



Codul proiectului: EC/101083410– WeH/ și POCIDIF/1147/2/1/161799

Titlul proiectului: Wallachia eHUB (WEH)

WP 3. Servicii de dezvoltare a competențelor și de formare profesională (Skills Development and Training Services)

Material de curs pentru sesiune de instruire pentru administrarea
rețelelor de calculatoare (Wired, WiFi)

Întocmit,

Manea Mihai-Laurențiu

USH_Trainer de coordonare a transformării digitale

Februarie 2025



Scurt istoric

Până la începutul anilor '80 din secolul trecut sistemele de calcul erau organizate în jurul unui calculator central capabil să rezolve problemele transmise de numeroși utilizatori. Datorită tendinței de trecere de la acest sistem centralizat, la soluția instalării de calculatoare la fiecare utilizator și asigurarea unor legături de comunicație eficientă între ele, a contribuit la dezvoltarea rețelor de calculatoare, ca o parte integrantă a societății moderne. O rețea de calculatoare (computer network) reprezintă un sistem de calcul complex, format din mai multe echipamente interconectate prin intermediul unui canal de comunicație (cablu coaxial, fibră optică, linie telefonică, ghid de unde) în scopul utilizării în comun de către mai mulți utilizatori a tuturor resurselor fizice, logice și informaționale, asociate calculatoarelor din rețea. Calculatoarele conectate la rețea sunt denumite noduri.

Administrarea rețelei constă în planificarea, configurarea și gestionarea tuturor elementelor rețelei: resurse locale și aflate la distanță, conturi de utilizator, dispozitive pentru conectivitate. Scopul administrării rețelei este de a crește productivitatea prin asigurarea accesului la resursele necesare.

Echipamentele rețelor de calculatoare nu sunt neapărat numai calculatoarele, ci și orice alt dispozitiv capabil să prelucreze date. Calculatoarele din rețele pot fi de tipuri diferite, atât ca hard cât și ca soft. De exemplu, folosirea telefoniei mobile poate servi drept o rețea de date; televiziunea digitală de asemenea reprezintă avantajele tehnologiilor din rețelele de calculatoare; jocurile de calculator au schimbat modul de folosire a timpului liber.

Administrarea rețelei constă în planificarea, configurarea și gestionarea tuturor elementelor rețelei: resurse locale și aflate la distanță, conturi de utilizator, dispozitive



pentru conectivitate. Scopul administrării rețelei este de a crește productivitatea prin asigurarea accesului la resursele necesare.

Înainte de a avea o rețea funcțională, administratorul de rețea trebuie să decidă cum gestionează accesul. Accesul include nu numai conectarea la o anumită stație de lucru, ci și accesarea resurselor. Înainte de a lua această decizie, administratorul trebuie să definească metoda care va fi utilizată pentru a stabili cerințe privind numele de utilizator și parolele. Principalele două tipuri de conturi de rețea care permit gestionarea utilizatorilor rețelei sunt conturile de utilizator și conturile de grup.

În rețelele bazate pe server, accesul este acordat fiecărui utilizator printr-un cont individual. Crearea conturilor de utilizator și atributele aplicate acestor conturi sunt elementele prin care se gestionează accesul la resurse.

Conturile de utilizator și cele de grup sunt create de obicei cu ajutorul unui utilitar furnizat de sistemul de operare de rețea (de exemplu, User Manager sau User Manager for Domains în Windows NT sau Windows 2000, Syscon for NetWare pentru versiunile 3.x sau NWAdmin pentru versiunile 4.x și 5.x). Utilitarele pot fi utilizate pentru a desemna opțiuni, precum exigențele pentru parole și apartenențele la grupuri.

Majoritatea sistemelor de operare în rețea creează în timpul instalării un cont administrator și unul guest (oaspete). Administratorul trebuie să creeze apoi conturi pentru toți utilizatorii rețelei, stabilindu-le drepturile de acces și apartenențele la grupuri.

Unul dintre cele mai importante aspecte ale securității rețelei îl reprezintă parolele. Parolele lungi sporesc securitatea rețelei, fiind greu de detectat. Acest lucru este valabil mai ales când sunt combinate caractere numerice și alfabetice. Păstrarea



unui istoric al parolelor reduce accesul neautorizat la rețea. Securitatea este sporită prin solicitarea ca parolele să fie schimbate periodic.

Grupurile sunt utilizate pentru a organiza utilizatorii în mulțimi logice pe baza modului în care aceștia au nevoie de acces la resursele rețelei. Utilizatorilor li se acordă permisiunile necesare la resurse pe baza grupului din care fac parte, nu în mod individual. Fiecare utilizator care este membru al grupului are aceleași permisiuni de acces ca și grupul.

Modelul de securitate pentru o rețea de calculatoare este structurat pe mai multe niveluri:

- **Securitatea fizică** este nivelul exterior al modelului de securitate și trebuie să asigure prevenirea accesului la echipamente și date. Este comună tuturor sistemelor electronice de calcul, distribuite sau nu;
- **Niveluri logice de securitate** destinate asigurării controlului accesului la resursele și serviciile sistemului.

Din punct de vedere al accesului la resursele sistemului întâlnim următoarea structurare:

- Nivelul de acces la sistem care determină dacă și când rețeaua este accesibilă utilizatorilor. La acest nivel se realizează gestiunea accesului și se stabilesc măsuri de protecție la conectare (deconectare forțată, interzicerea lucrului în afara orelor de program, limitarea lucrului la unele stații);
- nivelul de acces la cont care se referă la identificarea utilizatorilor după numele de utilizator asociate și autentificarea lor prin parola introdusă;



- nivelul drepturilor de acces care individualizează, pe fiecare utilizator sau pe grupuri de utilizatori, drepturile pe care le au aceștia (citire, scriere, ștergere, vizualizare etc.)

La *nivelul de securitate a serviciilor* se controlează accesul la serviciile sistemului cum ar fi echipamentele de intrare/ieșire, gestiunea serverului și pot fi individualizate astfel:

- nivelul de control al serviciilor care este responsabil de funcțiile de avertizare și de raportare a stării serviciilor;
- nivelul de drepturi la servicii care determină cum poate folosi un anumit utilizator un serviciu (de exemplu, drepturile unui operator asupra unei imprimante)

Securitatea fizică constă în împiedicarea pătrunderii în sistem a intrușilor, transmițându-le mesaje de avertizare, iar atunci când aceasta nu este posibil sunt create bariere care să stopeze sau să întârzie atacul. Pe lângă protecția contra atacurilor deliberate, securitatea fizică trebuie să asigure și protecția împotriva dezastrelor naturale. Măsurile prin care este asigurată securitatea fizică se referă la controlul accesului, asigurarea securității echipamentelor din rețea (calculatoare și echipamente periferice), protecția contra dezastrelor naturale, incendiilor sau inundațiilor, protecția bibliotecii de suporturi de date (magnetice, optice, magneto-optice).

Rețelele de calculatoare

La începuturile tehnologiei IT exista un număr redus de computere, ele fiind dispozitive extrem de costisitoare, de dimensiuni apreciabile, ceea ce făcea ca doar anumite instituții (universitățile sau armata) să le aibă în dotare. Această arhitectură



individuală nu utiliza eficient tehnologia, din această cauză trecându-se la conectarea lor, acțiune care a dus la posibilitatea ca resursele (bazele de date, aplicațiile și resursele fizice) să fie întrebuințate concomitent de un număr tot mai mare de utilizatori.

Avantajele rețelelor de calculatoare s-au dovedit extrem de benefice în practică și acest lucru a dus în cele din urmă la nașterea Internetului modern, care este, de fapt, o rețea de calculatoare cu răspândire globală. Conceptele teoretice ale tehnologiei au fost definite la începutul anilor '60, când mai mulți oameni de știință americani au evidențiat modalitățile de conectare a mai multor computere și a numeroasele avantaje care ar reieși. Printre aceștia se numără Paul Baran, Leonard Kleinrock, John Licklider.

Ideile lor au fost preluate de Departamentul apărării SUA care sponsoriza proiecte de cercetare militară la mai multe universități importante din țară. Pentru o muncă mai eficientă în această privință, cercetătorii au pus la punct protocoale și limbaje de programare care să permită transmiterea informațiilor de la un computer la altul la distanță. În acest fel a apărut prima rețea denumită ARPANET, care reunea computerele din patru universități americane.

Astfel, la 29 octombrie 1969 computerele Universității din Los Angeles au intrat în contact cu cele ale Universității Stanford. Un alt moment important a fost atins în 1972 când a fost creat sistemul de e-mail și a fost adoptat simbolul @ pentru semnalizarea unei adrese de e-mail. Următorul pas a fost conectarea ARPANET cu o altă rețea din Europa, apărând astfel prima rețea formată din mai multe rețele. Conexiunea aceasta a fost botezată Internet de către trei cercetători de la Universitatea Stanford (Vinton Cerf, Yogen Dalal, Carl Sunshine), care au pus la punct și primul



protocol care facilita schimbul de informații pe Internet, cunoscut sub numele de TCP (Transmission Control Protocol).

În 1974, Internetul devine comercial prin apariția furnizorilor de internet (ISP) și a Telenet-ului. În anii '80 s-a pus la punct o metodă prin care diferitele rețele din lume să poată comunica între ele apărând astfel Internetul modern, cunoscut sub numele de World Wide Web (www) al cărui părinte spiritual a fost Tim Berners-Lee, liderul unui grup de cercetători de la Institutul CERN din Elveția.

O rețea reprezintă un **ansamblu de dispozitive** (PC-uri, Routere, Switch-uri etc.) interconectate, care pot comunica (schimba informații) între ele.

1) Dimensiunea unei rețele de calculatoare

Retelele pot fi de mai multe tipuri:

- **LAN** – Local Area Network – ex: rețeaua ta (prin cablu) de acasă
- **MAN** – Metropolitan Area Network – ex: rețeaua extinsă, pe suprafața unui oraș
- **WAN** – Wide Area Network – ex: Internetul
- **WLAN** – Wireless LAN – rețeaua ta, wireless, de acasă

Pe lângă aceste tipuri de rețele de calculatoare mai există și altele de diferite dimensiuni sau care au total alte scopuri (ex: SAN – Storage Area Network).

O rețea de tip **LAN** este o rețea relativ mică care este locală unei organizații (și de obicei limitată din punct de vedere geometric).

De exemplu rețeaua ta de acasă este considerată o rețea LAN pentru că este limitată din punctul de vedere al numărului de dispozitive conectate la ea. O rețea a



unei scoli (desi este mai mare) va fi considerata tot LAN pentru ca leaga toate calculatoarele, serverele etc. in aceeasi rețea si sunt limitati din punct de vedere geografic.

Daca ar fi sa combinam mai multe rețele si sa permitem interconectarea lor pe raza unui oraș, atunci am forma un **MAN** (o rețea mai extinsa, la nivelul unui oraș, care oferă viteze mai ridicate de transfer de date față de viteza “la net obijnuită”).

O rețea **WAN** este o rețea este o rețea de rețele pentru ca se afla pe o zona geografica mai mare fata de cele enumerate mai devreme si permite extinderea pe mai multe orase, tari sau chiar continente.

O rețea de tipul **WLAN** este o rețea LAN la care ne putem conecta wireless de pe telefonul mobil, tableta, laptop sau orice alt dispozitiv. Acel mediu wireless este unul separat fata de cel fizic si contine proprietati (viteza, securitate, raza de acoperire, etc.) diferite fata de acesta.

O rețea este alcatuita din:

- **End-device** (PC, Laptop, Smartphone, Servere etc.)
- **Switch** – interconecteaza mai multe end-device-uri intr-o rețea
- **Router** – interconecteaza mai multe rețele
- **Firewall** – ne protejeaza rețeaua de posibile atacuri din Internet
- **Mediu de transmisie** – cablu (cupru), lumina (fibra optica), wireless (aer)



Clasificarea rețelelor de calculatoare

Rețelele de calculatoare moderne sunt prezente în orice colț al lumii și însumează o multitudine de tehnologii, componente, sisteme de operare și protocoale de transmisia datelor, ceea ce face ca sistemul să fie extrem de complex. Pentru a înțelege mai ușor rețelistica, utilizatorii de computere ar trebui să aibă câteva cunoștințe de bază despre acest domeniu, importantă fiind mai ales cunoașterea diferitelor tipuri de clasificări ale rețelelor de calculatoare.

O rețea de computere poate fi formată din două sau mai multe computere, răspândite într-o arie geografică mai mică sau mai mare. Aria de acoperire a rețelelor, modul de conectare, arhitectura de rețea și topologia constituie caracteristici diferite, pe care orice rețea le poate avea.

Rețelele de calculatoare în funcție de aria de acoperire

În funcție de dimensiunile rețelelor ocupă o arie mai mică sau mai mare, începând de la proximitatea imediată până la nivel planetar sau interplanetar:

- PAN (Personal Area Network) este formată din dispozitivele din apropierea unei persoane, care comunică între ele, ca de exemplu computerul și perifericele (monitorul, tastatura, mouse-ul, imprimanta, videoproiectorul, boxele). Comunicarea dintre aceste dispozitive poate fi făcută atât prin cabluri, cât și prin Bluetooth, sau chiar prin radiofrecvență (RFID);
- LAN (Local Area Network) este alcătuită dintr-un număr relativ redus de computere (între 2 și câteva sute) care comunică între ele ca o rețea privată în interiorul unei singure clădiri. Acest tip de rețea poate funcționa acasă, unde există 2 sau mai multe calculatoare, dar este mai întâlnit în cadrul unor firme care folosesc tehnologia informatică, punând la comun resursele. Rețelele LAN



pot fi conectate fie prin cablu sau, mai nou, printr-o rețea fără fir, cunoscută sub numele WI-FI (standardul IEEE 802.11). Componentele unei rețele LAN sunt calculatoarele conectate prin diferite metode, cu ajutorul unui switch. Rețelele LAN pot fi sau nu pot fi conectate la alte rețele cum ar fi Internetul, în funcție de dorințele administratorului de sistem;

- MAN (Metropolitan Area Network) este o rețea ce se întinde pe suprafața unei localități, unde unul sau mai mulți provideri (ISP) oferă servicii de Internet diverșilor utilizatori. Pentru transmiterea informațiilor se folosește cel mai adesea cabluri cu fibră optică ce permit obținerea unor viteze de transfer superioare;
- WAN (Wide Area Network) se întinde pe suprafețe imense, cum ar fi țările și continentele. Aceste tipuri de rețele sunt constituite prin conectarea împreună a mai multor rețele de tip LAN și MAN;
- GAN (Global Area Network) este rețea la nivel global, în prezent întreg globul pământesc aflându-se într-un fel sau altul în această arie de acoperire.

Rețelele de calculatoare după topologie

Topologia rețelelor desemnează diferitele moduri în care componentele pot fi așezate, cum sunt interconectate și ce medii de comunicare se folosesc:

- Tipologia de tip Bus (magistrală) este formată dintr-un cablu care conectează un număr de computere cu ajutorul unui conector de tip T. La capătul cablului se montează dispozitive numite terminatoare care împiedică reflectarea semnalelor electrice. Rețeaua este ușor de construit, dar are ca neajuns faptul că doar două computere o pot folosi în același timp, celelalte trebuind să aștepte până când cablul este liber. Rețeaua de tip Bus funcționează



bine doar atunci când numărul computerelor din ea este redus, calitatea scăzând proporțional cu adăugarea de noi computere;

- Topologia de tip Star (stea) este reprezentată de o rețea în care toate computerele se conectează împreună, prin intermediul unui switch central. Are ca avantaj funcționarea rețelei, chiar dacă legătura spre unul din computere are o problemă. Dezavantajul ar fi necesitatea unui echipament central și costurile mai mari pentru implementarea rețelei;
- Rețeaua de tip Ring (inel) este formată din calculatoare conectate între ele în mod circular. Pachetele de date trimise de un calculator sunt primite de următorul care verifică destinatarul, îl oprește dacă este el sau îl trimite mai departe până la cel corect. Acest tip de rețea oferă performanțe superioare, dar încetează să mai funcționeze dacă unul dintre computere are probleme;
- Topologia de tip Mesh (plasă) se realizează prin conectarea computerelor dintr-o rețea cu fiecare alt computer. Într-o astfel de rețea, în cazul apariției unei defecțiuni va fi găsită imediat o cale alternativă, ceea ce face ca rețeaua de tip plasă să fie perfectă în domeniile în care păstrarea contactului este obligatorie, indiferent de condiții (de exemplu, în domeniul militar sau în cercetare). Un neajuns este costul mare de realizare, cauzat de numărul ridicat de conexiuni între computere;
- Tipologia de tip tree (arbore) e formată dintr-un computer ce administrează rețeaua de care sunt legate mai multe switch-uri intermediare.



Rețelele de calculatoare în funcție de modul de conectare

În privința modului de conectare tehnologia a evoluat foarte mult, ceea ce a dus la creșterea sensibilă a performanțelor rețelelor. Inițial a fost utilizat cablul de tip coaxial format din doi conductori de cupru, cel din interior fir, iar cel din exterior plasă. Cablul coaxial a fost abandonat, deoarece avea viteze limitate, de până la zece Mbps, și a fost înlocuit de cablul de tip TP (perechi răsucite) format din opt fire de cupru răsucite în patru perechi.

Ultimul tip a fost preferat multă vreme pentru că era ieftin, permitea viteze de până la zece Gbps și putea fi conectat prin mufe. În prezent fibra optică este cea mai utilizată, deși are un preț superior cablului, permite viteze mari pentru transmiterea datelor, de până la 100Gbps.

Există și posibilitatea transmiterii informațiilor fără fir, prin intermediul undelor radio, realizându-se așa numitele rețele wireless, extrem de comode și care permit mobilitatea componentelor rețelei.

Rețelele de calculatoare în funcție de arhitectura de rețea

Arhitectura de rețea desemnează relațiile care au loc între componentele acesteia, putând fi de tip Active Networking Architecture, Client Server Architecture și Peer-to-Peer Architecture.



Securitatea rețelelor de calculatoare

Multe dintre informațiile transmise prin intermediul rețelelor de calculatoare sunt confidențiale și, din acest motiv, ele trebuie să fie protejate de acces nedorit, de distrugere sau de modificare. Din această nevoie a apărut o ramură a rețelisticii numită securitatea rețelelor, care are drept scop trei lucruri:

- confidențialitatea (accesul la date să fie permis doar celor care au dreptul);
- integritatea se referă la oprirea încercărilor de modificare a informației de către persoane care nu au acest drept;
- disponibilitatea (accesul la date să poată fi făcut în orice moment).

Tipuri de atacuri asupra rețelelor de calculatoare

Multe rețele de calculatoare sunt vulnerabile în fața atacurilor intenționate ale răuvoitorilor care urmăresc fie să distrugă, fie să obțină un avantaj financiar sau să afle informații confidențiale. Majoritatea problemelor sunt de natură umană, administratorii rețelelor fiind de multe ori slab pregătiți, fără să știe să implementeze corect softurile necesare pentru păstrarea securității.

Printre cele mai folosite tipuri de atacuri se numără:

- Spargerea parolelor poate fi făcută prin diverse metode și permite accesul persoanelor neautorizate la baze de date sau la conturi din diferite calculatoare ale rețelei;
- Floodingul se realizează prin trimiterea către un server a unui număr enorm de mare de pachete de date, care-l blochează pentru o perioadă mai lungă sau mai scurtă de timp;



- Sniffingul se face prin utilizarea unor programe de analiză a traficului, numite sniffere, care pot afla date confidențiale;
- Denial of Service (DoS) împiedică utilizatorii să acceseze resursele rețelei;
- Malware este un soft destinat să deterioreze sistemul de operare al unui computer și care se transmite de la un element la altul al rețelei. Acest tip de soft este folosit și pentru accesarea unor informații secrete din computere;
- Trojan Horse sunt softuri care la prima vedere par folositoare, dar care au funcții ascunse, ce permit accesarea computerelor de la distanță;
- Ransomware este un program care blochează datele criptându-le, cheia fiind oferită doar după plățirea unei răscumpărări;
- Virușii sunt diverși și pot provoca daune tuturor părților componente ale unei rețele.

Metode de protecție a rețelelor de calculatoare

Protecția rețelelor de calculatoare constituie una dintre principalele sarcini ale unui administrator de sistem. Precauțiile trebuie luate atât prin montarea unor componente fizice de ultimă generație, care să nu permită accesări neautorizate, cât și prin instalarea unor antivirusi puternici, actualizați periodic.

Una dintre cele mai bune metode este alegerea unor parole puternice, formate din mai multe caractere, care să cuprindă și majuscule sau semne speciale. În niciun caz nu se vor alege date de naștere, nume ale unor persoane apropiate sau nume de localități, deoarece aceste parole pot fi sparte foarte ușor de către persoanele rău intenționate.

În concluzie, cunoașterea unor elemente de bază despre rețelele de computere reprezintă o necesitate, nu doar pentru administratorii rețelelor, ci și pentru utilizatorii



obișnuți care doresc ca experiența lor online să fie sigură și lipsită de probleme costisitoare.

O rețea este alcătuită din:

- **End-device** (PC, Laptop, Smartphone, Servere etc.)
- **Switch** – interconectează mai multe end-device-uri într-o rețea
- **Router** – interconectează mai multe rețele
- **Firewall** – ne protejează rețeaua de posibile atacuri din Internet
- **Mediu de transmisie** – cablu (cupru), lumina (fibra optică), wireless (aer)

În continuare voi prezenta câteva elemente de rețea (din cele enumerate mai sus). Primele componente ale unei rețele vor fi chiar end-device-urile:

1. END-DEVICE

În general oamenii sunt cei care avem în componența un dispozitiv terminal (end-device). Cu toții avem un Laptop, PC sau smartphone cu care ne conectăm la Internet. Această conexiune poate fi făcută prin unul sau mai multe medii de transmisie (curent, lumina, aer). În momentul în care ne conectăm cu smartphone-ul la Internet, cel mai probabil vom folosi **mediul wireless**. Dacă folosim un **Laptop**, îl putem conecta fie prin **wireless** fie prin **cablu** de rețea (UTP).



Cablu de Retea Ethernet

Conexiunea prin fibra optica are loc atunci când dorim sa conectam mai multe echipamente de rețea sau servere între ele (ex: switch – switch, server – switch). Motivul este simplu: o legătură prin Fibra Optica poate fi mult mai rapida fata de cea prin cablu UTP sau prin Wireless.

II. SWITCH

Switch-ul este un echipament de rețea care interconectează mai multe PC-uri (si nu numai: imprimante, telefoane IP, AP-uri, etc) la ACEEASI rețea locala (LAN). El este caracterizat de un număr mare de port-uri (in general 24 sau 48) toate fiind capabile de viteze între 100 Mbps si 1 Gbps (sau chiar 10Gbps). Switch-ul folosește adresele MAC. (vom vorbi mai in detaliu in Capitolul 2).



O imagine cu un **Switch** profesional Cisco:



Switch de Retea

III. ROUTER

Un Router este un echipament de rețea care are rolul de a interconecta mai multe rețele (LAN) într-o rețea mai mare (WAN -Wide Area Network). Router-ul este dispozitivul care ne conectează la Internet. El se ocupă de trimiterea pachetelor, către rețeaua destinație din Internet. În comparație cu Switch-ul, Router-ul are mult mai puține porturi (între 2 – 5) la viteze asemănătoare (100 Mbps – 10Gbps, depinde de model). După cum spuneam scopul acestui echipament este să interconecteze rețelele. Toate aceste rețele au nevoie de un mod de identificare și astfel Routerurile folosesc adresele IP.



Acesta este un **Router** profesional Cisco:

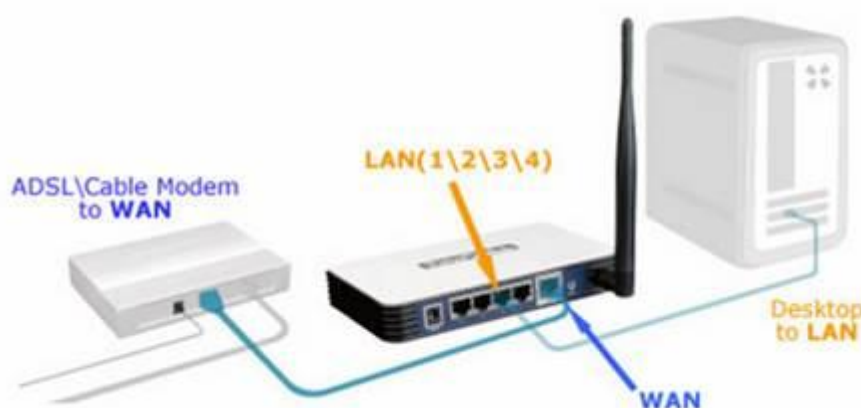


Router de rețea

Cum se configurează setările wireless de bază pe un router wireless

Ne conectezi prin cablu sau wireless un computer la routerul pe care dorim să îl configurăm (în imagine avem un routerul TP-Link)

Este recomandat să îl configurăm printr-o conexiune prin cablu.



Ne autentificăm în interfața Web a routerului parcurgând următorii pași:

Alegeți tipul de conectare (**Cablu** sau **Wireless**)

Pasul 1a: Dacă este **Wireless**, ne conectăm la rețeaua wireless emisă de routerul TP-Link



Pasul 1b: Dacă este prin **Cablu**, ne conectăm prin cablul de rețea la unul din cele patru porturi galbene de pe partea din spate a routerului TP-Link

Pasul 2

Deschidem un browser (ex: **Safari, Chrome, Firefox sau Internet Explorer**). În partea de sus a ferestrei în bara de adrese, introducem una din următoarele adrese: 192.168.0.1 , 192.168.1.1 sau <http://tplinkwifi.net>.



Adresa IP este diferită în funcție de model, trebuie să verificăm aceasta adresa pe eticheta de pe spatele echipamentului.

Pasul 3

Introduceți numele de utilizator (username) și parola (password) în pagina de autentificare. Numele de utilizator (username) și parola (password) implicite pentru dispozitivele TP-Link sunt **admin** și **admin**.



Toate literele pentru numele de utilizator (username) și parola (password) sunt minuscule.



Selecție Dual Band

Acest router suportă atât frecvența de 2.4GHz cât și 5GHz. Selectează frecvența pe care dorești să o folosești. Din meniu, trebuie să deschidem **Dual Band Selection**, apoi selectează frecvența dorită.

Dual Band Selection

This router supports dual band, please choose the frequency that you would like to work with:

☒ Concurrently with 2.4GHz and 5GHz (802.11a/b/g/n/ac)

☐ Only work in 2.4GHz (802.11b/g/n)

☐ Only work in 5GHz (802.11a/n/ac)

To turn off the wireless radio, you can switch the Wireless On/Off button located on the back

Save

În imaginea de mai sus, ambele rețele wireless de 2.4GHz și 5GHz sunt activate. Apoi, configuram rețelele wireless, după cum urmează:

Pentru rețeaua wireless de 2.4GHz

Pasul 1

Selectează **Wireless 2.4GHZ->Wireless Settings (2.4GHZ)** din meniul din partea stângă pentru a deschide setările wireless pentru 2.4GHz.

Wireless Settings (2.4GHz)

Wireless Network Name: TP-LINK_2.4GHz_10FF13 (Also called the SSID)

Region: United States

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Mode: 11bgn mixed

Channel Width: Auto

Channel: Auto

☒ Enable SSID Broadcast

☐ Enable WDS Bridging

Save



Wireless Network Name(Nume Rețea Wireless) sau **SSID**: Setam un nume pentru rețeaua wireless.

Region (Regiune): Selectam țara.

Channel(Canal) este pe Auto.

"Enable SSID Broadcast" trebuie bifat.

Pasul 2

Apasă click pe butonul **Save (Salvare)** pentru a salva setările.

După ce am apăsut butonul **Save (Salvare)**, apare un sfat (de culoare roșie) în partea de jos a paginii, după acest pas vom reporni routerul atunci când toate configurațiile necesare sunt făcute.

Pasul 3

Selectam **Wireless-> Wireless Security** în meniul din partea stângă. Este recomandat să folosești **WPA-PSK / WPA2-PSK** sau **WPA / WPA2 Personal**.

Version (Versiune): WPA-PSK sau WPA2-PSK

Encryption (Criptare): AES

PSK Password (Parola PSK): se completează parola WiFi. (Lungimea Parolei PSK să fie între 8 și 63 de caractere)



În cazul în care alegem **WEP**, utilizăm doar una dintre cele patru câmpuri.



Type: Automatic
WEP Key Format: ASCII
Key Selected: Key 1: 12345 Key Type: 64bit
Key 2: Disabled
Key 3: Disabled
Key 4: Disabled

We do not recommend using the WEP encryption if the device operates in 802.11n mode due to the fact that WEP is not supported by 802.11n specification.

Save

- Pentru criptare pe **64 biți** – putem introduce 10 caractere hexazecimale (orice combinație de 0-9, a-f, A-F, cheie nulă nu este permisă) sau 5 caractere ASCII.
- Pentru criptare pe **128 biți** - putem introduce 26 caractere hexazecimale (orice combinație de 0-9, a-f, A-F, cheie nulă nu este permisă) sau 13 caractere ASCII.
- Pentru criptare pe **152 biți** - putem introduce 32 caractere hexazecimale (orice combinație de 0-9, a-f, A-F, cheie nulă nu este permisă) sau 16 caractere ASCII.

Pasul 4

Apasăm **Save (Salvare)** pentru a salva setările.

Pasul 5

Apasăm butonul **Reboot (Restart)** pentru a restarta routerul; sau navigăm la **System Tools-> Reboot** pentru a restarta routerul.



Pentru rețeaua wireless de 5GHz

Pasul 1

Selectam **Wireless 5GHz->Wireless Settings(5GHz)** din meniul din partea stângă pentru a deschide pagina cu setările wireless.



Wireless Network Name (Nume Retea Wireless) sau SSID: Setam un nume pentru rețeaua wireless.



Region (Regiune): Selectam țara.

Channel (Canal) este pe Auto.

"Enable SSID Broadcast" trebuie bifat.

Pasul 2

Apasăm **Save (Salvare)** pentru a salva setările.

După apăsarea butonului **Save (Salvare)**, apare un sfat (de culoare roșie) în partea de jos a paginii. De fapt, nu este nevoie să repornim routerul după acest pas și vom reporni routerul atunci când toate configurațiile necesare sunt făcute.

Pasul 3

Selectam **Wireless->Wireless Security** din meniul din partea stângă și este recomandat să folosim **WPA-PSK / WPA2-PSK** sau **WPA / WPA2 Personal**.

Version (Versiune): WPA-PSK sau WPA2-PSK

Encryption (Criptare): AES

PSK Password (Parola PSK): se completează parola WiFi. (Lungimea Parolei PSK să fie între 8 și 63 de caractere)



În cazul în care alegi **WEP**, utilizează doar una dintre cele patru câmpuri. Pentru mai multe detalii, consultă nota din partea de jos.

WEP

Type: Automatic

WEP Key Format: ASCII

Key Selected	WEP Key (Password)	Key Type
Key 1: ☒	12345	64bit
Key 2: ☐		Disabled
Key 3: ☐		Disabled
Key 4: ☐		Disabled

We do not recommend using the WEP encryption if the device operates in 802.11n mode due to the fact that WEP is not supported by 802.11n specification.

Save

- Pentru criptare pe **64 biti** - putem introduce 10 caractere hexazecimale (orice combinație de 0-9, a-f, A-F, cheie nulă nu este permisă) sau 5 caractere ASCII.
- Pentru criptare pe **128 biti** - putem introduce 26 caractere hexazecimale (orice combinație de 0-9, a-f, A-F, cheie nulă nu este permisă) sau 13 caractere ASCII.
- Pentru criptare pe **152 biti** - putem introduce 32 caractere hexazecimale (orice combinație de 0-9, a-f, A-F, cheie nulă nu este permisă) sau 16 caractere ASCII.

Pasul 4

Apasăm **Save (Salvare)** pentru a salva setările.

Pasul 5

Apasăm butonul **Reboot (Restart)** pentru a restarta routerul, sau navigam la **System Tools-> Reboot** pentru a restarta routerul.



Pentru Guest Network

Routerele TP-Link Dual band suportă de asemenea **Guest Network**.

Pentru a configura **Guest Network**

Accesul la rețea pentru oaspeți **Guest Network** oferă acces Wi-Fi securizat pentru ca oaspeții să partajeze rețeaua de acasă sau de la birou. Când avem vizitatori în casa, apartamentul sau locul de muncă, putem activa rețeaua de oaspeți pentru aceștia.

Setam diferite opțiuni de acces pentru utilizatorii rețelei invitate, ceea ce este foarte eficient pentru a asigura securitatea și confidențialitatea rețelei dvs. principale.

Pasul 1

Ne conectăm la pagina de management web cu <http://tplinkwifi.net>

Pasul 2:

Accesăm **Guest Network** rețeaua de oaspeți

Pasul 3

Pentru routerele cu bandă dublă, putem alege să activăm rețeaua de oaspeți a uneia sau a ambelor benzi. Bifați „**Guest Network(2.4G)**” și/sau „**Guest Network(5G)**”



pentru a activa această funcție, apoi putem seta Guest Network's SSID and Security. Există doar două tipuri de securitate disponibile, **Disable Wireless Security & WPA/WPA2-Personal**. Se recomandă să selectați WPA/WPA2-Personal ca tip de securitate. Apoi introducem o parolă dorită Wireless Password.

Facem click pe Save (Salvare) pentru ca setările să intre în vigoare.

The screenshot displays the router's configuration page. On the left is a sidebar menu with options like Status, Quick Setup, Network, Dual Band Selection, Wireless 2.4GHz, Wireless 5GHz, Guest Network (highlighted), Wireless Settings, Storage Sharing, DHCP, USB Settings, NAT, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS, IPv6 Support, and System Tools. The main content area is divided into two sections: 'Guest Network (2.4G):' and 'Wireless 5GHz'. Both sections have a red box highlighting the 'Guest Network' checkbox, 'Network Name' field, and 'Wireless Security' dropdown. In the 2.4GHz section, 'Wireless Security' is set to 'WPA/WPA2-Personal'. In the 5GHz section, it is set to 'Disable Security'. The 'Access Time' section for both bands shows 'Schedule' selected, with 'All day-24 Hours' checked.

De asemenea putem configura timpul de acces al clienților invitați:

Există două tipuri de reguli pentru a controla timpul de acces:

1- Time Out:

Introducem perioada în care dorim ca, clienții/ oaspeți pot accesa internetul. Conexiunea se va întrerupe automat când ajunge la ora configurată. Clienții se pot reconecta și obține o altă perioadă de timp dacă doresc.



2- Schedule

Configuram un program specific pentru clienții oaspeți pentru a putea accesa internetul.

Trebuie sa ne asiguram că setările de oră sunt corecte pentru a vă asigura că programul va intra în vigoare.



Time Settings

Time zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore

Date: 4 22 2014 (MM/DD/YY)

Time: 11 49 15 (HH/MM/SS)

NTP Server 1: (Optional)

NTP Server 2: (Optional)

Get GMT

Enable Daylight Saving

Start: 2014 Mar 3rd Sun 2am

End: 2014 Nov 2nd Sun 3am

Daylight Saving Status:

Note: Click the "GET GMT" to update the time from the internet with the pre or entering the customized server (IP Address or Domain Name) in the ab

Save

Allow Guest – dacă dorim să permitem clienților din rețeaua de oaspeți să acceseze clienții din rețeaua locală, trebuie să bifam Allow Guest. Dacă nu, trebuie să-l păstrăm dezactivat. Dacă routerul este configurat ca AP, trebuie să îl bifăm, altfel nu există acces la internet al rețelei invitaților.

Guest Network Bandwidth Control - cu această caracteristică, puteți limita lățimea de bandă a rețelei oaspeților.

Guest Network Wireless Settings

Access And Bandwidth Control

Allow Guest To Access My Local Network: ☒

Enable Guest Network Bandwidth Control: ☒

Egress Bandwidth For Guest Network: 256 Kbps (Range:1~100000)

Ingress Bandwidth For Guest Network: 1024 Kbps (Range:1~100000)

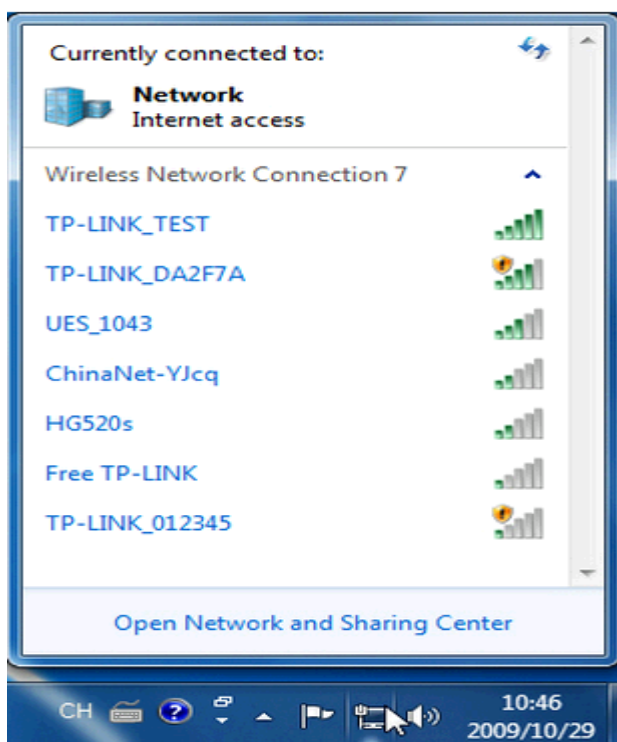
În prezent, toate routerele wireless dual-band TP-Link suportă **Guest Network**. În cazul în care **Guest Network** nu este disponibil pe routerul trebuie să actualizezi firmware-ul.



După ce am terminat configurarea, selectăm **System Tools-> Reboot** din meniul din partea stângă și apoi apasăm butonul **Reboot (Restart)** pentru a restarta routerul.



Dacă configurarea este reușită în colțul din dreapta jos al ecranului localizăm pictograma wireless. În lista de rețele wireless, selectăm rețeaua wireless și completăm parola.



Dispozitivele wireless care sunt echipate cu adaptoare de rețea wireless de 5GHz pot detecta rețeaua wireless de 5GHz a routerului.