



Configuring a Local Server for Secure, Multi-User Collaborative Access within a LAN

Abdulati Omara Almahdi Qaytoun ^{1*}, Mohammed Abdulla Ahmed Emeigel ²
^{1,2} Department of Computer Science, Faculty of Information Technology, Bani Waleed
University, Bani Walid, Libya

تكوين الخادم المحلي لتمكين الوصول المتعدد والتعاوني الآمن ضمن شبكة (LAN)

عبد العاطي اعمارة المهدي قيطون ^{1*}، محمد عبد الله أحمد معيقل ²
^{2,1} قسم علوم الحاسوب، كلية تقنية المعلومات، جامعة بني وليد، بني وليد، ليبيا

*Corresponding author: qitton@bwu.edu.ly

Received: September 17, 2025

Accepted: December 01, 2025

Published: December 13, 2025

Abstract:

This research aims to identify, understand, and analyse the technical and organizational aspects related to accessing a local server from other computers over a local network using wireless connectivity. It explores key concepts of local servers, data transfer protocols, secure connection mechanisms, and essential security considerations. The study discusses how to utilize services hosted on the server and evaluates performance optimization methods within a local network compared to remote access through the internet. The central problem addresses how a second computer can access the local server securely and functionally within the same network to enable website testing and benefit from server services. The research provides a methodology involving collecting network data, setting up the local server, configuring the firewall, ensuring devices are on the same network, linking the IP to the Apache server, and performing connection checks. Key findings include simulating the production environment, enhancing availability and speed, enabling cross-device compatibility testing, supporting task separation, and facilitating collaboration and peer review. The study concludes that correctly configuring the firewall, assigning a static IP address, and linking it to the Apache server ensures a stable connection and improves software quality and testing efficiency. The recommendations focus on regularly inspecting network devices, providing necessary security and antivirus software, and keeping software updated.

Keywords: local Server, Local Area Network (LAN), Firewall, Appserver, IP Address, Protocols, Router, Client.

المخلص

يهدف هذا البحث إلى تحديد وفهم وتحليل الجوانب التقنية والتنظيمية المتعلقة بالوصول إلى خادم محلي من أجهزة كمبيوتر أخرى عبر شبكة محلية باستخدام الاتصال اللاسلكي. يستكشف المفاهيم الأساسية للخوادم المحلية، وبروتوكولات نقل البيانات، وآليات الاتصال الآمنة، واعتبارات الأمان الضرورية. تناقش الدراسة كيفية الاستفادة من الخدمات المستضافة على الخادم وتقييم طرق تحسين الأداء ضمن الشبكة المحلية مقارنة

بالوصول عن بعد عبر الإنترنت. تتناول المشكلة المركزية كيفية وصول جهاز كمبيوتر ثانٍ إلى الخادم المحلي بشكل آمن وفعال ضمن نفس الشبكة لتمكين اختبار المواقع الإلكترونية والاستفادة من خدمات الخادم. يقدم البحث منهجية تتضمن جمع بيانات الشبكة، وإعداد الخادم المحلي، وتكوين جدار الحماية، والتأكد من وجود الأجهزة على نفس الشبكة، وربط عنوان IP بخادم Apache، وإجراء فحوصات الاتصال. تشمل النتائج الرئيسية محاكاة بيئة الإنتاج، وتعزيز التوافر والسرعة، والتمكين من اختبار التوافق بين الأجهزة، ودعم فصل المهام، وتسهيل التعاون ومراجعة الأقران. تخلص الدراسة إلى أن التكوين الصحيح لجدار الحماية، وتعيين عنوان IP ثابت، وربطه بخادم Apache يضمن اتصالاً مستقرًا ويحسن جودة البرمجيات وكفاءة الاختبار. تركز التوصيات على فحص الأجهزة الشبكية بانتظام، وتوفير برامج الأمان ومكافحة الفيروسات اللازمة، وتحديث البرامج باستمرار.

الكلمات المفتاحية: خادم محلي، شبكة المنطقة المحلية (LAN)، جدار الحماية، أبسيرفر، عنوان IP، البروتوكولات، الموجه، العميل.

Introduction

A local server is considered a key tool for developing and testing web applications and websites on personal computers before deploying them online. It is one of the most essential technologies utilized in education, administrative programming, and data storage, without requiring an active internet connection. When multiple computers are connected to the same local network (LAN), developers frequently need to access this environment from various devices in a secure and optimized manner—whether for website testing, file sharing, or system management. Such access, however, requires specific configurations and adjustments at both the network and system levels.

Research Problem

Many users face difficulties when attempting to access a local server from another computer connected to the same network. This issue is often caused by misconfigured ports, firewall restrictions, or improper local network settings.

Accordingly, the central research problem can be formulated as follows:

How can a second computer access the local server hosted on the first computer within the same network in a secure and functional manner, enabling website testing and benefiting from the services provided by the server?

Significance of the

The research provides several important benefits:

- Enables testing of websites and applications simultaneously from multiple computers.
- Supports teamwork and collaborative development within a single organization through a shared local server.
- Facilitates design compatibility and responsiveness testing across different operating systems prior to online deployment.
- Provides a secure internal environment for services without dependence on an internet connection.
- Reduces operational costs by eliminating the need for external hosting and allowing fully local work within the institution.
- Enhances data accessibility by allowing users to share a common local database.

Research Objective

The research objectives are to:

1. Understand the concept of a local server and how it is configured.
2. Identify the most common connection problems and propose practical solutions.

3. Outline the steps required to share a local server across multiple devices within the same network.
4. Provide a schematic workflow illustrating the communication process and different connection methods.

Technical Terminology

1. Localhost / Local Server

A computer that functions as a server within a local network, providing an operational environment that allows websites and databases to run locally without an Internet connection. It is a computer system that provides exceptional services. The data stored on the server includes complex documents and information. The service aims to meet clients' needs and provide users with access to information. Servers have an essential role in sending and receiving information more quickly. A server is a large-scale computer network that accommodates components such as processors and large-capacity RAM.

2. AppServer

A free software package that includes Apache, MySQL, and PHP, designed to simplify the creation of a local server on Windows, macOS, and Linux systems.

3. Static IP Address

A network address permanently assigned to a device, enabling direct and consistent access without changes.

4. Firewall

A security system that monitors and controls incoming and outgoing network traffic, preventing unauthorized applications from accessing the Internet or the internal network.

5. Router

A networking device that connects multiple devices and routes data packets between them. It distributes Internet access over a Local Area Network (LAN) or Wi-Fi and acts as an intermediary between the network devices and the Internet Service Provider.

6. Communication Protocols

Standards governing data exchange between devices. Examples include HTTP, FTP, HTTPS, and SSH, each featuring specific security levels and functional purposes.

The General Concept of a Local Server

The local server is a machine within a network that provides a specific service (such as HTTP, FTP, or a database). Through appropriate configuration and permissions on the local network, users can connect to this server and make use of its services. This concept is also referred to as the localhost and is commonly associated with the default IP address 127.0.0.1.

The General Concept of a Local Area Network (LAN)

A Local Area Network (LAN) is a group of devices interconnected within a geographically limited area, such as an office, home, or educational institution. Its main purpose is to enable these devices to share critical resources—such as printers, files, and internet access—and to communicate with one another quickly and efficiently.

Key characteristics of a LAN include:

- **Limited geographical scope:** It covers a relatively small area, in contrast to Wide Area Networks (WANs), which can span cities or regions.
- **Local administration:** The equipment and infrastructure of the network are managed and maintained locally by individuals or network administrators on site.
- **High speed:** LANs provide high data transfer rates between connected devices, depending on the underlying infrastructure (often on the order of 100 Mbps, 1 Gbps, or higher).
- **Shared components:** Such networks typically rely on common hardware components, including routers, switches, and Ethernet cabling.

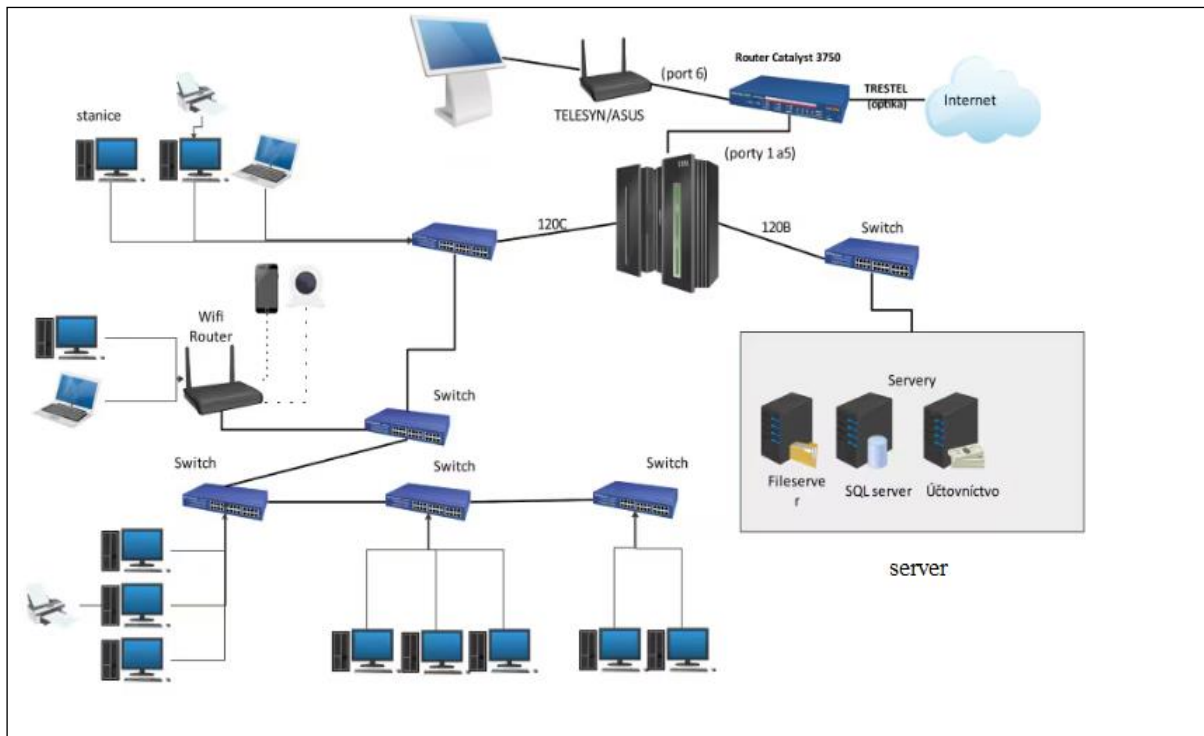


Figure (1): Connection of devices within the local network.

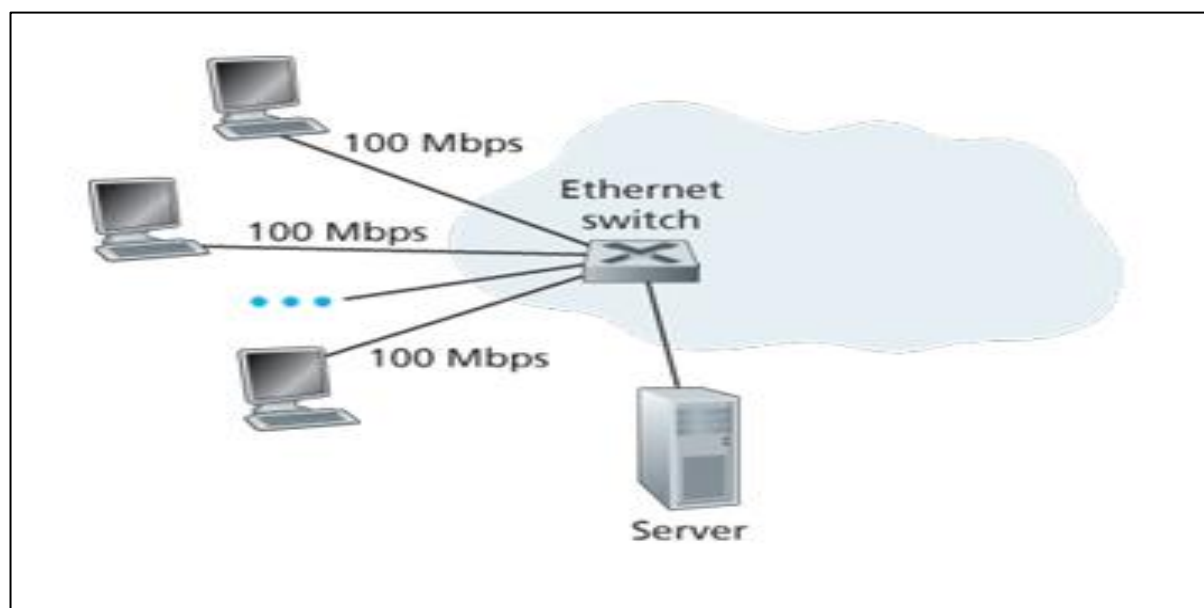


Figure (2): Connection of clients within the server.

Methodology for Accessing the Local Server Using Another Device

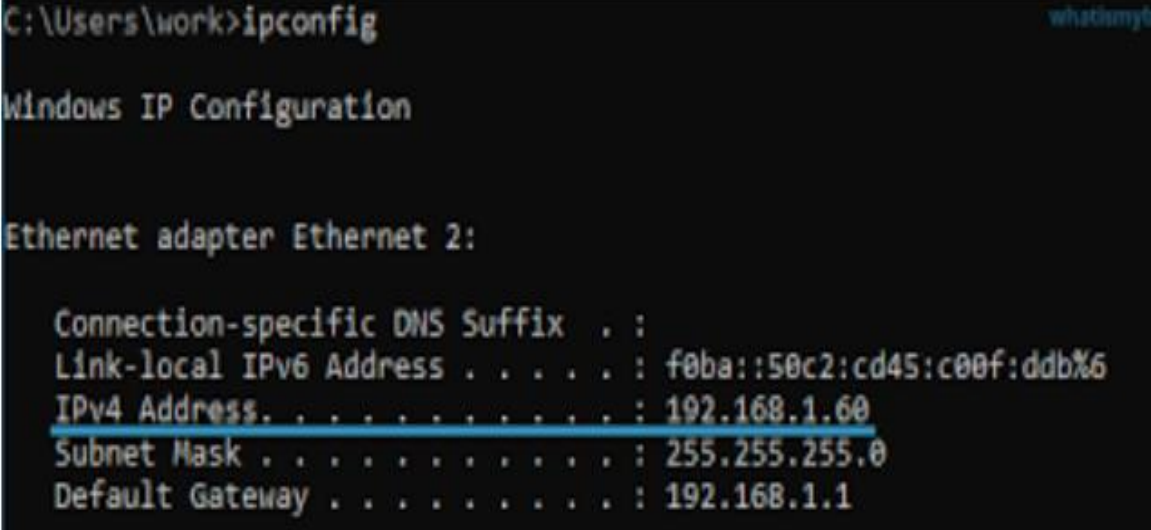
The methodology employed in this research outlines the systematic steps required to enable secure and functional multi-device access to a local server hosted on a single machine within the same Local Area Network (LAN). The process is divided into seven main, sequential stages:

1. Collecting Network Data and Server Status (Harkness, 2022)

At the initial stage, critical network information is collected from the device that hosts the server to ensure successful configuration and connectivity. This information includes:

- **IP Address (IPv4):** The host device's address on the local network.
- **Device Name (Optional):** The hostname of the server.
- **The Port Used:** The specific port number configured for the server service (e.g., Port 80 for HTTP/Apache, Port 8080, Port 3306 for MySQL).

The IPv4 address, essential for client connection, can be obtained by executing the command `ipconfig` in the Command Prompt (CMD) for Windows operating systems, or `ipconfig` for Linux and macOS environments. The output will provide the IPv4 address, typically in the format: (192.168.1.100). This process is illustrated in Figure 3.



```

C:\Users\work>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::50c2:cd45:c00f:ddb%6
    IPv4 Address. . . . . : 192.168.1.60
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
  
```

Figure (3): Obtaining the device's IP address

2. Setting Up the Local Server on the Host Machine (Bloom, 2002)

This stage involves preparing the server software and host operating system for external access. The steps include:

- **Starting Services:** Initiating the core server service (e.g., Apache HTTP Server) or the specific service needed (e.g., MySQL, FTP).
- **File Verification:** Verifying that the application files located within the server's root directory (e.g., `htdocs` or `www`) are functioning correctly when accessed via `localhost`.
- **Port Definition:** Confirming the operational port used by the server, which is typically Port 80 by default for web services.
- **Access Restriction Modification:** Editing the main server configuration file (commonly `httpd.conf` for Apache) to remove the default restriction to `localhost` only. This is done by modifying the access control directives to include a broader permission, such as replacing restrictive lines with `Require all granted` within the appropriate directory blocks, as per common server administration practices.
- **Assigning a Static IP Address:** Configuring the host machine with a Static IP address to ensure consistent access for client devices. This crucial step is executed through the operating system's network settings: Network and Sharing Center → Change Adapter Settings → Wi-Fi → Properties (on Windows). A static IP prevents the router's DHCP service from changing the address, thus ensuring reliable service availability (Iskali et al., 2025).

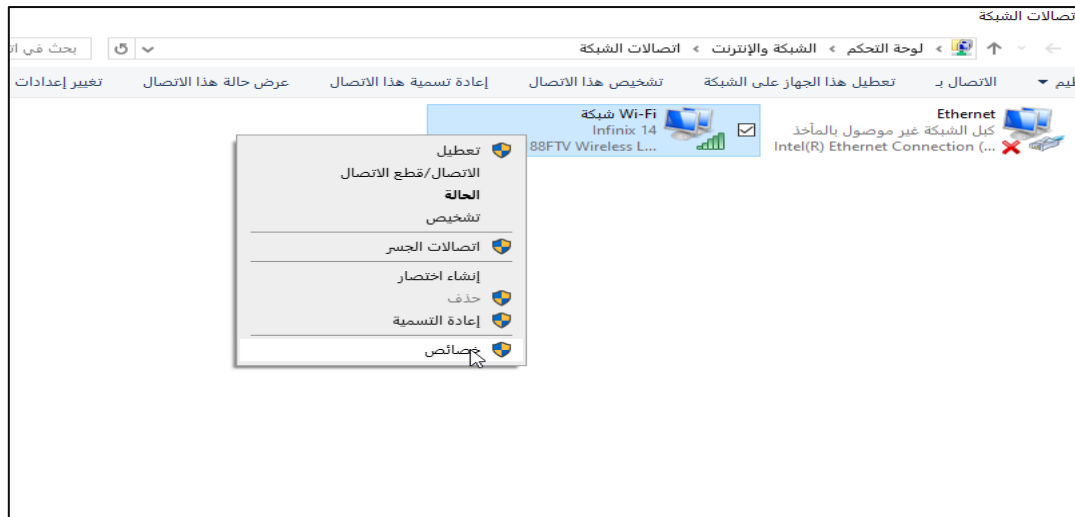


Figure (4): Method of accessing the network properties.

Internet Protocol Version 4(Tcp/Ipv4)

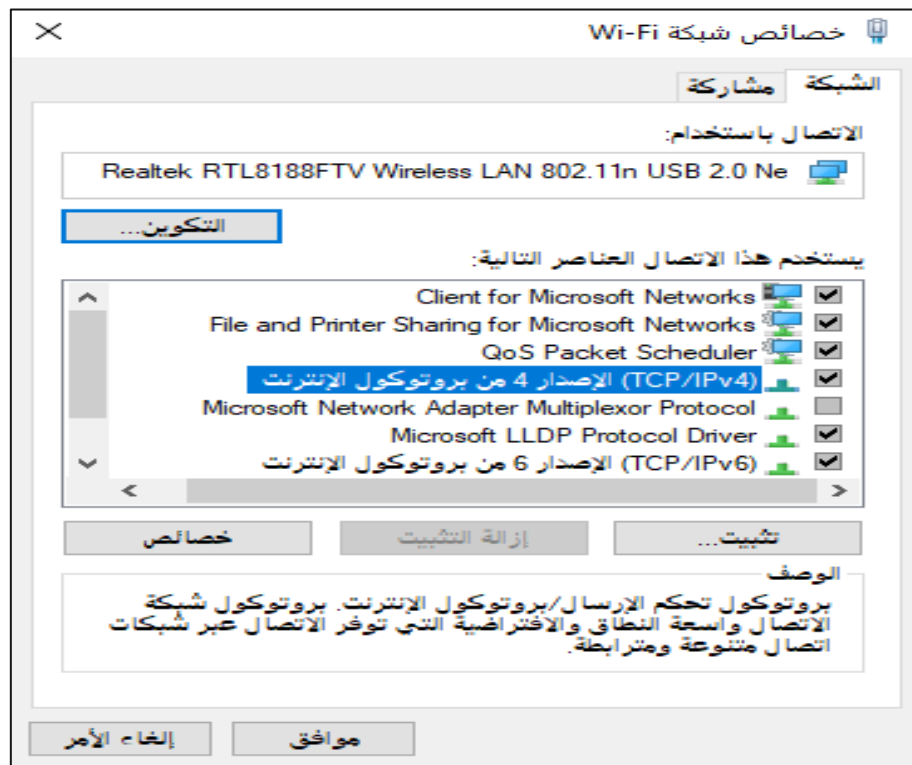


Figure (5): Accessing the Internet Protocol TCP/IPv4 settings

Use The Following Ip Address:

- **IP ADDRESS:** 192.168.1.XXX (REPLACE XXX by Unused number as 90)
- **Subnet mask:** 255.255.255.0
- **Default gateway:** 192.168.1.1
- **DNS:** 5
- **Preferred DNS:** 8.8.8.8
- **Alternate DNS:** 8.8.4.4

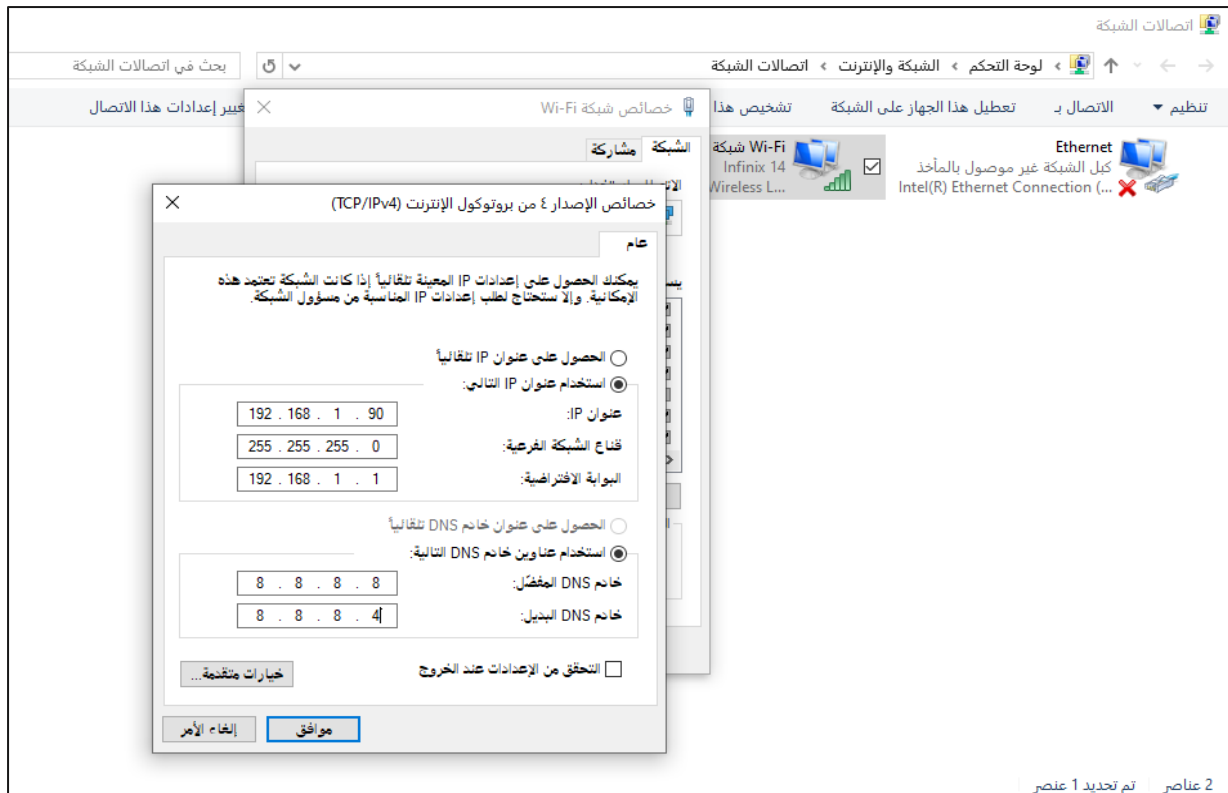


Figure (6): Using IP and DNS addresses.

3- Configuring the firewall:

The settings must be modified on the port in use to allow the following:

- Allow Apache or the server to make private (local) connections.
- Allow connections on the port in use, such as 80 or 8080.



Figure (7): Modifying Windows Defender settings

Search for Apache HTTP Server and make sure the Private option is enabled while the public option remains disabled.

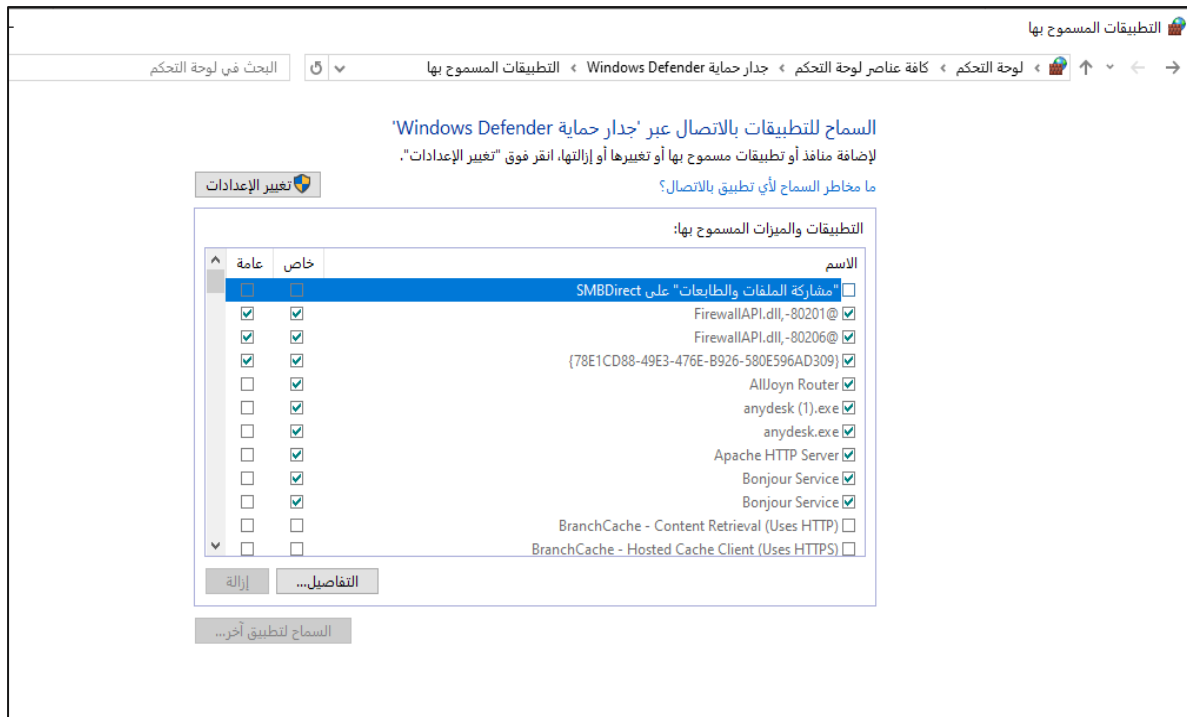


Figure (8): Changing Apache HTTP Server settings.

4-Ensuring that the devices are connected to the same network:

All devices must be connected to the same network, either through a router, a switch, or via a network cable.

The newest IEEE standard in the Wi-Fi category is 802.11n. It is designed to improve on the 802.11g in the amount of bandwidth supported by utilizing multiple wireless signals and antennas (called MIMO technology) instead of one. When this standard is finalized in November 2009 and industries started implementing this standard, 802.11n connections will support real-world data rates of well over 100 Mbps. Also, IPv6 is expected to replace IPv4 due to shortage of IP addresses in IPv4.

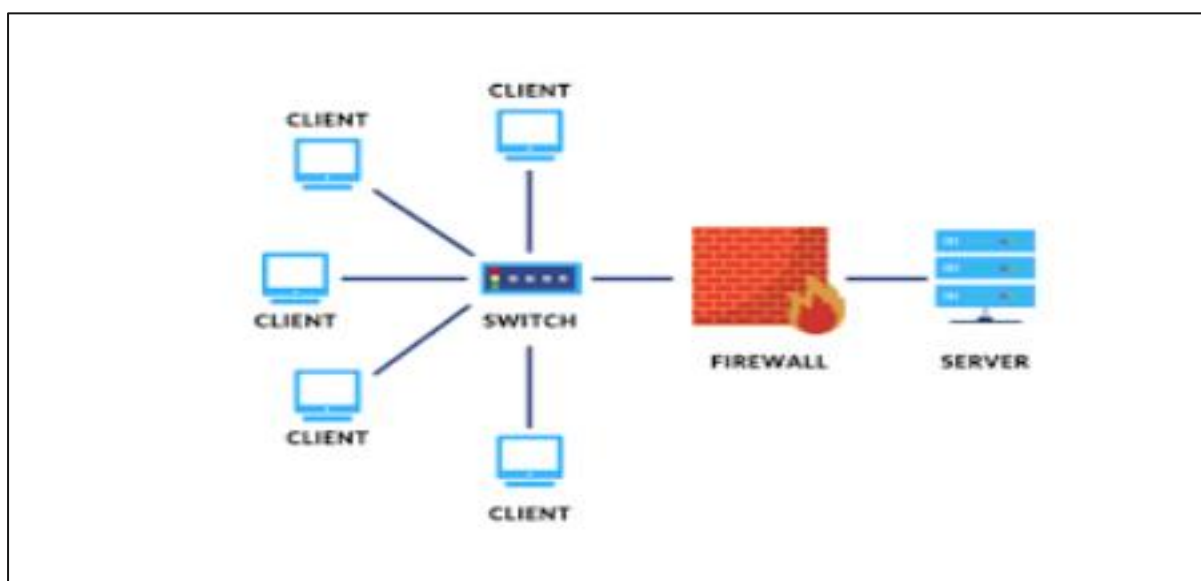


Figure (9): Connecting multiple devices using a switch.

5- Linking the IP to the Apache server via AppServ

After assigning a static IP address, the Apache settings can be modified so that the server becomes accessible over the network. This is done by editing the httpd.conf file, searching for the line:

Listen 192.168.1.10:80

Listen 80

and changing it to:

Listen 192.168.1.90:80

Listen 80

Then save the file and restart APACHE to ensure the changes take effect.

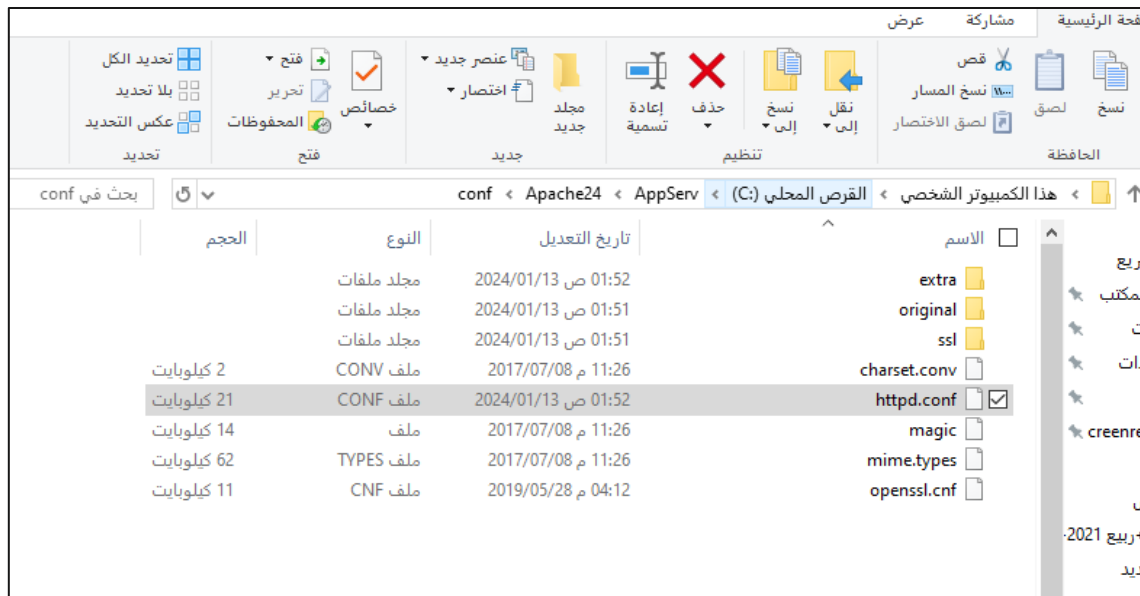


Figure (10): Accessing the local server.conf configuration files.

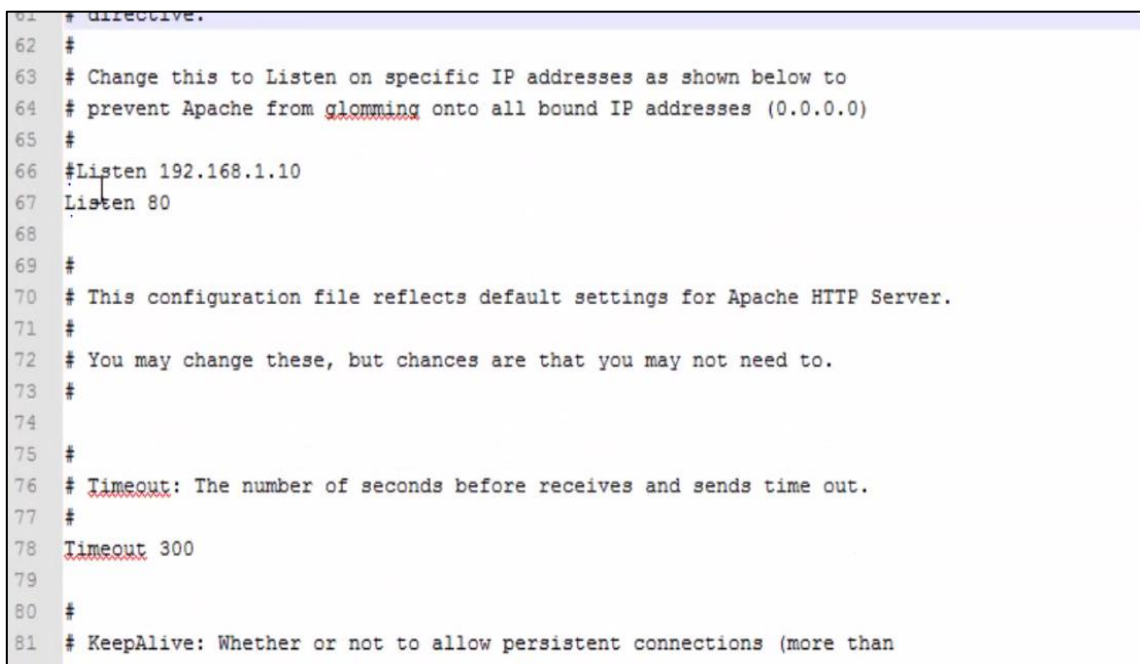


Figure (11): Accessing the local server .conf configuration files open

6– Connection checks and troubleshooting

If the server does not open, verify the following:

- Is the first machine powered on?
- Is the Apache server (or another server software) running?
- Is the port open?
- Does the firewall allow the connection?
- Are the devices really on the same network?
- Has the IP address changed?

7 – Security considerations to be taken into account

- Restricting access: do not leave the server open to any IP; instead, use specific IP ranges.
- Firewall settings: avoid opening unnecessary ports that are not needed.
- Continuous monitoring: always ensure that access and login attempts are monitored to prevent intrusions.

Conclusions

This practical application of configuring multi-device access to a local server offers significant features and benefits. The most important of these findings are:

1. **Simulation of the Production Environment:** This type of connection allows for testing the application or website's behavior when accessed by users from various devices (such as smartphones, tablets, or other computers). This closely resembles a real deployment scenario on the internet, thereby enhancing the relevance of local testing.
2. **Availability and Speed:** The configuration provides the ability to exchange information (in all its forms) to and from the server device more quickly and reliably within the high-speed Local Area Network (LAN).
3. **Cross-Device Compatibility Testing:** Since design responsiveness can vary across screen sizes, this setup makes it necessary and straightforward to properly test the website or application on diverse screens and device sizes without needing complex emulation tools on the host machine.
4. **Separation of Tasks:** Heavy tasks that require substantial resources (such as code compilation or running the server processes) can be run on the host machine, while another device (the client) is used to browse the results or test the user interface. This separation prevents resource contention and performance impact between the server processes and the user interface testing.
5. **Collaboration and Teamwork:** Team members or clients within the same organization can easily review project progress using their own devices, eliminating the need to physically access the main server machine.
6. **Peer Review:** Other developers can easily provide feedback or assist with debugging and quality assurance, provided that they are securely connected to the same network.

Associated Risks and Challenges

While beneficial, this setup introduces specific technical and security risks that must be acknowledged:

1. **Dependency on Availability:** The host machine must remain powered on and the server software running; otherwise, access to the server will not be possible for client devices.
2. **Local Vulnerabilities:** If the server is not properly secured (for example, if a database is configured with weak or default passwords), it may be exposed to unauthorized access or local intrusion from within the LAN.

3. **Firewall Configuration Complexity:** Modifying the host machine's firewall settings to allow incoming connections is necessary but can weaken the device's overall security if the rules are not configured with precision and strict access control.
4. **Network Complexity:** Initial difficulties may arise in achieving device visibility, especially when dealing with the transition between static and dynamic IP settings, or due to complex restrictions imposed by the router or network policy.

Recommendations

Based on the research findings, the following recommendations are crucial for maintaining an optimal and secure local server environment:

1. **Regular Network Inspection:** Regularly inspect the wireless devices or wired cables used to connect the local network to ensure physical integrity and optimal performance.
2. **Security Software Provision:** Ensure the provision and proper configuration of necessary security software, such as an application firewall and communication control software.
3. **Antivirus Implementation:** Install and maintain up-to-date antivirus software across all devices on the local network to protect against malware that may spread during data transfer between devices.
4. **Software Updates:** Consistently monitor and apply the latest software releases and security patches from manufacturers and vendors (for the operating system and the AppServer components like Apache and MySQL).

References

1. Altaï, S. S. A., Abdulaziz, W. B., & Algherini, M. M. A. (2025). Enhancing Server Security: Implementation and Evaluation of the Port Knocking Method on Ubuntu Virtual Servers. *Journal of Engineering and Sustainable Development*, 29(6), 753.
2. Akin, D., & Geier, J. (2004). 802.11 PHY layers. In *CWAP - certified wireless analysis professional official study guide*. McGraw-Hill.
3. Baghaei, N., & Hunt, R. (2004). IEEE 802.11 wireless LAN security performance using multiple clients. *Proceedings, The 12th IEEE International Conference on Networks*.
4. Bloom, R. B. (2002). *Apache Server: The Complete Reference*. McGraw-Hill, Inc.
5. Debagus, S. (2025). ANALYSIS AND DESIGN OF LOCAL NETWORK (LAN) IN SCHOOLS USING CISCO PACKET TRACER. *Digital Frontier: Journal of Computer and Science Innovation*, 1(1).
6. Ezedin, B., Mohammed, B., Amal, A., Al, S. H., Huda, K., & Al, M. M. (2006). Impact of Security on the Performance of Wireless-Local Area Networks. *Innovations in Information Technology*.
7. Harkness, D. J. (2022). *Apache essentials*. Apress LP.
8. Iskali, D., Barel, H., Shulman, A., & Leiba, T. (2025). Localhost detour from public to private networks: Vulnerabilities and mitigations. *Cryptography and Communications*.
9. Khoussainov, R., & Patel, A. (2000). LAN security: problems and solutions for Ethernet networks. *Computer Standards & Interfaces*.
10. Kolahi, S. S., et al. (2009). The impact of security on the performance of IPv4 and IPv6 using 802.11 n wireless LAN. *2009 3rd International Conference on New Technologies, Mobility and Security*. IEEE. (p. 2).
11. Kolahi, S. S., Narayan, S., D.D.T, Y. S., & Mani, P. (2008). The Impact of Wireless LAN Security on Performance of Different Windows Operating Systems. *IEEE Symposium on Computers and Communications*.
12. Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach*. Pearson.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of **SJPHRT** and/or the editor(s). **SJPHRT** and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.