ورود به دنیای میکروتیک و آماده‌سازی زیرساخت

۱ .معرفی سیستم‌عامل RouterOS و انواع لایسنس‌های آن

میکروتیک (MikroTik) یک شرکت لتونیایی است که با هدف ارائه تجهیزات شبکه‌ی قدرتمند و مقرون‌به‌صرفه وارد بازار شد. قلب تپنده‌ی تمام تجهیزات این شرکت، سیستم‌عاملی بر پایه لینوکس به نام RouterOSاست.

شما می‌توانید RouterOS را به دو شکل تهیه کنید:

۱. **RouterBOARDسخت‌افزار اختصاصی :(روترهای فیزیکی که سیستم‌عامل از پیش روی آن‌ها نصب شده است.**
۲. **نصب روی معماری x۸۶ یا ماشین مجازی :تبدیل یک کامپیوتر معمولی یا سرور مجازی به یک روتر قدرتمند.**

سطوح لایسنس (License Levels) در میکروتیک :میکروتیک برای کنترل دسترسی به قابلیت‌ها، از سیستم لایسنس‌دهی مبتنی بر "سطح" یا Level استفاده می‌کند. لایسنس‌ها مادام‌العمر هستند و روی هارد دیسک (یا فلش مموری) قفل می‌شوند.(Software ID)

- **Level ۰ (Trial):نسخه آزمایشی ۲۴ ساعته. پس از این زمان، روتر کار نخواهد کرد.**
- **Level ۱ (Free):نسخه رایگان با محدودیت‌های شدید) مثلاً فقط یک کاربر PPPoE یا.(VPN**
- **Level ۳ (CPE):مناسب برای تجهیزات سمت کلاینت در شبکه‌های وایرلس) فقط قابلیت اتصال به عنوان Station را دارد.(**
- **Level ٤ (AP):مناسب برای شبکه‌های کوچک و متوسط. قابلیت راه‌اندازی Access Point وایرلس را دارد (پشتیبانی تا ۲۰۰ کاربر همزمان در تونل‌ها).**
- **Level ٥ (ISP):مناسب برای شبکه‌های بزرگتر. پشتیبانی تا ۵۰۰ کاربر همزمان در سرویس‌هایی مثل PPPoEو.OVPN**
- **Level ٦ (Controller):لایسنس طلایی و بدون هیچ‌گونه محدودیت. مناسب برای هسته شبکه و سرویس‌دهنده‌های اینترنت.**

۲ .آموزش ۰ تا ۱۰۰ لایسنس سرور مجازی میکروتیک(CHR)

نسخه CHR (Cloud Hosted Router)یک نسخه ویژه از RouterOS است که منحصراً برای اجرا در محیط‌های مجازی) مانند VMware, KVM, Hyper-V طراحی شده است. تفاوت اصلی CHR با نسخه‌های معمولی در مدل لایسنس‌دهی آن است.

در CHR محدودیت‌ها بر اساس "تعداد کاربر" یا "ویژگی‌ها" نیست، بلکه بر اساس سرعت پورت شبکه (Bandwidth)است:

- **نسخه :Free سرعت محدود به ۱ مگابیت بر ثانیه (مناسب برای تست و یادگیری).**
- **لایسنس :P۱ سرعت محدود به ۱ گیگابیت بر ثانیه.**
- **لایسنس :P۱۰ سرعت محدود به ۱۰ گیگابیت بر ثانیه.**
- **لایسنس :P-Unlimited بدون محدودیت سرعت.**

نکته حرفه‌ای :برای دریافت لایسنس رایگان آزمایشی (Trial) به مدت ۶۰ روز با تمام امکاناتP-Unlimited ، کافی است در سایت mikrotik.comیک حساب کاربری بسازید. سپس در محیط روتر به مسیر System -> Licenseرفته و با وارد کردن نام کاربری و رمز عبور سایت، لایسنس Trial را فعال کنید.

۳ .آموزش نصب میکروتیک درVMware

برای پیاده‌سازی لابراتوارهای شبکه و توسعه سناریوهای دانشجویی، نصب میکروتیک روی VMware بهترین گزینه است.

مراحل نصب نسخه x۸۶ از طریق فایل:ISO

۱. **فایل ISO نسخه x۸۶ را از سایت میکروتیک دانلود کنید.**
۲. **در VMware یک ماشین مجازی جدید ایجاد کنید (سیستم‌عامل را روی Other Linux ٦٤-bit تنظیم کنید.(**
۳. **مقدار RAM (حتی ۲۵۶ مگابایت کافیست) و یک هارد دیسک کوچک) حداقل ۱ گیگابایت IDE یا (SATAاختصاص دهید.**
٤. **ماشین را با فایل ISO بوت کنید.**
٥. **در صفحه نصب، با فشردن کلید aتمام پکیج‌ها (Packages) را انتخاب کنید.**
٦. **با فشردن کلید iفرآیند نصب را تایید کنید.**

۷. پس از پایان نصب، کلید Enterرا بزنید تا روتر ری‌استارت شود) فراموش نکنید فایل ISO را از تنظیمات CD/ROM خارج کنید.(

مراحل راه‌اندازی نسخه) CHR روش سریع‌تر:(

۱. فایل تصویر ماشین مجازی OVA) یا (VMDK نسخه CHR را از سایت میکروتیک دانلود کنید.
۲. در VMware گزینه Openیا Importرا انتخاب کرده و فایل OVA را وارد کنید. ماشین مجازی در کمتر از ۳۰ ثانیه آماده کار است!

۴ .آموزش اتصال به روترهای میکروتیک با کابل کنسول

در سناریوهای دیتاسنتر یا زمانی که روتر به اصطلاح Brick شده و هیچ IP در دسترس نیست، کابل کنسول تنها راه نجات است. پورت کنسول معمولاً با پورت شبکه استاندارد (RJ۴۵) یا پورت سریال (RS۲۳۲) روی روترها مشخص می‌شود.

تجهیزات و نرم‌افزار مورد نیاز:

- کابل کنسول) معمولاً یک سمت RJ۴۵ و سمت دیگر USB برای اتصال به لپ‌تاپ.(
- نرم‌افزار ترمینال مانندPutty ، SecureCRTیاMobaXterm.

تنظیمات اتصال:(Serial Port Parameters)

- Baud Rate:در روتربردهای جدید ۱۱۵۲۰۰ (در مدل‌های خیلی قدیمی ممکن است ۹۶۰۰ باشد).
- Data Bits: ۸
- Parity: None
- Stop Bits: ۱
- Flow Control: None

پس از اعمال این تنظیمات در Putty و کلیک رویOpen ، با فشردن دکمه Enter در کیبورد، صفحه لاگین خط فرمان (CLI) میکروتیک ظاهر می‌شود.

۵ .اجرای وین‌باکس روی مک‌بوک(Apple Silicon M۱/M۲/M۳)

وین‌باکس (Winbox) ابزار اصلی، گرافیکی و بی‌رقیب مدیریت میکروتیک است. این نرم‌افزار به صورت Native فقط برای ویندوز توسعه داده شده است) فایل .(exe. اجرای آن روی سیستم‌عامل مک، یکی از دغدغه‌های همیشگی مهندسان شبکه است.

بهترین روش‌ها برای کاربران:macOS

۱. **استفاده از نرم‌افزار CrossOver یا :Parallels Desktop راهکارهای پولی و بسیار پایدار که ویندوز یا برنامه‌های آن را روی مک شبیه‌سازی می‌کنند.**
۲. **استفاده از Homebrew و) Wine روش پیشنهادی و رایگان برای چیپ‌های سری :(M ابتدا ترمینال مک را باز کرده و با استفاده از مدیریت پکیج brew، ابزار Wine را نصب کنید :دستور نصب brew :**
`install --cask wine-stable`سپس فایل `winbox.exe`را دانلود کرده و از طریق Wine آن را اجرا کنید.
۳. **نرم‌افزار غیررسمی :Winbox-mac پروژه‌های متن‌بازی در گیت‌هاب وجود دارند که وین‌باکس را با استفاده از کتابخانه‌های Wine در قالب یک اپلیکیشن استاندارد مک (.dmg) بسته‌بندی کرده‌اند. با جستجوی "Winbox-mac github" به راحتی قابل دانلود هستند.**

عملیات حیاتی و پیکربندی اولیه

در محیط‌های عملیاتی، مدیریت بحران و توانایی بازگرداندن روتر به چرخه کار، تفاوت بین یک تکنسین ساده و یک مهندس شبکه را مشخص می‌کند. در این بخش، عملیات‌های حیاتی روتر را بررسی می‌کنیم.

۱ .آموزش ریست کردن روتر میکروتیک (سخت‌افزاری و نرم‌افزاری)

گاهی اوقات به دلیل اشتباه در پیکربندی (مثلاً بستن پورت‌های ارتباطی خودمان) یا فراموشی رمز عبور، دسترسی به روتر قطع می‌شود. در این حالت باید روتر را به تنظیمات کارخانه برگردانیم.

الف) ریست نرم‌افزاری :(Soft Reset) زمانی که به روتر دسترسی داریم) از طریق Winbox یا (CLI اما می‌خواهیم تمام تنظیمات را پاک کنیم.

- **مسیر در وین‌باکس: System -> Reset Configuration**
- **در این پنجره با سه گزینه مهم روبرو می‌شوید:**
  - **Keep User Configuration: پسوورد‌ها و کاربران فعلی را پاک نمی‌کند.**
  - **No Default Configuration: بسیار مهم (تنظیمات پیش‌فرض کارخانه را اعمال نمی‌کند و یک روتر کاملاً خام (صفر کیلومتر) به شما می‌دهد. مهندسان حرفه‌ای همیشه این تیک را می‌زنند.**
  - **Do Not Backup: قبل از ریست، فایل بک‌آپ خودکار نمی‌سازد.**

دستور CLI برای ریست کاملاً خام: /system reset-configuration no-defaults=yes skip-backup=yes

ب) ریست سخت‌افزاری :(Hard Reset) زمانی که هیچ دسترسی به روتر نداریم. روی تمام روتربورد‌ها یک دکمه فیزیکی به نام RES وجود دارد .قانون تایمینگ دکمه ریست (بسیار مهم برای آزمون‌ها و کار عملی):

۱. **برق روتر را قطع کنید.**
۲. **دکمه RES را با یک سوزن نگه دارید و برق را وصل کنید.**
۳. **۵ ثانیه) چشمک زدن چراغ :(ACT اگر الان دکمه را رها کنید، روتر ریست می‌شود.**

٤. ۱۰ ثانیه) ثابت شدن چراغ :(ACT اگر رها کنید، روتر وارد حالت CAPsMAN(مدیریت متمرکز وایرلس) می‌شود.

٥. ۱۵ ثانیه) خاموش شدن چراغ :(ACT اگر رها کنید، روتر وارد حالت NetInstallمی‌شود (در ادامه بررسی می‌کنیم).

۲ .آموزش به‌روزرسانیRouterOS

آپدیت نگه داشتن میکروتیک برای رفع باگ‌ها و بستن حفره‌های امنیتی الزامی است. میکروتیک معماری جالبی دارد؛ شما باید دو بخش را آپدیت کنید Packages :(نرم‌افزار) و) Firmwareسخت‌افزار.(Bootloader/

میکروتیک نسخه‌های مختلفی ارائه می‌دهد:

- **:Stable / Mainنسخه پایدار و کاملاً تست شده (پیشنهاد برای محیط‌های واقعی).**
- **:Testing / Developmentدارای جدیدترین قابلیت‌ها اما باگ‌دار (فقط برای لابراتوار).**
- **:Long-termنسخه‌ای با بالاترین پایداری که فقط آپدیت‌های امنیتی می‌گیرد) مناسب برای دیتاسنتر و روترهای.(Core**

مراحل آپدیت استاندارد:

۱. **مسیر در وین‌باکس System -> Packages :روی دکمه Check for updatesکلیک کنید.**

۲. **Channelرا روی Stableقرار داده و دکمه Download & Installرا بزنید. روتر پس از دانلود ری‌استارت می‌شود.**

۳. **گام طلایی) آپدیت :(Firmware پس از بالا آمدن روتر، به مسیر RouterBOARD -> Systemبروید. اگر نسخه Upgrade Firmwareبالاتر از Current Firmwareبود، روی دکمه Upgradeکلیک کرده و روتر را یک بار دیگر ری‌استارت کنید.(System -> Reboot)**

۳ .احیای روتر با) NetInstall نجات از مرگ حتمی

اگر هنگام آپدیت برق قطع شود، یا فایل سیستم روتر آسیب ببیند، روتر دیگر بوت نمی‌شود و صدای "بیپ" معروف بالا آمدن را نمی‌دهد. در این حالت روتر نسوخته است، بلکه به ابزاری به نام NetInstallنیاز دارد Netinstall . سیستم‌عامل میکروتیک را از طریق کابل شبکه مجدداً فلش (Flash) می‌کند.

مراحل گام‌به‌گام (ترفندهای تجربی برای جلوگیری از خطا):

۱. **نرم‌افزار Netinstall و فایل سیستم‌عامل (Main Package) با فرمت npk.مطابق با معماری روتر مثلاً ARMیا (MIPSBE را از سایت میکروتیک دانلود کنید.**

۲. **ترفند فوق‌حرفه‌ای :فایروال ویندوز و آنتی‌ویروس را کاملاً خاموش کنید. تمام کارت شبکه‌های دیگر ویندوز) مثل Wi-Fi و کارت شبکه‌های (VMware را موقتاً Disable کنید تا فقط کارت شبکه متصل به روتر فعال باشد.**

۳. **روی کارت شبکه کامپیوتر خود یک IP دستی ست کنید (مثلاً .(۱۹۲.۱۶۸.۸۸.۲**

٤. **کابل شبکه را مستقیماً از کامپیوتر به پورت شماره ۱ (Ether۱) میکروتیک وصل کنید) در برخی مدل‌ها پورت دارای لیبل BOOT است.(**

٥. **برنامه Netinstall را باز کنید. روی دکمه Net bootingکلیک کرده، تیک آن را بزنید و یک IP در رنج سیستم خود (مثلاً (۱۹۲.۱۶۸.۸۸.۳به آن بدهید.**

٦. **برق روتر را بکشید، دکمه ریست را نگه دارید، برق را وصل کنید و دکمه را ۱۵ الی ۲۰ ثانیه نگه دارید تا نام روتر در لیست برنامه Netinstall ظاهر شود.**

۷. **حالا روتر را انتخاب کنید، فایل سیستم‌عامل را Browse کرده و دکمه Installرا بزنید. روتر پس از ۲ دقیقه زنده می‌شود!**

۴ .صرفاً جهت اطلاع: کانفیگ میکروتیک در چند کلیک باDefault Config

میکروتیک برای کاربران خانگی ابزاری به نام Quick Set(تنظیمات سریع) و یک تنظیمات پیش‌فرض (Default Configuration)دارد .به صورت پیش‌فرض، پورت ۱ به عنوان خروجی اینترنت (WAN) تنظیم شده و یک فایروال اولیه روی آن قرار دارد. پورت‌های ۲ تا ۵ نیز Bridge شده و نقش سوییچ شبکه داخلی (LAN) با IP آدرس ۱۹۲.۱۶۸.۸۸.۱و یک DHCP سرور را ایفا می‌کنند.

ما به عنوان مهندس شبکه هرگز از Quick Set و تنظیمات پیش‌فرض استفاده نمی‌کنیم. این تنظیمات در شبکه‌های پیچیده باعث تداخل (Loop) و مشکلات مسیریابی می‌شوند. به همین دلیل در زمان ریست کردن، همیشه تیک No Default Configurationرا می‌زنیم تا خط به خط سناریو را خودمان بنویسیم.

۵ .امن‌سازی روتر - (Hardening) مهم و ضروری

روتری که به اینترنت متصل می‌شود، روزانه هزاران بار مورد حملات Brute-force و اسکن پورت قرار می‌گیرد. پیش از اتصال به اینترنت، اجرای این ۴ گام حیاتی است:

۱. **حذف کاربر :admin ساخت یک کاربر جدید با گروه دسترسی full، انتخاب یک پسوورد پیچیده و در نهایت Disableکردن کاربر ادمینِ پیش‌فرض.**

۲. **بستن پورت‌های آسیب‌پذیر :مراجعه به IP -> Services و غیرفعال کردن .telnet, ftp, www همچنین تغییر پورت پیش‌فرض (۸۲۹۱) Winbox و.(۲۲) SSH**

۳. **محدودسازی کشف :(Discovery) مراجعه به IP -> Neighbor و محدود کردن کشف روتر فقط برای پورت‌های متصل به شبکه داخلی.(LAN)**

٤. **کنترل دسترسی لایه ۲ :مراجعه به Tools -> MAC Server و بستن دسترسی ورود با مک‌آدرس روی پورت‌های متصل به اینترنت.**

مدیریت سرویس‌های پایه شبکه

در این بخش، روتر خام خود را تبدیل به قلب تپنده‌ی شبکه داخلی می‌کنیم. ترتیب انجام این کارها در پروژه‌های واقعی بسیار مهم است و دقیقاً با همین استانداردی که در ادامه آمده انجام می‌شود.

۱ .مفهوم Bridge پل زدن اینترفیس‌ها

به صورت پیش‌فرض، هر پورت در روتر میکروتیک یک شبکه کاملاً مجزا Broadcast Domain) جداگانه (است. برای اینکه چند پورت (مثلاً پورت‌های ۲ تا ۵) دقیقاً مثل یک سوییچ سخت‌افزاری عمل کنند و همه در یک شبکه باشند، باید از قابلیت Bridge استفاده کنیم.

مراحل پیاده‌سازی:

۱. **ساخت بدنه :Bridge در وین‌باکس به منوی Bridgeبروید. در تب Bridgeروی دکمه +کلیک کرده و یک نام (مثلاً LAN-Bridge)برای آن انتخاب کنید.**

۲. **اضافه کردن پورت‌ها :حالا به تب Portsبروید. روی +کلیک کنید و پورت‌های مورد نظر (مثلاً ether۲, ether۳, و wlan۱)را یکی‌یکی انتخاب کرده و در قسمتBridge ، آن‌ها را به LAN-Bridgeمتصل کنید.**

نکته حرفه‌ای :(Hardware Offloading) در تبPorts ، تیک گزینه‌ی Hardware Offloadبه صورت پیش‌فرض روشن است. این یعنی میکروتیک ترافیک بین این پورت‌ها را به جای درگیر کردن پردازنده(CPU) ، مستقیماً به چیپستِ سوییچ (Switch Chip) می‌سپارد که باعث افزایش چشمگیر سرعت (Wire-speed) می‌شود.

دستور:CLI

Code snippet

```
/interface bridge add name=LAN-Bridge
/interface bridge port add bridge=LAN-Bridge interface=ether۲
/interface bridge port add bridge=LAN-Bridge interface=ether۳
```

۲ .اختصاص IP و آموزش راه‌اندازیDHCP Server

حالا که پورت‌های داخلی را یکی کردیم، باید به شبکه IP بدهیم تا کلاینت‌ها بتوانند با روتر صحبت کنند.

الف) تنظیم IP Address روی روتر:

۱. **به مسیر IP -> Addresses بروید. روی + کلیک کنید.**

۲. **آدرس IP روتر را همراه با Subnet Mask وارد کنید (مثلاً ۱۹۲.۱۶۸.۱۰.۱/۲۴).**

۳. **نکته طلایی: در قسمت Interface، حتماً باید LAN-Bridge را انتخاب کنید، نه پورت‌های فیزیکی!**

ب) راه‌اندازی DHCP Server توزیع خودکار (IP بهترین و کم‌خطاترین راه برای راه‌اندازی DHCP در میکروتیک، استفاده از ویزارد (Wizard) آن است.

۱. **به مسیر IP -> DHCP Server بروید و روی دکمه DHCP Setup کلیک کنید.**

۲. **DHCP Server Interface: اینترفیس LAN-Bridge را انتخاب کنید.**

۳. **DHCP Address Space: رنج شبکه شما را به صورت خودکار تشخیص می‌دهد.(۱۹۲,۱۶۸,۱۰,۰/۲٤)**

٤. **Gateway: آدرس روتر شماست.(۱۹۲,۱٦۸,۱۰,۱)**

٥. **Addresses to Give Out: بازه IP هایی که می‌خواهید به کلاینت‌ها اختصاص دهید .(Pool) می‌توانید آن را محدود کنید (مثلاً از ۱۹۲.۱۶۸.۱۰.۱۰۰ تا ۱۹۲.۱۶۸.۱۰.۲۰۰).**

٦. **DNS Servers: سرورهای نام‌دامنه (مثل ۸.۸.۸.۸).**

۷. **Lease Time: مدت زمان اجاره IP. برای شبکه‌های اداری معمولاً ۳ روز و برای مکان‌های عمومی (مثل کافه) بین ۱۰ تا ۳۰ دقیقه تنظیم می‌شود.**

نکته حرفه‌ای (Make Static): اگر می‌خواهید یک سیستم خاص (مثل پرینتر یا سرور حسابداری) همیشه یک IP ثابت بگیرد، در تب Leases روی سیستم مورد نظر کلیک راست کرده و گزینه Make Static را بزنید.

۳. آموزش مفهوم ARP و امنیت آن

پروتکل ARP (Address Resolution Protocol) وظیفه دارد آدرس IP را به آدرس فیزیکی (MAC Address) ترجمه کند. تمام دستگاه‌های متصل به روتر، در جدول IP -> ARP دیده می‌شوند.

سناریوی امنیتی قدرتمند با ARP: یکی از مشکلات رایج در شبکه‌ها، تغییر دادن IP توسط کاربران به صورت دستی (IP Spoofing) است تا محدودیت‌های سرعت یا فایروال را دور بزنند. برای جلوگیری از این کار:

۱. **در تنظیمات DHCP Server (پنجره مشخصات سرویسی که ساختید)، تیک Add ARP For Leasesرا بزنید) .این کار باعث می‌شود هر سیستمی که از روتر IP می‌گیرد، مک‌ادرس آن به صورت خودکار و معتبر در جدول ARP ثبت شود.(**

۲. **سپس به منوی Interfacesبروید، روی LAN-Bridgeدابل‌کلیک کنید و در تبGeneral ، گزینه ARPرا از حالت enabledبه reply-onlyتغییر دهید .*نتیجه: از این پس، اگر کاربری به صورت دستی IP سیستم خود را تغییر دهد، شبکه او کاملاً قطع خواهد شد، زیرا روتر فقط به دستگاه‌هایی سرویس می‌دهد که توسط DHCP تایید شده باشند!***

۴ .مقدمات Queue مدیریت پهنای باند و سرعت

برای جلوگیری از اینکه یک کاربر با دانلود سنگین، کل اینترنت شبکه را مختل کند، از Queue استفاده می‌کنیم. در میکروتیک به این کار Bandwidth Management یا Traffic Shaping می‌گویند.

۱. **به مسیر Queuesبروید و در تب Simple Queuesروی +کلیک کنید.**

۲. **Name:یک نام دلخواه (مثلاً .(۱-Limit-PC**

۳. **Target:آدرس IP کاربر مورد نظر (مثلاً ۱۹۲.۱۶۸.۱۰.۵۰یا کل رنج شبکه.(۱۹۲,۱۶۸,۱۰,۰/۲٤)**

٤. **Max Limit:در اینجا سقف سرعت آپلود (Target Upload) و دانلود (Target Download) را بر اساس بیت بر ثانیه (مثلاً ۲Mبرای ۲ مگابیت) مشخص می‌کنید .رنگ آیکون صف (Queue) وضعیت مصرف را نشان می‌دهد: سبز (آزاد)، زرد (نزدیک به سقف) و قرمز (استفاده از حداکثر ظرفیت).**

دستور:CLI

Code snippet

```
/queue simple add max-limit=۲M/۵M name=Limit-PC-۱ target=۱۹۲,۱٦۸,۱۰,۵۰
```

۵ .آموزش راه‌اندازی NTP Client و NTP Server در میکروتیک

روترها باتری داخلی (CMOS) برای نگهداری زمان ندارند. با هر بار خاموش شدن، تاریخ و ساعت آن‌ها به هم می‌ریزد. تنظیم بودن زمان روتر برای عملکرد صحیح سیستم‌های بک‌آپ‌گیری، لاگ‌ها(Logs) ، تانل‌های امنیتی (VPN/IPsec)و زمان‌بندها (Scheduler) صد در صد الزامی است.

برای همگام‌سازی زمان روتر با سرورهای جهانی:(Network Time Protocol)

۱. **NTP Client: به مسیر (System -> SNTP Client یا در نسخه‌های جدیدتر NTP Clientبروید.**

۲. **تیک Enabledرا بزنید.**

۳. **در قسمت Primary NTP Server آدرس سرورهای زمان را وارد کنید. (بهترین گزینه عمومی : pool.ntp.orgاست. روتر به صورت خودکار آن را به IP تبدیل می‌کند.(**

٤. **تنظیم منطقه زمانی :(Timezone) سپس به مسیر System -> Clockبروید و در تب Time Zone Name، کشور مورد نظر (مثلاً Asia/Tehranرا انتخاب کنید.**

تبدیل روتر به :NTP Server اگر شبکه‌ی ایزوله‌ای دارید که کلاینت‌ها (مثل دوربین‌های مداربسته) به اینترنت دسترسی ندارند، می‌توانید به مسیر System -> NTP Serverبروید، آن را Enableکنید تا خود روتر میکروتیک به عنوان مرجع زمان برای دوربین‌ها و سایر تجهیزات شبکه داخلی عمل کند.

امنیت، فایروال و سرویس‌های دسترسی(VPN)

فایروال میکروتیک بر اساس IPtablesلینوکس طراحی شده و بسیار قدرتمند است. برای درک آن، ابتدا باید مفهوم Packet Flowو Chainsرا درک کنیم.

۱ .فایروال میکروتیک(Filter Rules)

در میکروتیک، ترافیک در سه مسیر اصلی یا "Chain" قرار می‌گیرد:

- **Input:ترافیکی که مقصدش خودِ روتر است (مثلاً کسی می‌خواهد به وین‌باکس وصل شود).**
- **Output:ترافیکی که توسط خود روتر تولید شده و به بیرون می‌رود (مثلاً پینگ کردن از داخل ترمینال روتر).**
- **Forward:ترافیکی که از یک اینترفیس وارد و از اینترفیس دیگر خارج می‌شود (ترافیک کلاینت‌ها که از روتر عبور می‌کند).**

مثال عملی: بستن دسترسی یک IP خاص به اینترنت

۱. **به مسیر IP -> Firewallو تب Filter Rulesبروید.**

۲. **روی +کلیک کنید. در تبGeneral ، بخش Chainرا روی forwardقرار دهید.**

۳. **در قسمت Src. Addressآدرس IP کلاینت (مثلاً ۱۹۲.۱۶۸.۱۰.۵۰)را بنویسید.**

٤. **به تب Actionبروید و آن را روی dropقرار دهید.**

نکته طلایی (ترتیب قوانین) :فایروال قوانین را از بالا به پایین چک می‌کند. به محض اینکه ترافیک با یک قانون تطبیق (Match) پیدا کند، بقیه قوانین نادیده گرفته می‌شوند. بنابراین همیشه قوانین جزئی (Specific) را بالا و قوانین کلی (General) را پایین قرار دهید.

۲ .سرویس) NAT اشتراک‌گذاری اینترنت و انتقال پورت

بدونNAT ، کلاینت‌های شبکه داخلی که IP Private دارند، نمی‌توانند وارد دنیای اینترنت شوند.

الف) Masquerade (اینترنت‌دار کردن کلاینت‌ها:(

۱. به مسیر IP -> Firewall -> NAT بروید و روی +کلیک کنید.

۲. Chain: روی srcnat باشد.

۳. Out. Interface: اینترفیسی که اینترنت به آن وصل است (مثلاً ether۱-WAN) را انتخاب کنید.

٤. Action: روی masquerade قرار دهید.

ب) Destination NAT (انتقال پورت یا Port Forwarding): اگر بخواهید از بیرون شبکه (اینترنت) به یک سرویس در داخل شبکه (مثل دوربین یا سرور) دسترسی داشته باشید.

۱. در تب NAT ، یک قانون جدید بسازید Chain. را روی dstnat قرار دهید.

۲. Protocol: روی ۶ (tcp) باشد و Dst. Port پورت مورد نظر (مثلاً ۸۰۸۰) را بنویسید.

۳. In. Interface: همان پورت WAN اینترنت را انتخاب کنید.

٤. Action: روی dst-nat بگذارید و در فیلد To Addresses، آی‌پی داخلی سرور و در فیلد To Ports پورت واقعی آن (مثلاً ۸۰) را وارد کنید.

۳. سرویس‌های VPN (PPTP و PPPoE)

میکروتیک می‌تواند هم به عنوان کلاینت VPN عمل کند (برای دور زدن محدودیت‌ها) و هم به عنوان سرور (برای اتصال امن کارمندان از راه دور).

راه‌اندازی PPPoE Server) مدیریت اینترنت کلاینت‌ها:(

۱. به منوی PPP بروید. در تب Profiles یک پروفایل بسازید و DNS ها و محدودیت‌های سرعت را تعیین کنید.

۲. در تب Secrets نام کاربری و رمز عبور برای کلاینت تعریف کنید.

۳. در تب PPPoE Servers روی +کلیک کرده و اینترفیس LAN خود را انتخاب کنید تا سرویس روی آن فعال شود.

۴. MAC Winbox & MAC Telnet Server .

این سرویس‌ها اجازه می‌دهند بدون داشتن IP و فقط با داشتن آدرس MAC به روتر متصل شوید.

- **خطر :اگر این سرویس روی پورت WAN (اینترنت) باز باشد، یک حفره امنیتی بزرگ است.**
- **امن‌سازی :به مسیر Tools -> MAC Serverبروید. در تمام تب‌ها (MAC WinBox, MAC Telnet, MAC Ping)تنظیمات را از allبه اینترفیس لیستِ LANتغییر دهید.**

۵ .هک روتر میکروتیک و مقابله با آن(Mitigation)

بیشتر حملات به میکروتیک از طریق پورت‌های باز و سرویس‌های مدیریت نشده انجام می‌شود.

رایج‌ترین حملات:

۱. **Brute Force:تلاش مداوم برای حدس پسوورد SSH یا.Winbox**
   - ***مقابله :*تغییر پورت‌های پیش‌فرض و استفاده از قابلیت Address Listبرای مسدود کردن خودکارIP های مهاجم (با نوشتن یک اسکریپت ساده در فایروال).**
۲. **DNS Amplification:استفاده از روتر شما به عنوان واسطه برای حملات DDoS به دیگران.**
   - ***مقابله :*در مسیر IP -> DNSتیک Allow Remote Requestsرا فقط زمانی بزنید که در فایروال دسترسی به پورت ۵۳ را از سمت WAN بسته‌اید.**
۳. **Vulnerabilityدر نسخه‌های قدیمی :سوءاستفاده از باگ‌هایی مثل .Chimay-Red**
   - ***مقابله :*همیشه از آخرین نسخه Stableاستفاده کنید و پورت سرویس wwwرا غیرفعال کنید.**

مسیریابی (Routing) و ارتباط شبکه‌ها

۱ .آموزش راه‌اندازیStatic Route

مسیریابی (Routing) به زبان ساده یعنی روتر بداند بسته‌های اطلاعاتی (Packets) را از چه راهی به مقصد برساند. اگر مقصدی در شبکه‌های متصل به خود روتر (Directly Connected) نباشد، روتر بسته را دور می‌اندازد، مگر اینکه ما مسیر را به او معرفی کنیم.

مسیریابی در میکروتیک به دو دسته) Dynamicمثل OSPF و (BGP و Static(دستی) تقسیم می‌شود. برای شبکه‌های کوچک و متوسط، Static Routeبهترین انتخاب است.

مفهوم) Default Route مسیر پیش‌فرض :(مهم‌ترین مسیری که روی هر روتر نوشته می‌شود، مسیر اینترنت است. اینترنت شامل میلیاردها IP است و ما نمی‌توانیم همه را بنویسیم. بنابراین می‌گوییم: "هر مقصدی را که نمی‌شناختی، بفرست به سمت مودم/روتر بالادستی ."به این مسیر ۰.۰.۰.۰/۰می‌گویند.

سناریو عملی: اینترنت‌دار کردن روتر با Static Route فرض کنید روتر شما از طریق پورت ۱etherبه یک مودم با IP آدرس ۱۹۲.۱۶۸.۱.۱متصل است.

۱. **مسیر در وین‌باکس :به منوی IP -> Routesبروید و تب Routesرا باز کنید.**

۲. **روی دکمه +کلیک کنید.**

۳. **Dst. Address:این فیلد را روی ۰.۰.۰.۰/۰(یعنی همه مقاصد ناشناس) تنظیم کنید.**

٤. **Gateway:آدرس IP مودم بالادستی (۱۹۲,۱٦۸,۱,۱) را وارد کنید.**

٥. **روی OKکلیک کنید. اگر ارتباط فیزیکی برقرار باشد، عبارت reachableدر کنار Gateway نمایش داده می‌شود.**

ابزارهای مدیریت، مانیتورینگ و اتوماسیون

۱ .استراتژی‌های بک‌آپ‌گیری Local وCLI

داشتن نسخه پشتیبان، خط قرمز مدیریت شبکه است. میکروتیک دو روش کاملاً متفاوت برای بک‌آپ‌گیری دارد که شناخت تفاوت آن‌ها حیاتی است:

الف) روش Backup باینری :(این روش از کل روتر (شامل تنظیمات، پسوواردها، لایسنس و فایل‌ها) یک فایل رمزنگاری شده با پسوند backup.می‌سازد.

- ***کاربرد :*فقط و فقط برای بازگردانی روی همان روتر فیزیکی)یا روتری دقیقاً با همان مدل سخت‌افزاری.(**
- ***اجرا :*مراجعه به منوی Filesو کلیک روی دکمه .Backup**

ب) روش) Export متنی :(CLI / این روش تنظیمات روتر را به شکل خطوط فرمان (اسکریپت) در یک فایل با پسوند rsc.استخراج می‌کند. پسوواردها در این روش ذخیره نمی‌شوند.

- ***کاربرد :*برای انتقال تنظیمات به یک روتر جدید (Migration) یا بررسی خط به خط کانفیگ.**
- ***اجرا (در ترمینال) :***

Code snippet

/export file=Liantel-Core-Config

با این دستور، فایلی به نام Liantel-Core-Config.rscدر منوی Files ساخته می‌شود که می‌توانید آن را روی سیستم خود دانلود کنید.

۲ .آموزش) Cloud Backup بک‌آپ ابری میکروتیک(

نگهداری بک‌آپ روی خود روتر خطرناک است (اگر روتر بسوزد، فایل بک‌آپ هم از بین می‌رود). میکروتیک یک فضای ابری رایگان بر اساس شماره سریال (SN) دستگاه به شما می‌دهد.

۱. **به مسیر System -> Cloudبروید.**

۲. **تیک DDNS Enabledرا بزنید تا ارتباط روتر با سرورهای میکروتیک برقرار شود.**

۳. **سپس روی دکمه Backupکلیک کنید و در پنجره باز شده دکمه Upload Backupرا بزنید.**

٤. **در صورت خرابی روتر، کافیست با یک روتر دیگر وارد همین بخش شوید، شماره سریال دستگاه قبلی را وارد کنید و دکمه Download Backupرا بزنید!**

۳ .مانیتورینگ با ابزار جذابNetwatch

مدیر شبکه نباید منتظر بماند تا کاربران قطعی را گزارش دهند! ابزار Netwatch با ارسال پینگ (ICMP) به صورت دوره‌ای، وضعیت یک دستگاه (مثلاً سرور حسابداری یا مودم اینترنت) را چک می‌کند و در صورت قطعی یا وصلی، می‌تواند دستوری را اجرا کند.

١. **به مسیر Tools -> Netwatchبروید و روی +کلیک کنید.**

٢. **Host:آدرس IP سروری که می‌خواهید مانیتور کنید (مثلاً ۸.۸.۸.۸برای چک کردن اینترنت**

٣. **Interval:فاصله زمانی بین پینگ‌ها (مثلاً هر ۰۰:۰۱:۰۰یعنی ۱ دقیقه**

٤. **در تب Downمی‌توانید یک اسکریپت بنویسید (مثلاً فعال کردن اینترنت پشتیبان یا ارسال پیامک/ایمیل هشدار).**

٥. **در تب Upدستور بازگشت به حالت عادی را می‌نویسید.**

۴ .اتوماسیون با Scheduler مثال: قطع/وصل وای‌فای در ساعات مشخص

ابزار Scheduler برای اجرای خودکار دستورات در زمان‌های تعیین شده استفاده می‌شود .فرض کنید می‌خواهیم وای‌فای شرکت (اینترفیس wlan۱)هر روز ساعت ۸ صبح روشن و ساعت ۶ عصر خاموش شود.

١. **به مسیر System -> Schedulerبروید و روی +کلیک کنید.**

٢. **نامWiFi-ON :**

٣. **Start Time: ۰۸:۰۰:۰۰**

٤. **Interval: ۱d ۰۰:۰۰:۰۰تکرار هر ۱ روز**

٥. **On Event:دستور روشن کردن وای‌فای را بنویسید) interface wireless enable wlan۱/ *.برای نسخه ۷ و پکیج wifiwave2 دستور متفاوت است(interface wifi enable wifi1/ :***

٦. **همین مراحل را برای ساخت زمان‌بندی WiFi-OFFدر ساعت ۱۸:۰۰:۰۰با دستور disableتکرار کنید.**

۵ .راه‌اندازی فایل سرور سبک با سرویسSMB

اگر روتر شما پورت USB دارد، می‌توانید یک فلش مموری به آن وصل کرده و آن را تبدیل به یک NAS (فایل سرور) سبک برای اشتراک‌گذاری فایل‌ها در شبکه کنید.

۱. **فلش را وصل کنید و از منوی System -> Disksآن را فرمت کنید.**

۲. **به منوی IP -> SMBبروید و تیک Enabledرا بزنید.**

۳. **در تب Shares، یک پوشه اشتراکی به مسیر فلش مموری بسازید.**

٤. **در تب Users، یک نام کاربری و رمز عبور برای دسترسی به فایل‌ها تعریف کنید) *.اکنون کاربران شبکه می‌توانند با وارد کردن \\x.x.x.x۱۹۲.۱۶۸در ویندوز، به فایل‌ها دسترسی داشته باشند.(***

۶ .ترفندهای سخت‌افزاری LED :و دکمهMode

میکروتیک اجازه می‌دهد سخت‌افزار روتر را برای نیازهای خود شخصی‌سازی کنید.

- **برنامه‌ریزی LED ها :به منوی System -> LEDsبروید. می‌توانید یک چراغ روی روتر را طوری تنظیم کنید که با عبور ترافیک از یک پورت خاص، یا با روشن شدن یک تانلVPN ، چشمک بزند (یک داشبورد فیزیکی عالی برای عیب‌یابی سریع).**
- **دکمه :Mode روی برخی روترها دکمه‌ای به نام Mode وجود دارد. در مسیر System -> RouterBOARD -> Mode Buttonمی‌توانید یک اسکریپت به آن اختصاص دهید) *.کاربرد جالب: نوشتن اسکریپتی که با فشردن این دکمه، تمام LED های روتر خاموش شوند تا در شب مزاحمتی ایجاد نکنند.(Dark Mode -***

۷ .قابلیت جادویی) WoL روشن کردن کامپیوتر از طریق شبکه(

تکنولوژی Wake on LAN به شما اجازه می‌دهد کامپیوترهای خاموشِ داخل شبکه را از راه دور روشن کنید) به شرطی که مادربورد کلاینت از این قابلیت پشتیبانی کند و در BIOS فعال شده باشد.(

این کار با ارسال یک "بسته جادویی (Magic Packet) "حاوی مک‌آدرس کامپیوترِ خاموش انجام می‌شود .اجرا از طریق CLI میکروتیک:

Code snippet

/tool wol mac=AA:BB:CC:DD:EE:FF interface=LAN-Bridge

به جای مقادیر بالا، مک‌آدرس سیستم هدف و نام اینترفیس بریج شبکه را وارد می‌کنید

هر شبکه‌ای، فارغ از اینکه چقدر سیستم‌عامل‌ها و پروتکل‌های پیچیده‌ای روی آن در حال اجرا باشد، در نهایت به کابل‌ها، سوکت‌ها، سوییچ‌ها و روترها متصل است. در دنیای شبکه، تجهیزات به دو دسته اصلی تقسیم می‌شوند : تجهیزات فعال (Active) و تجهیزات غیرفعال.(Passive)

بخش اول: تجهیزات غیرفعال(Passive Network Equipment)

تجهیزات پسیو به دستگاه‌ها و قطعاتی گفته می‌شود که به جریان برق متصل نمی‌شوند، هیچ‌گونه پردازشی روی اطلاعات انجام نمی‌دهند و صرفاً وظیفه انتقال سیگنال، سازمان‌دهی و محافظت از زیرساخت را بر عهده دارند.

۱ .کابل‌های شبکه و پچ‌کورد(Patch Cord)

رگ‌های حیاتی شبکه شما هستند. در شبکه‌های محلی (LAN) معمولاً از کابل‌های مسی زوج‌به‌هم‌تابیده (Twisted Pair)استفاده می‌شود.

- **دسته‌بندی :(Category) امروزه در پروژه‌ها حداقل از کابل‌های Cat٦ (با سرعت ۱ گیگابیت) یا Cat٦a (با سرعت ۱۰ گیگابیت) استفاده می‌شود.**
- **پچ‌کورد :(Patch Cord) به کابل‌های کوتاه (معمولاً از ۳۰ سانتی‌متر تا ۵ متر) که دو سر آن‌ها از کارخانه سوکت‌زده شده است، پچ‌کورد می‌گویند. از این کابل‌ها برای اتصال کامپیوتر به پریز شبکه یا اتصال سوییچ به پچ‌پنل استفاده می‌شود.**

۲ .کیستون (Keystone) و فیس‌پلیت(Faceplate)

- **کیستون :همان پریز شبکه است که در داخل دیوار یا ترانک (داکت‌های پهن) قرار می‌گیرد. کابل اصلی شبکه که از رک کشیده شده، در پشت کیستون پانچ می‌شود.**

- **فیس‌پلیت :قاب پلاستیکی روی دیوار است که کیستون داخل آن قرار می‌گیرد تا ظاهر تمیز و استانداردی داشته باشد.**

۳ .پچ پنل(Patch Panel)

یکی از مهم‌ترین قطعات برای نظم‌دهی در اتاق سرور است. پچ‌پنل یک قطعه مستطیلی با تعداد مشخصی پورت (مثلاً ۲۴ یا ۴۸ پورت) است.

- **دیدگاه مهندسی :ما هرگز کابل‌های بلندی که از اتاق‌ها آمده‌اند را مستقیماً به سوییچ وصل نمی‌کنیم! ابتدا تمام کابل‌ها را در پشت پچ‌پنل پانچ می‌کنیم و سپس با استفاده از پچ‌کوردهای کوتاه، پورت‌های روی پچ‌پنل را به سوییچ متصل می‌کنیم. این کار باعث می‌شود اگر کابلی کشیده شد، سوییچ گران‌قیمت ما آسیب نبیند و عیب‌یابی بسیار آسان شود.**

۴ .رک(Rack)

محفظه‌ای فلزی است که برای نگهداری، محافظت و تهویه تجهیزات شبکه (سوییچ، سرور، روتر) استفاده می‌شود.

- **واحد اندازه‌گیری :(Unit) ارتفاع رک‌ها و تجهیزات داخل آن‌ها با واحدی به نام "یونیت (U) "سنجیده می‌شود. هر یونیت معادل ۴.۴۴ سانتی‌متر است. (مثلاً یک سوییچ استاندارد ۱ یونیت و یک سرور ممکن است ۲ یا ۴ یونیت فضا اشغال کند).**
- **انواع رک:**
  - **رک دیواری :(Wall-mount) معمولاً ۴ تا ۱۲ یونیت هستند و برای شبکه‌های کوچک یا طبقات ادارات استفاده می‌شوند.**
  - **رک ایستاده :(Standing) از ۲۲ تا ۴۷ یونیت ارتفاع دارند و در دیتاسنترها و اتاق سرورهای مرکزی قرار می‌گیرند. عمق این رک‌ها (۶۰، ۸۰ یا ۱۰۰ سانتی‌متر) بسیار مهم است؛ مثلاً یک سرور HP درون رک با عمق ۶۰ جا نمی‌شود**

بخش دوم: تجهیزات فعال(Active Network Equipment)

تجهیزات اکتیو دستگاه‌هایی هستند که به برق متصل می‌شوند، دارای پردازنده (CPU) و حافظه هستند، بسته‌های اطلاعاتی (Packets) را می‌خوانند، مسیریابی می‌کنند و ساختار منطقی شبکه را می‌سازند.

۱ .کارت شبکه(NIC - Network Interface Card)

پل ارتباطی بین کامپیوتر و شبکه فیزیکی است. هر دستگاهی که به شبکه وصل می‌شود (موبایل، لپ‌تاپ، پرینتر) یک کارت شبکه دارد.

- **آدرس فیزیکی :(MAC Address) هر کارت شبکه دارای یک آدرس فیزیکی و یکتای ۴۸ بیتی است که در کارخانه روی چیپ آن حک می‌شود.**
- **انواع :کارت‌های شبکه می‌توانند سیمی(Ethernet) ، بی‌سیم (Wi-Fi) یا فیبر نوری) با استفاده از ماژول‌های (SFP باشند.**

۲ .سوییچ شبکه(Switch)

سوییچ قلب تپنده شبکه داخلی (LAN) است. وظیفه آن اتصال چندین دستگاه به یکدیگر در یک شبکه محلی است. سوییچ‌ها هوشمند هستند؛ آن‌ها آدرس MAC گیرنده را می‌خوانند و اطلاعات را فقط به همان پورتِ مقصد ارسال می‌کنند.

- **سوییچ‌های غیرمدیریتی :(Unmanaged) هیچ نیازی به تنظیمات ندارند .(Plug and Play) کابل را وصل می‌کنید و کار می‌کنند. مناسب برای شبکه‌های کوچک.**
- **سوییچ‌های مدیریتی :(Managed) دارای سیستم‌عامل هستند و قابلیت‌های پیشرفته‌ای مثل VLAN بندی، مدیریت پهنای باند و امنیت پورت (Port Security) را به ادمین می‌دهند) مانند سوییچ‌های.(Cisco**
- **قابلیت :PoE (Power over Ethernet) سوییچ‌های PoE می‌توانند علاوه بر دیتا، برق را نیز از طریق همان کابل شبکه تامین کنند. این قابلیت برای روشن کردن دوربین‌های مداربسته، تلفن‌های تحت شبکه (VoIP)و اکسس‌پوینت‌ها بدون نیاز به آداپتور جداگانه، فوق‌العاده کاربردی است.**

۳ .روتر(Router)

اگر سوییچ دستگاه‌ها را در داخل یک شبکه به هم وصل می‌کند، روتر شبکه‌های مختلف را به یکدیگر متصل می‌کند . روتر دروازه خروج از شبکه محلی (Gateway) است.

- **عملکرد :روتر در لایه ۳ مدل OSI کار می‌کند و بر اساس IP Address تصمیم‌گیری می‌کند. وقتی دانشجو مرورگر را باز می‌کند و درخواستی می‌فرستد، این روتر است که کوتاه‌ترین و بهترین مسیر را در شبکه جهانی اینترنت برای رسیدن به سرور مقصد پیدا می‌کند.(Routing)**
- **همانطور که در مباحث قبلی دیدیم، تجهیزاتی مثل روتربوردهای میکروتیک دقیقاً همین نقش را با سیستم‌عامل RouterOS ایفا می‌کنند و ترافیک را بین LAN خصوصی شرکت و WAN (اینترنت) هدایت می‌کنند.**

۴ .اکسس پوینت(Access Point / AP)

دستگاهی است که زیرساخت سیمی شبکه را به یک شبکه بی‌سیم (Wi-Fi) تبدیل می‌کند. در واقع اکسس‌پوینت مانند یک سوییچ بی‌سیم عمل می‌کند تا لپ‌تاپ‌ها و موبایل‌ها بتوانند به شبکه متصل شوند.

۵ .فایروال سخت‌افزاری(Hardware Firewall)

دستگاهی اختصاصی است که در لبه شبکه (معمولاً بین اینترنت و روتر/سوییچ مرکزی) قرار می‌گیرد و ترافیک ورودی و خروجی را بر اساس قوانین امنیتی به شدت پردازش و فیلتر می‌کند تا جلوی حملات، بدافزارها و دسترسی‌های غیرمجاز را بگیرد (مانند تجهیزات Fortinet یا.(Sophos