# CompTIA

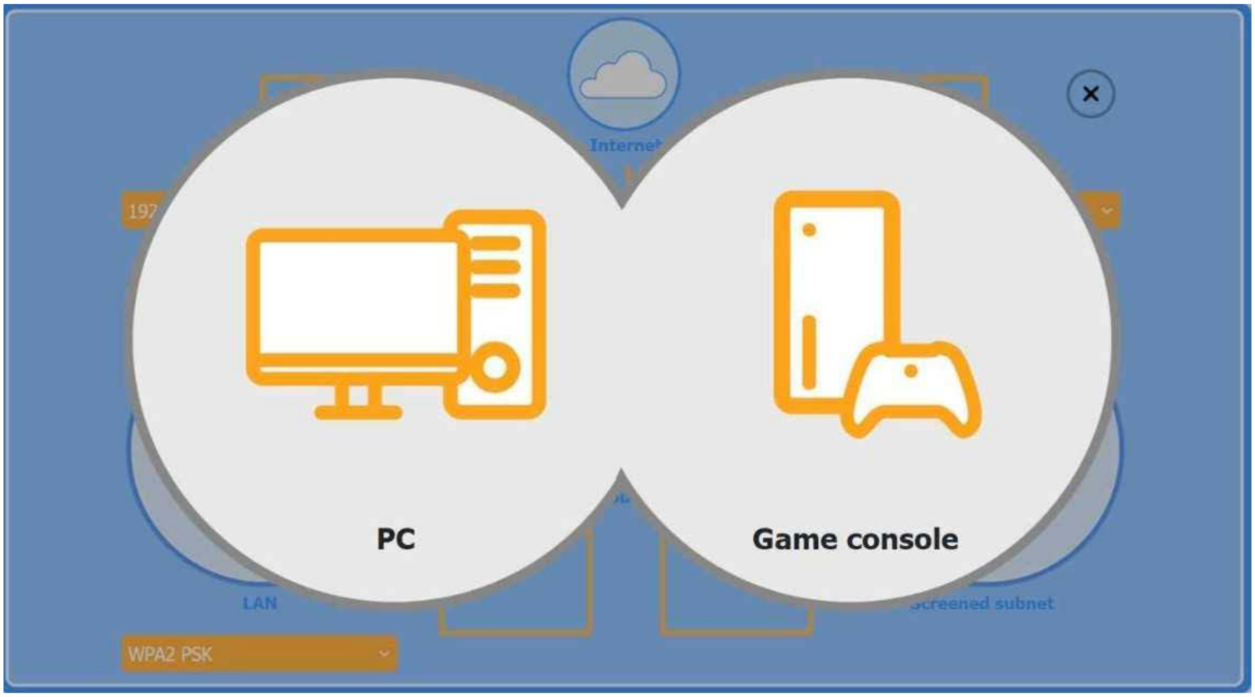
## 220-1202

## CompTIA A+ Core 2 2025 Exam

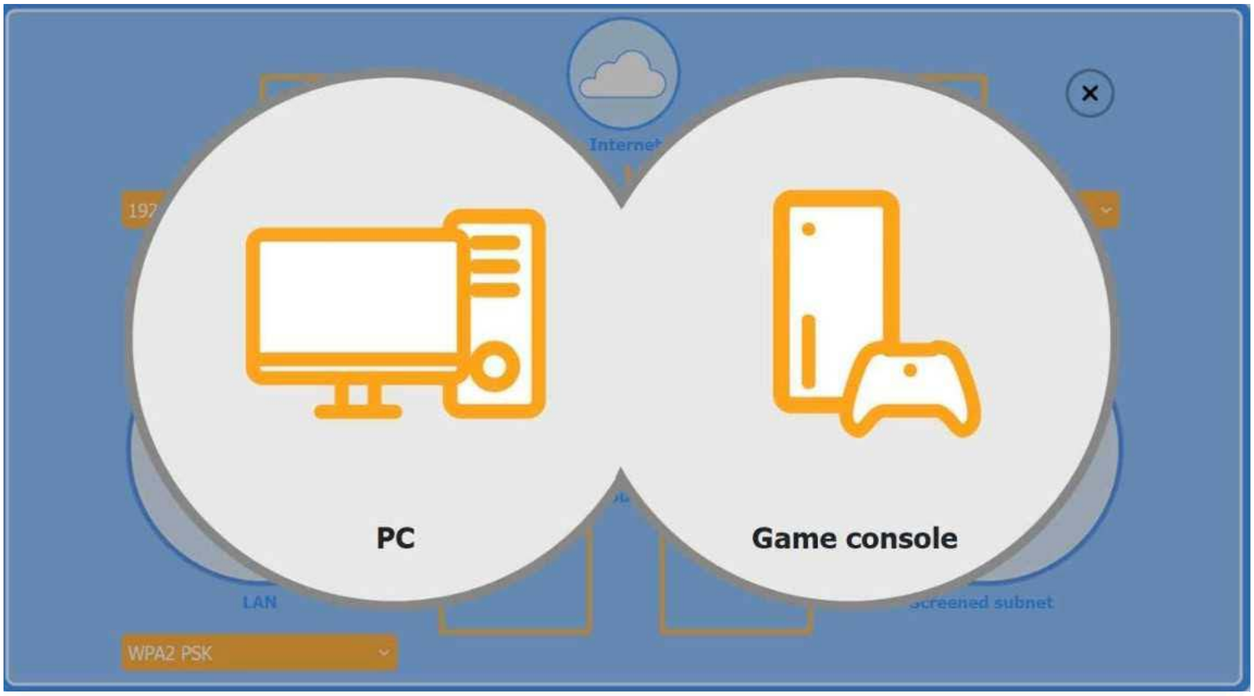
# Latest Version: 12.2

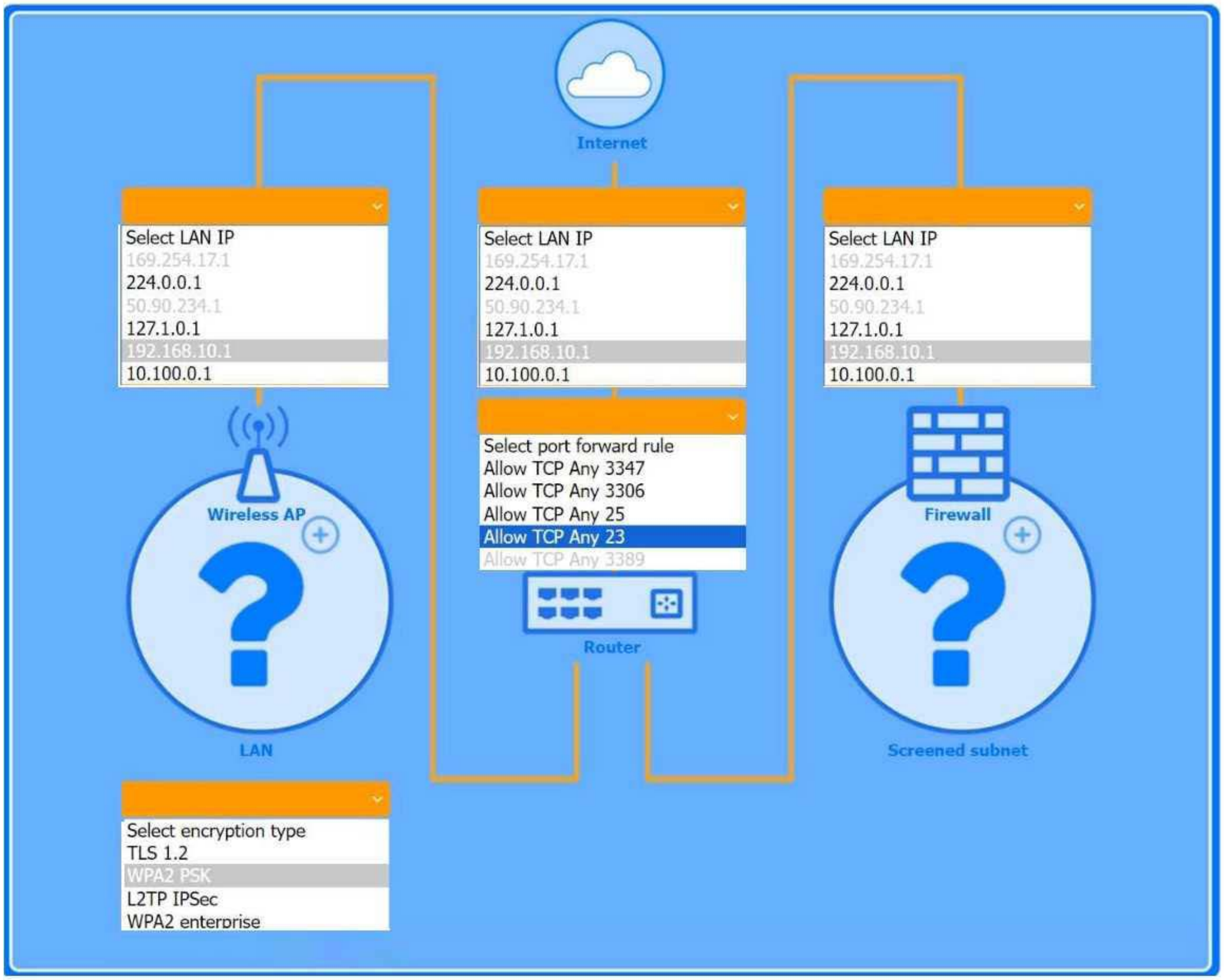
## Question: 1

SIMULATION
You are configuring a home network for a customer. The customer has requested the ability to access a Windows PC remotely, and needs all chat and optional functions to work in their game console.
INSTRUCTIONS
Use the drop-down menus to complete the network configuration for the customer. Each option may only be used once, and not all options will be used.
Then, click the + sign to place each device in its appropriate location.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Wireless AP LAN



Firewall Screened Subnet


Internet
192
PC
Game console
LAN
Screened subnet
WPA2 PSK


Internet
Select LAN IP
169.254.17.1
224.0.0.1
50.90.234.1
127.1.0.1
192.168.10.1
10.100.0.1
Select LAN IP
169.254.17.1
224.0.0.1
50.90.234.1
127.1.0.1
192.168.10.1
10.100.0.1
Select LAN IP
169.254.17.1
224.0.0.1
50.90.234.1
127.1.0.1
192.168.10.1
10.100.0.1
Select port forward rule
Allow TCP Any 3347
Allow TCP Any 3306
Allow TCP Any 25
Allow TCP Any 23
Allow TCP Any 3389
Wireless AP
Router
Firewall
LAN
Screened subnet
Select encryption type
TLS 1.2
WPA2 PSK
L2TP IPSec
WPA2 enterprise

**Answer: See explanation below.**

The completed configuration:
1. Wireless AP (LAN side)
1. LAN IP: 192.168.10.1
2. Encryption: WPA2 PSK
2. Router (port-forward rule)
1. Allow TCP Any 3389
This forwards inbound RDP traffic (TCP/3389) from the Internet to the Windows PC, enabling Remote Desktop access.
3. Firewall (screened subnet side)
1. LAN IP: 10.100.0.1
4. Device placement
1. PC: place behind the router (where the port-forward rule points).
2. Game console: place on the Wireless AP (so it can use chat and extra services over WPA2 PSK).
3. Firewall: place in front of the screened subnet (with its 10.100.0.1 IP facing that subnet).
The Windows PC is placed in the screened subnet (behind the firewall) for enhanced security.
Remote access to this PC requires port forwarding of TCP port 3389 (RDP), which is correctly configured through the router.
The Game Console is placed on the Wireless AP LAN, using WPA2 PSK for a secure wireless connection. Game consoles typically use peer-to-peer chat and online services that require open access without firewall restrictions, which is why the console is not placed behind the firewall.
CompTIA A+ 220-1102 Reference Points:
Objective 3.4: Given a scenario, implement best practices associated with data and device security.
Objective 2.4: Given a scenario, use appropriate tools to support and configure network settings.
Study Guide Reference: CompTIA A+ Core 2 guides recommend using screened subnets (a type of DMZ) for systems needing controlled external access, such as remote desktops, while placing gaming and media devices on less restricted networks for full functionality.

## Question: 2

A technician needs to provide remote support for a legacy Linux-based operating system from their Windows laptop. The solution needs to allow the technician to see what the user is doing and provide the ability to interact with the user's session. Which of the following remote access technologies would support the use case?

A. VPN
B. VNC
C. SSH
D. RDP

**Answer: B**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
The correct answer isVNC (Virtual Network Computing). VNC is a graphical desktop-sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It is platform-independent and widely supported on Linux, which makes it ideal for providinginteractive remote support for a Linux-based operating system. It allows the technician not only to view the remote desktop session but also tocontrol it, fulfilling the need to see and interact with the user's session.
A . VPN(Virtual Private Network) creates a secure tunnel to a network but doesnot provide desktop sharing or session controlby itself.
C . SSH(Secure Shell) provides secure command-line access to Unix/Linux systems but does not offergraphical desktop interaction, which is a requirement in this case.
D . RDP(Remote Desktop Protocol) is primarily a Microsoft protocol, and although it can be made to work on Linux, it isnot natively supported on legacy Linux systems, and thusless suitablethan VNC in this scenario.
CompTIA A+ 220-1102 Core 2 Objective Reference:
Objective 1.8 – Given a scenario, use features and tools of the operating system.
Under this objective, candidates are expected to be familiar with remote access technologies, includingRDP, SSH, and VNC, and understand their appropriate uses and limitations on different platforms such as Windows and Linux.

## Question: 3

A technician is attempting to join a workstation to a domain but is receiving an error message stating the domain cannot be found. However, the technician is able to ping the server and access the internet. Given the following information:
IP Address – 192.168.1.210
Subnet Mask – 255.255.255.0
Gateway – 192.168.1.1
DNS1 – 8.8.8.8
DNS2 – 1.1.1.1
Server – 192.168.1.10
Which of the following should the technician do to fix the issue?

A. Change the DNS settings.
B. Assign a static IP address.
C. Configure a subnet mask.
D. Update the default gateway.

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The issue described—"domain cannot be found" despite the ability to ping the server and access the internet—indicates aDNS resolution problem, not a network connectivity issue. The workstation is currently usingpublic DNS servers (8.8.8.8 and 1.1.1.1)whichcannot resolve internal domain names, such as the ones used in Active Directory environments. To resolve this, the technician needs

tochange the DNS settings to point to the internal DNS server, which in most domain setups is thedomain controller itself (likely 192.168.1.10 in this case).

Here’s the breakdown of the incorrect options:

B . Assign a static IP address: The IP is already assigned and functioning; the device can ping and reach the network and internet.

C . Configure a subnet mask: The subnet mask is appropriate for the network range (Class C /24).

D . Update the default gateway: The gateway is valid and allows internet access; this is not the issue.

CompTIA A+ 220-1102 Core 2 Objective Reference:

Objective 1.8 – Given a scenario, use features and tools of the operating system.

Under this objective, candidates must know how to troubleshoot OS-based network configurations, includingproper DNS settings in domain environments.

—

## Question: 4

A network technician notices that most of the company's network switches are now end-of-life and need to be upgraded. Which of the following should the technician do first?

A. Implement the change
B. Approve the change
C. Propose the change
D. Schedule the change

**Answer: C**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The first step in the IT change management process is to identify and propose the change. In this case, the technician notices a need (end-of-life network switches), so the appropriate action is to formally propose a change. This proposal would be documented and submitted for approval before any planning or implementation occurs.

According to the CompTIA A+ 220-1102 objectives under Operational Procedures (Domain 4.0), the change management process follows these typical steps:

Submit a change request (Propose the change)
Review and approval (Approve the change)
Planning and scheduling (Schedule the change)
Implementation
Documentation and review

Therefore, proposing the change is the correct first step in accordance with standard ITIL-based change management practices.

Reference:

CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information management.

Study Guide Section: Change Management Process

==========================

## Question: 5

MFA for a custom web application on a user's smartphone is no longer working. The last time the user remembered it working was before taking a vacation to another country. Which of the following should the technician do first?

A. Verify the date and time settings
B. Apply mobile OS patches
C. Uninstall and reinstall the application
D. Escalate to the website developer

**Answer: A**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multi-Factor Authentication (MFA) apps, especially time-based one-time password (TOTP) apps (e.g., Google Authenticator, Authy), rely on accurate time synchronization between the device and the authentication server. If the user recently traveled internationally, the device may have incorrect date/time settings due to time zone changes or failed synchronization, leading to MFA failure.
The most logical and non-intrusive first step is to verify and correct the date and time settings. This aligns with basic troubleshooting principles—start with the simplest and most likely cause before taking more drastic action.
Reference:
CompTIA A+ 220-1102 Objective 2.6: Given a scenario, apply cybersecurity best practices to secure a workstation.
Study Guide Section: Authentication technologies and MFA troubleshooting
==========================

# Thank You for Trying Our Product