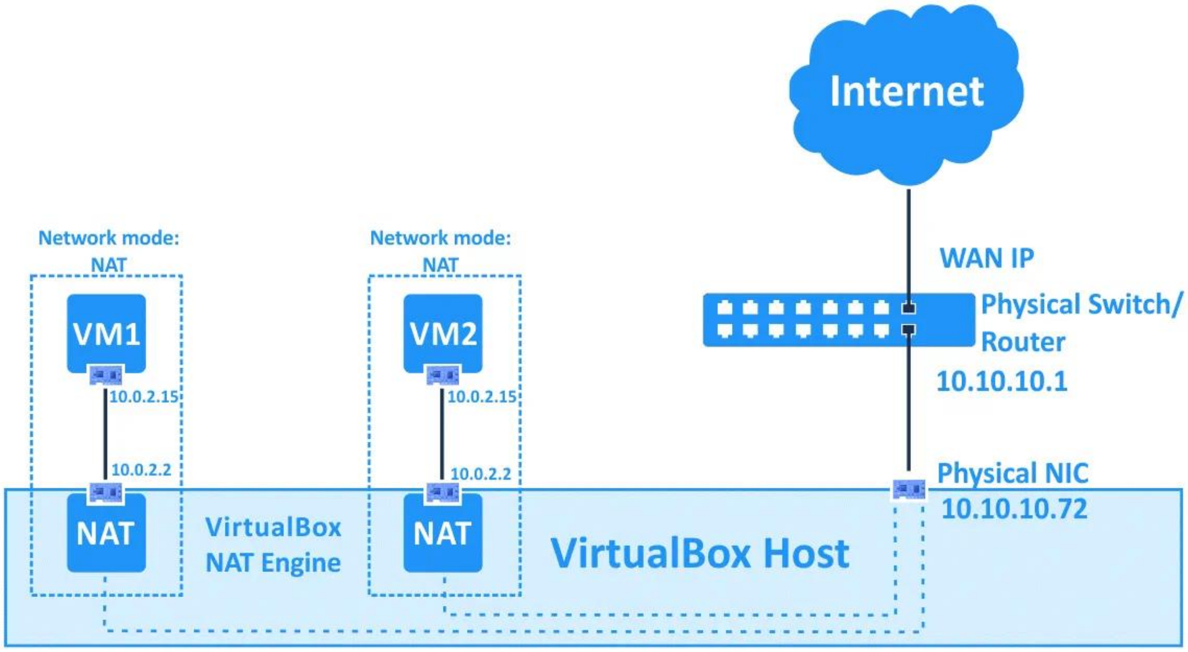
RESEARCH AND EXPLAIN THE DIFFERENT TYPES OF VIRTUALBOX NETWORK CONFIGURATIONS

Aaron Amran Bin Amiruddin

MOSSÉ CYBERSECURITY INSTITUTE
Student ID: nxCLnZGLgyOUMpnDw16rtDvYuTF2

Types of VirtualBox Network Configurations

NAT

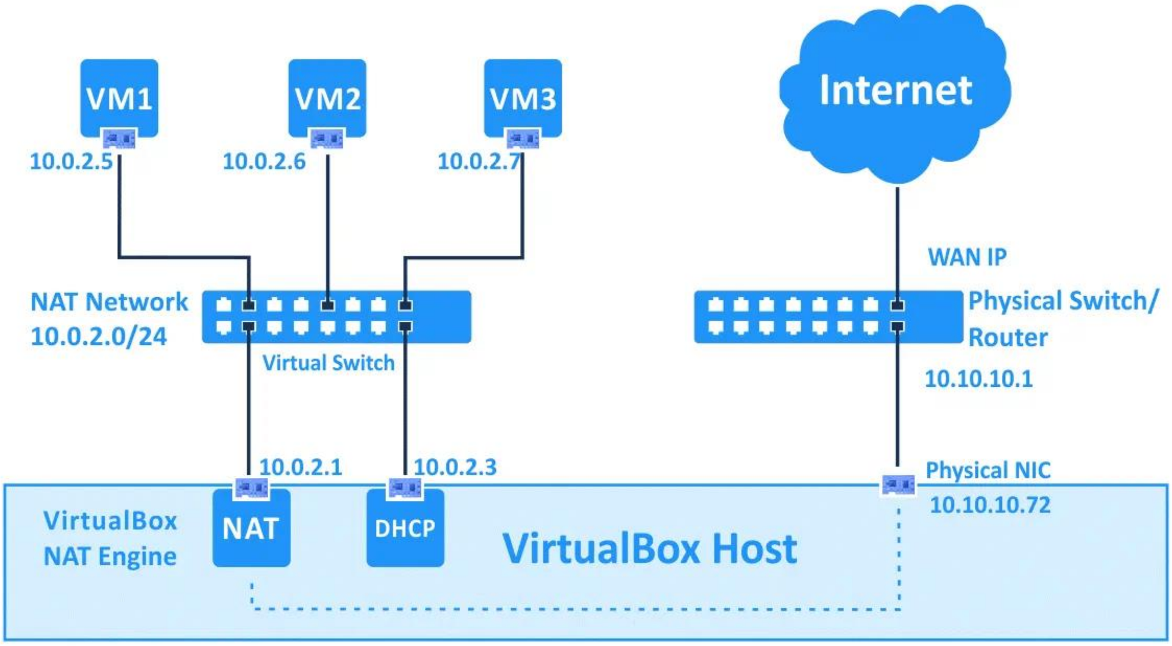


NAT (Network Address Translation) is a technique that allows a virtual machine (VM) to access external networks, such as the internet. It works by mapping multiple private IP addresses from a local network to a single public IP address, enabling communication with the outside world. In VirtualBox, this functionality is provided by the Oracle VM VirtualBox networking engine, which acts as a virtual router. This virtual router facilitates connectivity between the VMs and the host machine, emulating the behavior of a physical device accessing the internet through a traditional router.

NAT is typically used in environments where VM needs internet access without requiring any complex network configurations. NAT is used when quick setup of multiple virtual machines is needed.

Using NAT would increase security because by default, the VMs cannot communicate with each other due to a layer of separation. Despite the increased security, NAT has no direct VM-to-VM communication, unless port forwarding or host-only adapters are configured. It also causes restricted inbound access because it makes the services running on the VM not accessible from outside without port forwarding, which makes it unsuitable for running a server.

NAT Network



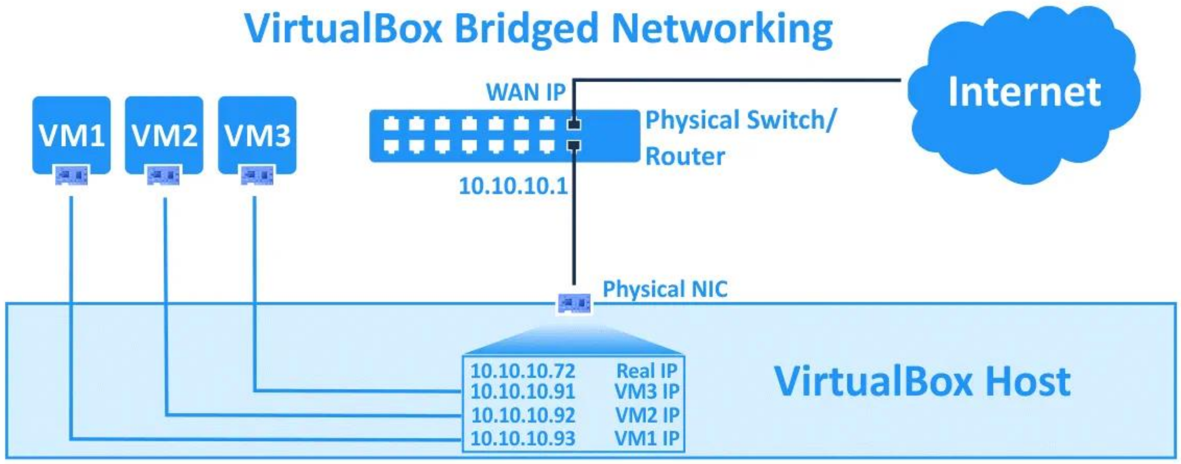
The NAT Network mode in virtualization is similar to configuring a router for home networking. When using NAT Network mode, multiple virtual machines (VMs) can communicate with each other through a private network. These VMs can also access other devices on the physical network, as well as external networks like the internet. However, external systems—whether on the physical network or the internet—cannot directly access VMs configured to use NAT Network mode. This behaviour mirrors how a router isolates devices on a home network while providing them internet access.

It’s important to note that in NAT Network mode, the host machine cannot access guest machines directly unless port forwarding is explicitly configured in the global VirtualBox network settings. The built-in VirtualBox NAT router uses the physical network interface controller (NIC) of the host machine as its external interface, much like traditional NAT mode.

NAT Network mode offers several benefits, particularly in scenarios requiring secure and isolated environments for virtual machines (VMs). This mode ensures that VMs are shielded from unauthorised access originating from external networks or the physical network, thereby enhancing security. Additionally, it allows seamless communication between VMs connected to the same NAT network, facilitating collaboration and shared services. Another advantage is that it provides VMs with internet access and connectivity to external networks without the need for complicated configurations, making it a convenient choice for many use cases.

Despite its advantages, NAT Network mode has certain limitations that may impact its usability in advanced scenarios. One drawback is the restricted connectivity between the host machine and guest VMs; the host cannot directly access the VMs unless port forwarding is manually configured. Moreover, devices on external networks or the physical network cannot communicate directly with the VMs, limiting external accessibility. For tasks such as running a server on a VM that needs to be accessible from the host or other devices, the additional complexity of configuring port forwarding can pose challenges, especially for users requiring straightforward or flexible network setups.

Bridged Adapter



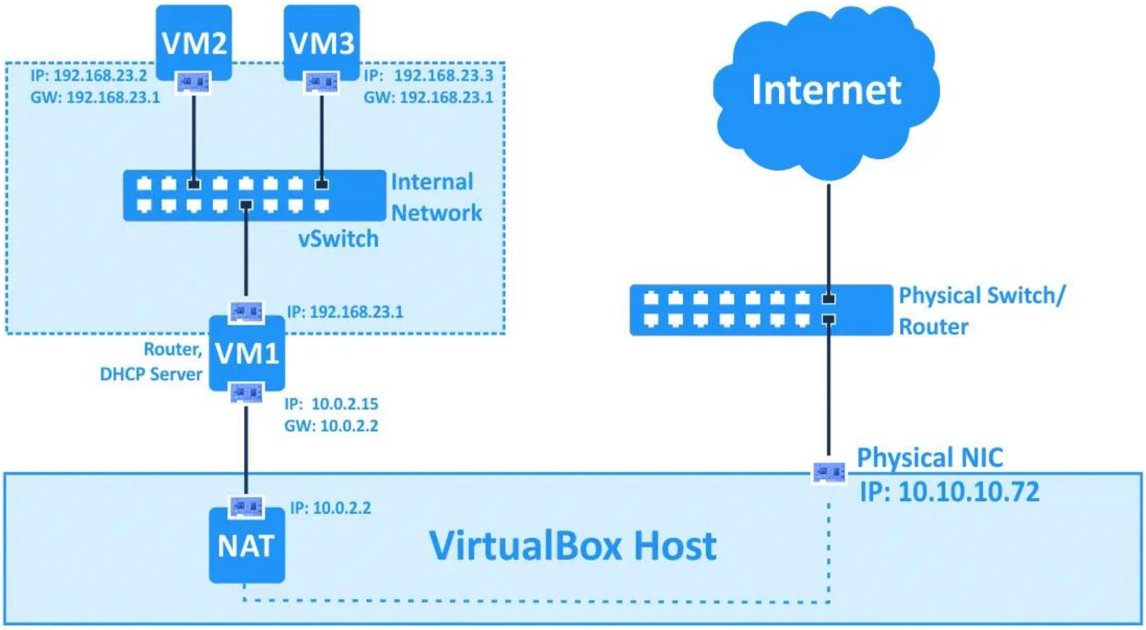
The Bridged network mode in VirtualBox allows a virtual machine (VM) to connect directly to the same physical network as the host machine. The virtual network adapter of the VM leverages the host's physical network interface for network connectivity, with packets sent and received directly by the VM's network adapter without additional routing. VirtualBox uses a special network filter driver to enable this direct communication by filtering data from the physical network adapter on the host.

This mode is particularly useful for running servers on VMs that need to be fully accessible from the physical local area network (LAN). When configured in Bridged mode, VMs can communicate with the host machine, other devices on the physical network, and external networks, including the internet. Additionally, the VM can be accessed by the host and by other devices on the same physical network. For environments with multiple physical network adapters on the host machine (such as Ethernet and Wi-Fi), users must manually select the desired adapter in the VirtualBox network settings. It is important to note that using a Wi-Fi adapter in Bridged mode limits certain features, such as selecting or managing Wi-Fi networks directly from the VM or enabling low-level modes like monitor mode. These tasks must be performed on the host machine. In Bridged mode, the VM's virtual network adapter can obtain an IP address from the same subnet as the host machine. If a DHCP server is present in the network, the VM's adapter will automatically acquire an IP address, provided the guest OS is set to obtain one automatically. The default gateway for the VM will match that of the host machine, ensuring seamless integration into the network.

Bridged mode offers the highest level of integration with physical networks, making it ideal for running network services or servers on a VM that need to be accessible by other devices on the LAN. It allows for full two-way communication between the VM, host, and physical network, providing flexibility for both testing and production environments. The mode also eliminates the need for complex routing configurations, as the VM operates as if it were another device on the network.

Despite its benefits, Bridged mode comes with some limitations. For example, using a Wi-Fi adapter in Bridged mode restricts low-level Wi-Fi features, which can hinder certain testing or monitoring tasks. Additionally, configuring the correct network adapter in systems with multiple physical adapters can be cumbersome. Bridged mode also exposes VMs to the physical network, which could increase their vulnerability to network attacks if proper security measures are not in place.

Internal Network



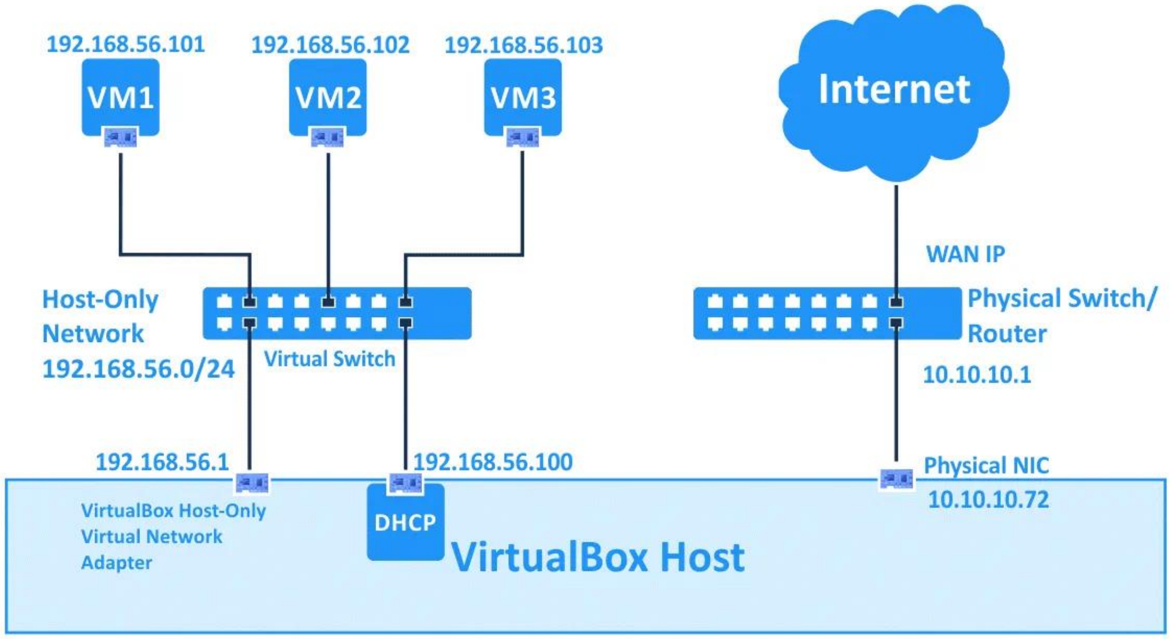
VirtualBox’s Internal Network mode connects virtual machines (VMs) to an isolated virtual network, allowing them to communicate exclusively with each other. VMs configured in this mode cannot interact with the VirtualBox host machine, any physical network, or external networks. Similarly, they are not accessible from the host or other devices. This isolation makes the VirtualBox internal network a useful tool for modelling real-world networks in a controlled, virtual environment.

For example, you can configure three VMs with their first virtual network adapter (Adapter 1) connected to the internal network, assigning IP addresses manually from a defined subnet. One of these VMs (VM1) could be configured with an additional virtual network adapter operating in NAT mode. VM1, acting as a router, can facilitate internet access for other VMs (e.g., VM2 and VM3) connected only to the internal network by setting the IP address of VM1's internal network adapter as the default gateway in the network settings of VM2 and VM3. For routing purposes, Linux with IPTABLES is often recommended for robust configurations, but simpler solutions can be used for VirtualBox testing.

The Internal Network mode is highly useful for testing and simulating isolated network environments. It allows VMs to communicate with each other while remaining disconnected from external networks, enhancing security and reducing risk. This mode is particularly beneficial for scenarios like testing network configurations, developing custom routing setups, or conducting penetration tests in a sandboxed environment.

The primary limitation of this mode is its lack of connectivity with the host machine or external networks, which may complicate setups requiring broader communication. Any external access for VMs within this mode requires additional configuration, such as creating a VM-based router. Manually assigning IP addresses can also introduce complexity, particularly for users unfamiliar with networking concepts, making setup more challenging compared to other modes like NAT. Internal Network mode is ideal for advanced network simulation and testing, though its isolated nature and manual configuration requirements may not suit simpler or more general use cases.

Host-Only Adapter



Host-Only network mode in VirtualBox facilitates communication between the host machine and virtual machines (VMs). In this configuration, VMs connected to the host-only network can interact with each other as well as with the host machine. The host machine also has full access to all VMs on the host-only network, making it a suitable option for scenarios requiring direct communication between the host and VMs.

Virtual network adapters in Host-Only mode do not include a gateway in their IP configuration, as this mode does not allow connectivity to devices or networks outside the host-only environment. For added flexibility, multiple host-only network adapters can be created to establish different isolated networks. This can be achieved by pressing the **Create** button in VirtualBox. Unused host-only network adapters can be easily removed by selecting them and clicking the **Remove** button.

Host-Only mode provides a secure, isolated environment for communication between the host and VMs. This mode is particularly useful for testing applications or services that require direct interaction between the host and VMs without involving external networks. It also offers flexibility in network segmentation by allowing the creation of multiple host-only networks, enabling users to organise VMs into distinct, isolated groups.

The primary limitation of Host-Only mode is its restricted connectivity. Since VMs in this mode lack a gateway, they cannot access external networks, including the internet, which can hinder scenarios requiring external communication or software updates. Additionally, users seeking broader network interaction must reconfigure the VM network settings, making it less versatile compared to other modes like NAT or Bridged.

Host-Only mode is ideal for isolated testing and development tasks that prioritise secure, host-focused connectivity. However, its limited external access may require supplemental configurations for more comprehensive networking needs.

Generic Driver

The Generic Driver mode in VirtualBox allows users to share a generic network interface by selecting a suitable driver. This driver can either be distributed via an extension pack or included within VirtualBox itself, depending on the configuration. Generic Driver mode supports two sub-modes: UDP Tunnel and VDE (Virtual Distributed Ethernet) Networking, each catering to specific use cases.

In **UDP Tunnel mode**, virtual machines running on separate hosts can communicate seamlessly over an existing network infrastructure, enabling cross-host VM communication without complex configurations. In contrast, **VDE Networking** allows virtual machines to connect to a virtual distributed switch on Linux or FreeBSD hosts. However, this feature requires VirtualBox to be compiled from source, as it is not included in standard VirtualBox packages.

This mode provides significant flexibility by enabling advanced networking scenarios. UDP Tunnel mode simplifies cross-host VM communication, making it ideal for distributed virtual environments. VDE Networking further extends capabilities by integrating with virtual distributed switches, allowing users to create sophisticated virtual network architectures on Linux or FreeBSD hosts. These features make Generic Driver mode particularly useful for developers and network engineers requiring custom solutions.

While versatile, Generic Driver mode comes with certain limitations. Configuring and managing this mode can be complex, especially for users unfamiliar with network virtualization. UDP Tunnel mode relies on the existing network infrastructure, which may introduce performance or security concerns in shared environments. Additionally, VDE Networking requires compiling VirtualBox from source, adding a layer of complexity and making it less accessible for users relying on prebuilt VirtualBox packages. Generic Driver mode is a powerful feature for advanced networking needs, but its steep learning curve and setup requirements may deter users seeking simpler solutions.

Cloud Network

Cloud Network mode in VirtualBox is designed to connect virtual machines (VMs) to external cloud-based networks. This feature allows VMs to access cloud services or infrastructure seamlessly by leveraging VirtualBox’s integration with specific cloud providers, such as Oracle Cloud Infrastructure (OCI). Through this mode, VMs can communicate with cloud-based resources and other VMs or systems hosted in the same cloud network, offering a flexible solution for hybrid environments or cloud-based development.

To use this mode, the user must configure VirtualBox to connect the VM’s network adapter to the cloud network. The configuration is straightforward, especially for Oracle Cloud, where VirtualBox provides tools to simplify the process. Once connected, VMs can function as if they are part of the cloud network, enabling scenarios like hosting cloud-accessible services or interacting with distributed systems deployed in the cloud.

Cloud Network mode is highly useful for users working in hybrid cloud setups or those who need seamless interaction between local VMs and cloud-hosted resources. It simplifies the development and testing of cloud-native applications by enabling direct access to cloud networks without additional network bridging or tunneling configurations. For teams collaborating across different environments, this mode ensures VMs are easily accessible within the cloud infrastructure, fostering better integration with modern development pipelines. Additionally, for organizations using

Oracle Cloud or similar supported platforms, this mode offers an efficient way to extend local virtualized environments into the cloud. It minimizes setup time while providing a flexible platform for scaling workloads or testing deployments in realistic cloud-based environments.

The reliance on specific cloud providers can be a limitation, as this mode works best with services like Oracle Cloud. Users relying on other platforms may need additional configurations or might not have the same level of support. Moreover, since this mode connects VMs to cloud environments, it could introduce costs associated with cloud usage, such as data transfer fees or virtual network expenses, which need to be monitored. Another consideration is security. While cloud providers offer robust security features, the user must ensure that VMs connected to the cloud are adequately secured to prevent unauthorized access. Misconfigurations in cloud networking settings could expose local resources to potential threats. Cloud Network mode is an excellent option for developers and organizations leveraging cloud infrastructures for their workloads, offering a bridge between local virtualization and the cloud. However, its dependency on specific providers and potential cost implications require careful planning.

Not Attached

The "Not Attached" networking configuration simulates the disconnection of an Ethernet network cable when using a physical network adapter. This mode is commonly used for testing scenarios such as verifying how a DHCP client reacquires an IP address after disconnection or assessing whether an application can resume downloading correctly after a link interruption or packet loss.

The advantages of this mode is it gives users the ability to test resilience, for example, how applications and services handle network disruptions. It also provides a controlled environment because it is a safe and predictable way to simulate network disconnection without physically unplugging cables. Repeated testing of scenarios like DHCP address re-acquisition or interrupted downloads without manual intervention is also allowed when using this mode.

On the other hand, the “Not Attached” mode has limited realism because it may not replicate the nuances of physical disconnections or real-world network conditions. Another disadvantage is that if this mode is left enabled accidentally, it could lead to unnecessary troubleshooting.

References

Oracle. (2020). *6.3. Network Address Translation (NAT)*. Retrieved from docs.oracle.com: https://docs.oracle.com/en/virtualization/virtualbox/6.0/user/network_nat.html

Team, N. (2019, July 16). *VirtualBox Network Settings: Complete Guide*. Retrieved from nakivo.com: https://www.nakivo.com/blog/virtualbox-network-setting-guide/