťovým koncepcím k přihlednutím k produktu.

Tato dokumentace je určena síťovým administrátorům stejně jako koncovým uživatelům, kteří mají jen základní znalost síťových struktur a produktů.

Předpokládá se, že na hostitelském počítači byl již nainstalován TCP/IP a že již funguje připojení k internetu. Jsou zde popsány postupy pro operační systémy Windows 98SE/ME/2000/XP. Je možné, že pro další operační systémy bude potřeba se odvolat na dokumentaci vašeho operačního systému síťování.

Jak používat tento dokument

Tento dokument může být odstraněn. V tomto případě naleznete jeho poslední verzi na: <http://www.compex.com.sg>

Tento dokument je psán takovým způsobem, aby bylo pro uživatele pohodlné najít konkrétní informace náležící k tomuto produktu. Skládá se z kapitol, ve kterých jsou detailně vysvětleny instalace a konfigurace Compexu WP54AG.

Programové vybavení

Tento manuál je založen na programovém vybavení verze 1.02 build 1115.

Zásady

V tomto dokumentu jsou použity speciální zásady, které slouží k jasnému předložení informací. Compex Wireless-AG 54Mbps XR™ Access Point je často označován jako *WP54AG* nebo *access point* nebo *AP*. Následuje seznam nejčastěji užívaných zásad.



POZNÁMKA
Důležité instrukce

Table of Contents



VÝSTRAHA

Toto se týká rizika poškození, zničení systému nebo ztráty dat



VAROVÁNÍ

Nebezpečí vážného poškození

Odkazy na menu příkazů, Push Button, Radio Button, LED a nadpis jsou psány tučně př. "stiskněte tlačítko **OK**".

Table of Contents

Copyrights © 2005 Compex Systems Pte Ltd.....	i
Informace o obchodních značkách.....	i
Odvolaání	i
Vaše reakce	i
FCC NOTICE	ii
OProhlášení o shodě.....	ii
Informace technické podpory	iii
O tomto dokumentu	iv
Jak používat tento dokument.....	iv
Programové vybavení.....	iv
Zásady.....	iv

KAPITOLA 1: OBECNĚ O PRODUKTU 1

Úvod.....	1
Vlastnosti a výhody	2
Balení Compex WP54AG	3
Kdy použít který mod	3
Mod Access Point	4
Mod Access Point Client.....	5
Mod Point to Point	6
Mod Point to Multiple point.....	7
Mod Wireless Routing Client.....	8
Mod Gateway	9

KAPITOLA 2: INSTALACE HARDWARU 11

Požadavky při nastavení.....	11
Instalace hardwaru	11
První možnost: Napájení WP54AG pomocí síťového adaptéru.....	11
Druhá možnost: Napájení WP54AG pomocí Compex PoE.....	13

KAPITOLA 3: PŘÍSTUP NA WEBOVÉ ROZHRAŇÍ 16

Přístup na webové rozhraní pomocí uConfig	16
Ověření IP adresy Compexu WP54AG pomocí NpFind.....	20
Manuální přístup na webové rozhraní přes Internet Explorer.....	21

Table of Contents

KAPITOLA 4: BĚŽNÁ KONFIGURACE26

Nastavení Management Portu	26
Nastavení vašeho LAN	27
Pro přehled aktivních DHCP leases.....	30
Pro rezervaci specifických IP adres pro předem stanovené DHCP klienty	
31	
Nastavení WLAN	34
Pro konfiguraci základního nastavení bezdrátového modu	35
Pro konfiguraci bezpečnostního nastavení bezdrátového modu	44
Pro konfiguracei pokročilého nastavení bezdrátového modu	44
Statistiky.....	46
Nastavení WAN	53
(poporované jen mody Wireless Routing Client a Gateway)	53
Nastavení SNMP	61
Nastavení STP	62
(Dostupné jen v modech Access Point, Point to Point a Point to Multiple Point)	62
MAC Filtrace.....	67

KAPITOLA 5: BEZPEČNOST WLAN.....71

Jak nastavit WEP	72
Jak nastavit WPA-PSK/WPA2-PSK/WPA-PSK-AUTO (dostupné jen v modu Access Point)	73
Jak nastavit 802.1x/RADIUS (dostupné jen v modu Access Point).....	75
Jak nastavit WPA EAP/WPA2-EAP/WPA-EAP-AUTO (jen mod Access Point podporuje WPA2-EAP a WPA-EAP-AUTO)	77

KAPITOLA 6: ROZŠÍŘENÉ BEZDRÁTOVÉ VLASTNOSTI80

Kontrola přístupu – Bezdrátový Pseudo VLAN (jen v modu Access Point)..	80
Bezdrátový Pseudo VLAN Per Node	81
Bezdrátový Pseudo VLAN Per Group.....	84
Bezdrátové nastavení – Bezdrátový distribuční systém (WDS) (jen v modu Access Point).....	88
Parametry dlouhé vzdálenosti.....	94

KAPITOLA 7: POKROČILÁ KONFIGURACE.....97

Routing (Podporován jen mody Wireless Routing Client a Gateway)	97
--	-----------

Table of Contents

Pro konfiguraci statického Routing Complexu WP54AG.....	98
NAT (Podporován jen mody Wireless Routing Client a Gateway).....	99
Pro konfiguraci virtuálních serverů založených na hostování v demilitarizační zóně (DMZ)	100
Pro konfiguraci virtuálních serverů založených na odesílání portu	102
Pro konfiguraci virtuálních serverů založených na odesílání IP.....	104
Vzdálený Management (podporovaný jen mody Wireless Routing Client a Gateway)	106
Pro nastavení vzdáleného Managementu	106
Paralelní připojení (podporované jen v modem Gateway)	107
Pro aktivaci parallel broadband na Complexu WP54AG.....	108
Oznámení Emailu.....	109
Překlad statické adresy (podporováno jen mody Wireless Routing Client a Gateway)	111
Přesměrování DNS (podporováno jen mody Wireless Routing Client a Gateway)	113
Pro aktivaci/deaktivaci přesměrování DNS	115
Nastavení Dynamic DNS	115
Pro aktivaci/deaktivaci nastavení Dynamic DNS	116
Pro spravování seznamu Dynamic DNS (DDNS)	116

KAPITOLA 8: BEZPEČNOSTNÍ KONFIGURACE 121

Filtrace balení	121
Pro konfiguraci filtrace balení.....	121
Filtrace URL	125
Pro konfiguraci filtrace URL.....	125
Konfigurace Firewall.....	126
Pro konfiguraci SPI Firewall	126
Firewall Logy.....	130
Pro náhled Firewall Logů.....	130

KAPITOLA 9: SYSTEMOVÉ UTILITY 131

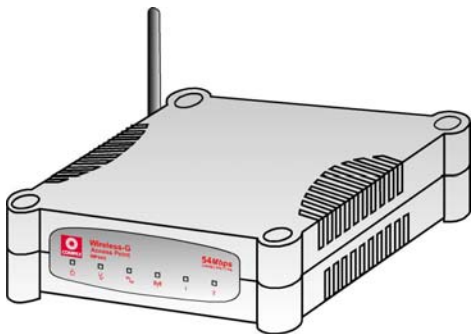
Použití menu SYSTEM TOOLS.....	131
Ping Utilita	131
Systémová Identita	132
Nastavení hodin systému.....	133
Upgrade programového vybavení	134
zálohování a resetování Nastavení	136
Restart Systému	139

Table of Contents

Změna hesla.....	140
odhlášení	141
Použití HELP menu	142
Dostaňte technickou podporu.....	142
O Systému.....	143
DODATEK I: OBNOVA PROGRAMOVÉHO VYBAVENÍ.....	144
DODATEK II: KONFIGURACE TCP/IP	146
Pro Windows 95/98/98SE/ME/NT	146
pro Windows XP/2000.....	148
DODATEK III: VZHLED PANELU & POPISKY	150
DODATEK IV: TECHNICKÉ SPECIFIKACE	153

Kapitola 1: Obecně o produktu

Úvod



The Complex WP54AG Wireless-AG 54Mbps XR™ Access Point je vysoce výkonný AP, který je vyroben jak pro podnikové, tak pro veřejné přístupové aplikace. Je postaven na Atheros chipsetu a může se pochlubit síťovou stabilitou a širokým síťovým pokrytím. Je založen na technologii 802.11g a umožňuje vysokorychlostní přenos dat až do 54Mbps na 2.4GHz a 5.4GHz.

Access point je schopný operovat v 6 modech: **Access Point**, **Access Point Client**, **Point-to-Point**, **Point-to-Multi Point**, **Wireless Routing Client** a **Gateway**, což ho činí vhodným pro širokou škálu bezdrátových aplikací včetně rozmístění na dálku.

Access point poskytuje širší pokrytí vaší sítě, a to hlavně díky vybavení SMA konektorem pro podporu vnější antény. Navíc jeho integrované napájení přes ethernet (PoE) umožňuje, aby byl WP54AG použit v oblastech, ve kterých není snadný přístup k elektrické zásuvce.

WP54AG je vybaven mnoha bezdrátovými bezpečnostními vlastnostmi jako např. Wi-Fi Protected Access (WPA), WPA2 (se zdokonaleným kódováním standardním kódováním) MAC Address Filtering, IEEE 802.1x Authentication a 64/128-bit WEP (Wired Equivalent Privacy), což slouží k větší bezpečnosti a k zajištění soukromí všech uživatelů v rámci stejného bezdrátového LAN.

WP54AG také spojuje unikátní vlastnosti jako – vlastnost Parallel Broadband, který umožňuje seskupení šířky pásma a schopnost redundance při výpadku; bezdrátový distribuční systém (WDS) sloužící k tomu, aby spolu bezdrátově propojil všechny access pointy; parametry dlouhé vzdálenosti, které zajišťují, aby WP54AG sám vypočítal parametry jako např. time sloty, ACK časové prodlevy a CTS časové prodlevy, aby dosáhl delšího rozsahu; Spanning Tree Protocol (STP), který poskytuje bezdrátové síti větší redundanci a tím i spolehlivost, (v případě změn v síťovém připojení se síť sama překonfiguruje); Pseudo VLAN feature, který umožňuje vytvoření bezdrátového izolovaného uzlu

Product Overview

nebo pracovní skupiny bezdrátových klientů, aby zvýšil síťové soukromí v bezdrátovém LAN.

VLASTNOSTI A VÝHODY

Access point byl vyroben, aby podával vysoký výkon a nabízí širokou řadu vlastností, se kterými byste se měli seznámit, aby byl využit plný potenciál access pointu.

- **Bezdrátový distribuční systém (WDS)**

Tato vlastnost umožňuje spojit několik access pointů, virtuálně vytváří širší síťovou infrastrukturu, což umožňuje mobilním uživatelům bezdrátový pohyb a stále mít možnost přístupu k síťovým zdrojům.

- **Bezdrátový Pseudo VLAN**

Unikátní technologie Wireless Pseudo VLAN je vlastnost, která umožňuje bezdrátovým klientům rozdělit se po jednotlivcích nebo do pracovních skupin, a takto blokovat přístup jiným uživatelským počítačům a zvýšit soukromí bezdrátového klienta. Tato vlastnost je užitečná hlavně v případě umístění na veřejném místě.

- **Vysoce zabezpečená bezdrátová síť**

Access point podporuje nejlepší dostupné bezdrátové bezpečnostní: Wi-Fi Protected Access 2. WPA2 má dva odlišné mody: WPA2-PSK pro uživatele v SOHO a WPA2-EAP pro podnikové uživatele. Access point také podporuje IEEE 802.1x, což slouží k bezpečnému a centralizovanému uživatelskému ověření. Bezdrátoví klienti jsou tímto požádáni k ověření vysoce bezpečnými metodami, jako např. EAP-TLS, EAP-TTLS, a EAP-PEAP, aby docílili přístupu k síti.

- **Smart Select**

Tato vlastnost automaticky prohlíží a doporučuje ty nejvhodnější kanály, které access point může využívat.

- **Utilita uConfig**

Exklusivní utilita **uConfig** umožňuje uživateli pohodlný přístup na webové konfigurační rozhraní access pointu bez nutnosti změny nastavení TCP/IP pracovní stanice.

- **STP**

Spanning-Tree Protokol poskytuje redundanci cesty, zatímco předchází nežádoucím smyčkám v síti. To nutí určitá redundantní datové cesty, aby

Product Overview

zůstaly ve stavu zálohy. Jestliže síťový segment ve Spanning-Tree Protokolu není dostupný, nebo jestliže ve Spanning-Tree Protokolu dojde ke změnám, algoritmus spanning-tree rekonfiguruje topologii spanning-tree a založí nově spojení aktivací zálohované cesty.

BALENÍ COMPEX WP54AG

Balení Complex WP54AG 1a obsahuje následující položky:

- 1 x Complex WP54AG 1a
- 1 x Vnější napájecí adaptér
- 1 x 2dBi SMA Anténa
- 1 x Upozornění před použitím
- 1 x Instalační CD

KDY POUŽÍT KTERÝ MOD

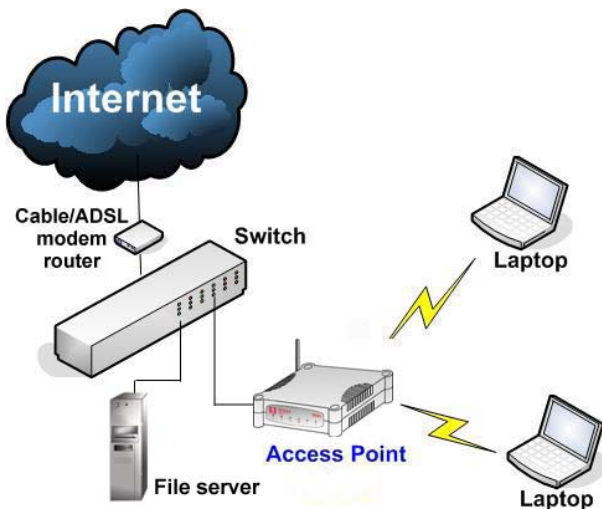
Access point je všestranný ve smyslu, že dokáže pracovat v šesti různých typech modů: **Access Point Mode**, **Client Mode**, **Point to Point**, **Point to Multiple Point**, **Wireless Routing Client** a **Gateway**.

Tato sekce představuje stručný náčrt různých síťových aplikací, které mohou být akomodovány přes různé mody access pointu.

Product Overview

MOD ACCESS POINT

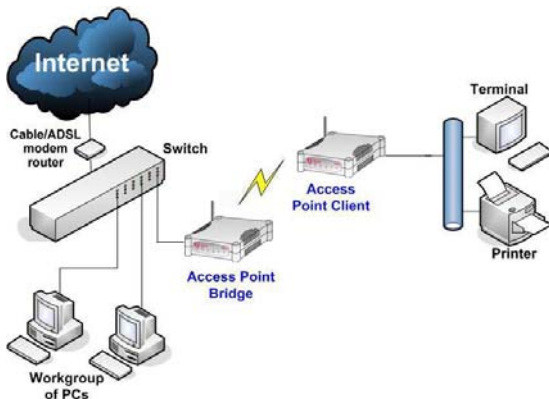
Toto je standardní mod Access pointu. Mod **Access Point** vám umožňuje vytvořit most mezi bezdrátovým klientem a drátovou síťovou infrastrukturou, což poslouží k vzájemné komunikaci.



Horní příklad ukazuje, jak budou bezdrátoví uživatelé schopní přistupovat k file serveru, připojenému ke switchi přes access point v modu **Access Point**.

MOD ACCESS POINT CLIENT

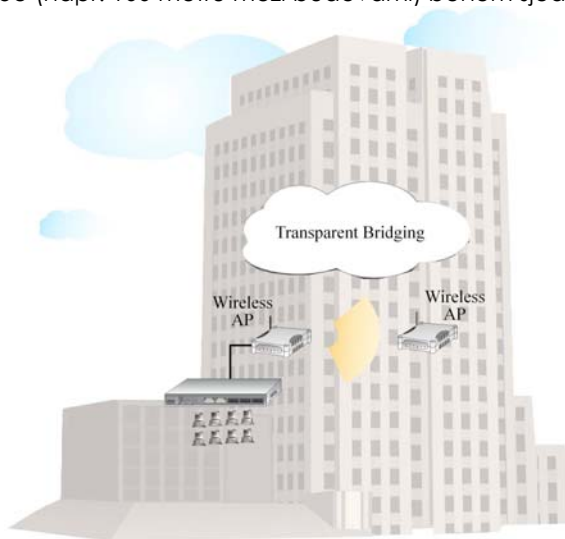
V modu **Access Point Client**, hraje access point roli bezdrátového klienta, který je schopný bzezdrátově operovat s jiným access pointem, což vytváří přemostění mezi dvěma rychlými ethernetovými sítěmi. Access Point klient nemůže komunikovat přímo s jakýmkoliv jiným bezdrátovým zařízením.



Horní příklad ukazuje, jak bude pracovní skupina počítačů schopná přístupu k tiskárně připojené k access pointu v modu **Access Point Client**.

MOD POINT TO POINT

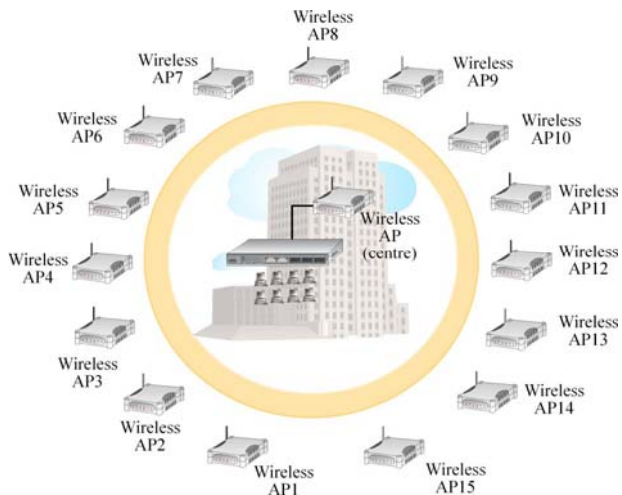
V modu **Point to Point** umožňuje access point směrové spojení mezi různými budovami. Umožňuje vám to vytvořit most mezi bezdrátovými klienty, kteří jsou kilometry od sebe (např. 100 metrů mezi budovami) během sjednocování sítě.



Příklad nahoře ukazuje, jak můžete konfigurovat dva access pointy, abyste vytvořili průhledné přemostění mezi dvěma budovami.

MOD POINT TO MULTIPLE POINT

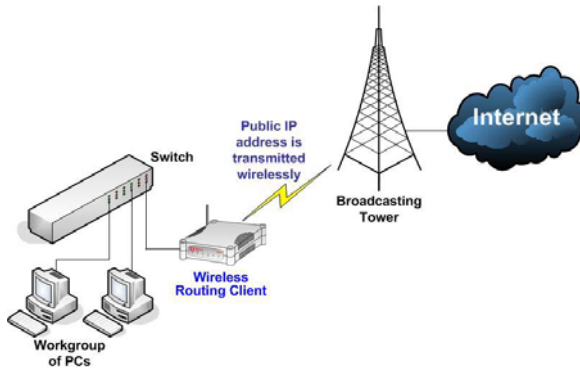
Modu **Point to Multiple Point** je podobný modu Point to Point. Rozdílem je to, že access point umístěný v jednom zařízení je schopný připojit se až k 8 access pointům (AP) instalovaným v jakémkoliv směru od tohoto zařízení (to znamená od 0 do 360 stupňů).



Horní ilustrace ukazuje, jak tento mod operuje. Pozor na obrázku je chybně uvedeno 15 peerů, maximum je 8.

MOD WIRELESS ROUTING CLIENT

Aplikace tohoto modu by byla pro ethernetový port **Wireless Routing Client** vhodná k použití pro spojení dalších zařízení na síti, zatímco přístup k internetu by byl dosahován pomocí bezdrátové komunikace s bezdrátovým ISP.

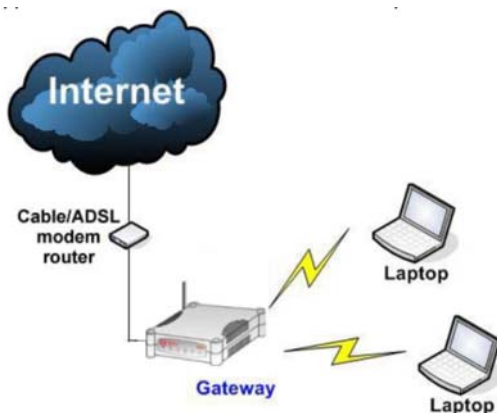


Horní ilustrace ukazuje, jak tento mod operuje.

MOD GATEWAY

Nebo zjednodušeně, sdílení širokopásmového internetu bezdrátovou sítí!

Protože access point podporuje několik typů širokopásmového připojení, je prvním krokem při nastavování access pointu jako *Broadband Internet Gateway* identifikace typ širokopásmového internetového přístupu, který používáte.



Statická IP adresa

Použijte tento typ připojení pokud máte u vašeho poskytovatele internetových služeb předplacenou fixní IP adresu nebo řadu fixních IP adres.

Dynamická IP adresa

Pokud používáte tento typ připojení, access point vás požádá o IP adresu, která mu bude automaticky přiřazená vašim poskytovatelem internetových služeb.

Tento typ připojení se vztahuje např. na:

- Předplatitele Singapore Cable Vision
- Uživatele @HOME Cable Service

PPP over Ethernet (PPPoE)

Zvolte tento typ připojení v případě, že užíváte službu ADSL v zemi, která pro ověřování využívá standardní PPP over Ethernet.

Product Overview

Například:

Pokud jste v Německu, které používá připojení T-1 nebo pokud používáte SingNet Broadband nebo Pacific Internet Broadband v Singapuru.

PPTP

Zvolte tento typ připojení, pokud užíváte služby ADSL v zemi, která využívá připojení a ověření PPTP.

Kapitola 2: Instalace hardwaru

POŽADAVKY PŘI NASTAVENÍ

Předtím než začnete, prosíme ověřte dostupnost následujícího:

- CAT5/5e síťový kabel
- Alespoň na jednom počítači je nainstalován webový prohlížeč a drátový nebo bezdrátový síťový ethernet adaptér
- TCP/IP protokol je nainstalován a parametry IP adresy jsou správně konfigurované na všech síťových modech

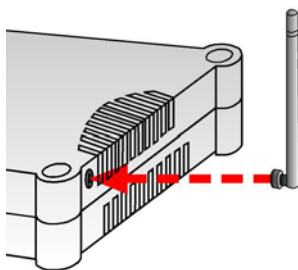
INSTALACE HARDWARU

Access point může být napájen buď použitím přiloženého napájecího adaptéru nebo pomocí CompeX PoE Injector. Instalační proces k oběma možnostem je popsán níže.

PRVNÍ MOŽNOST: NAPÁJENÍ WP54AG POMOCÍ SÍŤOVÉHO ADAPTÉRU

Krok 1:

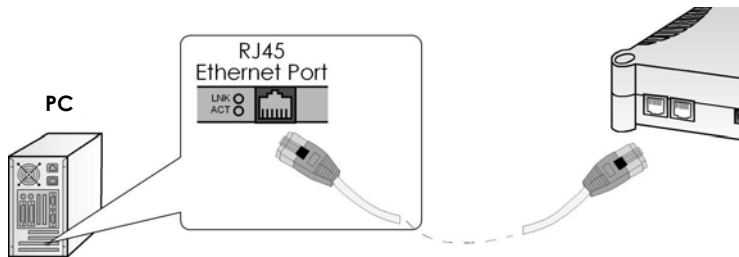
Připojte vnější anténu do SMA konektoru access pointu.



Krok 2:

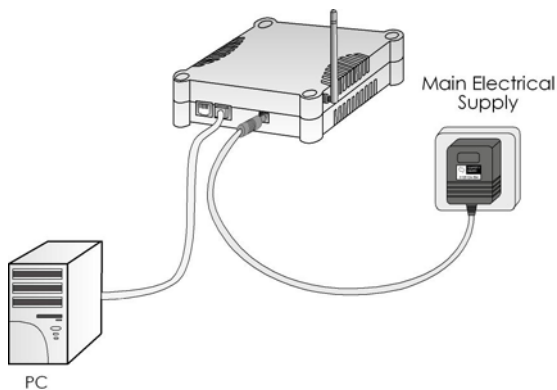
Vložte jeden konec RJ45 ethernetového kabelu do kteréhokoli LAN portu na access pointu a druhý konec kabelu do ethernetového síťového adaptéru na vašem počítači.

Hardware Installation



Krok 3:

Připojte napájecí adaptér k hlavnímu zdroji elektřiny a zapojte zástrčku access pointu do zásuvky.



Krok 4:

Zapněte svůj počítač. Všimněte si, že LED: **Power** a **Port 1** nebo **2** (podle toho, do kterého jste připojili RJ45 ethernetový kabel) se rozsvítily. To je známkou toho, že spojení mezi access pointem a vaším počítačem bylo úspěšné.

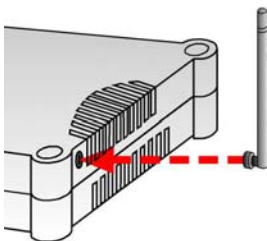
DRUHÁ MOŽNOST: NAPÁJENÍ WP54AG POMOCÍ COMPEX POE

Access point je plně kompatibilní se sadou Compex Power-Over-Ethernet (PoE). Tento doplněk dodává operační napájení do bezdrátového AP přes ethernetové kabelové připojení.

Uživatelé, kteří si již koupili Compex PoE a chtějí ho použít k napájení access pointu mohou při instalaci postupovat podle následujícího popisu:

Krok 1:

Zapojte vnější anténu do SMA konektoru access pointu.



Krok 2:

Použijte RJ45 ethernetový kabel – jeden konec zapojte do ethernetové zásuvky Injectoru a druhý konec do jednoho z LAN portů access pointu.

Varování:

V případě, že je jeden port používán k PoE, druhý port nesmí být spojen s jiným síťovým zařízením.



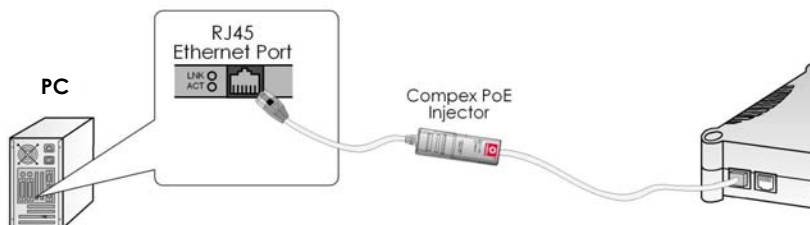
Maximální délka kabelu RJ45 je 100 metrů.

Hardware Installation

Krok 3:

Dále spojte RJ45 ethernetový kabel, který je připojen ke Compexu PoE Injector, s ethernetovým síťovým adaptérem vašeho počítače.

Jakmile jste dokončili konfiguraci vašeho access pointu, můžete připojit RJ45 ethernetový kabel PoE Injectoru k síťovému zařízení, jako např. ke switchi nebo hubu.

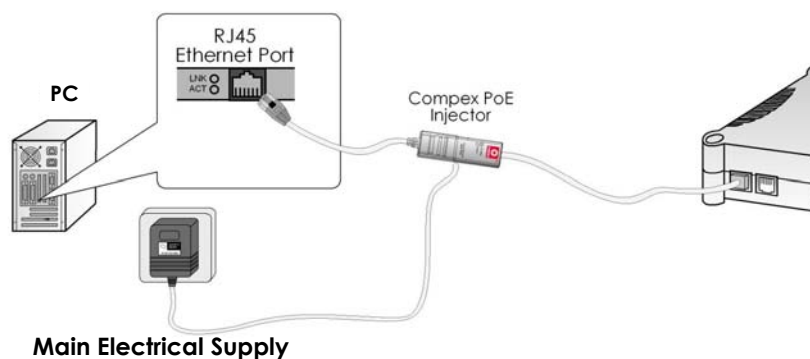


Krok 4:

Připojte napájecí adaptér sady Compex PoE do hlavního zdroje elektřiny a elektrickou zástrčku do zásuvky na injektoru.

Poznámka:

Napětí a proud v napájecím adaptéru a v sedě Compexu PoE napájecím adaptéru jsou různé. Nezaměňujte napájecí adaptéry.



Krok 5:

Nyní zapněte napájecí adaptér. Všimněte si, že LED: **Power** a **Port 1** nebo **2** (podle toho, který port jste připojili k PoE injector) se rozsvítila. To je známkou toho, že access point je napájen elektřinou přes Compex PoE Injector a že spojení mezi access pointem a vaším počítačem bylo úspěšné.

Kapitola 3: Přístup na webové rozhraní

Existují dvě metody přístupu na webové rozhraní u access pointu:

- **Pomocí Complex Utility – uConfig**
Můžete se dostat na webové rozhraní přímo, bez nutnosti změny IP adresy vašeho počítače.
- **Zadáním IP adresy access pointu do adresové kolonky Internetu Exploreru**
Musíte zapsat IP adresu vašeho počítače, např. 192.168.168.xxx, kde x může být jakákoli hodnota od 2 do 254, aby byla ve stejné podsíti jako Access point.

PŘÍSTUP NA WEBOVÉ ROZHRAŇÍ POMOCÍ UCONFIG

Complex vyvinul výkonnou uConfig utilitu, která umožňuje bezproblémový přístup na webové rozhraní.

Krok 1:

Vložte instalační CD do CD-ROMu. CD se rozběhne automaticky.

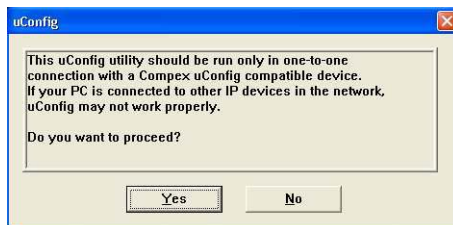
Krok 2:

Ze sekce **Utilities** vyberte možnost nainstalovat **uConfig** na váš hard disk.

Krok 3:

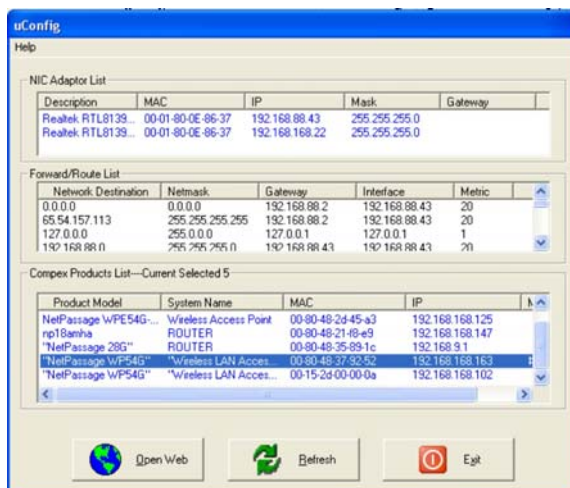
Když je tato pomůcka nainstalována, klikněte dvakrát na ikonku **uConfig** .
Objeví se následující tabulka, klikněte na tlačítko **Yes** a program bude pokračovat.

Access to Web-based Interface



Krok 4:

Vyberte **NetPassage WP54G** v sekci **Compx Products List** a klikněte na tlačítko **Open Web**. K tomu, aby se vám znovu zobrazil seznam dosažitelných zařízení, klikněte na tlačítko **Refresh**.



Access to Web-based Interface

Krok 5:

Neukončujte program uConfig program, zatímco probíhá přístup na webové rozhraní. To vás odpojí od zařízení. Klikněte na tlačítko **OK** program bude pokračovat.



Krok 6:

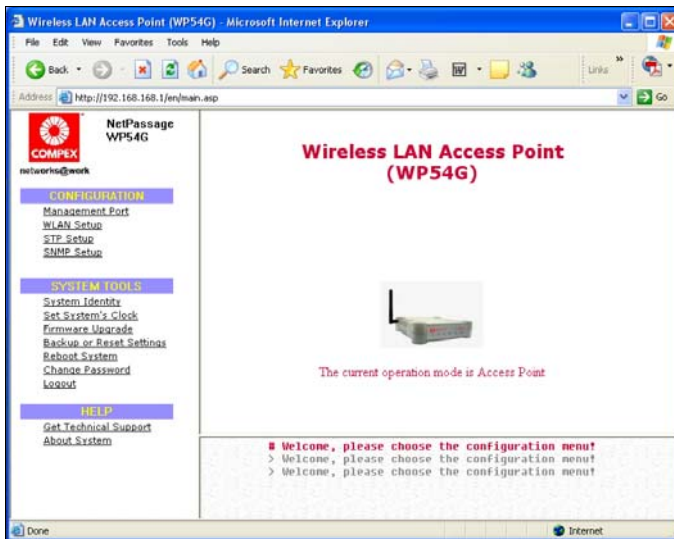
Na ověřovací stránce klikněte na tlačítko **LOGIN!** a vstoupíte na hlavní konfigurační stránku. Přednastavené heslo je "password".



Access to Web-based Interface

Krok 7:

Dostanete se na domovskou stránku webového rozhraní access pointu.



OVĚŘENÍ IP ADRESY COMPEXU WP54AG POMOCÍ NPFind

CompeX vytvořil další pomocný program - **NpFind**, který vám má pomoci ověřit IP adresu produktu CompeX.

Pro kontrolu IP adresy vašeho access pointu postupujte podle následujících kroků.

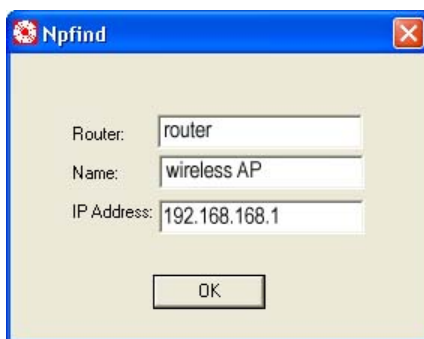
Krok 1:

Vložte instalační CD do CD-ROMu. Rozběhne se automaticky.

Krok 2:

Klikněte na **Utilities** a vyberte program **NpFind**.

Na obrazovce se objeví IP adresa objeveného zařízení CompeX.



MANUÁLNÍ PŘÍSTUP NA WEBOVÉ ROZHRANÍ PŘES INTERNET EXPLORER

Při použití této metody musíte nejdříve zadat IP adresu do vašeho počítače tak, aby patřila do stejné podsítě jako váš access point. V tomto případě používáme pro ilustraci Windows XP. Pokud máte Windows 98/98SE/2000/NT/ME, nahlédněte do **Dodatku II "TCP/IP Konfigurace"**.

Krok 1:

Na ploše klikněte pravým tlačítkem na ikonu **My Network Places** a vyberte možnost **Properties**.

Krok 2:

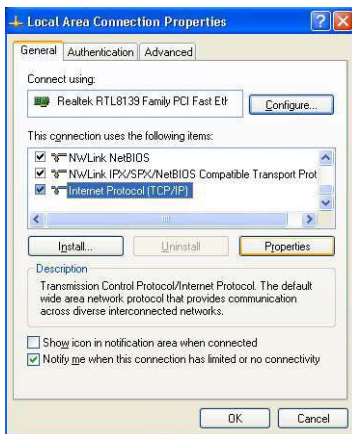
Klikněte pravým tlačítkem na ikonu síťového adaptéru a vyberte možnost **Properties**.



Access to Web-based Interface

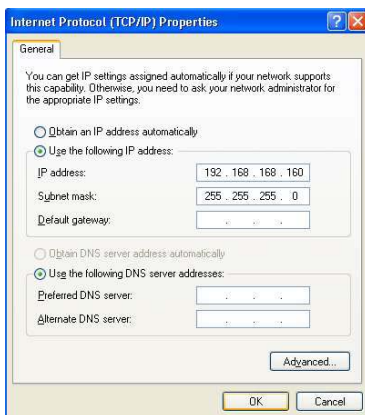
Krok 3:

Označte **Internet Protocol (TCP/IP)** a klikněte na tlačítko **Properties**.



Krok 4:

Zvolte možnost **Use the following IP address**. Zadejte IP adresu a masku podsítě např. 192.168.168.x a 255.255.255.0, kde x může být jakékoliv číslo od 2 do 254, kromě 1. V tomto případě používáme 192.168.168.160 jako statickou IP adresu.



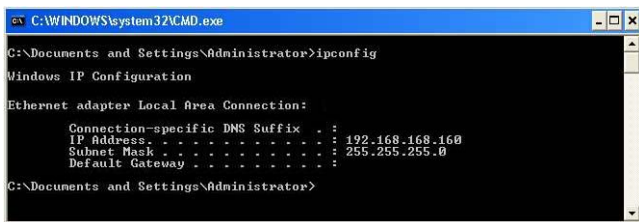
Access to Web-based Interface

Krok 5:

Klikněte na tlačítko **OK** a všechna okna se zavřou.

Krok 6:

Z důvodu kontroly, jestli byla IP adresa do vašeho počítače zadána správně, ve **Start** menu vyberte možnost **Accessories**, dále možnost **Command Prompt** a napište příkaz *ipconfig/all*.



```
C:\WINDOWS\system32\CMD.exe
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.168.160
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Documents and Settings\Administrator>
```

Váš počítač je nyní připraven konfigurovat váš access point.

Krok 7:

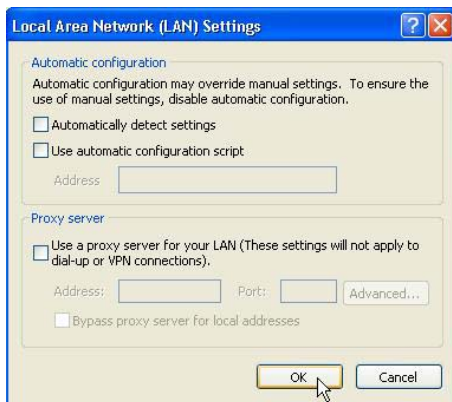
Spusťte Web prohlížeč. Z nabídky **Tools**, zvolte možnost **Internet Options**.



Access to Web-based Interface

Krok 8:

Otevřete tab **Connections** a v sekci **LAN Settings** nenechte žádné z možných boxů označené. Klikněte na tlačítko **OK**, aby se aktualizovaly změny.



Krok 9:

Do adresové kolonky zadejte `http://192.168.168.1` a na klávesnici zmáčkněte **Enter**.

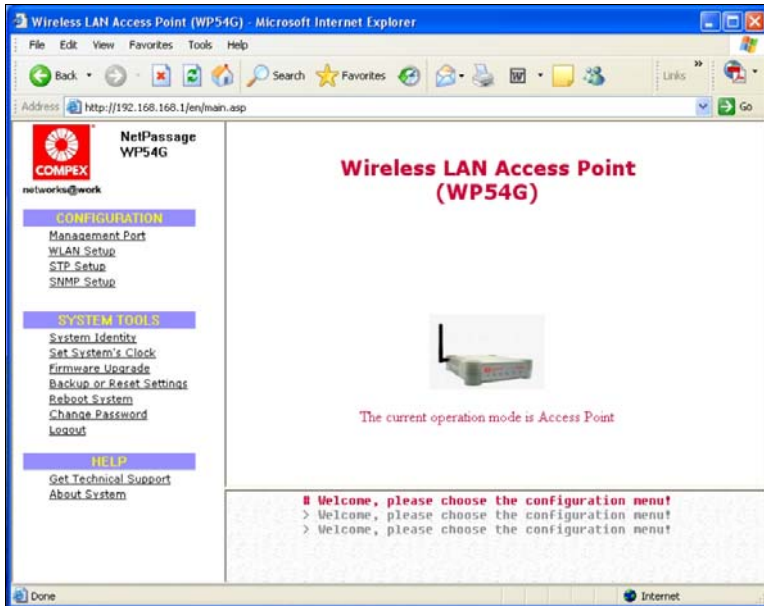
Krok 10:

Na logovací stránce klikněte na tlačítko **LOGIN!**. Tím vstoupíte na konfigurační stránky.



Access to Web-based Interface

Následně se dostanete na domovskou stránku webového rozhraní vašeho access pointu.



Kapitola 4: Běžná konfigurace

Tato kapitola ilustruje následující vlastnosti, které jsou dostupně ve VŠECH operačních modech vašeho access pointu, pokud není stanoveno jinak.

- **Management Port**
- **WLAN základní nastavení**
- **WLAN bezpečnost**
- **STP nastavení**
- **SNMP**
- **MAC filtrace**

NASTAVENÍ MANAGEMENT PORTU

Tato sekce vám ukáže, jak uzpůsobit parametry vašeho access pointu, aby vyhovovaly potřebám sítě. Také je zde vysvětleno jak využít vestavěný server DHCP vašeho access pointu.

Common Configuration

NASTAVENÍ VAŠEHO LAN

Můžete si zvolit přizpůsobit přednastavené hodnoty vašeho access pointu a upravit nastavení sítě.

Krok 1:

Klikněte na možnost **Management Port** z **CONFIGURATION** menu.

Na stránce **Nastavení Management Portu** podle dolní tabulky nahraďte přednastavené hodnoty acces pointu příslušnými hodnotami, které budou sedět potřebám vaší sítě.

Management Port Setup

IP Address:	<input type="text" value="192.168.168.1"/>
Network Mask:	<input type="text" value="255.255.255.0"/>
Management Gateway IP:	<input type="text"/>
DHCP Start IP Address:	<input type="text" value="192.168.168.100"/>
DHCP End IP Address:	<input type="text" value="192.168.168.254"/>
DHCP Gateway IP Address:	<input type="text" value="192.168.168."/>
DHCP Lease Time:	<input type="text" value="3600"/> (seconds)
<input type="checkbox"/> Always use these DNS servers	
Primary DNS IP Address:	<input type="text"/>
Secondary DNS IP Address:	<input type="text"/>
DHCP Server:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Advanced DHCP Server Options

Krok 2:

Klikněte na tlačítko **Apply**, tím se uloží vaše nové parametry.

Tato tabulka popisuje parametry, které mohou být modifikována na stránce **Nastavení Management Portu**.

Common Configuration

Parametry	Popis
IP Adresa	<p>Pokud je server DHCP na routeru povolen, tato LAN IP Adresa by byla přidělena jako Default Gateway DHCP klienta.</p> <p>IP adresa Acces pointu je přednastavená na 192.168.168.1.</p>
Síťová maska	<p>Síťová maska slouží k identifikaci podsítě, ve které sídlí access point. Přednastavená síťová maska je 255.255.255.0.</p>
Management Gateway IP	<p>(dobrovolné) Access point většinou nekomunikuje se zařízeními v jiných IP podsítích. Nicméně Management Gateway je zde kvůli komunikaci s jinými IP rozsahy než je Default Gateway počítače, aby umožnil access pointu komunikovat se zařízeními v jiných podsítích. Například pokud chcete dosáhnout access pointu z Internetu nebo z routeru na LAN, můžete nastavit IP adresu access pointu jako Management Gateway IP.</p> <p>Management Gateway IP adresa vašeho access pointu je přednastavena na nulu.</p>
<p>Následující dvě pole (DHCP počáteční IP Adresa a DHCP koncová IP Adresa) vám dovolují definovat řadu IP adres, ze kterých může server DHCP přiřadit IP adresu LANu.</p>	
DHCP počáteční IP Adresa	<p>Toto je první IP adresa, kterou server DHCP přidělí. Hodnota, kterou zde zapíšete by měla patřit do stejné podsítě jako váš access point. Např. pokud jsou IP adresa a síťová maska vašeho access pointu 192.168.168.1 respektive 255.255.255.0, DHCP počáteční IP adresa by měla být 192.168.168.X, kde X může být jakákoliv hodnota od 2 do 254. Přednastavená hodnota je 192.168.168.100.</p>
DHCP koncová IP Adresa	<p>Toto je poslední IP adresa, kterou server DHCP přidělí. Měla by také patřit do stejné podsítě jako váš access point. Například pokud jsou IP adresa a síťová maska vašeho access pointu 192.168.168.1 respektive 255.255.255.0, DHCP koncová IP Adresa by měla být 192.168.168.X, kde X může být jakákoliv hodnota od 2 do 254. Přednastavená hodnota je 192.168.168.254.</p>

Common Configuration

Parametry	Popis
DHCP Gateway IP Adresa	<p>Ačkoliv obvykle hraje server DHCP roli jako Default Gateway DHCP klienta, access point vám dá možnost definovat jinou DHCP Gateway IP Adresu, která bude vymezena jako Default Gateway DHCP klienta. DHCP klient tak obdrží svou dynamickou IP adresu od access pointu, ale přístup na internet a na další LAN mu bude umožněn přes Default Gateway definované DHCP Gateway IP Adresou.</p> <p>Například pokud je access point užíván v modu Access Point Client a je připojen k internetové gateway, X, počítač drátově připojený k access pointu nebude schopný získat dynamickou IP adresu přímo od X. Ale pokud můžete uvolnit server DHCP access pointu a nastavit IP adresu X jako DHCP Gateway IP Adresu, počítač pak získá IP adresu z access pointu a přístup na internet přes X.</p>
Vždy používejte tyto DNS servery	Uvolněte zatrhávající rámeček, pokud chcete, aby access point používá jen ty DNS servery, které jste dole specifikovali.
Primární DNS IP Adresa	IP adresa DNS serveru je většinou poskytována vaší ISP.
Sekundární DNS IP Adresa	Toto dobrovolné pole je rezervováno pro IP adresu sekundárního DNS serveru.
DHCP Server	Pokud vyřadíte DHCP server, budete potřebovat manuálně konfigurovat TCP/IP parametry každého počítače ve vaší síti.

PRO PŘEHLED AKTIVNÍCH DHCP LEASES

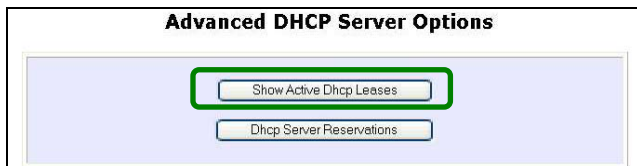
Následuje průvodce na stránku zobrazující dobu platnosti aktivních IP adres, které byly vymezeny vestavěným DHCP serverem Access pointu.

Krok 1:

Z **CONFIGURATION** menu vyberte a klikněte na možnost **Management Port**.

Krok 2:

Vstupte do sekce **Advanced DHCP Server Option**, klikněte na tlačítko **Show Active DHCP leases**.



Tabulka **DHCP Aktivních nájmu** zobrazí:

- **Hostitelské jméno** DHCP klienta
- **IP Adresa**, která byla přidělena DHCP klientovi
- Jeho **hardwarovou adresu (MAC)**
- Datum a čas, kdy nájem IP adresy vyprší



POZNÁMKA

Neplatné datum a čas se zobrazí v kolonce **Lease Expired Time** a ukazují, že hodiny vašeho access pointu nebyly nastaveny správně. Prosíme podívejte se do sekce **SYSTEM TOOLS**, kde se dozvíte více detailů o tom, jak nastavit hodinový systém.

Common Configuration

PRO REZERVACI SPECIFICKÝCH IP ADRES PRO PŘEDEM STANOVENÉ DHCP KLIENTY

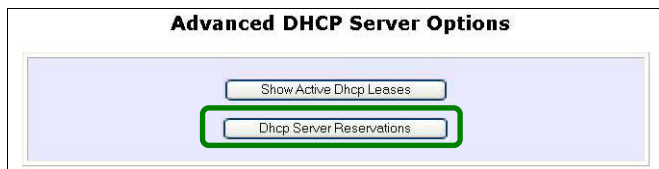
Rezervováním IP adresy jste informováni, že DHCP server vyřadil IP adresu z fondu volných IP adres, to vede k alokaci dynamických IP adres.

Například, pokud nastavíte veřejně přístupný FTP/HTTP server v rámci vašeho soukromého LAN, zatímco server by požadoval fixní IP adresu, vy byste stále chtěli, aby DHCP server dynamicky alokoval IP adresy do zbytku počítačů v LANu.

Následující kroky vám ukáží, jak rezervovat konkrétní IP adresu.

Krok 1:

Ze sekce možností **Advanced DHCP Server** klikněte na tlačítko **DHCP Server Reservations**.



Krok 2:

Klikněte na tlačítko **Add**.



Common Configuration

Krok 3:

Vyplňte:

Část **IP Adresy**, kterou chcete rezervovat.

Adresu hardwaru, ve dvojicích dvou hex hodnot

Zmáčkněte tlačítko **Apply**, aby byl váš nově zadáný údaj úspěšně zapsán.

DHCP Server Reservations

IP Address:

Hardware Address: (XX-XX-XX-XX-XX-XX)

Stránka **DHCP Server Reservations** se obnoví a ukáže aktuálně rezervované IP adresy.

DHCP Server Reservations

IP Address	Hardware Address
192.168.168.20	00-80-45-e5-0d-05


Common Configuration

SMAZÁNÍ REZERVACE DHCP SERVERU

Jestliže již nepotřebujete, aby vám DHCP server rezervoval IP adresu, můžete rezervaci smazat.

Krok 1:

Klikněte na rezervovanou IP adresu, kterou si přejete smazat, např. *192.168.168.20*.

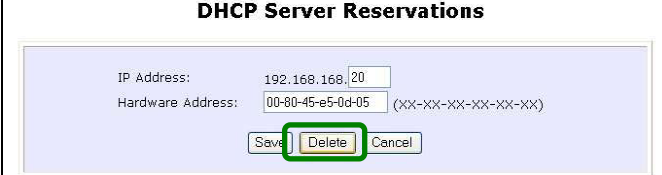


The screenshot shows a window titled "DHCP Server Reservations". It contains a table with two columns: "IP Address" and "Hardware Address". The first row has the IP address "192.168.168.20" and the hardware address "00-80-45-e5-0d-05". The IP address cell is highlighted with a green box. Below the table are "Add" and "Back" buttons.

IP Address	Hardware Address
192.168.168.20	00-80-45-e5-0d-05

Krok 2:

Klikněte na tlačítko **Delete**.



The screenshot shows the "DHCP Server Reservations" form. It has two input fields: "IP Address" with the value "192.168.168.20" and "Hardware Address" with the value "00-80-45-e5-0d-05" and a placeholder "(XX-XX-XX-XX-XX-XX)". Below the fields are "Save", "Delete", and "Cancel" buttons. The "Delete" button is highlighted with a green box.

IP Address: 192.168.168.20
Hardware Address: 00-80-45-e5-0d-05 (XX-XX-XX-XX-XX-XX)

Tabulka **DHCP Server Reservations** se obnoví a zobrazí se změny.

NASTAVENÍ WLAN

Tato sekce vám ukazuje, jak fungují následující funkce:

Základní:

Tato funkce vykonává základní nastavení bezdrátových operačních módů: **Access Point mode**, **Access Point Client mode** a dalších operačních módů.

Bezpečnost:

Tato funkce vykonává kódování dat a ochranu access pointu.

Pro detaily se podívejte do Kapitoly 5 na **Bezpečnost WLAN**.

Nadstandardní:

Tato funkce rozvíjí základní konfiguraci access pointu tím, že nastaví přidatné systémové parametry: **Wireless Pseudo VLAN**, **WDS konfigurace** a **Parametry dlouhé vzdálenosti**.

Pro detaily se podívejte do Kapitoly 6 na **Rozšířené bezdrátové vlastnosti**.

Statistiky:

Tato funkce používá **vlastnost Scan** k monitorování a vypsání sesbíraných statistických dat.

MAC Filtrace (aplikovatelné jen na mod Access Point):

MAC Filtrace funguje jako bezpečnostní opatření – omezuje uživatelský přístup na síť přes jejich MAC adresy.

Common Configuration

PRO KONFIGURACI ZÁKLADNÍHO NASTAVENÍ BEZDRÁTOVÉHO MODU

Následující kroky vás provedou konfigurací základního nastavení bezdrátového modu, který jste si vybrali.

Krok 1:

Klikněte na **WLAN Setup** z **CONFIGURATION** menu. Uvidíte rozšířené pod-menu pod **WLAN Setup**. Klikněte na **Basic**.

Přednastavený operační mod access pointu je mod **Access Point**.



WLAN Basic Setup

The Current Mode: **Access Point**

ESSID:

Wireless Profile:

Country:

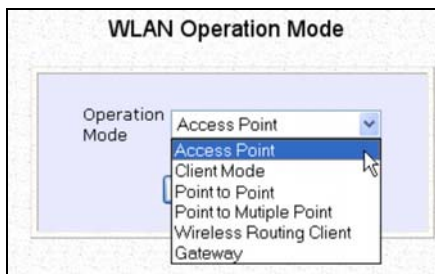
Channel:

Tx Rate:

Closed System: disable enable

Krok 2 :(Volitelný: Změna aktuálního modu)

Pokud si přejete změnit aktuální mod vašeho access pointu, klikněte na možnost **Change**, vyberte **Operation Mode** a klikněte na tlačítko **Apply**. Tím vstoupíte na nastavovací stránku vámi vybraného modu. Následně budete vyzváni, abyste restartovali access point, aby se mod nastavil.



WLAN Operation Mode

Operation Mode:

- Access Point
- Access Point
- Client Mode
- Point to Point
- Point to Multiple Point
- Wireless Routing Client
- Gateway

Common Configuration

Krok 3:

Do příslušných políček zadejte parametry, klikněte na tlačítko **Apply** a restartujte zařízení, aby se změny provedly.

Všimněte si, že stránka **WLAN Basic Setup** pro mod **Client** je odlišná od stránky modu **Access Point**.

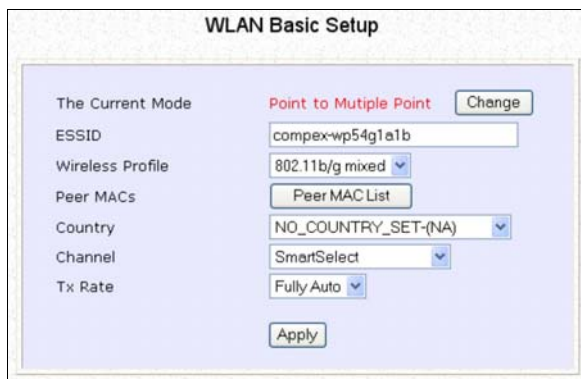
The screenshot shows the 'WLAN Basic Setup' configuration page for Client Mode. The current mode is 'Client Mode', with a 'Change' button next to it. The configuration fields are: ESSID (text input: 'compex-wp54g1a1b'), Wireless Profile (dropdown: '802.11b/g mixed'), Country (dropdown: 'NO_COUNTRY_SET-(NA)'), and Tx Rate (dropdown: 'Fully Auto'). There is a 'Site Survey' button to the right of the ESSID field and an 'Apply' button at the bottom. Below the configuration area is a 'Link Information' section with a 'Show Link Information' button.

Pokud si přejete nastavit access point do modu **Point to Point**, klikněte na **Change** a vyberte možnost **Point to Point**. Potom se vám zobrazí tato stránka:

The screenshot shows the 'WLAN Basic Setup' configuration page for Point to Point Mode. The current mode is 'Point to Point', with a 'Change' button next to it. The configuration fields are: ESSID (text input: 'compex-wp54g1a1b'), Wireless Profile (dropdown: '802.11b/g mixed'), Peer MAC (text input: '(XX-XX-XX-XX-XX-XX)'), Country (dropdown: 'NO_COUNTRY_SET-(NA)'), Channel (dropdown: 'SmartSelect'), and Tx Rate (dropdown: 'Fully Auto'). There is an 'Apply' button at the bottom.

Common Configuration

Pokud si přejete nastavit access point do modu **Point to Multiple Point**, klikněte na **Change** a vyberte možnost **Point to Multiple Point**. Potom se vám zobrazí tato stránka.



The screenshot shows the 'WLAN Basic Setup' configuration page. It features several fields and buttons:

- The Current Mode:** Set to 'Point to Multiple Point' with a 'Change' button next to it.
- ESSID:** Text input field containing 'compex-wp54g1a1b'.
- Wireless Profile:** Dropdown menu set to '802.11b/g mixed'.
- Peer MACs:** Button labeled 'Peer MAC List'.
- Country:** Dropdown menu set to 'NO_COUNTRY_SET-(NA)'.
- Channel:** Dropdown menu set to 'SmartSelect'.
- Tx Rate:** Dropdown menu set to 'Fully Auto'.
- Apply:** Button at the bottom.

Pro vytvoření nového peer MAC klikněte na tlačítko **Peer MAC List**. Zobrazí se tato stránka. (Prosíme všimněte si, že **PtMP** znamená **Point to Multiple Point**).



The screenshot shows the 'PtMP Configuration' page. It contains a table with three columns: 'Link No.', 'Hardware Address', and 'Comments'. Below the table is an 'Add' button.

Link No.	Hardware Address	Comments
----------	------------------	----------

Klikněte na **Add** a budete vyzváni k zadání **Adresy Hardwaru** a **Comment (poznámky)**.



The screenshot shows the 'Add WDS Entry' dialog box. It has two input fields: 'Hardware Address' and 'Comment'. The 'Hardware Address' field has a placeholder '(XX-XX-XX-XX-XX-XX)'. Below the fields are 'Add' and 'Cancel' buttons.

Hardware Address: (XX-XX-XX-XX-XX-XX)

Comment:

Common Configuration

Tato tabulka popisuje parametry, které mohou být modifikované na stránce **WLAN Basic Setup**.

Parametry	Popis
Běžný mod	<p>Přednastavený mod access pointu je mod Access Point. Access point operuje v 6 modchs:</p> <ul style="list-style-type: none">• Access Point• Client• Point to Point• Point to Multiple Point• Wireless Routing Client• Gateway <p>Můžete přepnout mod kliknutím na tlačítko Change.</p>
ESSID	<p>Zadejte preferované jméno pro bezdrátovou síť. Vaši bezdrátoví klienti musí být konfigurováni se stejným ESSID.</p> <p>Tento záznam citlivý na rozlišování písmen může obsahovat maximálně 32 znaků.</p>
Přehled stránky	<p>Seznam bezdrátových zařízení které jsou detekovány vaším access pointem ve WLAN. V seznamu mohou být nalezeny informace, jako např. MAC adresa, kanál, SSID, algoritmus a síla signálu.</p> <p>Tato vlastnost je podporována mody Access Point Client a Wireless Routing Client.</p>
Bezdrátový profil	<p>Výběr typů prostředí sítě, ve kterých může access point operovat:</p> <ul style="list-style-type: none">•• 802.11a pouze Tento mod podporuje bezdrátové A klienty s rychlostí přenosu dat až do 54Mbps kmitočtového rozsahu 5.4GHz.• 802.11b pouze Tento mod podporuje bezdrátové B klienty s rychlostí přenosu dat až do 11Mbps kmitočtového rozsahu 2.4GHz.

Common Configuration

	<ul style="list-style-type: none">• 802.11b/g smíšený Tento mod podporuje jak B klienty, tak G klienty.• 802.11g pouze Tento mod podporuje bezdrátové G klienty, kteří nabízejí přenosovou rychlost do 54Mbps v kmitočtovém pásmu 2.4GHz.
Peer Mac (Jen v modu Point-to-Point)	Tento mod může podporovat více než jeden access point. Tato vlastnost umožňuje vytvořit nový peer MAC pro jiný access point, aby se router operující v modu access point mohl připojit k jinému access pointu.
Peer MACs (Jen v modu Point-to-Multiple Point)	Tento mod může podporovat až 15 access pointů. Tato vlastnost umožňuje vytvořit až 15 peer MAC adres, aby se router mohl připojit ke stejnému číslu access pointů.
Země	Vyberte Country (zemi) , ve které se nacházíte.
Kanál	Tato možnost vám umožňuje vybrat si frekvenční kanál pro bezdrátovou komunikaci. Tento parametr je dostupný pouze v modech Access Point, Point to Point a Point to Multiple Point.
Tx Rychlost	Umožňuje vám vybrat rychlost přenosu dat od 1Mbps do Plně automatický .
Zavřený systém (Closed System)	Access point nebude vysílat svůj WLAN název (ESSID) , když je spuštěn Closed system . Standardně je Closed system vypnut.

Common Configuration

SCAN PRO PŘEHLED DOSTUPNÝCH SÍTÍ (JEN PRO MODY CLIENT A WIRELESS ROUTING CLIENT)

Krok 1:

Na stránce **Mode Setup** klikněte na tlačítko **Site Survey**.

WLAN Basic Setup

The Current Mode: **Client Mode**

ESSID:

Wireless Profile:

Country:

Tx Rate:

Link Information

Stránka **Site Survey** vám nabídne seznam **MAC adres (BSSID)** a **SSID** zjištěných sousedících access pointů, používaných **Chan** (kanály), **Auth** (Ověření), **Alg** (Algoritmus) a sílu přijímaného signálu.

Site Survey

Bssid	SSID	Chan	Auth	Alg	Signal
<input type="radio"/> 008048003472	PMD-28G-Online	6	WPA-PSK	TKIP	8
<input type="radio"/> 008048015403	wp54-1C	1	RSN-PSK	AES	3
<input type="radio"/> 00804830b5bd	wpe-A	6	WPA-PSK	TKIP	3
<input type="radio"/> 00804821f877	np18a-tang	10	WPA-EAP	TKIP	2
<input type="radio"/> 00804835891e		10	OPEN	NONE	22
<input type="radio"/> 00804800348d	OMEGA1	8	OPEN	NONE	9
<input type="radio"/> 00804800345d	compex-np28g-with-super-g-super-gg	7	OPEN	NONE	5
<input type="radio"/> 00804824c675	Any	3	OPEN	NONE	3
<input type="radio"/> 008048358961	compex-np28g	6	OPEN	NONE	7

Common Configuration

Krok 2:

K připojení WP54AG-klienta k jednomu ze zjištěných access pointů:
Vyberte tlačítko korespondující access pointu, ke kterému se chcete připojit.

Krok 3:

Klikněte na tlačítko **Apply**, tím se změny uloží a vrátíte se na nastavovací stránku.

Krok 4:

Klikněte na tlačítko **Refresh**, aby se tato obrazovka aktualizovala.

Tato tabulka popisuje parametry sousedících access pointů, které jsou vidět na výpisu ze stránky **Site Survey (Přehled stránky)**.

Parametry	Popis
Bssid	V infrastruktuře bezdrátové sítě odkazuje BSSID k MAC adrese access pointu.
SSID	Odkazuje k názvu sítě, který výjimečně identifikuje síť, ke které je access point připojen.
Chan	Odkazuje na kanály, které jsou užívány k přenosu.
Auth	Odkazuje na typy ověření, jako např. WPA, WPA-PSK atd., které jsou používány access pointem.
Alg	Odkazuje na typy algoritmů, jako např. WEP, TKIP atd., které jsou používány access pointem.
Signál	Popisuje sílu signálu, která byl procentuálně přijímán.

Common Configuration



POZNÁMKA

Důvodem k používání **Site Survey** je skenování a zobrazování všech access pointů založených na aktuálním bezpečnostním nastavení vašeho access pointu. Například následující informace nabízen na Site Survey (Přehled stránky) podle bezpečnostního nastavení je vysvětlován:

- Pokud je bezpečnostní mod nastaven na **None** nebo **WEP**, prohlížeč ukáže všechny dostupné access pointy, které nemají žádné bezpečnostní nastavení, nebo mají bezpečnost WEP
 - Pokud je bezpečnostní mod nastaven na **WPA-PSK**, ukáže prohlížeč všechny dostupné access pointy, které mají jakékoli typy bezpečnostního nastavení od žádného, přes bezpečnost **WEP** až po bezpečnost **WPA-PSK**.
-

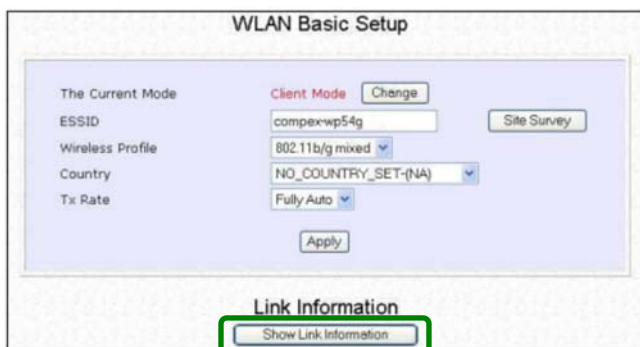
Common Configuration

SHOW LINK INFORMATION

(JEN PRO MODOY CLIENT A WIRELESS ROUTING CLIENT)

Krok 1:

Pokud chcete vidět status spojení, když je WP54G-klient spojen s jiným access pointem, klikněte na tlačítko **Show Link Information**.



Tabulka **Link Information** zobrazuje následující data:

Link Information	
State	Scanning; ff: ff: ff: ff: ff: ff
Current Channel	11
TxRate	1Mbps
Signal Strength	6

Tato tabulka popisuje parametry, které můžete vidět na stránce **Link Information**.

Parametry	Popis
Stav	Odkazuje na MAC adresu BSS (AP, ke kterému je WP54G-klient připojen).
Aktuální kanál	Kanál, který je momentálně používán pro přenos.
Tx Rychlost	Tx rychlost přenosu dat v Mbps.
Síla signálu	Dána v procentech, ukazuje intenzitu přijímaného signálu.

Common Configuration

PRO KONFIGURACI BEZPEČNOSTNÍHO NASTAVENÍ BEZDRÁTOVÉHO MODU

Pro detaily o nastavení různých bezpečnostních modů access pointu se podívejte na Kapitolu 5 na **WLAN Security**.

PRO KONFIGURACI POKROČILÉHO NASTAVENÍ BEZDRÁTOVÉHO MODU

Následující kroky vás provedou konfigurací pokročilého nastavení bezdrátového modu, který jste si vybrali.

Krok 1:

Klikněte na **WLAN Setup** ve **CONFIGURATION** menu – rozšíří se na čtyři podmenu. Tady klikněte na **Advanced**.

Krok 2:

Na stránce **WLAN Advanced Setup** zadejte parametry.

Krok 3:

Klikněte na tlačítko **Apply**, aby se změny aktualizovaly.

WLAN Advanced Setup

Beacon Interval	<input type="text" value="100"/>	(100:20-1000)
Data Beacon Rate (DTIM)	<input type="text" value="1"/>	(1:1-16384)
RTS/CTS Threshold	<input type="text" value="512"/>	(512:1-2312)
Frag Threshold	<input type="text" value="2346"/>	(2346:256-2346)
Transmit Power	<input type="text" value="Maximum"/>	

Extended Features

Common Configuration

Tato tabulka popisuje parametry, které mohou být modifikovány na stránce **WLAN Advanced Setup**.

Parametry	Popis
Interval světelného signálu (Jen v modu Access Point)	Interval světelného signálu je množství času mezi přenosem světelného signálu. Světelný signál je naváděcí signál poslaný access pointem, aby oznámil svojí přítomnost jiným zařízením v síti. Předtím, než klient zadá šetřící mod, musí interval světelného signálu vědět, kdy být v bdělém stavu k obdržení světelného signálu (a naučit se, jestli má access point rámy s vyrovnávací pamětí).
Rychlost datového světelného signálu (DTIM) (Jen v modu Access Point)	Rychlost datového signálu (DTIM) předurčuje, jak často obsahuje signál doručení zprávy indikace trafiku (DTIM). DTIM identifikuje, který klient (v šetřícím modu) má datové rámce, které na ně čekají ve vyrovnávací paměti access pointu. Jestliže je perioda světelného signálu nastavena na 100 (standardní hodnota) a rychlost datového signálu je nastavena na 1 (standardní hodnota), pak access point pošle signál obsahující DTIM každých 100 Kμsecs (1 Kμsec se rovná 1,024 μsec).
RTS/CTS práh	Hodnota Prahu RTS/CTS předurčuje minimální velikost paketů v bytech, který spustí mechanismus RTS/CTS.
Frag práh	Hodnota prahu Frag ukazuje maximální velikost, kterou může packet dosáhnout bez fragmentace. Tato hodnota se rozprostírá od 256 do 2346 bytů, kde 0 indikuje, že všechna balení by měla být přenášena pomocí RTS.
Přenosová síla	Seznam Přenosové síly vás nechá vybrat z řady přenosových sil.

Common Configuration

Pro více detailů o konfiguraci Wireless Pseudo VLAN, WDS a Long Distance Parameters, se podívejte na kapitolu 6 na **Wireless Extended Features**.



POZNÁMKA

Hodnoty vynesené v příkladech jsou navrhované hodnoty pro jejich příslušné parametry.

STATISTIKY

Následující kroky vás informují o bezdrátovém zařízení, které je připojené k WLAN.

V MODU ACCESS POINT

Krok 1:

Klikněte na **WLAN Setup** z **CONFIGURATION** menu. Uvidíte pod-menu, které se ukáže u **WLAN Setup**. Klikněte na **Statistics**.

Bezdrátoví klienti, kteří jsou připojeni k WLAN se ukáží na seznamu stanic WLAN.

Krok 2:

Klikněte na tlačítko **Refresh**. Tím dostanete nejnovější informace o dostupných bezdrátových klientech v bezdrátové síti.

WLAN Station List			
ID	MAC Address	RSSI	TxRate
AP	00:80:48:37:86:dd	1	36Mbps

Common Configuration

Krok 3:

Pro kontrolu detailů individuálního bezdrátového klienta klikněte na MAC adresu v seznamu zařízení WLAN.

Následující obrazovka vám ukáže statistiku vybraných bezdrátových klientů.

00:80:48:37:86:dd Statistics						
Authentication Type			Encryption			
Open-System			No			
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	2122	0	0
Transmit	0	0	0	11	0	0

[Back](#)

Common Configuration

V MODU CLIENT

Klikněte na **WLAN Setup** z **CONFIGURATION** menu. Uvidíte pod-menu, které se ukáže u **WLAN Setup**. Klikněte na **Statistics**.

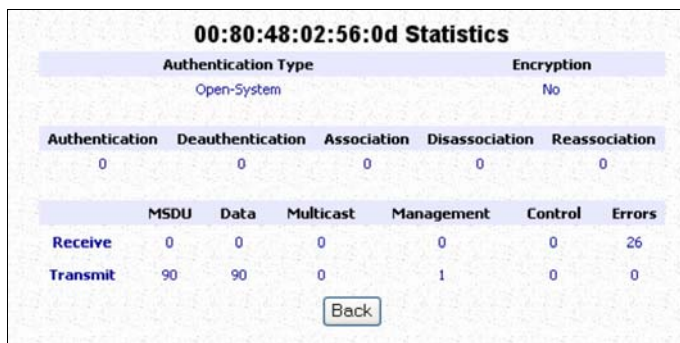
00:80:48:37:86:dd Statistics						
Authentication Type			Encryption			
Open-System			No			
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	2122	0	0
Transmit	0	0	0	11	0	0
<input type="button" value="Back"/>						

V modu **Client** vám není povoleno nahlížení na statistiky ostatních bezdrátových klientů. K tomu, aby bylo možné nahlížet na informace, potřebujete změnit mod na mod Access point.

Common Configuration

V MODU POINT TO POINT

Klikněte na **WLAN Setup** z **CONFIGURATION** menu. Uvidíte pod-menu, které se vám ukáže u **WLAN Setup**. Klikněte na **Statistics**.



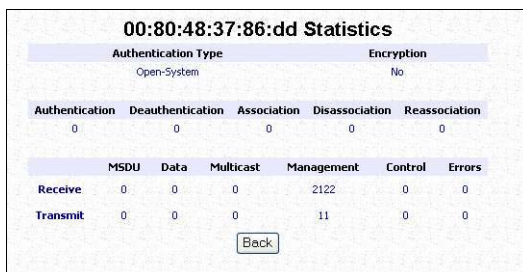
00:80:48:02:56:0d Statistics						
Authentication Type			Encryption			
Open-System			No			
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	0	0	26
Transmit	90	90	0	1	0	0
<input type="button" value="Back"/>						

V modu **Point to Point** vám není povoleno nahlížet na statistiky jiných bezdrátových klientů. K tomu, aby bylo možné nahlížet na informace, potřebuje změnit mod na mod Access point.

Common Configuration

V MODU POINT TO MULTIPLE POINT

Klikněte na **WLAN Setup** z **CONFIGURATION** menu. Uvidíte pod-menu, které se vám ukáže u **WLAN Setup**. Klikněte na **Statistics**.



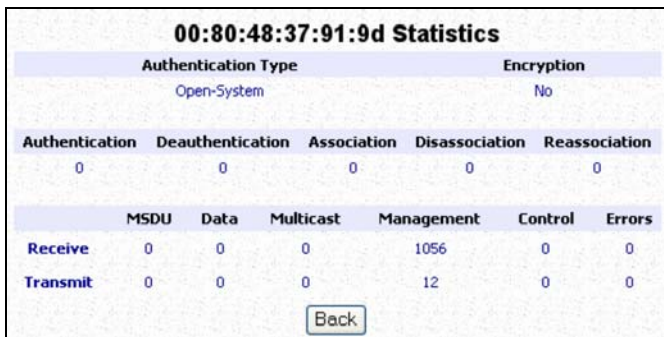
00:80:48:37:86:dd Statistics						
Authentication Type			Encryption			
Open-System			No			
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	2122	0	0
Transmit	0	0	0	11	0	0

V modu **Point to Multiple Point** vám není povoleno nahlížet na statistiky jiných bezdrátových klientů. K tomu, aby bylo možné nahlížet na informace, musíte změnit mod na mod Access point.

Common Configuration

V MODU WIRELESS ROUTING CLIENT

Klikněte na **WLAN Setup** z **CONFIGURATION** menu. Uvidíte pod-menu, které se vám ukáže u **WLAN Setup**. Klikněte na **Statistics**.



00:80:48:37:91:9d Statistics

Authentication Type		Encryption				
Open-System		No				
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	1056	0	0
Transmit	0	0	0	12	0	0

V modu **Wireless Routing Client** vám není povoleno nahlížet na statistiky jiných bezdrátových klientů. K tomu, aby bylo možné nahlížet na informace, musíte změnit mod na mod Access point.

Common Configuration

V MODU GATEWAY

Klikněte na **WLAN Setup** z **CONFIGURATION** menu. Uvidíte pod-menu, které se vám ukáže u **WLAN Setup**. Klikněte na **Statistics**.

00:80:48:37:91:9d Statistics						
Authentication Type				Encryption		
Open-System				No		
Authentication	Deauthentication	Association	Disassociation	Reassociation		
0	0	0	0	0		
	MSDU	Data	Multicast	Management	Control	Errors
Receive	0	0	0	1056	0	0
Transmit	0	0	0	12	0	0
<input type="button" value="Back"/>						

V modu **Gateway** vám není povoleno nahlížet na statistiky jiných bezdrátových klientů. K tomu, aby bylo možné nahlížet na informace, musíte změnit mod na mod Access point.

NASTAVENÍ WAN

(POPOROVANÉ JEN MODY WIRELESS ROUTING CLIENT A GATEWAY)

Správné nastavení **WAN** vám umožňuje úspěšné sdílet vaše internetové připojení mezi drátovými i bezdrátovými klienty access pointu. Aby se tak stalo, musíte identifikovat typ širokopásmového internetového přístupu, který máte předplacený. Když používáte:

- **Kabelový internet, kde vám ISP dynamicky určuje WAN IP adresu**, vztahuje se to k nastavení WAN – kabelový internet s dynamickým určením IP.
- **Kabelový internet, kde vám ISP poskytne fixní IP adresu** (nebo řadu fixních IP adres), vztahuje se to k nastavení WAN – kabelový internet se statickým určením IP.
- **ADSL Internet, který požaduje standardní Point to Point Tunneling Protocol (PPTP)** pro ověření, vztahuje se to k nastavení WAN – ADSL Internet užívající Point to Point Tunneling Protocol (PPTP).

Nastavení WAN – Kabelový internet s dynamickým určením IP

Access point je předkonfigurován, aby podporoval typ WAN, který dynamicky získá IP adresu od ISP. Nicméně si můžete ověřit nastavení WAN podle následujících kroků:

Krok 1: V **CONFIGURATION** menu klikněte na **WAN Setup**.



Krok 2:

Na obrazovce **WAN Dynamic Setup**, která následuje, ověřte, že **WAN Type** čte **Dynamic (DHCP)** v červené barvě. Jinak klikněte na tlačítko **Change**.

Common Configuration

The screenshot shows the 'WAN Dynamic Setup' configuration page. It features a list of fields on the left: WAN Type, IP Address, Network Mask, Gateway IP Address, Primary DNS, and Secondary DNS. The 'WAN Type' field is currently set to 'Dynamic (DHCP)' and has a 'Change' button next to it. The 'IP Address' field has a 'Refresh' button next to it. The background is light blue.

Krok 3:

Jednoduše vyberte **Dynamic IP Address** a zmáčkněte tlačítko **Apply**.

Prosíme klikněte na **Reboot System** v sekci **SYSTEM TOOLS** a zmáčkněte tlačítko **Reboot**, aby bylo nastavení účinné.

The screenshot shows the 'Select WAN Type' configuration page. It features a list of radio button options: Static IP Address, Dynamic IP Address, PPP over Ethernet, and PPTP. The 'Dynamic IP Address' option is selected. At the bottom, there are three buttons: 'Apply', 'Cancel', and 'Help'. The background is light blue.

Poznámka: Existují výjimečné případy, kdy je konfigurace vyžadována předtím, než je IP adresa alokována do access pointu vaším ISP

- Někteří ISP používají MAC adresu prvního zařízení, které je používáno k připojení širokopásmového kanálu a WAN IP adresu ukáže jen tehdy, když se MAC adresa shoduje s tou která je nahlášena. Proto pokud nemáte předplacený kabelový internet (např. váš počítač je původně připojen přímo ke kabelovému modemu), přeskočte přímo na kroky 4 – 5, kde je možné naklonovat "schválené" MAC adresy do access pointu.
- Určitá ISP požadují ověření přes DHCP klientské ID před vydáním veřejné IP adresy. Access point používá Jmenný systém v Systému identit jako DHCP klientské ID.

Proto jestliže je toto ten případ, vyhledejte v ISP správné DHCP klientské ID a postupujte podle kroků 6 – 7, čímž dokončíte nastavení.

Krok 4:

Common Configuration

Kroky 4 – 5 jsou pro ty, kteří potřebují naklonovat svou MAC adresu ethernetového adaptéru.

Ve **WAN Setup** pod **CONFIGURATION** menu, uvidíte možnost **Advanced WAN Options**. Klikněte na **MAC Clone** a program bude pokračovat.

Krok 5:

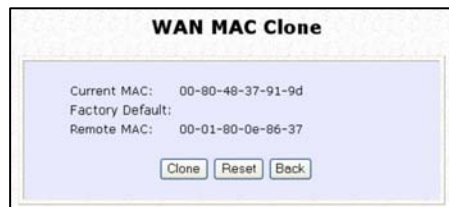
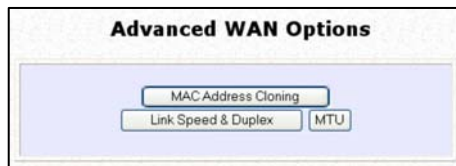
Jednoduše klikněte na tlačítko **Clone**, aby váš access point naklonoval MAC adresu vašeho ethernetového adaptéru, rozezanou vaším ISP.

Prosíme nezapomeňte kliknout na **Reboot System** pod možností **SYSTEM TOOLS** a zmáčkněte tlačítko **Reboot**, aby bylo nastavení účinné.

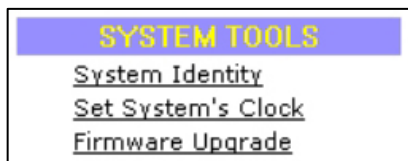
Krok 5:

Kroky 6 - 7 jsou pro ty, kteří potřebují nastavit **System Name** v **System Identity**, aby to ISP mohlo ověřit jako platné DHCP klientské ID.

Klikněte na **System Identity** v **SYSTEM TOOLS** příkazovém menu.



Poznámka: (Pokud to je zapotřebí, můžete vyresetovat MAC adresu access pointu zpět na výrobní přednastavení tím, že kliknete na **Reset** na té samé stránce.



Common Configuration



System Identity

System Name : Wireless LAN Access Point

System Contact : unknown

System Location : unknown

Apply

Krok 5:

Na následující obrazovce zadejte vaše ISP přiřazené DHCP klientské ID jako **System Name** (Mohli byste také chtít zadat preferovanou osobu v **Systems Contact** a **System Location** vašeho access pointu). Pro dokončení klikněte na tlačítko **Apply**.

Prosíme nezapomeňte kliknout na **Reboot System** v **SYSTEM TOOLS** a zmáčkněte tlačítko **Reboot**, aby bylo nastavení účinné.

Common Configuration

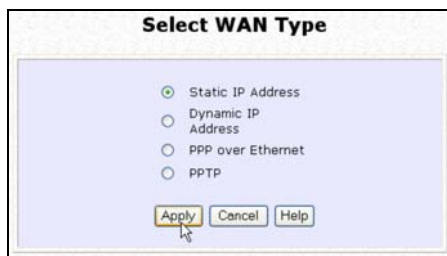
Nastavení WAN – Kabelový internet se statickým určením IP

Pokud máte ISP, které najímá statickou WAN IP na předplatné, budete potřebovat adekvátně konfigurovat WAN typ vašeho access pointu. Například pokud vám poskytuje ISP následující informace o nastavení, můžete nastavit WAN podle následujícího popisu.

IP Adresa : 203.120.12.240
Síťová maska : 255.255.255.0
Gateway IP Adresa : 203.120.12.2

Krok 1:

V **CONFIGURATION** příkazovém menu klikněte na **WAN Setup**.



Krok 2:

Dostaňte se na stránku **Select WAN Type** a vyberte **Static IP Address** před tím, než kliknete na tlačítko **Apply**. Dostanete se na následující stránku, na které od vás budou požadovány vstupy.

Krok 3:

Vyplňte vaším ISP poskytnuté informace do kolonek **IP Address (IP adresa)**, **Network Mask (síťová maska)** a **Gateway IP Address** předtím, než kliknete na tlačítko **Apply**.

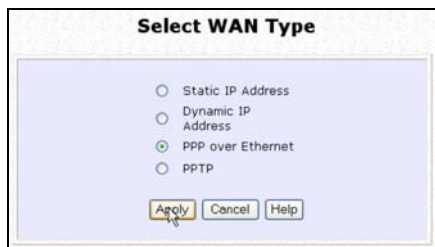
Prosíme nezapomeňte kliknout na **Reboot System** v **SYSTEM TOOLS** a zmáčkněte tlačítko **Reboot**, aby bylo nastavení účinné.



Common Configuration

Nastavení WAN - ADSL Internet užívající PPP over Ethernet (PPPoE)

Pokud máte předplacenou službu ADSL užívající PPP over Ethernet (PPPoE) ověřování, můžete nastavit WAN typ vašeho access pointu podle následujících kroků. Například můžete konfigurovat účet, kde uživatelské jméno je "guest", jak je uvedeno dole:



Krok 3:

Jako **Username (uživatelské jméno)**, zaklínujte jméno účtu určené vaší ISP (např. "guest" jako v tomto případě) následuje **Password (heslo)** vašeho účtu.

Krok 4:

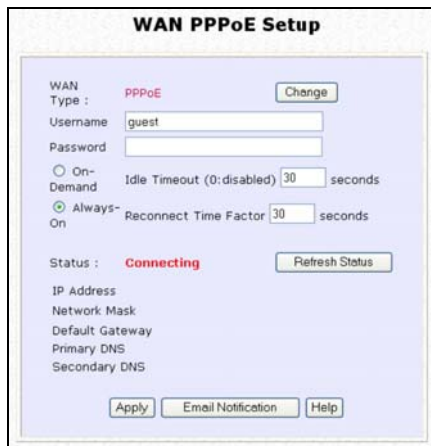
Zvolte možnost **Always-On** pokud chcete, aby váš access point vždy udržoval spojení s ISP. Jinak můžete vybrat možnost **On-Demand**. Access point se následně spojí s ISP automaticky když obdrží internetovou žádost od počítačů v síti.

Krok 1:

V **CONFIGURATION** příkazovém menu klikněte na **WAN Setup**.

Krok 2:

Dostaňte se na stránku **Select WAN Type** a vyberte **PPP over Ethernet** před tím, než kliknete na tlačítko **Apply**. Dostanete se na následující stránku, na které od vás budou požadovány vstupy.



Common Configuration

Nastavení **Idle Timeout (prázdný časový limit)** je spojováno s možností **On-Demand**, která vám umožňuje specifikovat hodnotu (v sekundách), po které access point ukončí spojení s ISP po poslední aktivitě internetu. Hodnota "0" vyřadí prázdný časový limit. **Reconnect Time Factor** je spojován s možností **Always-on** a specifikuje maximální čas, po který access point počká před tím, než se znovu pokusí o spojení s ISP. Zmáčkněte tlačítko **Apply** a **Reboot**.

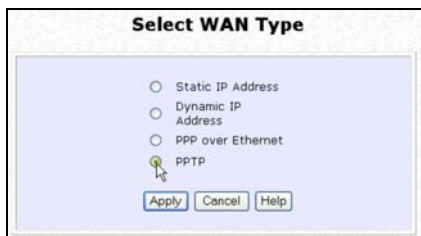
Nastavení WAN – ADSL Internet užívající PPTP

Pokud máte předplacenou službu ADSL užívající Point to Point Tunneling Protocol (PPTP) ověření, můžete nastavit WAN typ vašeho access pointu podle následujících kroků. Například pokud vám ISP poskytl následující informace o nastavení, můžete nastavit WAN podle popisu dole:

IP Adresa : 203.120.12.47
Síťová maska : 255.255.255.0
VPN Server : 203.120.12.15

Krok 1:

V **CONFIGURATION** příkazovém menu klikněte na **WAN Setup**.



Krok 2:

Dostaňte se na stránku **Select WAN Type** a vyberte **PPTP** před tím, než kliknete na tlačítko **Apply**. Dostanete se na následující stránku, na které od vás budou požadovány vstupy.

Krok 3:

Vyplňte vaším ISP poskytnuté informace do kolonek **IP Address (IP adresa)**, **Network Mask (síťová maska)** a **VPN Server** předtím, než kliknete na tlačítko **Apply**.

Prosíme nezapomeňte kliknout na **Reboot System** v **SYSTEM TOOLS** a

Common Configuration

zmáčkněte tlačítko **Reboot**, aby bylo nastavení účinné.

Nastavení **Idle Timeout (prázdný časový limit)** vám umožňuje specifikovat hodnotu (v sekundách) po které access point ukončí spojení s ISP po poslední aktivitě internetu. Hodnota "0" vyřadí prázdný časový limit.

WAN PPTP Setup

WAN Type: **PPTP**

IP Address:

Network:

Mask:

Username:

Password:

VPN Server:

Idle Timeout: (30-3600, 0: disabled)

Status: **Disconnected**

IP Address

Network

Mask

Gateway IP Address

NASTAVENÍ SNMP

Simple Network Management Protocol (SNMP) je sada komunikačních protokolů, které oddělují strukturu managementu od struktury hardwarových zařízení.

Krok 1:

Klikněte na **SNMP z CONFIGURATION** menu.



SNMP Setup

SNMP State: Enable

Read Password:

Read/Write Password:

Apply

Krok 2:

Vyberte možnost **Enable** ze seznamu, který se vyroluje, když zadáte **SNMP State**.

Přednastavené heslo **Read Password** je veřejné, zatímco přednastavené heslo **Read/Write Password** je soukromé.

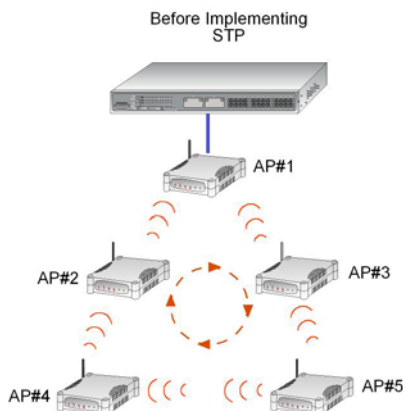
Krok 3:

Klikněte na tlačítko **Apply**.

NASTAVENÍ STP

(DOSTUPNÉ JEN V MODECH ACCESS POINT, POINT TO POINT A POINT TO MULTIPLE POINT)

Spanning Tree Protocol (STP) je spojovací management protokol, který pomáhá předcházet výskytu nežádoucích smyček v síti. Aby ethernetová síť fungovala správně, je potřeba, aby existovala jen jedna aktivní cesta mezi dvěma stanicemi. Pokud v síťové topologii existuje smyčka, objeví se duplikace zpráv, což může zmařit zasilatelský algoritmus a duplikáty mohou být odeslány.

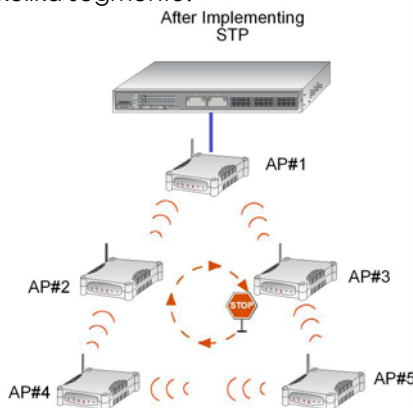


Common Configuration

Krátce – hlavní důvod aktivace STP je předcházet vytváření smyček, když existují redundantní cesty v síti. Bez aktivace STP způsobí redundantní topologie broadcast storming.

K založení redundance cesty STP vytvoří strom, který obsáhne všechny zařízení v rozšířené síti, což přinutí redundantní cesty zůstat ve stavu zálohy nebo blokace, ale vytvoří se redundantní linky jako rezerva pro případ, že aktivní linka selže. Jestliže se STP změní, nebo jeden ze síťových segmentů v STP se stane nedosažitelný, spanning tree algoritmus rekonfiguruje spanning tree topologii a znovu zavede spojení aktivací zálohované cesty. Pokud nebude spanning tree na místě, je možné, že bude současně probíhat více než jedno spojení, což by vyústilo v nekonečnou smyčku datového toku v LAN síti.

Operace Spanning-Tree protokolu jsou pro konečné stanice transparentní. Ty si nejsou vědomy toho, jestli jsou připojeny k jednomu segmentu LAN nebo změněnému LANu několika segmentů.



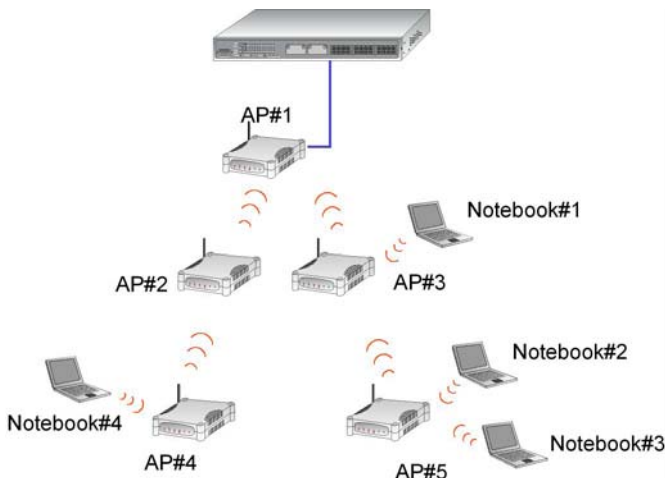
Používána bude cesta s nejmenšími náklady a extra redundantní cesta bude vyřazena.

Common Configuration

K vysvětlení účinku STP & Pseudo VLAN na bezdrátové klienty srovnáme 3 samostatné scénáře.

Scénář #1 – (bez STP, bez Pseudo VLAN)

Podle spodního obrázku – pokud Spanning Tree Protocol (STP) a Pseudo VLAN nejsou v síti zrealizovány, všichni klienti (Notebook#1, #2, #3 & #4,) mohou získat přístup jeden k druhému, což vyústí v nízkou úroveň ochrany dat. Vzhledem k redundantním cestám, které byly v síti nalezeny, bude vysílání zdvojnásobeno a odesláno a výsledkem nakonec bude broadcast storm.



Common Configuration

Scénář #2 – (s STP, bez Pseudo VLAN)

Pokud je STP zavedeno, extra redundantní síťové cesty mezi access pointy budou vyřazeny, což předejde četným aktivním síťovým cestám mezi jakýmkoliv access pointy.

Pokud jeden z access pointů nefunguje, STP algoritmus reaktivuje jednu z redundantních cest, aby se síťové spojení neztratilo.

Všichni bezdrátoví uživatelé spolu budou moci komunikovat, pokud jsou přidružení k access pointům, které jsou ve stejné WDS zóně.



Common Configuration

MAC FILTERACE

MAC Filtrace funguje jako míra ochrany tím, že kontroluje přístupy uživatelů k síti přes jejich MAC adresy. Můžete mít buď seznam MAC adres, který bude korespondovat seznamu uživatelů, kteří mají na síť povolen přístup, nebo můžete mít seznam MAC adres uživatelů, kteří mají přístup zakázán.

Krok 1:

Klikněte na **MAC Filtering** z **CONFIGURATION** menu. **Enable** funkci MAC Filtrace.

MAC Address Filtering

MAC Filtering : **Enable** ▼

Allow PCs listed to access network

Prevent PCs listed from accessing network

MAC Address List

Activation	MAC Address	Comments
------------	-------------	----------

(All changes will take effect after reboot)

Krok 2:

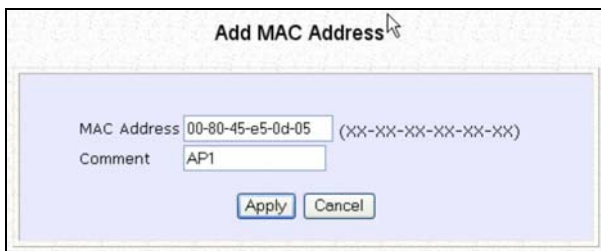
Klikněte na tlačítko **Add**, tím se vytvoří klient v seznamu MAC adres.

Common Configuration

Krok 3:

V poli **Mac Address** zadejte bezdrátovou MAC adresu klienta ve formátu **xx-xx-xx-xx-xx-xx**, kde x může být jakákoliv hodnota od 0-9 nebo a-f. Potom napište text v poli **Comment**, abyste měli identifikaci MAC adresy, kterou jste právě přidali.

Klikněte na tlačítko **Apply**.

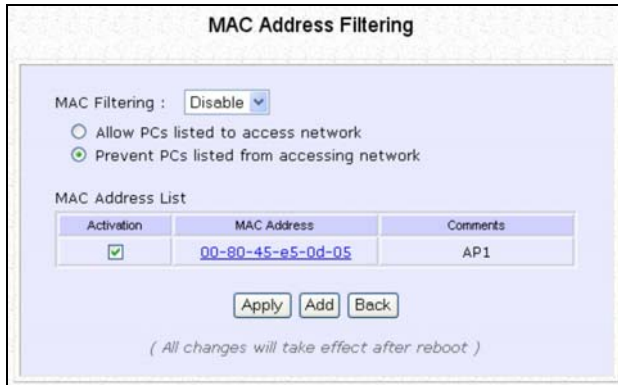


Add MAC Address

MAC Address: (XX-XX-XX-XX-XX-XX)

Comment:

Všimněte si, že MAC adresa byla přidána na seznam.



MAC Address Filtering

MAC Filtering :

Allow PCs listed to access network

Prevent PCs listed from accessing network

MAC Address List

Activation	MAC Address	Comments
<input checked="" type="checkbox"/>	00-80-45-e5-0d-05	AP1

(All changes will take effect after reboot)

Krok 4:

Dále si můžete vybrat, jestli chcete uživatelům ze seznamu MAC adres povolit nebo zakázat přístup na síť. Jednoduše klikněte na kulaté zatrhávací políčko vedle **Allow PCs listed to access network(povolit přístup)** respektive **Prevent PCs listed from accessing network(zamezit přístupu)**.

Common Configuration

Krok 5:

Klikněte na tlačítko **Apply**, aby se změny aktualizovaly.



POZNÁMKA

Pokud funguje MAC filtrace s pravidlem **Allow PCs listed to access network** (povolit přístup), Nesmí být seznam MAC adres prázdný.

PŘIDAT DALŠÍ MAC ADRESU NA SEZNAM MAC ADRES

Následujte proceduru popsanou v krocích 2 – 3.

UPRAVIT/SMAZAT MAC ADRESU ZE SEZNAMU MAC ADRES

Krok 1:

V tabulce klikněte na **MAC address**, jak je naznačeno dole.

Activation	MAC Address	Comments
<input checked="" type="checkbox"/>	00-80-45-e5-0d-05	AP1

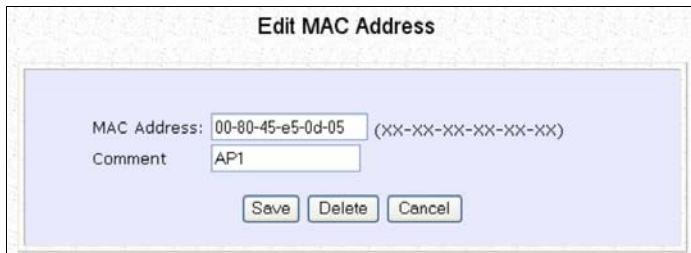
Všimněte si, že je v seznamu MAC adres kolonka označená **Activation**. Pokud je zaškrtnutá, dojde k akci (buď povolení nebo zamezení přístupu na síť) týkající se počítače, který má korespondující MAC adresu.

Common Configuration

Krok 2:

Ze stránky [Edit MAC Address](#)

Klikněte na tlačítko **Delete**, pokud chcete odstranit MAC adresu, nebo klikněte na tlačítko **Save** potom co jste upravil zápis.



The screenshot shows a web form titled "Edit MAC Address". It contains two input fields: "MAC Address" with the value "00-00-45-e5-0d-05" and a placeholder "(XX-XX-XX-XX-XX-XX)", and "Comment" with the value "AP1". Below the fields are three buttons: "Save", "Delete", and "Cancel".

Kapitola 5: Bezpečnost WLAN

Tato sekce popisuje, jak to udělat, aby byl WLAN více zabezpečený. Všechny nody ve vaší síti MUSÍ sdílet stejné bezdrátové nastavení, jinak nebudou schopní komunikovat.

Ukážeme vám, jak konfigurovat zvlášť každý z typů bezpečnostních modů.

Pro začátek postupujte podle následujících předběžných kroků, které vedou k výběru nejvhodnějšího bezpečnostního přístupu pro ochranu bezdrátové komunikace.

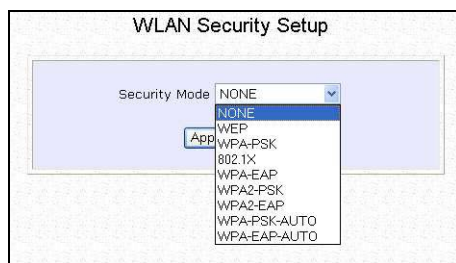
Krok 1:

Klikněte na **WLAN Setup** z **CONFIGURATION** menu pro výběr **Security(bezpečnosti)**.

Krok 2:

Vyberte si z vyrolovaného menu **Security Mode(bezpečnostní mod)**. **Security Mode** je přednastaven na možnost **NONE** (žádný).

Klikněte na tlačítko **Apply**.



JAK NASTAVIT WEP

Pokyny vám pomůžou nastavit váš access point pro používání WEP.

Na stránce **WEP Setup**,

WEP Setup

Key String Type:
 Hex (0~9, a~f, A~F) Length 10 or 26
 Ascii (0~9, a~z, A~Z) Length 5 or 13

Transmission key: Key 1

Key 1: 64Bit 128Bit
[Text Input] [Reset]

Key 2: 64Bit 128Bit
[Text Input] [Reset]

Key 3: 64Bit 128Bit
[Text Input] [Reset]

Key 4: 64Bit 128Bit
[Text Input] [Reset]

[Apply]

Krok 1:

Specifikujte **key entry type** (typ zápisu klíče) tím, že vyberete jedno z:

- **Use Hexadecimal (použit šestnáctkový):**
- **Use ASCII (použit ASCII)**

Krok 2:

Vyberte **Transmission Key** (klíč přenosu) z vyrolovaného menu:

- **Key 1**
- **Key 2**
- **Key 3**
- **Key 4**

Access point vás nechá definovat až čtyři různé klíče přenosu. Definuje to sada sdílených klíčů bezpečnosti sítě. Musíte zadat alespoň jeden WEP klíč, aby mohl být bezpečnostní klíč použit.

Krok 3:

Zvolte **length** (délku) každého kódovacího klíče:

- **64-bit WEP**
10 šestnáctkových nebo 5 ASCII Text
- **128-bit WEP**
26 šestnáctkových nebo 13 ASCII Text

Pro smazání hodnot, které jste zadali, klikněte na tlačítko **Reset**.

Klikněte na tlačítko **Apply** a restartujte váš access point.

JAK NASTAVIT WPA-PSK/WPA2-PSK/WPA-PSK-AUTO (dostupné jen v modu Access Point)

Následující pokyny vám pomohou nastavit access point na používání WPA-PSK. Prosíme následujte kroky, pokud jste aktivovali bezpečnostní mody **WPA-PSK**, **WPA2-PSK** nebo **WPA-PSK-AUTO**.

Na stránce **WPA1/2-PSK Setup**,

WPA1/2-PSK Setup

Key String Type:
 Hexadecimal(64 hex digits)
 Passphrase(8~63 ascii characters)

WPA-PSK:

Cipher Type: ▼

GTK Update(seconds): (60~9999)

Krok 1:

Specifikujte **key entry type (typ zápisu klíče)** tím že si vyberete jedno z:

- **Passphrase (Alfanumerické znaky)**
- **Hexadecimal (šestnáctkový)**

Krok 2:

Vyplňte **WPA-PSK** (dříve sdílený síťový klíč):

Pokud používáte formát **Passphrase**, může váš zápis obsahovat minimálně 8 alfanumerických znaků nebo maximálně 63 alfanumerických znaků.

Pokud používáte šestnáctkový formát, MUSÍ 64 šestnáctkových znaků.

Krok 3:

Pro WPA-PSK

Nastavte **Cipher Type (typ šifry)** na **TKIP**.

WPA nahradí WEP silnou kódovací technologií nazvanou Temporal Key Integrity Protocol (TKIP) s Message Integrity Check (MIC).

Pro WPA2-PSK

Nastavte **Cipher Type (typ šifry)** na **AES**.

Advanced Encryption Standard (AES) je silnější symetrická 128-bitová bloková technika kódování dat. AES je požadavek WPA2 podle norem IEEE 802.11i.

Pro WPA-PSK-AUTO

Nastavte **Cipher Type (typ šifry)** na **Auto**, čímž umožníte access pointu, aby automaticky vyhledal jaký typ cifer má použít.

Krok 4:

Vložte **GTK (Group Transient Key) Updates**.

Toto je délka času, po které access point automaticky vygeneruje nový sdílený klíč k bezpečnému multicastovému vysílání mezi všemi stanicemi, které s ním komunikují. Standardní doba je 600 sekund.

WLAN Security

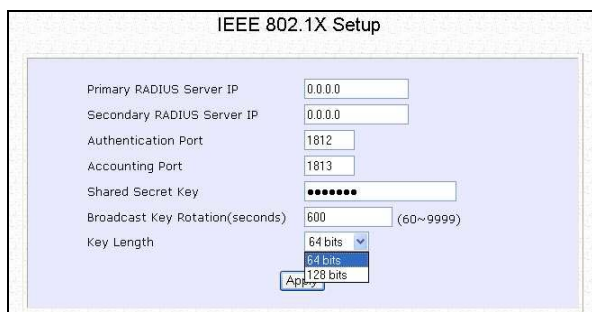
Krok 5:

Zmáčkněte tlačítko **Apply** a restartujte systém. Tím se stane nastavení účinným.

JAK NASTAVIT 802.1x/RADIUS (DOSTUPNÉ JEN V MODU ACCESS POINT)

Následující pokyny vám pomohou nastavit access point na používání 802.1x/RADIUS.

Na stránce IEEE 802.1x Setup,



IEEE 802.1X Setup	
Primary RADIUS Server IP	0.0.0.0
Secondary RADIUS Server IP	0.0.0.0
Authentication Port	1812
Accounting Port	1813
Shared Secret Key
Broadcast Key Rotation(seconds)	600 (60~9999)
Key Length	64 bits
	64 bits
	128 bits
	Apply

Krok 1:

Zaklínujte IP adresu **Primary RADIUS Serveru** ve vašem WLANu. Můžete podle vlastního uvážení přidat IP adresu **Secondary RADIUS Serveru**, pokud nějakou máte.

Server RADIUS ověřování MUSÍ být ve stejné podsíti jako access point.

Krok 2:

Standardně je hodnota pro číslo **Authentication Port** - **1812**. Tuto hodnotu můžete ponechat. Tato hodnota musí být stejná jako ta v serveru RADIUS .

Krok 3:

Standardně je hodnota pro číslo **Accounting Port** . **1813**. Tuto hodnotu můžete ponechat. Tato hodnota musí být stejná jako ta v serveru RADIUS.

Krok 4:

Do pole, které vám je nabídnuto, запиšte **Shared Secret Key** (sdílený tajný klíč).

Krok 5:

Standardně je **Broadcast Key Rotation (rotace vysílacího klíče)** nastavena na **600** sekund. Tuto hodnotu můžete ponechat.

Krok 6:

Vyberte **length (délku)** každého kódovacího klíče:

- **64-bitů**
10 šestnáctkový nebo 5 ASCII Text
- **128-bitů**
26 šestnáctkový nebo 13 ASCII Text

Krok 7:

Zmáčkněte tlačítko **Apply** a restartujte systém. Tím se stane nastavení účinné.

JAK NASTAVIT WPA EAP/WPA2-EAP/WPA-EAP-AUTO (JEN MOD ACCESS POINT PODPORUJE WPA2-EAP A WPA-EAP-AUTO)

Následující pokyny vám pomohou nastavit access point na používání WPA-EAP. Pokud jste zvolili WPA nebo WPA1-EAP, WPA2-EAP nebo WPA-EAP-AUTO, prosíme postupujte podle následujících kroků.

Na stránce **WPA1/2-EAP Setup**,

WPA1/2-EAP Setup

Primary RADIUS Server IP	<input type="text" value="0.0.0.0"/>
Secondary RADIUS Server IP	<input type="text" value="0.0.0.0"/>
Authentication Port	<input type="text" value="1812"/>
Accounting Port	<input type="text" value="1813"/>
Shared Secret Key	<input type="password" value="....."/>
Cipher Type:	<input type="button" value="AUTO"/>
GTK update(seconds):	<input type="text" value="TKIP"/> <input type="text" value="AES"/> <input type="text" value="AUTO"/> (60~9999)

Krok 1:

Zaklíňte IP adresu **Primary RADIUS Serveru** ve vašem WLANu.

Pokud chcete, můžete přidat IP adresu **Secondary RADIUS Serveru**, pokud nějakou máte. Server ověřování RADIUS MUSÍ být ve stejné podsíti jako access point.

Krok 2:

Standardně je hodnota čísla **Authentication Port** - **1812**. Tuto hodnotu můžete buď ponechat, nebo můžete zaklíňovat odlišný Authentication Port, který se ale MUSÍ shodovat s portem serveru RADIUS.

Krok 3:

Standardně je hodnota pro **Accounting Port - 1813**. Tuto hodnotu můžete ponechat. Tato hodnota musí být stejná jako ta v serveru RADIUS.

Krok 4:

Zadejte **Shared Secret Key (sdílený tajný klíč)**, který je používán k potvrzení platnosti komunikace klientského serveru RADIUS.

Krok 5:

Zvolte **length** (délku) každého kódovacího klíče:

- **64-bitů**
10 šestnáctkových nebo 5 ASCII Text
- **128-bitů**
26 šestnáctkových nebo 13 ASCII Text

Krok 6:

Pro WPA-EAP

Nastavte **Cipher Type (typ šifry)** na **TKIP**.

WPA nahradí WEP silnou kódovací technologií nazvanou Temporal Key Integrity Protocol (TKIP) s Message Integrity Check (MIC).

Pro WPA2-EAP (jen v moci Access Point)

Nastavte **Cipher Type** (typ šifry) na **AES**.

Advanced Encryption Standard (AES) je silnější symetrická 128-bitová bloková technika kódování dat. AES je požadavek WPA2 podle norem IEEE 802.11i.

Pro WPA-EAP-AUTO (jen v modu Access Point)

Nastavte **Cipher Type (typ šifry)** na **Auto**, čímž umožníte access pointu, aby automaticky vyhledal jaký typ šifer má použít.

Wireless Extended Features

Krok 7:

Vložte **GTK (Group Transient Key) Updates**.

To je délka času, po které access point automaticky vygeneruje nový sdílený klíč k bezpečnému multicastovému vysílání mezi všemi stanicemi, které s ním komunikují. Standardní doba je 600 sekund.

Krok 8:

Zmáčkněte tlačítko **Apply** a restartujte systém. Tím se stane nastavení účinné.

Kapitola 6: Rozšířené bezdrátové vlastnosti

Tato sekce ukazuje, jak konfigurovat rozšířené bezdrátové vlastnosti. Pro začátek postupujte podle následujících předběžných kroků.

KONTROLA PŘÍSTUPU – BEZDRÁTOVÝ PSEUDO VLAN (JEN V MODU ACCESS POINT)

VLAN je skupina počítačů nebo jiných síťových zdrojů, které se chovají jako by byly připojeny k jednoduchému síťovému segmentu, ačkoli mohou být fyzicky umístěny na odlišném segmentu LANu.

Tyto stanice, které jsou přiděleny ke stejným Vlan sdíleným síťovým zdrojům a šířce pásma, jako by byly připojeny ke stejnému segmentu. Naopak jen stanice ve stejném VLANu mohou mít jedna ke druhé přístup.

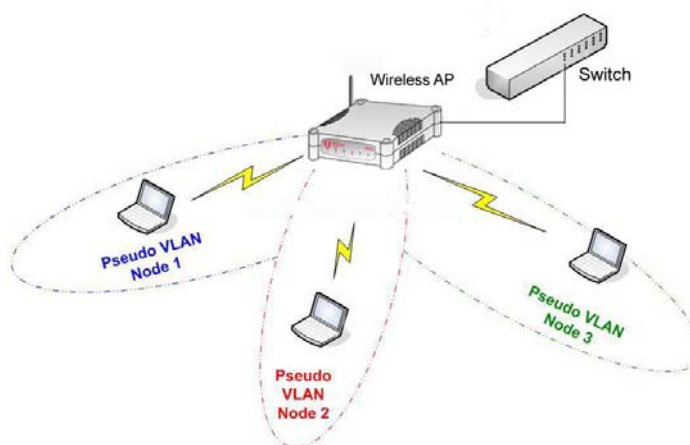
Činností **Bezdrátového Pseudo VLANu** je segregovat jednoduchý bezdrátový LAN do několikačetného bezdrátového VLANu, aby komunikovat mohli jen klienti v rámci stejného VLANu.

Při operování v modu **Access Point** vám Access point umožní *Bezdrátový Pseudo VLAN Per Node* a *Bezdrátový Pseudo VLAN Per Group*.

Pokud se chcete dozvědět víc o exkluzivním **Bezdrátovém Pseudo VLANu** firmy Compex, můžete se obrátit na internetové stránky www.cpx.com nebo www.compex.com.sg.

BEZDRÁTOVÝ PSEUDO VLAN PER NODE

Pokud je tento mod zrealizován, izoluje každého bezdrátového kliento do vlastního pseudo VLANu. Bezdrátoví klienti proto mají přístup ke zdrojům v drátové síti ale nejsou schopní vidět jeden druhého a nemají navzájem přístup ke svým datům.



Wireless Extended Features

Následující kroky demonstrují jak nastavit bezdrátový Pseudo VLAN per Node.

Krok 1:

Z možnosti **WLAN Setup** pod **Configuration** menu, klikněte na možnost **Advanced**, čímž se vám ukáže stránka **WLAN Advanced Setup**.

Krok 2:

Jděte do sekce **Extended Features** a klikněte na tlačítko **Wireless Pseudo VLAN**.

The screenshot shows two parts of a configuration interface. The top part is titled "WLAN Advanced Setup" and contains a table of settings:

Beacon Interval	100	(100:20-1000)
Data Beacon Rate (DTIM)	1	(1:1-16384)
RTS/CTS Threshold	512	(512:1-2312)
Frag Threshold	2346	(2346:256-2346)
Transmit Power	Maximum	

Below the table is an "Apply" button. The bottom part of the screenshot shows the "Extended Features" section with three buttons: "Wireless Pseudo VLAN" (highlighted with a blue box), "WDS Configuration", and "Long Distance Parameters".

Krok 3:

Funkce **Wireless Pseudo VLAN** není standardně zapnutá. Klikněte na tlačítko **Change**, abyste zrealizovali vaši volbu typu Pseudo VLANu.

Wireless Extended Features

Krok 4:

Vyberte kruhové zaškrtnávací políčko **Per node** a klikněte na tlačítko **Apply**.

Select Wireless Pseudo VLAN Type

Disable

Per node

Per group

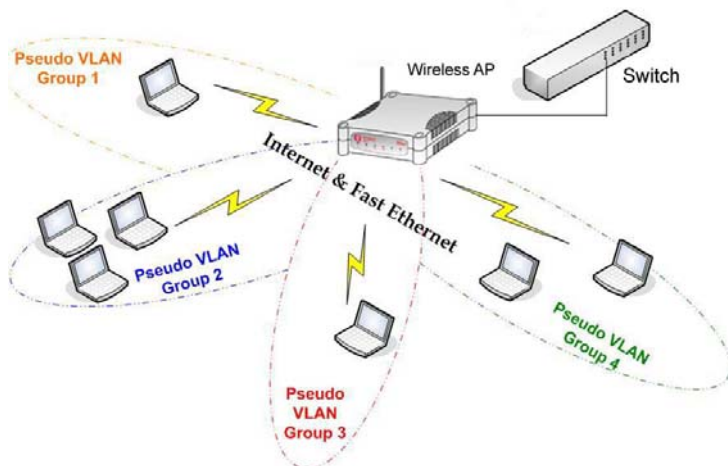
Bezdrátový Pseudo VLAN se nakonfiguroval jako Per node.

Wireless Pseudo VLAN

Type : Per node

BEZDRÁTOVÝ PSEUDO VLAN PER GROUP

Access point může nakonfigurovat až 32 'skupin' bezdrátových klientů identifikovaných jejich MAC adresami. Kdykoliv bezdrátový klient požádá o přístup na síť, access point nejdříve ověří, jestli je jeho MAC adresa přítomná v některé ze skupin Pseudo VLANu. Když to tak je, access point povolí přístup zdrojům drátového systému a všem ostatním bezdrátovým klientům, kteří patří do stejné skupiny Pseudo VLAN.



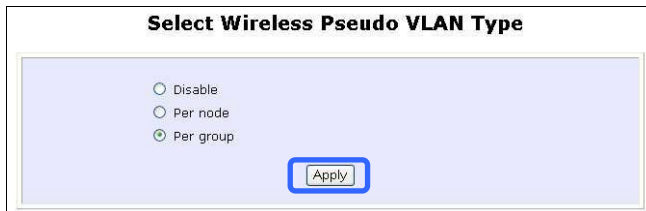
Wireless Extended Features

Následující kroky ukazují jak nastavit Bezdrátový Pseudo VLAN Groups.

VYTVOŘENÍ KLIANTA VE SKUPINĚ PSEUDO VLAN

Krok 1:

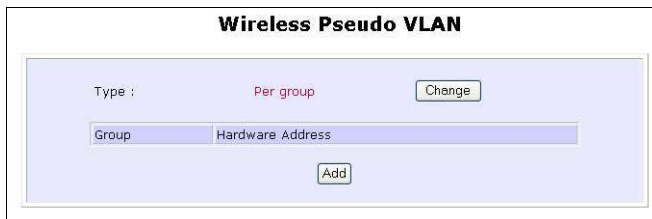
Ze stránky **Select Wireless Pseudo VLAN Type** vyberte možnost **Per group** a klikněte na tlačítko **Apply**.



The screenshot shows a configuration window titled "Select Wireless Pseudo VLAN Type". It contains three radio button options: "Disable", "Per node", and "Per group". The "Per group" option is selected. Below the options is a button labeled "Apply".

Krok 2:

Klikněte na tlačítko **Add**, aby se vytvořil klient ve skupině Bezdrátového Pseudo VLANu.



The screenshot shows a configuration window titled "Wireless Pseudo VLAN". It displays "Type : Per group" with a "Change" button next to it. Below this is a table with two columns: "Group" and "Hardware Address". At the bottom of the table is an "Add" button.

Wireless Extended Features

Krok 3:

Vyberte číslo skupiny z vyrolovaného seznamu **Group**.

Add Wireless Pseudo VLAN Entry

Group:

Hardware Address: (xx-xx-xx-xx-xx-xx)

Krok 4:

Do políčka **Hardware Address (adresa hardwaru)** vyplňte MAC adresu klienta ve formátu **xx-xx-xx-xx-xx-xx**, kde x je jakákoliv hodnota ve škále 0-9 nebo a-f.

Krok 5:

Klikněte na tlačítko **Add** aby se změny aktualizovaly.

Skupina Pseudo VLAN byla přidána do seznamu, jak je to ukázáno na obrázku.

Wireless Pseudo VLAN

Type : Per group

Group	Hardware Address
01	00-80-45-e5-0d-05



POZNÁMKA

Klient může být členem více než jedné skupiny Pseudo VLAN. Například pokud je klient členem skupiny 01 a 02 bezdrátového Pseudo VLANu, bude schopný komunikovat s ostatními klienty z obou skupin.

Wireless Extended Features

PŘIDAT DALŠÍHO KLINTA DO SKUPINY PSEUDO VLAN

Postupujte podle kroků 3-5. Můžete vytvořit až 32 členů skupiny bezdrátového Pseudo VLAN.

UPRAVIT/VYMAZAT KLIENTA ZE SKUPINY PSEUDO VLAN

Krok 1:

Klikněte v tabulce na **MAC adresu**, jak je zde ukázáno.

Wireless Pseudo VLAN

Type : Per group

Group	Hardware Address
01	00-B0-45-e5-0d-05

Krok 2:

Ze stránky **Edit Wireless Pseudo VLAN Entry**,

Klikněte na tlačítko **Delete**, pokud chcete odstranit klienta ze skupiny, nebo Klikněte na tlačítko **Save**, pokud jste zápis upravovali.

Edit Wireless Pseudo VLAN Entry

Group:

Hardware Address: (XX-XX-XX-XX-XX-XX)

Wireless Extended Features

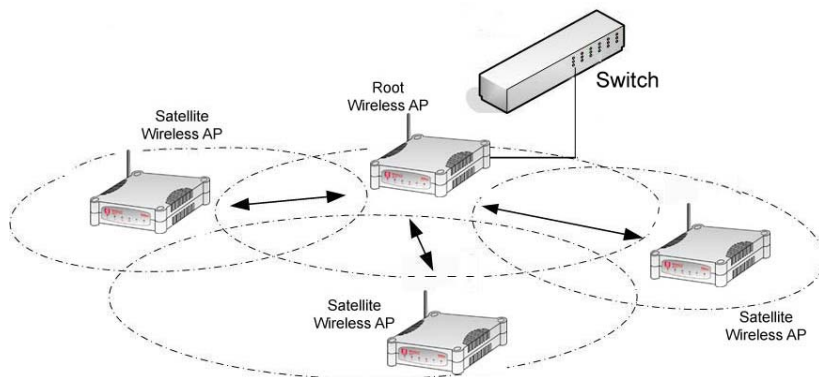
BEZDRÁTOVÉ NASTAVENÍ – BEZDRÁTOVÝ DISTRIBUČNÍ SYSTÉM (WDS) (jen v modu Access Point)

Bezdrátový distribuční systém spojuje několik access pointů a vytváří širší síť, ve které mohou mobilní uživatelé bloumat zatímco zůstanou připojení k dostupným zdrojům sítě.

V WDS může access point řídit zároveň buňku drátových i bezdrátových klientů připojením k ostatním access pointům. To vyžaduje, aby byl operační frekvenční kanál v rámci buňky kontrolovaná access pointem stejný jako jeho bezdrátová spojení k jiným access pointům.

Hvězdicová konfigurace WDS

U hvězdicové konfigurace WDS jsou založená spojení mezi jedním základním access pointem a několika satelitními bezdrátovými access pointy umístěnými tak, aby zvýšily pokrytí oblasti.



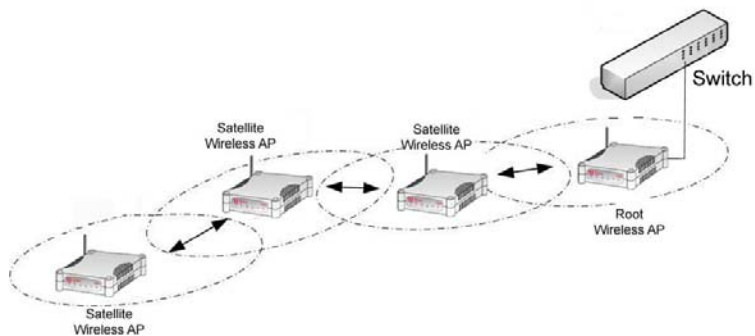
Tady je základní bezdrátový access point připojen ke drátové síti a udržuje tři WDS spojení, zatímco každý satelitní bezdrátový access point udržuje WDS spojení pro komunikace s základním AP.

Wireless Extended Features

Řetězová konfigurace WDS

Řetězová konfigurace WDS může obsáhnout oblast do dálky, například dlouhou chodbu. Satelitní access pointy jsou spolu řetězově spojeny, na začátku je základní access point.

Access point na kterémkoli konci řetězu bude mít pouze jedno WDS spojení, zatímco access pointy ve středu budou mít dvě WDS spojení nakonfigurované k přiřazenění k sousedícímu access pointu směrem nahoru a dolů po řetězu.



Wireless Extended Features

Následující kroky vás provedou nastavením WDS na vašem access pointu.

VYTVOŘIT KLIENTA VE WDS

Krok 1:

Z možností **WLAN Setup** pod **Configuration** klikněte na možnost **Advanced**, čímž se vám ukáže stránka **WLAN Advanced Setup**.

Krok 2:

Jděte do sekce **Extended Features** a klikněte na tlačítko **WDS Configuration**.

The screenshot shows the 'WLAN Advanced Setup' page. It contains a table of configuration options:

Beacon Interval	100	(100:20-1000)
Data Beacon Rate (DTIM)	1	(1:1-16384)
RTS/CTS Threshold	512	(512:1-2312)
Frag Threshold	2346	(2346:256-2346)
Transmit Power	Maximum	

Below the table is an 'Apply' button. Underneath is the 'Extended Features' section, which includes three buttons: 'Wireless Pseudo VLAN', 'WDS Configuration' (highlighted with a blue box), and 'Long Distance Parameters'.

Krok 3:


Jak je ukázáno ve **WDS Setup**, není vlastnost **WDS** standardně aktivována. Klikněte na tlačítko **Change**.

The screenshot shows the 'WDS Configuration' page. It displays the 'WDS Status' as 'Disable' and a 'Change' button (highlighted with a blue box).

Wireless Extended Features

Krok 4:

Ze stránky **Enable/Disable WDS** zvolte možnost **Enable** a klikněte na tlačítko **Apply**.



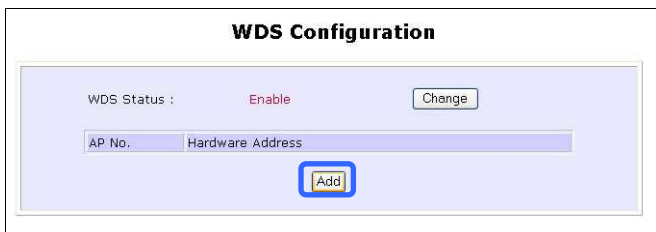
Enable/Disable WDS

Enable Enable the wireless wds function
 Disable Disable the wireless wds function

Apply

Krok 5:

Klikněte na tlačítko **Add**, čímž se vytvoří MAC adresa klienta.



WDS Configuration


WDS Status : **Enable** **Change**

AP No. Hardware Address

Add

Krok 6:

Aby se zařízení zahrnuo do vašeho WDS, vyplňte do políčka **Hardware Address** jeho bezdrátovou MAC adresu. Použijte formát xx-xx-xx-xx-xx-xx, kde x je jakákoliv šestnáctková hodnota 0-9 nebo a-f.



Add WDS Entry

Hardware Address : 00-80-45-e5-0d-05 (xx-xx-xx-xx-xx-xx)

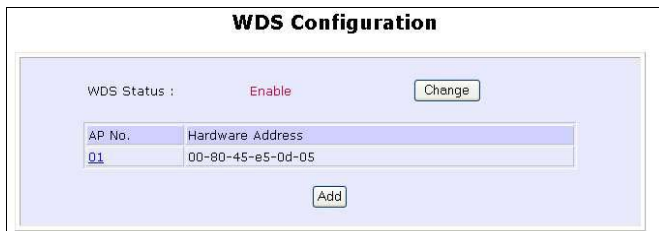
Add Cancel

Klikněte na tlačítko **Add**, aby se tabulka aktualizovala.

Wireless Extended Features

Krok 7:

Na stránce **WDS Configuration** si všimněte, že byla MAC adresa přidána do tabulky, jak to ukazuje tento obrázek.



WDS Configuration

WDS Status : Enable

AP No.	Hardware Address
01	00-80-45-e5-0d-05



POZNÁMKA

Ke konfiguraci WDS musí všechny vaše access pointy používat stejný kanál a stejná bezpečnostní moc a oba access pointy na opačných koncích WDS spojení musí mít navzájem své bezdrátové MAC adresy.

PŘIDAT DALŠÍHO KLIENTA DO SKUPINY PSEUDO VLAN

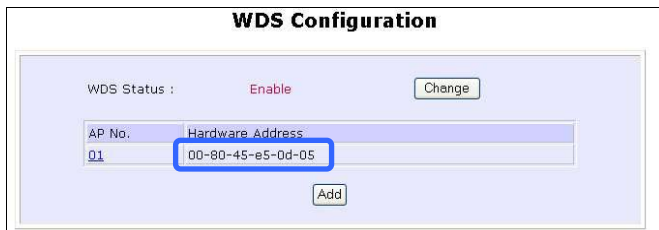
Postupujte podle pokynů u kroků 5 až 7.

Wireless Extended Features

UPRAVIT/VYMAZAT KLIENTA Z WDS

Krok 1:

V tabulce klikněte na **MAC adresu**, jak ukazuje obrázek.



WDS Configuration

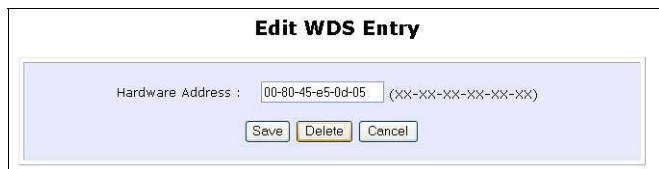
WDS Status : Enable

AP No.	Hardware Address
01	00-80-45-e5-0d-05

Krok 2:

Na stránce **Edit WDS Entry**,

Klikněte na tlačítko **Delete**, pokud chcete odstranit klienta z WDS, nebo klikněte na tlačítko **Save** potom, co jste upravili zápis.



Edit WDS Entry

Hardware Address : (XX-XX-XX-XX-XX)

Wireless Extended Features

PARAMETRY DLOUHÉ VZDÁLENOSTI

Toto nastavení umožňuje access pointu, aby vypočítal a navrhnul parametry použitelné pro delší vzdálenosti access pointů. Následující kroky ukazují jak konfigurovat Parametry dlouhé vzdálenosti.

Krok 1:

Z možností **WLAN Setup** pod **Configuration** klikněte na možnost **Advanced**, čímž se vám zobrazí stránka **WLAN Advanced Setup**.

Krok 2:

Jděte do sekce **Extended Features** a klikněte na tlačítko **Long Distance Parameters**.

WLAN Advanced Setup

Beacon Interval	<input type="text" value="100"/>	(100:20-1000)
Data Beacon Rate (DTIM)	<input type="text" value="1"/>	(1:1-16384)
RTS/CTS Threshold	<input type="text" value="512"/>	(512:1-2312)
Frag Threshold	<input type="text" value="2346"/>	(2346:256-2346)
Transmit Power	<input type="text" value="Maximum"/>	

Extended Features

Wireless Extended Features

Krok 3:

Jak je ukázáno na stránce nastavení **Long Distance Parameters (parametrů dlouhé vzdálenosti)**, není vlastnost **Outdoor** standardně aktivována. Zvolte možnost **Enable** z vyrolovatelného menu.

Long Distance Parameters

Outdoor: Enable

Distance(meter): 120

SlotTime(us): 9

ACKTimeOut(us): 18

CTSTimeOut(us): 18

Show Reference Data

Note: Enter the distance of the client from the AP, a set for recommended parameters for SlotTime, ACKTimeOut and CTSTimeOut will be computed. You can use the recommended parameters or make your own fine tunings. Changes made will only take effect after rebooting.

Apply

Krok 4:

Access point může automaticky vykalkulovat hodnoty vstupních parametrů založených na vzdálenosti mezi vaším access pointem a dalšími bezdrátovými zařízeními. Zadejte vzdálenost v metrech a klikněte na **Show Reference Data**.

Long Distance Parameters

Outdoor: Enable

Distance(meter): 100

Show Reference Data

Microsoft Internet Explorer

Recommended slottime: 10 ;acknowdege timeout: 23; cts timeout:23

OK

Note: Enter the distance of the client from the AP, a set for recommended parameters for SlotTime, ACKTimeOut and CTSTimeOut will be computed. You can use the recommended parameters or make your own fine tunings. Changes made will only take effect after rebooting.

Wireless Extended Features

Krok 5:

Můžete zadat parametry podle doporučených hodnot z vyskakovacího okna. Dále klikněte na tlačítko **Apply**, aby se změny aktualizovaly.

Tato tabulka popisuje parametry, které mohou být modifikovány na stránce **Long Distance Parameters** (parametry dlouhých vzdáleností).

Parametry	Popis
Outdoor	Parametr Outdoor není standardně aktivován. Pokud ho nastavíte na Zapojit, parametr Outdoor bude nakonfigurován pro venkovní komunikaci na krátkou nebo dlouhou vzdálenost (záleží na specifikaci).
Vzdálenost	Tento parametr určuje vzdálenost mezi vaším access pointem a vzdáleným access pointem. Vzdálenost by měla být zadána v metrech.
Slot Time	Čas je rozdělen a každá jednotka času je nazývána jeden time slot.
ACK časová lhůta	Tento parametr určuje časovou lhůtu za kterou musí odesílající klient obdržet potvrzení od přijímacího klienta. Pokud neobdrží během této lhůty žádné potvrzení, odesílatel bude předpokládat, že příjemce neobdržel packet a pokusí se jej odeslat znovu.
CTS časová lhůta	Clear-to-Send time je čas, po který bude bezdrátový odesílatel čekat na CTS balení signalizující, že je kanál prázdný a je možné začít s přenosem dat. Pokud není během této lhůty obdržen žádné CTS balení, odesílatel bude předpokládat, že je kanál příliš zaměstnaný a počká před dalším pokusem odeslat to.

Kapitola 7: Pokročilá konfigurace

ROUTING (PODPOROVÁN JEN MODOY WIRELESS ROUTING CLIENT A GATEWAY)

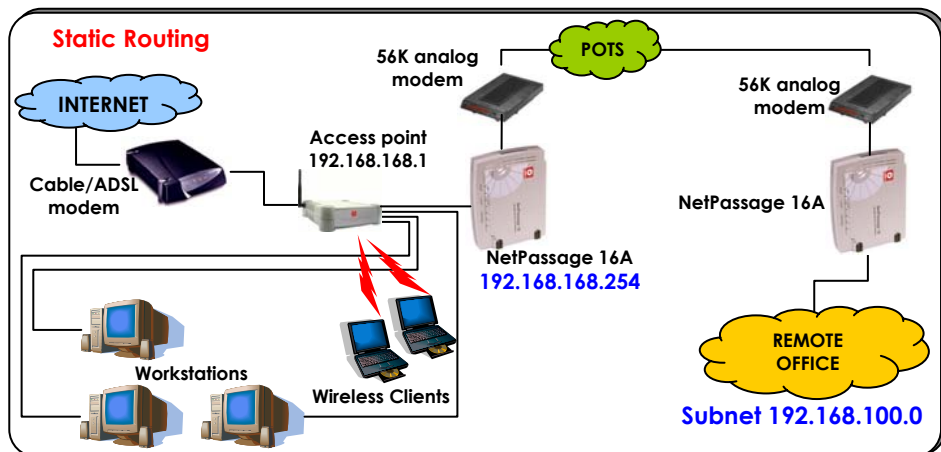
Access point umožní síťovému administrátorovi přidat do směrovací tabulky statický routovací zápis, aby mohl access point přesměrovat IP packety jinému access pointu v síti. Tato vlastnost je velmi užitečná, pokud máte více jak jeden access point.



Důležité:

Nesmíte nastavit žádné směrovací informace, pokud jednoduše konfigurujete access point pro sdílení širokopásmového internetu. Nesprávná směrovací konfigurace bude mít nežádoucí účinky.

Následující diagram ukazuje případ, ve kterém máte dva routery v síti. Jeden router je používán k sdílení širokopásmového internetu, zatímco druhý router je spojen se vzdálenou kanceláří. Potom můžete definovat statický směrovací zápis v access pointu, aby přesměroval balení do vzdálené kanceláře. V této



síti obsahuje hlavní kancelář podsítě 192.168.168.0 dva routery: kancelář je

Advanced Configuration

připojena na internet přes access point (192.168.168.1) a ke vzdálené kanceláři přes NetPassage 16A (192.168.168.254). Vzdálená kancelář sídlí v podsíti 192.168.100.0.

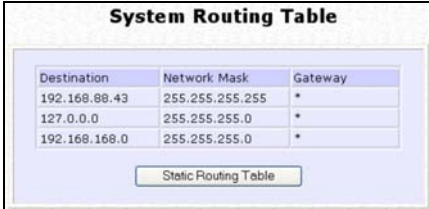
Můžete přidat statický směrovací zázpis do směrovacích tabulek access pointu, aby bylo IP balení od klienta v hlavní kanceláři s destinací IP adresy 192.168.100.X (kde x je jakékoliv číslo od 2 do 254) směrováno do NetPassage 16A Router, který funguje jako brána do této podsítě.

PRO KONFIGURACI STATICKÉHO ROUTING COMPEXU WP54AG

Pokud porozumíte tomu, jak může přidání statického směrovacího zázpisu usnadnit nastavení sítě, jak bylo popsáno výše, můžete konfigurovat access point.

Krok 1:

Z **CONFIGURATION** příkazového menu klikněte na možnost **Routing**. Tím se dostanete na **System Routing Table** – na obrázku napravo. Nejdřív bude tabulka obsahovat standardní přednastavené směrovací zápisy zapsané do access pointu.



Destination	Network Mask	Gateway
192.168.88.43	255.255.255.255	*
127.0.0.0	255.255.255.0	*
192.168.168.0	255.255.255.0	*

Static Routing Table



Destination	Network Mask	Gateway
-------------	--------------	---------

Add Back

Krok 2:

Klikněte na tlačítko **Static Routing Table**.

Na této stránce klikněte na tlačítko **Add**.

Krok 3:

Můžete zde specifikovat **Destination IP Address (cílová IP adresa)**, **Destination Net Mask (cílová síťová maska)** a **Gateway IP Address**. Pro tento případ jimi jsou 192.168.100.0, 255.255.255.0 respektive 192.168.168.254. K dokončení



Static Routing Table	
Destination IP Address :	192.168.100.0
Destination Net Mask :	255.255.255.0
Gateway IP Address :	192.168.168.254

Add Cancel

Advanced Configuration

zmáčkněte tlačítko **Add**.

Přidaný zápis se ukáže v **Static Routing Table**.

Destination	Network Mask	Gateway
192.168.100.0	255.255.255.0	192.168.168.254

NAT (PODPOROVÁN JEN MODY WIRELESS ROUTING CLIENT A GATEWAY)

Základním účelem NATu je sdílet jednotlivou veřejnou IP adresu v případě, že je několik počítačů v soukromé síti. To je umožněno použitím odlišných TCP portů k identifikaci žádostí přicházejících z různých počítačů. NAT je standardně aktivován.

Díky NATu nebudou počítače v soukromém LANu za access pointem přímo dostupné z internetu. Nicméně použitím virtuálních serverů vás nechá hostit internetové servery za NATem cestou zasílání IP/Portů stejně jako hostováním demilitarizační zóny.

Pokud se chcete dozvědět více o NATu a doplňkových technologiích, prosíme obraťte se na NAT Technology Primer na instalačním CD.

Learn more from our [NAT Technology Primer](#)

Krok 1:

V **CONFIGURATION** příkazovém menu klikněte na **NAT**. NAT je standardně aktivován. K odpojení klikněte na **Disable**.



Krok 2:

Klikněte na tlačítko **Apply**, aby bylo nastavení účinné.

Advanced Configuration



Důležité:

NAT odpojte jen v nezbytném případě. Odpojení NATu zamezí také efektivnímu sdílení širokopásmového internetu.

PRO KONFIGURACI VIRTUÁLNÍCH SERVERŮ ZALOŽENÝCH NA HOSTOVÁNÍ V DEMILITARIZAČNÍ ZÓNĚ (DMZ)

Díky absolvování primárních technologií NATu na instalačním CD můžete nyní dobře porozumět tomu, jak DMZ učiní, aby byl počítač v síti, ve které je aktivován NAT, přímo dostupný z internetu.

Pokud je NAT aktivován, jde internetový dotaz klienta v rámci soukromé sítě nejdříve k access pointu, který žádost přijme, access point sleduje, který klient užívá které číslo portu. Protože odpověď z internetu jde také jako první k access pointu, ví access point (díky číslu portu v balíčku odpovědi) kterému klientovi odpověď odeslat. Pokud access point číslo portu nepozná, odpověď vyřadí.

Pokud používáte DMZ na počítači, jakákoliv odpověď nerozeznaná access pointem bude odeslána do počítače s aktivovaným DMZ.



Krok 1:

V **CONFIGURATION** příkazovém menu klikněte na možnost **NAT**. Téměř na konci stránky naleznete možnost **Advanced NAT Options**.

Krok 2:

Klikněte na tlačítko **DMZ**, aby se konfiguroval virtuální server založený na De-Militarized Zone.

Krok 3:

Na stránce **NAT DMZ IP Address** musíte definovat **Private IP Address** (Soukromou IP adresu) hostitele DMZ. V tomto příkladě jsme

Advanced Configuration

zaklínovali privátní IP adresu pro počítač, který jsme chtěli umístit do DMZ : 192.168.168.55

(Zadejte **0.0.0.0** jako **Private IP Address** a DMZ bude deaktivováno).

Nezapomeňte kliknout na tlačítko **Apply**.



NAT DMZ IP Address

Private IP Address : 192.168.168.55

Apply Back

NOTE



POZNÁMKA

1. Pokud aktivujete DMZ, doporučuje se pro hostitele DMZ konfiguraci statické IP adresy. Jinak se může adresa vymezená DHCP změnit a DMZ nebude fungovat správně.
2. DMZ umožňuje hostitele vystavit VŠECHNY své části na internetu. Hostitel DMZ je tak citlivý na zákeřné útoky z internetu.

Advanced Configuration

PRO KONFIGURACI VIRTUÁLNÍCH SERVERŮ ZALOŽENÝCH NA ODESÍLÁNÍ PORTU

Virtuální server založený na odesílání portu je realizován, aby odesílal žádosti z internetu, které přicházejí na rozhraní WAN access pointu, založeném na jejich TCP portech, aby specifikoval počítač v soukromé síti. Pokud vás zajímají další informace týkající se této funkce, prosíme nahlédněte do instalačního CD na NAT Technology Primer.



Krok 1:

V **CONFIGURATION** příkazovém menu klikněte na možnost **NAT**. Téměř na konci stránky naleznete možnost **Advanced NAT Options**.

Krok 2:

Klikněte na tlačítko **DMZ**, aby se konfiguroval virtuální server založený na odesílání portu.

Krok 3:

Na stránce **Port Forward Entries** zmáčkněte tlačítko **Add**.



Advanced Configuration

Add Port Forward Entry

Known Server

Server Type :

Private IP Address :

Custom Server

Server Type :

Protocol :

Public Port :

From :

To :

Private IP Address :

Private Port From :

Krok 4:

Na následující obrazovce **Add Port Forward Entry** můžete nastavit virtuální server jako typ **Known Server (známý server)** tím, že ho vyberete z vyrolovaného menu, NEBO můžete definovat **Custom Server (uživatelský server)**.

Pro vysvětlení detailů prosíme nahlédněte do NAT Technology Primer na instalačním CD.

Learn more from our [NAT Technology Primer](#)

Známý server

Typ serveru : Vyberte z vyrolovaného seznamu všech známých typů serveru: (HTTP, FTP, POP3 nebo Netmeeting).

Soukromá IP adresa : Specifikujte LAN IP adresu vašeho PC serveru v rámci soukromé sítě.

Uživatelský server

Typ serveru : Definujte název pro typ serveru, který chcete konfigurovat.

Protokol : Vyberte z vyrolovaného seznamu typ protokolu buď **TCP** nebo **UDP**.

Veřejný port : Vyberte jestli chcete definovat jednotlivý port nebo řadu veřejných portů.

Z : Počáteční veřejné číslo

Do : Konečné veřejné číslo portu. Pokud je typ veřejného čísla portu jednoduchý, bude toto políčko ignorováno.

Soukromá IP adresa : Specifikujte IP adresu vašeho počítačového serveru v soukromé síti.

Soukromý port z : Počáteční soukromé číslo portu. Konečné soukromé číslo portu bude automaticky vykalkulováno podle rozsahu veřejného portu.

Advanced Configuration

Například pokud chcete na vašem počítači nastavit server webu s IP adresou 192.168.168.55, zvolte HTTP jako **Server Type** a zadejte **192.168.168.55** jako **Private IP Address (soukromá IP adresa)**. Klikněte na tlačítko **Add**. Zápis se zobrazí jak je to ukázáno na obrázku vpravo.

Server Type	Protocol	Public Port	Private IP	Private Port
HTTP	TCP	80	192.168.168.55	80

Add Back

PRO KONFIGURACI VIRTUÁLNÍCH SERVERŮ ZALOŽENÝCH NA ODESÍLÁNÍ IP

Pokud jste si u svého ISP předplatili více než jednu IP adresu, můžete definovat Virtuální servery založené na odesílání IP, pro které jsou všechny internetové požadavky, bez ohledu na porty, odesílány do vymezených počítačů v soukromé síti. Pokud požadujete více informací o této funkci, nahlédněte do NAT Technology Primer na instalačním CD. Následují kroky jak to nastavit:

Advanced NAT Options

DMZ Port Forwarding IP Forwarding

Krok 1:

Z **CONFIGURATION** příkazového menu klikněte na možnost **NAT**. Téměř na konci stránky najdete **Advanced NAT Options**.

Krok 2:

Klikněte na tlačítko **IP Forwarding**, čímž se konfigurují Virtuální servery založené na odesílání IP.

Krok 3:

Na další obrazovce **Add IP Forward Entry** musíte specifikovat **Private IP Address (soukromou IP adresu)** a **Public IP Address (veřejnou IP adresu)**. V tomto příkladě jsme chtěli, aby byly všechny požadavky na 213.18.213.101 poslány na počítač s **Private IP**

Add IP Forward Entry

Private IP Address : 192.168.168.55

Public IP Address : 213.18.213.101

Add Cancel

Advanced Configuration

Address (soukromou IP adresou)

192.168.168.55.

Krok 4:

Pro pokračování klikněte na tlačítko

Add.

IP Forward Entries

Private IP	Public IP
192.168.168.55	213.18.213.101

Krok 5:

Stránka **IP Forward Entries** zobrazí vaše dodatky.



POUNÁMKA

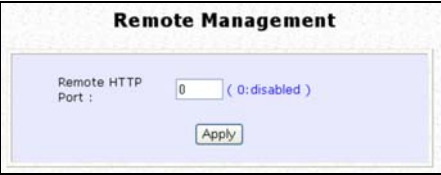
U kroku 3 se ujistěte, že jste si předplatil veřejnou IP adresu, ze které hodláte.

VZDÁLENÝ MANAGEMENT (PODPOROVANÝ JEN MODY WIRELESS ROUTING CLIENT A GATEWAY)

Pokročilejší správce sítě potěší, že vzdálený management je podporován na access pointu. Pokud si tuto vlastnost aktivujete, bude vám umožněno získat přístup na webové konfigurační stránky access pointu odkudkoliv z internetu a zvládat svou domácí a kancelářskou síť na dálku.

PRO NASTAVENÍ VZDÁLENÉHO MANAGEMENTU

Pro nastavení vzdáleného managementu pro access point jsou požadovány pouze dva kroky.



Krok 1:
Z **CONFIGURATION** příkazového menu klikněte na možnost **Remote Management** a to vás přenese na stránku zobrazenou nalevo.

Krok 2:
Pro aktivaci **Vzdáleného Managementu** zadejte číslo portu, které není používáno jinými aplikacemi v síti. Doporučuje se použít jiné číslo portu než číslo 80, protože některé ISP toto číslo blokují.



POZNÁMKA

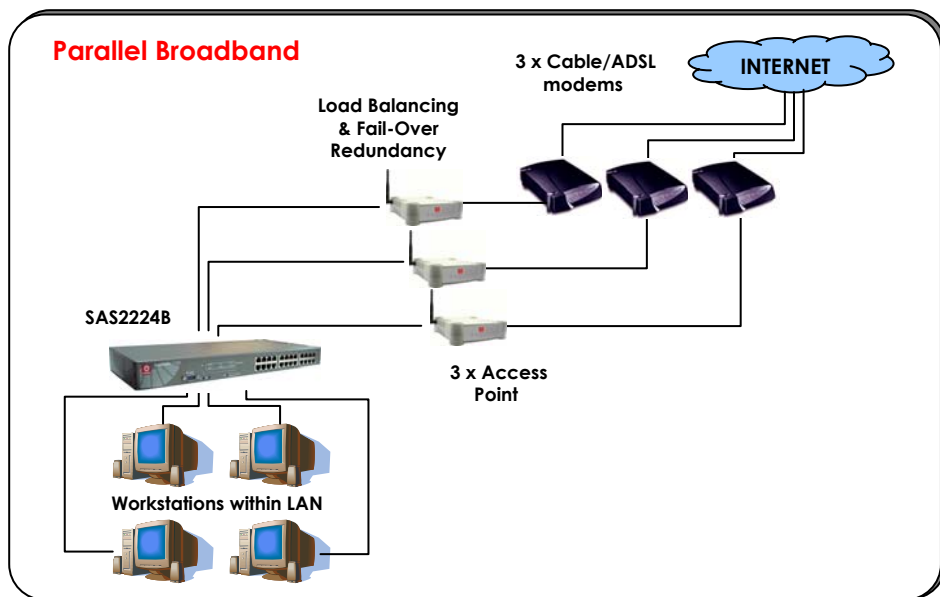
Pro předcházení neoprávněnému managementu ze vzdálených lokací nezapomeňte nahradit přednastavené heslo heslem novým.

Je také dobré toto heslo čas od času měnit, což slouží k ochraně před zákeřnými útočníky.

PARALELNÍ PŘIPOJENÍ (PODPOROVANÉ JEN V MODEM GATEWAY)

Access point je vybaven exkluzivní technologií parallel broadband, aby poskytl možnost maximálního využití připojení k internetu díky technologiím Load Balancing a Fail-Over Redundancy.

Instalováním několika jednotek access pointu kaskádově a s použitím technologie parallel broadband je možné využít všech připojení k internetu tím, že jsou data posílána po všech linkách najednou v závislosti na rychlosti linek! Pokud některá z připojovacích linek selže, použije kaskádově sestavený access point zbývající funkční širokopásmové kanály, což vám díky technologii Fail-over redundancy zajistí stabilní připojení.



Pro realizaci parallel broadband bude potřeba nainstalovat do sítě dva nebo více access pointů a každý připojit k vlastnímu internetovému připojení. Připojení může být jakéhokoliv typu (kabel nebo ADSL). Takže můžete mít jeden access point připojen ke kabelovému internetu a druhý na linku ADSL.

Advanced Configuration

Pokud se chcete dozvědět více o parallel broadband, podívejte se na www.cpx.com nebo www.complex.com.sg.

PRO AKTIVACI PARALLEL BROADBAND NA COMPEXU WP54AG

Předtím, než začnete, ujistěte se, že každý access point v síti je správně nakonfigurován na připojení k vlastnímu připojení. Potom se ujistěte buď že:

- Je každý access point v síti připojen k ethernetovému portu, jak ukazuje horní obrázek, nebo že
- Jsou access pointy navzájem spojeny WDS, nebo že
- Jsou access pointy k sobě navzájem spojeny drátem.

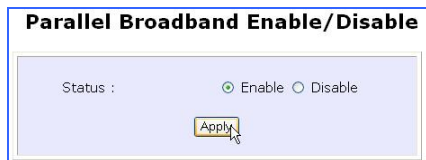
Teď jste připraveni na přístup ke konfiguraci každého access pointu a k aktivaci vlastnosti parallel broadband. Nezapomeňte navzájem spojit všechny access pointy.

Krok 1:

Z **CONFIGURATION** příkazového menu klikněte na možnost **Parallel Broadband**.

Krok 2:

Vyberte možnost **Enable** a klikněte na tlačítko **Apply**, čímž se stanou změny účinnými.



Krok 3:

Toto opakujte u každého access pointu ve vaší síti a oni spolu budou komunikovat a přiřadí každého nového uživatele k access pointu, který má nejmenší zatížení, aby měl každý access point přibližně stejný počet uživatelů.



Důležité:

Pokud máte jen jeden access point, nerealizujte vlastnost parallel broadband pro sdílení šířky pásma internetu.

OZNÁMENÍ EMAILU

Access point poskytuje tuto vlastnost kvůli oznámení emailem o změnách ve WAN IP adrese, která vám byla dříve dodána.

The screenshot shows the 'WAN PPPoE Setup' configuration page. The 'WAN Type' is set to 'PPPoE'. The 'Username' is 'guest'. The 'Password' field is empty. The 'Always-On' radio button is selected. The 'Idle Timeout' is set to 30 seconds and the 'Reconnect Time Factor' is also 30 seconds. The status is 'Connecting'. At the bottom, there are buttons for 'Apply', 'Email Notification', and 'Help'.

Krok 1:

Z **CONFIGURATION** příkazového menu klikněte na možnost **WAN PPPoE Setup** nebo **WAN PPTP Setup**, čímž se dostanete na stránku zobrazenou nalevo.

Krok 2:

Klikněte na tlačítko **Email Notification**.

The screenshot shows the 'Email Notification' configuration page. The 'Email Notification' radio buttons are set to 'Disable'. The 'Email address of Receiver' field is empty. The 'IP address of Mail Server' field is empty and has a 'Needs Authentication' checkbox. The 'User Name' and 'Password' fields are empty. The 'Email address of Sender' field is empty. The status is 'Status:'. At the bottom, there are buttons for 'Apply', 'Back', and 'Refresh'.

Krok 3:

Klikněte na tlačítko **Enable** a zaklíňte následující pole tak, jak je popsáno níže:

- **Emailová adresa příjemce:**

Toto je emailová adresa příjemce, kterému bude zpráva zaslána.

- **IP adrea emailového serveru:**

Toto je IP adresa serveru SMTP přes který bude adresa odeslána. (Doporučuje se použít server SMTP ISP).

Advanced Configuration

- **Jméno uživatele:**

Toto je jméno uživatele mailového účtu, které by mělo být zadáno, pokud je vyžadováno ověření.

- **Heslo:**

Toto je heslo uživatele mailového účtu, které by mělo být zadáno, pokud je vyžadováno ověření.

- **Emailová adresa odesílatele:**

Toto je emailová adresa odesílatele, od kterého zpráva přijde.

Krok 4:

Standardně není zaškrťovací box vedle možnosti **Needs Authentication** zaškrtnut. Tato možnost vám umožňuje specifikovat, jestli požaduje server SMTP ověření.

Krok 5:

Potom klikněte na tlačítko **Apply**.

PŘEKDLAD STATICKÉ ADRESY (PODPOROVÁNO JEN MODY WIRELESS ROUTING CLIENT A GATEWAY)

Pokud používáte v kanceláři notebook, je pravděpodobné, že ho používáte i doma, připojujete se na internet, vybíráte emaily a surfujete na webu. Protože jsou nejspíš vaše domácí a kancelářská sdílená širokopásmová síť odlišné, měli byste pokaždé při použití notebooku na jiném místě potíže s rekonfigurováním nastavení TCP/IP. Access point poskytuje vlastnost Překlad statické adresy (SAT), aby mohli uživatelé těmto problémům předejít.

Řekněme, že IP adresa vašeho notebooku je v práci 203.120.12.47 ale access point, který připojuje vaši domácí síť k internetu používá IP adresu 192.168.168.1. Aktivovali jste na vašem routeru SAT a chcete mít přístup na internet bez toho, abyste museli měnit IP adresu notebooku, protože ho budete používat další den v práci.

Protože je nastavení TCP/IP nastaveno na používání v práci, pokusí se notebook kontaktovat IP adresu vaší kancelářské brány na internetu. Když access point zjistí, že se notebook snaží zkontaktovat zařízení, které leží v jiné podsíti než je podsíť domácí sítě, informuje notebook, že bránou na internet je access point sám.

Jakmile byl jednou notebook informován, že bránou na internet je access point, bude ho kontaktovat při přístupu na internet, bez požadavku změny nastavení TCP/IP.



POZNÁMKA

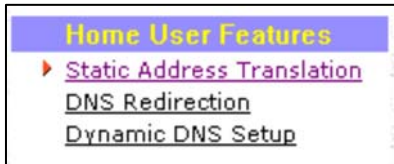
Aby SAT fungoval správně:

1. Měla by IP adresa notebooku patřit do jiné podsítě než je podsíť LAN IP adresy access pointu.
 2. <Default Gateway> v nastavení TCP/IP vašeho notebooku by nemělo zůstat prázdné.
-

Advanced Configuration

Krok 1:

Z **Home User Features** příkazového menu klikněte na možnost **Static Address Translation**.



Krok 2:

Potom zde můžete vybrat možnost **Enable (aktivovat)** nebo **Disable (deaktivovat)** překlad statické adresy, potom klikněte na tlačítko **Apply**. (SAT je standardně deaktivován)



Advanced Configuration

PŘESMĚROVÁNÍ DNS (PODPOROVÁNO JEN MODY WIRELESS ROUTING CLIENT A GATEWAY)

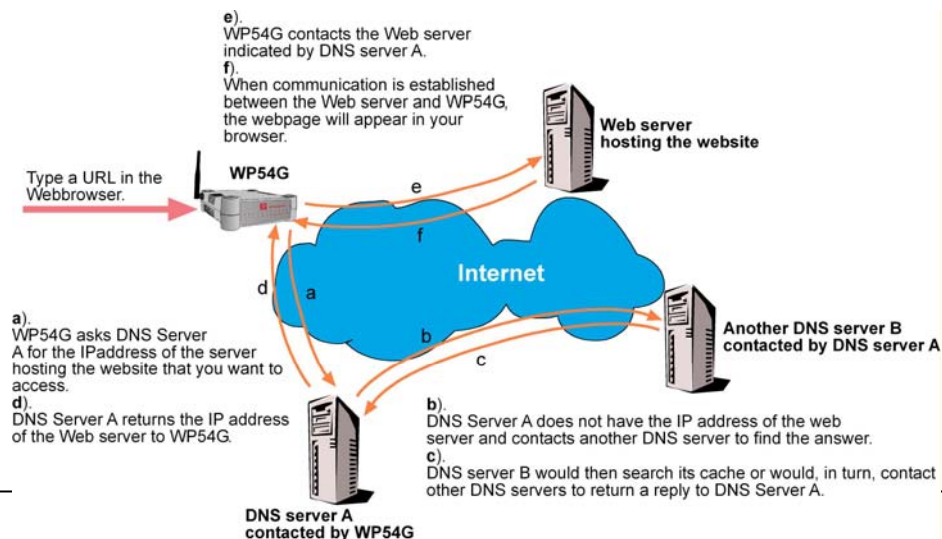
Když do vašeho internetového browseru zadáte URL, požádá browser o překlad jména na IP adresu ze serveru Domain Name System (DNS), aby byl schopný lokalizovat webový server.

Server DNS naopak vyhledá odpověď ve vlastní vyrovnávací paměti a pokud najde náležitý zápis, pošle tuto IP adresu zpět browseru. Jinak by musel kontaktovat jiné DNS servery než se daný problém vyřeší.

Pokud aktivujete vlastnost Přesměrování DNS, budou DNS požadavky LAN klientů zpracovány access pointem. Pokud jste již v LAN nastavení nepřidali specifický server DNS, který by měl být vždy používán, kontaktuje access point server DNS přiřazený pomocí ISP, aby vyřešil požadavky DNS.

Pokud je přesměrování DNS aktivováno, vyřídí server DNS access pointu ten definovaný nastavením TCP/IP LAN klientů. To access pointu umožní, aby nasměroval požadavky DNS přímo od LANu do bližšího serveru DNS, o kterém ví, čímž zlepší čas odpovědi.

Vlastnost přesměrování DNS také poskytuje správcům sítě lepší kontrolu. V případě změn v serveru DNS může označit IP adresu aktuálního serveru DNS v LAN nastavení access pointu a aktivuje přesměrování DNS, bez nutnosti rekonfigurace nastavení DNS každého klienta.





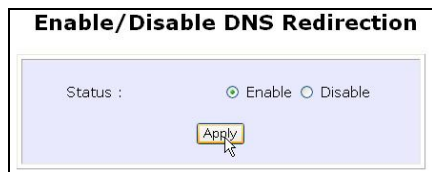
POZNÁMKA

Pro internetový přístup nenechávejte políčko serveru DNS počítačového TCP/IP majetku prázdné. Jednoduše zaklínujte jakékoukoliv legální IP adresu (např. 10.10.10.10), i když nemáte přesnou DNS IP adresu.

PRO AKTIVACI/DEAKTIVACI PŘESMĚROVÁNÍ DNS

Krok 1:

Z **Home User Features** příkazového menu klikněte na možnost **DNS Redirection**.



Krok 2:

Jednoduše vyberte **Enable**
(aktivovat) nebo **Disable**
(deaktivovat) pro **Status**
přesměrování DNS.

Krok 3:

Dokončete nastavení kliknutím na tlačítko **Apply**.

NASTAVENÍ DYNAMIC DNS

Je obtížné zapamatovat si IP adresy počítačů komunikujících na internetu. Ještě více se to zkomplikuje, když IPS mění pravidelně IP adresu, jako je to v případě, když je typem internetového připojení Dynamic IP nebo PPPoE.

Pokud na vašem počítači děláte web hosting a používáte Dynamic IP, budou muset internetoví uživatelé udržet krok se změnami IP adresy před tím, než získají přístup na váš počítač.

Pokud si u poskytovatele Dynamic Domain Name Service (DDNS), zaregistruje neměnicí název domény, např. **MyName.Domain.com**. Můžete nakonfigurovat váš access point, aby automaticky kontaktoval poskytovatele DDNS kdykoliv access point detekuje, že jeho adresa byla změněna. Potom se access point naloguje na váš účet a aktualizuje nejnovější IP adresu.

Advanced Configuration

Pokud někdo napíše do webového browseru vaší adresu: **MyName.Domain.com**, dojde tento požadavek poskytovateli DDNS, který potom přeměruje požadavek na váš počítač, bez ohledu na to, která IP adresa mu ISP přiřadil.

PRO AKTIVACI/DEAKTIVACI NASTAVENÍ DYNAMIC DNS

Krok 1:

Z **Home User Features** příkazového menu klikněte na možnost **Dynamic DNS Setup**.



Krok 2:

Vyberte **Enable (aktivovat)** nebo **Disable (deaktivovat)** Dynamic DNS a následně klikněte na tlačítko **Apply**. (Dynamic DNS je standardně deaktivován)



PRO SPRÁVOVÁNÍ SEZNAMU DYNAMIC DNS (DDNS)

Krok 1:

Z **Home User Features** příkazového menu klikněte na možnost **Dynamic DNS Setup**.

Krok 2:

Pokud jste již vytvořili seznam dříve, klikněte na tlačítko **Refresh** a tím se seznam aktivuje.



Advanced Configuration

Krok 3:

Pokud chcete na seznam přidat nový Dynamic DNS, klikněte na tlačítko Add a objeví se stránka **Choice DDNS Provider**. Jsou zde dva přednastavení poskytovatelé, které můžete použít. Níže jsou vysvětleny následující parametry:

- **Volba :**

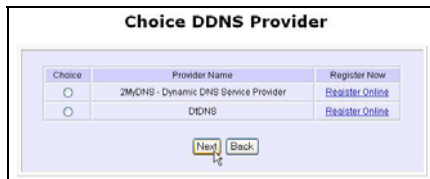
Toto vám umožní zaškrtnout kulaté zaškrťovací tlačítko vámi preferovaného poskytovatele DDNS.

- **Název poskytovatele :**

Toto je název vámi preferovaného poskytovatele DDNS.

- **Registrujte se nyní:**

Toto vám umožňuje jít na webovou stránku vámi preferovaného poskytovatele DDNS, kde si můžete zaregistrovat účet.



Pro vás existují dva předdefinovaní poskytovatelé DDNS. Nezapomeňte, že musíte být připojeni k internetu, aby jste si mohli registrovat svůj účet DDNS.

Pro výběr **2MyDNS – Poskytovatel služeb Dynamic DNS** jako poskytovatel služeb DDNS

Krok 1:

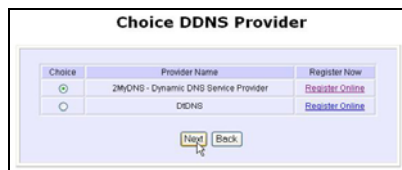
Z kolonky **Choice** v **Choice DDNS Provider** zaškrtněte kulaté zaškrťovací tlačítko vedle **2MyDNS – DNS Service Provider**. Pro pokračování potom klikněte na tlačítko **Next**.

Krok 2:

Zadejte **Domain Name (název domény)**.

Krok 3:

Zvolte **Auto Detect**, aby server



Advanced Configuration

DDNS zjistil aktuální WAN IP adresu. Zadejte **Username (uživatelské jméno)** a **Password (heslo)** vašeho DDNS účtu.

Krok 4:

(dobrovolný) Pokud aktivujete službu wildcard service, vašemu hostitelskému jménu bude povoleno několik identit.

Například pokud si zaregistrujete:

mydomain.2mydns.net,

Uživatelé hledající

www.mydomain.2mydns.net nebo

ftp.mydomain.2mydns.net mohou

stále dosáhnout vašeho hostitelského jména.

Krok 5:

(dobrovolný) V políčku Mail Exchanger zapíšete statickou WAN IP adresu mailového serveru konfigurovaného aby se staral o email pro vaši doménu. Zvolte možnost **Backup Mail Exchanger**, aby se služba aktivovala.

Krok 6:

Klikněte na tlačítko Add, tím se uloží vaše dodatky.

Krok 7:

Nová doména je přidána do tabulky se seznamem Dynamic DNS.

Dynamic DNS Add

Provider : 2MyDNS - Dynamic DNS Service Provider

Domain Name : 2mydns.net

WAN IP : 2myip.com

Username : esearchyonline.net

Password : mycoding.com

Wildcard : YES NO

Mail Exchanger : logplanet.net

Dynamic DNS List

Domain Name	Update Status
MyCoding.mxcoding.com	
esocafe.onlinepeople.net	
logplanet.net	

Add Refresh

Advanced Configuration

Krok 8:

Objeví se jako hyperlink, na který můžete kliknout, aby jste se dostali zpátky na stránku Dynamic DNS Edit (úprava). Z této stránky můžete aktualizovat jakékoliv parametry, zmazat název domény nebo vyresetovat všechny parametry, aby byly zase prázdné.

Dynamic DNS Edit

Provider : 2MyDNS - Dynamic DNS Service Provider
Domain Name : people . onlinepeople.net
WAN IP : Auto Detect
Username :
Password :
Wildcard : YES NO
Mail Exchanger :
Backup Mail Exchanger : YES NO

Advanced Configuration

Pro výběr **DtDNS jako** poskytovatel služeb DDNS

Krok 1:

Z kolonky **Choice** v tabulce **Choice DDNS Provider** zaškrtněte kulaté zaškrťovací políčko vedle možnosti **DtDNS**. Pro pokračování potom klikněte na tlačítko **Next**.

Choice	Provider Name	Register Now
<input type="radio"/>	2M/DNS - Dynamic DNS Service Provider	Register Online
<input checked="" type="radio"/>	DtDNS	Register Online

Next Back

Krok 2:

Zadejte **Domain Name (název domény)**.

Provider : DtDNS
Domain Name : .3d-game.com
WAN IP : Auto Detect
Password :

Add Reset Back

Krok 3:

Vyberte **Auto Detect**, aby server DtDNS zjistil aktuální WAN IP adresu. Zadejte **Username (uživatelské jméno)** a **Password (heslo)** svého účtu DtDNS.

Krok 4:

Potom klikněte na tlačítko **Add**.

Krok 5:

V našem příkladě, zatímco se nový název domény **cool.3d-game.com** přidává do seznamu, zobrazí se zpráva 'Waiting in queue...' (čekání ve frontě) pod kolonkou **Update Status** tabulky **Dynamic DNS List**.

Domain Name	Update Status
people.onlinepeople.net	
cool.3d-game.com	Waiting in queue...

Add Refresh

Kapitola 8: Bezpečnostní konfigurace

Tato kapitola popisuje bezpečnostní konfiguraci hlavně v modech **Wireless Routing Client** a **Gateway**.

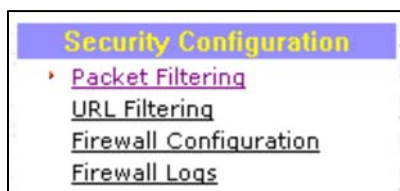
FILTRACE BALENÍ

Jako část úplného zabezpečení balení nalezeném v access pointu, může IP filtrace packetů fungovat tak, že výběrově povolí/zakáže určitým aplikacím připojení na internet.

PRO KONFIGURACI FILTRACE BALENÍ

Krok 1:

Z **Security Configuration** příkazového menu klikněte na možnost **Packet Filtering**.



Packet Filter Configuration

Packet Filter Type : Disabled

Change

Krok 2:

Nejdříve si musíte vybrat **Packet Filter Type (typ filtrace balení)** tím, že kliknete na tlačítko **Change**.

Krok 3:

Vyberte si z možností: **Disabled (deaktivovaný)**, **Sent (odeslaný)**, **Discarded (vyřazený)**, potom klikněte na tlačítko **Apply**. Standardní je možnost **Disabled**, která umožňuje, aby byly poslány všechny packety

Select Packet Filtering Type

- Disabled All IP packets will be sent
- Sent All IP packets will be sent except for those matching one or more of the rules
- Discarded All IP packets will be discarded except for those matching one or more of the rules

Apply

Security Configuration

Packet Filter Configuration

Packet Filter Type : **Sent**

Rule Name	IP Address(es)	Destination Port(s)	Day of the week	Time of the Day
<input type="button" value="Add"/>				

Krok 4:

Klikněte na tlačítko **Add** a budete moci definovat detaily vašeho **Packet Filter Rule (pravidla filtrace balení)** podle obrazovky ukýžané napravo.

4a). Zadejte **Rule Name (název pravidla)** pro toto nové pravidlo filtrace balení, např. *BlockCS*

4b). Z vyrolovaného seznamu pod kolonkou **IP Address** zvolte, jestli aplikujete pravidlo na:

- **Range (rozsah)** IP adresy
V tomto případě budete muset definovat (**From - od**) které IP adresy (**To - ke**) které IP adrese rozsah sahá.

- **Single (Určitou)** IP adresu
Zde potřebujete jen specifikovat zdrojovou IP adresu v (**From - z**) políčku.

- **Any (jakoukoliv)** IP adresu
Zde můžete nechat obě políčka (**From - z**) stejně jako (**To - k**) prázdná. Toto pravidlo bude aplikováno na všechny IP adresy.

Add a new Packet Filter rule

Rule Name :

IP Address : **Any**

From : 192.168.168.

To : 192.168.169.

Destination Port : **Any**

From :

To :

Day of the Week : **Any**

From : **Mon**

To : **Fri**

Time of the Day : **Any** (hh: 00-23, mm: 00-59)

From : (hh:mm)

To : (hh:mm)

Rule Name :

IP Address : **Range**

From : 192.168.168. 25

To : 192.168.168. 75

IP Address : **Single**

From : 192.168.168. 25

To : 192.168.168.

IP Address : **Any**

From : 192.168.168.

To : 192.168.168.

Destination Port : **Range**

From : 21

To : 81

Security Configuration

4c). Z vyrolovaného seznamu **Destination Port (cílový port)** vyberte jedno z:

- **Range (rozsah)** TCP portů
V tomto případě budete muset definovat (**From - od**) kterého portu (**To - ke**) kterému portu pravidlo sahá.

- **Single (určitou)** TCP port
Zde musíte jen specifikovat zdrojový port v políčku (**From - z**).

- **Any (jakýkoliv)** IP port
Zde můžete nechat obě políčka (**From - z**) stejně jako (**To - k**) prázdná. Pravidlo se aplikuje na všechny porty.

4d). Z vyrolovaného seznamu **Day of the Week (den v týdnu)** vyberte, jestli by se mělo pravidlo aplikovat na:

- **Range (rozsah)** dnů
Zde budete muset vybrat (**From - od**) kterého dne (**To - do kterého**) dne

- **Any (jakýkoliv)** den
V tomto případě můžete vynechat obě políčka - (**From - od**) i (**To - do**).

4e). Ve vyrolovaném seznamu **Time of the Day (čas dne)** si také můžete zvolit, aby bylo pravidlo aplikováno na:

Destination Port :	Single
From :	25
To :	

Destination Port :	Any
From :	
To :	

Day of the Week :	Range
From :	Wed
To :	Fri

Day of the Week :	Any
From :	Sun
To :	Sun

Time of the Day :	Range	(hh: 00-23, mm: 00-59)
From :	08:00	(hh:mm)
To :	21:30	(hh:mm)

Time of the Day :	Any	(hh: 00-23, mm: 00-59)
From :		(hh:mm)
To :		(hh:mm)

Security Configuration

- **Range (rozsah)** času

V tomto případě musíte čas specifikovat ve formátu **HH:MM**, kde **HH** může mít jakoukoliv hodnotu od 00 do 23 a **MM** jakoukoliv hodnotu od 00 do 59.

- **Any (jakýkoliv)** čas

Zde můžete nechat obě políčka, **(From - od)** i **(To - do)** prázdná.

Krok 1:

Klikněte na tlačítko **Apply**, čímž se nové pravidlo stane efektivní.

Tabulka **Filtering Configuration** (**filtrační konfigurace**) bude aktualizována.

Add a new Packet Filter rule

Rule Name :

IP Address :

From : To :

Destination Port :

From : To :

Day of the Week :

From : To :

Time of the Day : (hh: 00-23, mm: 00-59)

From : (hh:mm) To : (hh:mm)

Krok 2:

V tomto příkladě řekněme chceme blokovat aplikaci nazvanou CS z jakéhokoliv počítače (jakékoliv IP adresy v rámci sítě) od pondělí do pátku, od 7 do 18 hodin. Tato aplikace užívá číslo portu 27015.

Proto pravidlo nazveme BlockCS a přidáme zápisy zobrazené nalevo. Kliknutím na tlačítko **Add** se stane vaše pravidlo účinným.

Security Configuration

FILTRACE URL

Access point podporuje filtraci URL, která vám umožní jednoduše nastavit pravidla pro blokaci problematických webových stránek z vašich LAN uživatelů.

PRO KONFIGURACI FILTRACE URL

Krok 1:

Z **Security Configuration** příkazového menu klikněte na možnost **URL Filtering**.



Krok 2:

Nyní můžete definovat **URL Filter Type (typ URL filtru)** tím, že kliknete na tlačítko **Change**.

Krok 3:

Zvolte možnost **Block (blokovat)** nebo **Allow (povolit)** a potom klikněte na tlačítko **Apply**. Standardně je nastavená možnost **Disabled (deaktivován)**, což umožňuje, aby byly všechny webové stránky přístupné.

Když vás to vrátí na stránku zobrazenou nahoře, klikněte na tlačítko **Add**.



Krok 4:

Do políčku **Host Name (hostitelské jméno)** vložte adresu webové stránky, kterou chcete blokovat. Pro dokončení nastavení klikněte na tlačítko **Add**.

Security Configuration

KONFIGURACE FIREWALL

Na access pointu může být aktivován více než jen firewall "NAT" - a to možnost firewall Stateful Packet Inspection (SPI). Ten srovnává určité klíčové části packetů s databází důvěryhodných informací před tím, než jim dovolí projít. Díky tomuto SPI firewallu mohou být zmařeny útoky hackerů, jako např. IP Spoofing, Port Scanning, Ping of Death a SynFlood.

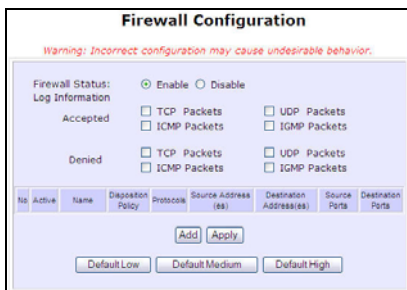
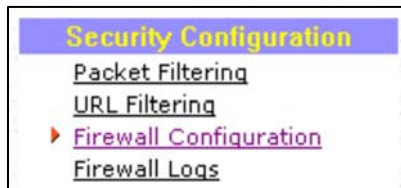
Pokud se chcete dozvědět více, podívejte se na www.cpx.com nebo www.complex.com.sg.

PRO KONFIGURACI SPI FIREWALL

Následující kroky popisují konfiguraci SPI firewall na Compexu. Je třeba, aby jste pečlivě naplánovali pravidla bezpečnosti firewall, protože nesprávná konfigurace může mít za následek nežádoucí síťové chování.

Krok 1:

Z **Security Configuration** příkazového menu klikněte na možnost **Firewall Configuration**.



Krok 2:

Nejdřív aktivujte firewall. Můžete si vybrat mezi bezpečnostními možnostmi **Default Low (standardně nízké)**, **Default Medium (standardně střední)** nebo **Default High (standardně vysoké)** pro vhodné nastavení.

Krok 3:

Potom si můžete zvolit typ informace o síťové aktivitě, který chcete

Security Configuration

nalogovat kvůli odkazům. Aktivitu dat vycházející z odlišného typu protokolu je možné zaznamenat.

Typy paketů, které jste si vybrali v sekci **Accepted** se zobrazí ve firewall logu, pokud je firewall zaznamená. Stejně je to u sekce **Denied**.

Krok 4:

Ze specifických bezpečnostních důvodů můžete přidat více pravidel pro firewall. Klikněte na kulaté zaškrťovací tlačítko **Add** na obrazovce, která je ukázána výše, následně klikněte na tlačítko **Edit** na obrazovce ukázané nalevo.

Název pravidla : Zadejte jednoznačný název k identifikaci tohoto pravidla pro firewall.

Metoda uspořádání : Tento parametr určuje, jestli by packet, který splňuje pravidla, měl být firewallem akceptován nebo zamítnut. Zvolte mezi Accept (akceptovat) nebo Deny (zamítnout).

Protokoly : Uživateli je umožněno, aby si vybrali typ datového balení z: TCP, UDP, ICMP, IGMP nebo ALL (všechny).

Pokud uživatelé vyberou ICMP nebo IGMP, musí si dále vybrat z typů ICMP respektive IGMP.

Typy ICMP : Tento IP protokol je užíván, aby ohlašoval chyby v routingu IP balení. ICMP slouží jako forma kontroly toku, ačkoli u zpráv ICMP není ani garantováno, že dojdou, ani že byly odeslány.

Security Configuration

Typ packetu ICMP	Popis
Požadavek Echa	Určuje zda je IP node (hostitel nebo router) v síti dostupný.
Echo Odpověď	Odpovídá na ICMP požadavek echa.
Cíl nedosažitelný	Informuje hostitele, že datagram nemůže být doručen.
Potlačení zdrojů	Informuje hostitele, aby kvůli přetížení snížil rychlost, ve které posílá datagramy.
Přesměrovat	Informuje hostitele o preferovaných cestách.
Čas vypršel	Ukazuje, že Time-to-Live (TTL) IP datagram vypršel.
Problém v parametru	Informuje hostitele, že v jednom z ICMP parametrů je problém.
Požadavek časové značky	Informace z datového balení ICMP.
Požadavek informací	Informace z datového balení ICMP.
Informační odpověď	Informace z datového balení ICMP

Typy IGMP

- : Tento IP protokol je používán k zavedení hostitelského členství v konkrétních skupinách na jednoduché síti. Mechanismus protokolu umožňuje hostiteli, aby informoval lokální router použitím Host Membership Reports (Zprávy o hostitelském členství).

Zpráva o hostitelském členství	Informace z datového balení IGMP.
Dotaz na hostitelské členství	Informace z datového balení IGMP.
Zanechat hostiteli zprávu	Informace z datového balení IGMP.

Zdroje IP

- : Tento parametru dovoluje specifikovat pracovní stanice tím, že vygeneruje datové balení. Uživatelé mohou buď nastavit jednoduchou IP adresu nebo řadu IP adres.

Security Configuration

Cílová IP	: Tento parametr vás nechá specifikovat nastavení pracovních stanic, které dostávají datová balení. Uživatelé mohou nastavit buď jednoduchou IP adresu nebo řadu IP adres.
Zdrojový Port	: Můžete kontrolovat požadavky pro používání specifických aplikací tím, že zde zadáte číslo portu. Uživatelé mohou nastavit buď jednoduché číslo portu nebo řadu čísel portů.
Cílový Port	: Tento parametr vymezuje aplikaci od specifikovaného cílového portu. Uživatelé mohou nastavit buď jednoduché číslo portu nebo řadu čísel portů.
Kontrola možností	: Tento parametr okazuje na možnosti v záhlaví balení. Dostupný výběr možností uvádějí zkratky: SEC – Security (bezpečnost) LSRR – Loose Source Routing (ztráta zdrojového routingu) Timestamp – Timestamp (časová značka) RR – Record Route (zaznamenat cestu) SID – Stream Identifier (identifikátor toku) SSRR – Strict Source Routing (striktní zdrojový routing) RA – Router Alert (výstraha routeru)
Kontrola TTL	: Tento parametr vás nechá zobrazit packety podle jejich hodnoty Time-To-Live (TTL). Dostupné možnosti jsou: 1. Equal (rovno) 2. Less than (méně než) 3. Greater than (více než) 4. Not equal (nerovno)

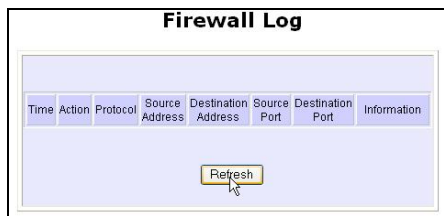
FIREWALL LOGY

Když SPI firewall access pointu operuje, hodnotné způsoby provozu v síti budou zachyceny a uchovány ve Firewall logech. Z těchto logů můžete vytáhnou detailní informace o typu datového provozu, čas, zdroj a cílovou adresu/port stejně jako akce, které SPI firewall prováděla. Můžete si vybrat, na které typy balení se nalogovat z **Konfigurace Firewall**.

PRO NÁHLED FIREWALL LOGŮ

Krok 1:

Z **SECURITY CONFIGURATION** příkazového menu klikněte na možnost **Firewall Logs**.



Krok 2:

Klikněte na tlačítko **Refresh** a uvidíte nové informace zachycené v logu.

Kapitola 9: Systemové Utility

POUŽITÍ MENU SYSTEM TOOLS

PING UTILITA

Tato vlastnost určuje, jestli může access point komunikovat (ping) s ostatními síťovými hostiteli. Tato vlastnost je dostupná jen v modech **Wireless Routing Client** a **Gateway**.

Krok 1:

Zvolte možnost **Ping Utility** z **SYSTEM TOOLS** příkazového menu.

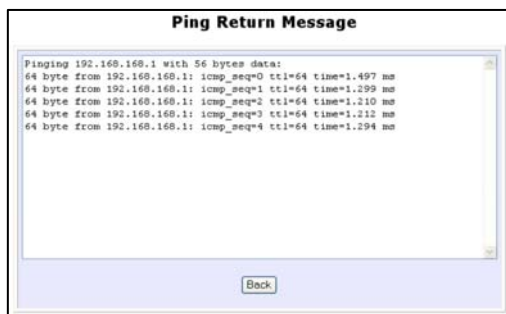


Krok 2:

Zadejte IP adresu cílového hostitele, na který chcete, aby na něj access point odesílal ping.

Krok 3:

Aby access point začal vysílat pingy, klikněte na **Start**.



Krok 4:

Zobrazí se ping zprávy.

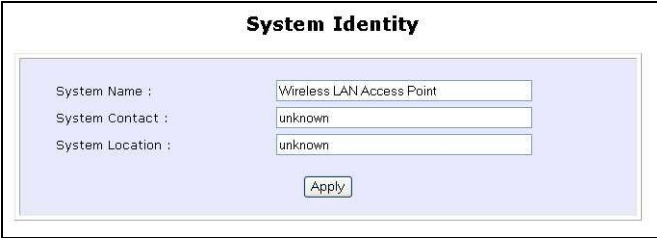
SYSTÉMOVÁ IDENTITA

Pokud paracuje vaše síť s několika access pointy, považovali byste za užitečné mít prostředek, který by každé zařízení identifikoval.

Můžete definovat Systémovou identitu vašeho access pointu, aby byl identifikovatelný podle následujících kroků:

Krok 1:

Klikněte na možnost **System Identity** z **SYSTEM TOOLS** menu.



The screenshot shows a window titled "System Identity" with a light blue background. It contains three text input fields and an "Apply" button. The first field is labeled "System Name :" and contains the text "Wireless LAN Access Point". The second field is labeled "System Contact :" and contains the text "unknown". The third field is labeled "System Location :" and contains the text "unknown".

Field Label	Value
System Name :	Wireless LAN Access Point
System Contact :	unknown
System Location :	unknown

Apply

Krok 2:

Do políčka **System Name** zapište jednoznačný název.

Krok 3:

Do políčka **System Contact** zapište jméno osoby, kterou chcete kontaktovat.

Krok 4:

Vyplňte políčko **System Location**. Pokud máte v síti nebo v budově více zařízení, pomůže tento zápis identifikovat lokaci zařízení.

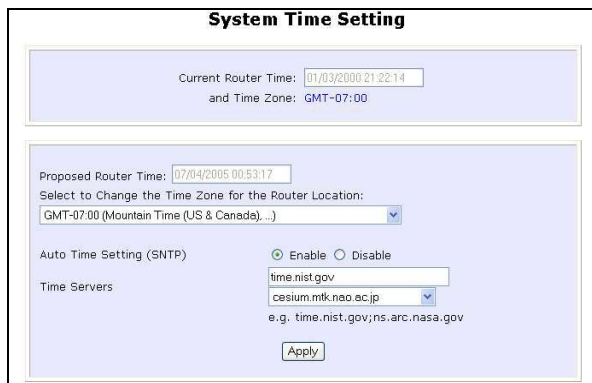
Krok 5:

Klikněte na tlačítko **Apply** a změny budou účinné.

NASTAVENÍ HODIN SYSTÉMU

Krok 1:

Klikněte na možnost **Set System's Clock** z **SYSTEM TOOLS** menu.



The screenshot shows the 'System Time Setting' configuration page. At the top, it displays the 'Current Router Time' as 01/03/2000 21:22:14 and the 'Time Zone' as GMT-07:00. Below this, the 'Proposed Router Time' is shown as 07/04/2005 00:53:17. A section titled 'Select to Change the Time Zone for the Router Location:' contains a dropdown menu currently set to 'GMT-07:00 (Mountain Time (US & Canada) ...)'. Underneath, the 'Auto Time Setting (SNTP)' section has two radio buttons: 'Enable' (which is selected) and 'Disable'. The 'Time Servers' section includes a text input field containing 'time.nist.gov' and a dropdown menu with 'cesium.mtk.nao.ac.jp' selected. A small note below the dropdown reads 'e.g. time.nist.gov;ns.arc.nasa.gov'. At the bottom of the form is an 'Apply' button.

Krok 2:

Z vyrolovaného seznamu **Select to Change the Time Zone for the Router Location** vyberte vhodné časové pásmo.

Krok 3:

Enable (aktivujte) kulaté zaškrťovací políčko Auto Time Setting (SNTP). **SNTP** znamená Simple Network Time Protocol a je používán k synchronizaci počítačových hodin.

Krok 4:

Vyplněte políčko **Time Servers (časový server)** a klikněte na tlačítko **Apply** a změny budou účinné.

UPGRADE PROGRAMOVÉHO VYBAVENÍ

Aktualizujte svůj access point tím, že si stáhnete nejnovější revizi programové ho vybavení ze stránek firmy Compex - www.compex.com.sg nebo www.cpx.com pře tím, než začnete postupovat podle následujících kroků. Můžete zkontrolovat typ a verzi vašeho programového vybavení tím, že kliknete na možnost **About System** v **HELP** menu.

Na začátku se ujistěte, že jste na svůj lokální pevný disk stáhli nejnovější programové vybavení.

Krok 1:

Klikněte na možnost **Firmware Upgrade** z **SYSTEM TOOLS** menu.



Krok 2:

Klikněte na tlačítko **Browse**, čímž lokalizujete soubor.

Krok 3:

Klikněte na tlačítko **Upgrade**.

System Utilities

Postupujte podle informací, které se vám zobrazí během aktualizacího procesu.



Krok 4:

Po aktualizaci programového vybavení musíte systém restartovat.



POZNÁMKA

Proces aktualizace programového vybavení NESMÍ být přerušen, jinak by se zařízení mohlo stát nepoužitelným.

ZÁLOHOVÁNÍ A RESETOVÁNÍ NASTAVENÍ

Můžete se vybrat buď uložit svůj aktuální profil konfigurace, nebo vytvořit v paměti pevného disku zálohu, nebo znovu zavést dřívější uložený profil nebo vyresetovat access point, aby se obnovilo standardní nastavení.

RESETOVÁNÍ VAŠEHO NASTAVENÍ

Krok 1:

Klikněte na možnost **Backup or Reset Settings** z **SYSTEM TOOLS** menu.

Krok 2:

Pro vyřazení VŠECH konfigurací, které jste vytvořili, a obnovení původního výrobního nastavení access pointu klikněte na tlačítko **Reset**.

Backup or Reset Settings

Erase the Machine's configuration, restore its factory default settings ==>

Backup the Machine's configuration ==>

Restore the Machine's configuration (path and file name)

Krok 3:

Systém vás požádá o restartování systému. Pro pokračování klikněte na tlačítko **Reboot**.

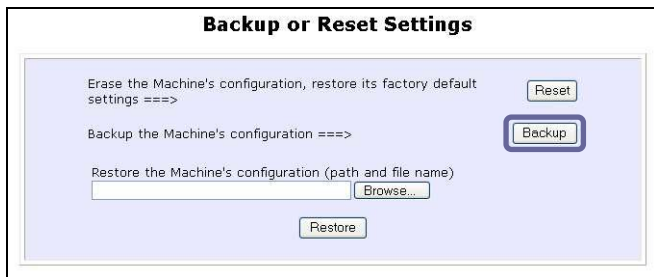
ZÁLOHOVÁNÍ VAŠEHO SETTINGS

Krok 1:

Klikněte na možnost **Backup or Reset Settings** z **SYSTEM TOOLS** menu.

Krok 2:

Pokud chcete zálohovat současné nastavení vašeho access pointu do paměti pevného disku, klikněte na tlačítko **Backup**.



Krok 3:

Na lokální disk uložte konfigurační soubor.



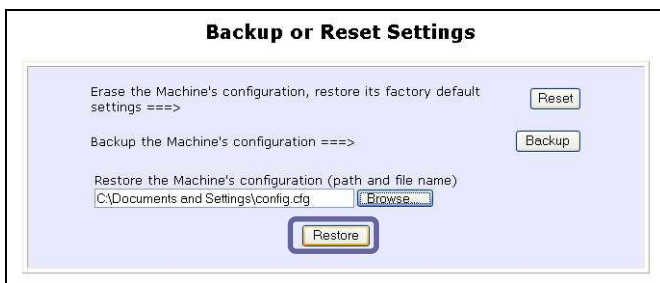
OBNOVENÍ VAŠEHO SETTINGS

Krok 1:

Klikněte na možnost **Backup or Reset Settings** z **SYSTEM TOOLS** menu.

Krok 2:

Pokud chcete obnovit nastavení, které jste si dříve uložili, klikněte na tlačítko **Browse....** Pokračujte do složky, kam jste si uložili konfigurační soubor.



Klikněte na tlačítko **Restore** a systém vyzve, abyste restartoval zařízení.

RESTART SYSTÉMU

Většina změn, které v systému uděláte, vyžadují restartování systému před tím, než se stanou nové parametry účinné.

Krok 1:

Klikněte na možnost **Reboot System** z **SYSTEM TOOLS** menu.

Krok 2:

Klikněte na tlačítko **Reboot**.



Krok 3:

Počkejte, až se systém restartuje a zobrazí se logovací stránka.



ZMĚNA HESLA

Je vhodné, abyste si změnili přednastavené heslo, které je přednastaveno na **password**.

Krok 1:

Klikněte na možnost **Change Password** z **SYSTEM TOOLS** menu.

Krok 2:

Zaklínujte **Current Password (aktuální heslo)**. Výrobní přednastavení je *password*.

Zadejte nové heslo do políčka **New Password** stejně jako do políčka **Confirm Password**.

Krok 3:

Pro aktualizaci změn klikněte na tlačítko **Apply**.



The screenshot shows a dialog box titled "Change Password". It contains three input fields for "Current Password", "New Password", and "Confirm Password", each with a masked password field (dots). Below the fields is an "Apply" button.

Change Password	
Current Password:
New Password:
Confirm Password:
<input type="button" value="Apply"/>	

ODHLÁŠENÍ

Pro opuštění webového rozhraní postupujte podle následujících kroků.

Krok 1:

Klikněte na možnost **Logout** z **SYSTEM TOOLS** menu.

Krok 2:

Pro návrat na konfigurační rozhraní access pointu klikněte na tlačítko **LOGIN!**.

Wireless LAN Access Point Management



Please enter your password:

[Forgot your password? - see the User's Guide for instructions]

POUŽITÍ HELP MENU

DOSTAŇTE TECHNICKOU PODPORU

Tato stránka představuje kontaktní informaci o centrech technické podpory Compexu na celém světě.

Krok 1:

Klikněte na možnost **Get Technical Support** z **HELP** menu.

Support Information

For technical support email to: support@compex.com.sg
For updates connect to the following Web Sites:
<http://www.cpx.com>
<http://www.compex.com.sg>

Regional Technical Support Centers

U.S.A., Canada, Latin America and South America :

Compex Inc.
840 Columbia Street, Suite B, Brea, CA92821,USA
Tel : (714) 482-0333
Fax : (714) 482-0332
800 Line: (800) 279-8891
Support email: support@cpx.com

Asia, Australia, New Zealand, Middle East and the rest of the world :

Compex Systems Pte. Ltd.
135, Joo Seng Road, #06-01,
PM Industrial Building
Singapore 368363
HotLine : (65) 6-286-1805
Fax : (65) 6-283-8337

Access point zařízení nabitě vlastnostmi. Pokud potřebujete více informací než poskytuje manuál nebo záznamový list, kontaktujte jedno z center technické podpory Compexu emailem, poštou, faxem nebo po telefonu.

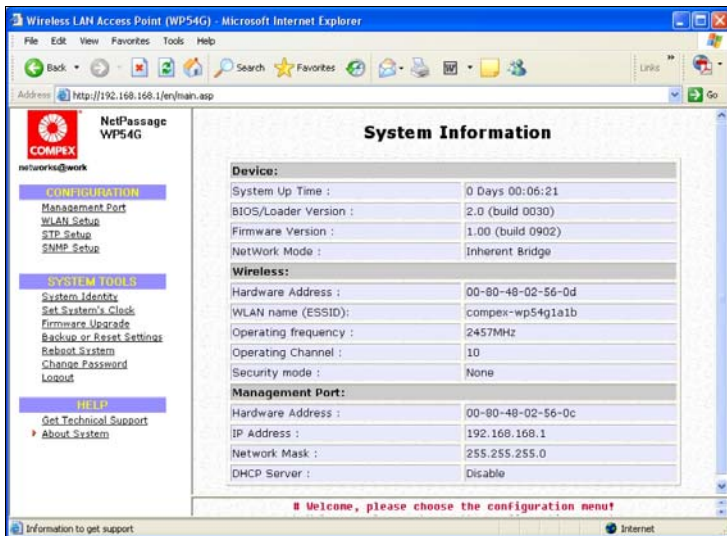
O SYSTÉMU

Stránka **About System (o systému)** zobrazuje shrnutí informací o konfiguraci systému. Podporující technici, když řeší problémy při konfiguraci, mohou vyžadovat specifické informace o datech systému. Můžete využít informace zobrazené na této stránce k tomu, abyste rychle našli data, která potřebují k vyřešení problému v systému.

Krok 1:

Klikněte na možnost **About System** z **HELP** menu.

Stránka **System Information (informace o systému)** vám poskytne informace týkající se nastavení konfigurace vašeho access pointu.



The screenshot shows a web browser window titled "Wireless LAN Access Point (WP54G) - Microsoft Internet Explorer". The address bar shows "http://192.168.168.1/evl/man.asp". The page content includes a navigation menu on the left with sections for CONFIGURATION, SYSTEM TOOLS, and HELP. The main content area is titled "System Information" and displays the following data:


Device:	
System Up Time :	0 Days 00:06:21
BIOS/Loader Version :	2.0 (build 0030)
Firmware Version :	1.00 (build 0902)
Network Mode :	Inherent Bridge
Wireless:	
Hardware Address :	00-80-48-02-56-0d
WLAN name (ESSID) :	complex-wp54g1a1b
Operating frequency :	2457MHz
Operating Channel :	10
Security mode :	None
Management Port:	
Hardware Address :	00-80-48-02-56-0c
IP Address :	192.168.168.1
Network Mask :	255.255.255.0
DHCP Server :	Disable

At the bottom of the page, there is a red message: "Welcome, please choose the configuration menu!"

Dodatek I: Obnova programového vybavení

Tato sekce ukazuje, jak přehrát programové vybavení do access pointu, pokud by se systém nespustil správně. V takovýchto případech se access point automaticky přepne do modu loader a diagnostické světélko LED se rozsvítí a zůstane svítit.

Tato tabulka ukazuje chování diagnostického LED (Y).

Stav access pointu	Stav diagnostického LED 
Porušené programové vybavení – access point se automaticky přepne do modu loader	Bliká velmi rychle
Obnova postupuje	Svídí
Úspěšný obnova	Bliká velmi pomalu

Před začátkem zkontrolujte diagnostický LED, aby jste zjistili, jestli se selhání programového vybavení neobjevilo.

Krok 1:

Vypněte access point a odpojte ho ze sítě.

Krok 2:

Pro spojení LAN portu access pointu a LAN portu vašeho počítače použijte kabel MDI.

Krok 3:

Zapněte access point a pak zapněte váš počítač. Doporučuje se nastavit IP adresu počítače na 192.168.168.100 a jeho síťovou masku na 255.255.255.0.

Krok 4:

Do CD drivu vašeho počítače vložte instalační CD Complexu WP54AG.

Krok 5:

Ve **Start** menu klikněte na možnost **Run** a napište **cmd**. Když se objeví výzvací okno, napište do něj následující příkaz:

X:\recovery\TFTP -i 192.168.168.1 PUT image_name.IMG, kde **X** odkazuje na CD drive a **image_name.IMG** na název souboru programového vybavení nalezené ve složce Recovery (obnova) na instalačním CD.

Krok 6:

Pokud jste se stáhli novější programové vybavení a uložili ho na lokální pevný disk jako: **C:\WP54G\WP54Axxx.IMG**, nahradte příkaz touto novou cestou a názvem programového vybavení. V našem příkladě:

C:\WP54AG\TFTP -i 192.168.168.1 PUT WP54Axxx.img

Nyní se odehraje proces obnovy. Můžete zkontrolovat, jestli diagnostický LED monitoruje postup v obnovovacím procesu.

Když je obnova programového vybavení dokončena, restartuje access point a ten bude nyní připravený fungovat.

Dodatek II: Konfigurace TCP/IP

Jakmile byl jednou hardware nastaven, musíte svému počítači přiřadit IP adresu, aby byl ve stejné podsíti jako access point. Standardně je IP adresa access pointu nastavena na 192.168.168.1; a jeho podsíťová maska je 255.255.255.0. Musíte konfigurovat IP adresu vašeho počítače na 192.168.168.xxx; a jeho podsíťovou masku na 255.255.255.0, kde xxx může být jakékoliv číslo od 2 do 254. Pro konfiguraci nastavení TCP/IP vašeho počítače jednoduše postupujte podle následujících kroků.

PRO WINDOWS 95/98/98SE/ME/NT

Následující informace jsou založeny na Windows 98.

Krok 1:

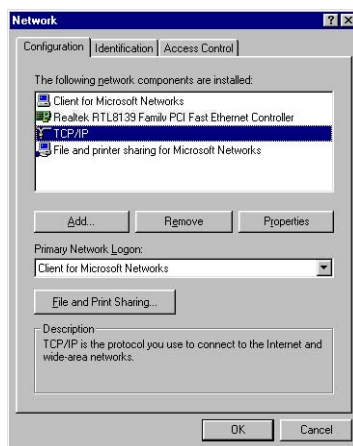
Na ploše vyberte ikonu **Network Neighborhood (Okolní počítače)** a zvolte možnost **Properties (Vlastnosti)**.

Krok 2:

Vyberte síťový adaptér, který používáte, klikněte pravým tlačítkem a vyberte možnost **Properties (Vlastnosti)**.

Krok 3:

Označte **TCP/IP** a klikněte na tlačítko **Properties (Vlastnosti)**.

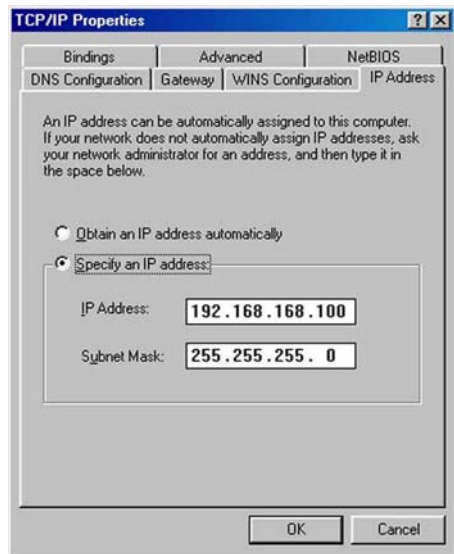


TCP/IP Configuration

Krok 4:

Vyberte kulaté zaškrtnuté tlačítko u **Specify an IP address**.

Zadejte IP adresu a podsíťovou masku jako 192.168.168.X a 255.255.255.0, kde X může být jakékoliv číslo od 2 do 254. V tomto případě používáme jako statickou IP adresu 192.168.168.160.

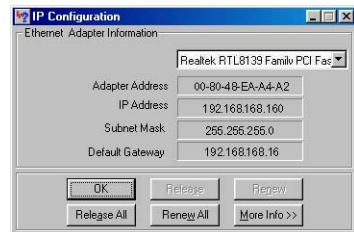


Krok 5:

Pro kontrolu, že IP adresa byla vašemu počítači přiřazena správně, jděte do **Start** menu, zvolte možnost **Run (Spustit)** a zadejte příkaz *winipcfg*.

Z vyrolovaného seznamu vyberte příslušný ethernetový adaptér a klikněte na **OK**.

Nyní je váš počítač připraven komunikovat s vaším access pointem.



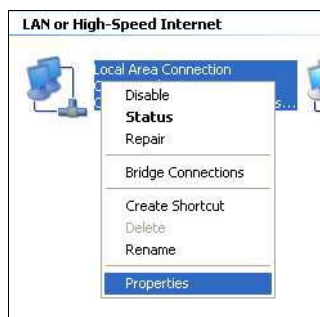
PRO WINDOWS XP/2000

Krok 1:

Na ploše klikněte pravým tlačítkem na ikonu **My Network Places (Okolní počítače)** a vyberte možnost **Properties (Vlastnosti)**.

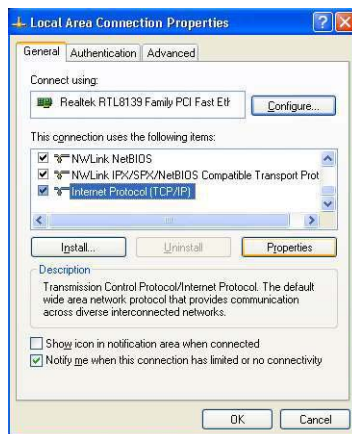
Krok 2:

Jděte na ikonu vašeho síťového adaptéru, klikněte pravým tlačítkem a vyberte možnost **Properties (Vlastnosti)**.



Krok 3:

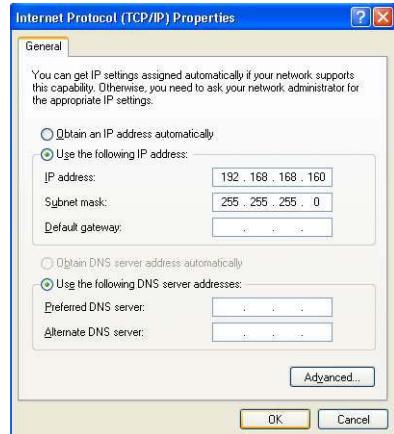
Označte **Internet Protocol (TCP/IP)** a klikněte na tlačítko **Properties (Vlastnosti)**.



TCP/IP Configuration

Krok 4:

Zvolte kulaté zaškrťovací tlačítko u **Use the following IP address**. Zadejte IP adresu a podsíťovou masku jako 192.168.168.X a 255.255.255.0, kde X může být jakékoliv číslo od 2 do 254. V tomto případě používáme statickou IP adresu 192.168.168.160.



Krok 5:

Pro zavření okna klikněte na **OK**.

Krok 6:

Pro kontrolu, že byla IP adresa vašemu počítači přiřazena správně, jděte do **Start** menu, **Accessories (Příslušenství)**, vyberte možnost **Command Prompt (Příkazový řádek)** a napište příkaz *ipconfig/all*.

```
C:\WINDOWS\system32\CMD.exe
C:\Documents and Settings\Administrator>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

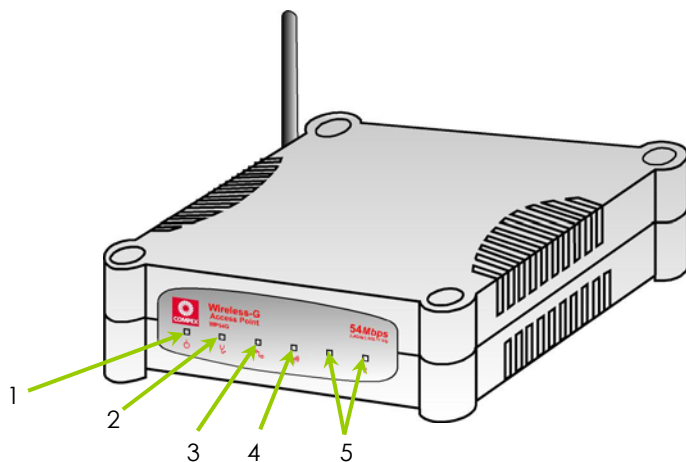
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.168.160
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

C:\Documents and Settings\Administrator>
```

Váš počítač je nyní připraven komunikovat s vaším access pointem.

Dodatek III: Vzhled panelu & popisky

Pohled na Access Point zepředu

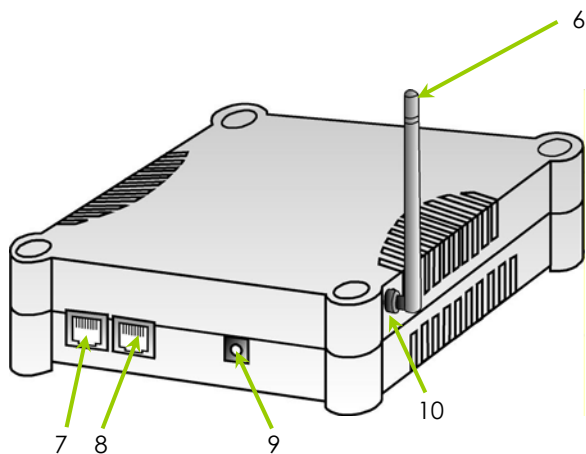


	Název	Popis	
1	LED (napájení)	Svítlící modrá	Zařízení je napájeno.
		zhasnuto	Zařízení není napájeno.
2	LED (Diagnostická)	Blikající zelená	To označuje zablesknutí během napájení. Světlo zhasne, jakmile diagnostická fáze skončí.
3	LED (WAN Link/Act)	Svítlící zelená	WAN připojení je umožněno.
		Blikající zelená	Přenos dat ve WAN připojení.
4	LED (WLAN)	Svítlící zelená	Alespoň jeden bezdrátový klient je přítomen.

Panel Views & Descriptions

	Link/Act LED)	Blikající zelená	V bezdrátové síti je zaznamenaná aktivita.
5	1 2 LED (Port 1 & 2 LEDs)	Svítilící zelená	Mezi zařízením a sítí bylo navázáno spojení.
		Blikající zelená	V síti je zaznamenaná aktivita.
		zhasnuto	Bez síťového spojení.

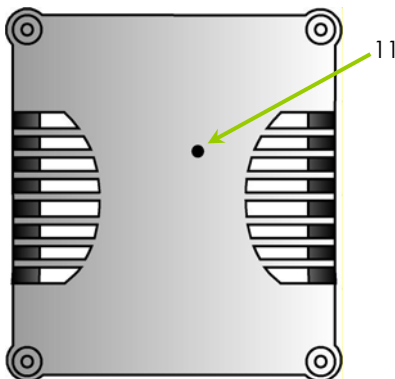
Pohled na Access Point zezadu



	Název	Popis
6	Vnější anténa	2dBi SMA anténa
7	Ethernetový Port 2	Ethernetový LAN Port (RJ45)
8	Ethernetový Port 1	Ethernetový LAN Port (RJ45)
9	DC jack	Příváděný výkon
10	Zpětný SMA konektor	Pro zapojení vnější antény

Panel Views & Descriptions

Pohled na Access Point zespodu



	Název	Popis
11	Tlačítko Reset	<p>Pro restartování stiskněte jednou.</p> <p>Pro reset hesla – zmáčkněte a držte tlačítko 5 sekund. Předtím, než pustíte tlačítko, začne světélko DIAG blikat rychlostí přibližně 5 bliknutí za sekundu.</p> <p>Pro obnovení původního nastavení z výroby, zmáčkněte a držte tlačítko po dobu delší než 10 sekund. Předtím, než pustíte tlačítko, začne světélko DIAG blikat pomaleji, přibližně 10 bliknutí za sekundu.</p>

Dodatek IV: Technické specifikace

Bezpečnostní elektromagnetická Kompatibilita	a	<ul style="list-style-type: none"> FCC část 15 odstavec B a odstavec C (pro bezdrátový modul) EN 300 328-2 EMC CE EN 301 489 (EN300 826) EN 55022 (CISPR 22)/EN 55024 Třída B EN 61000-3-2 EN61000-3-3 CE EN 60950
Normy		<ul style="list-style-type: none"> IEEE 802.11b IEEE 802.11g IEEE 802.11a
Možnosti		<ul style="list-style-type: none"> Síťová rychlost se dynamicky mění mezi 1,2, 5,5, 11, 12, 18, 24, 36, 48, 54 Mbps Uvnitř: 20 m (54 Mbps) Venku: 80 m (54 Mbps)
Frekvenční rozsah		<p>IEEE 802.11b: 2.4 ~ 2.4835 GHz</p> <p>IEEE 802.11g: 2.4 ~ 2.497 GHz</p> <p>IEEE 802.11a: 5.15 ~ 5.35 GHz (US & Canada) 5.15 ~ 5.25 GHz (Japonsko) 5.15 ~ 5.35 GHz & 5.47 ~ 5.725GHz (Evropa)</p>
Bezdrátové operační mody		<ul style="list-style-type: none"> Access Point Access Point Client Point to Point Point to Multiple Point Wireless Routing Client Gateway
Bezpečnost		<ul style="list-style-type: none"> 64 - bit / 128 - bit WEP WPA-EAP, WPA-PSK, WPA2-EAP, WPA2-PSK Pseudo Virtual LAN Indikátor VLAN IEEE 802.1x – TLS, TTLS, PEAP, EAP-SIM Filtace bezdrátové MAC adresy (v modu Access Point)
Síťové rozhraní		2 10/100 Mbps samovyjednávací ethernetové porty (RJ45)
Modulační techniky		OFDM (BPSK, QPSK, 16-QAM, 64-QAM), DSSS (BPSK, QPSK, CCK)
Hodnoty výstupu		<p>IEEE 802.11b: 20 dBm</p> <p>IEEE 802.11g: 19 dBm</p> <p>IEEE 802.11a: 17 dBm</p>
Operační kanály		<ul style="list-style-type: none"> 11 kanálů (Spojené státy a Kanada) 13 kanálů (Evropa) 14 kanálů (Japonsko)

Panel Views & Descriptions

Pokročilé vlastnosti	bezdrátové	<ul style="list-style-type: none"> • Systém bezdrátové distribuce (WDS) • Nastavení parametrů dlouhé vzdálenosti • Bezdrátový Pseudo VLAN <ul style="list-style-type: none"> - Per Node - Per Group - Indikátor VLAN • Nastavitelná kontrola síly přenosu (po 1dB)
Anténa		Oddělitelná 2dBi anténa s SMA konektorem
Management		<ul style="list-style-type: none"> • HTTP Webový Management • SNMP <ul style="list-style-type: none"> - SNMP (RFC1157) - SNMP (RFC1213)
Zabudovaný DHCP	server	ano
Rezervace DHCP		Pomocí MAC adresy
Zálohování a obnovení konfigurace		ano
Upgrade programového vybavení		ano
Požadavky na napájení Použití napájecího adaptéru: použití PoE:		výstup 9VDC (umístěn v zemi prodeje) Compex PoE Injector
Požadavky na prostředí Operační teplota: Teplota při skladování: Operační vlhkost:		0°C až 70°C -15°C až 70°C 5% až 95% RH Vlhkost (RH – Relativní vlhkost):
Fyzické rozměry		145mm x 132mm x 41mm (výška x šířka x hloubka)