This private internal network provides the connections necessary to monitor and manage the zBX internode. Each node in the ensemble includes as many as five distinct networks, four of which are depicted in the illustration below.

1. **interconnect management network (INN)**
   - The INN provides the necessary connections to monitor and control components of the node, such as virtual servers or physical switches.
   - The INN connects to OA adapters with card bus cards.

2. **virtual LAN (VLAN) network**
   - The VLAN is the network for all internal data exchange, including application data communications within the ensemble.
   - It connects to OA adapters with CHPID type OSX in the zBX BladeCenter.
   - This network connects all nodes, including z196 and zBX frames, together. It is the network that will be virtualized for the use of the virtual servers in the ensemble.

3. **customer management network**
   - Also known as the OAM, the OAM provides a high-speed communication link between Hardware Management Consoles (HMCs) and the nodes. It connects to OA adapters with card bus cards.

4. **physical network**
   - This network is the physical network for the virtual data communication network.
   - It is attached to Open Systems Adapters (OSAs) such as OSA-DS, in the z196 node, just as it has been attached to previous System z machines. In addition, this network may optionally be connected directly to the IDEN, depending on your configuration requirements.

- The IDEN is the network used for application communications within an ensemble.
  - It exists only within an ensemble, although it might also have a connection to the customer data network.
  - It is implemented as a flat layer-2 network, which means that all the network interfaces can communicate directly with each other as if they were all connected to a single network switch.
  - No routers are necessary to communicate across the IDEN.
  - While there are physical network switches that are part of the IDEN, the appearance of a single network is maintained through virtualization.
  - The physical construction of the IDEN contributes to the security and reliability of the ensemble.

- In addition to the layer-3 protocol, there are inside the frames the layer-2 switches or routers that provide the option to point-to-point between the frames.
- Data rate limitations are enforced, and rules determine the opportunity to form a layer-2 network throughout the ensemble.
- The switches are managed and configured only from the zEnterprise System firmware.

From a network perspective, it is possible to isolate the virtual servers from the physical definitions of the network interfaces and devices. This allows the virtual servers to be placed anywhere within the ensemble without changing the network definitions and infrastructure.

- It isolates the virtual servers from ‘burned-in’ addresses on physical network interface cards which allows failed servers to be replaced without losing configuration.

- Finally, the formal provisioning process is defined to provide a virtual network interface card (VNIC) that has IPv6 connectivity. This makes it possible to define a complete virtual network infrastructure.

- VLANs are a proven method for separating data traffic for multiple applications, as might be required for privacy rules, regulatory requirements, and even separation of production and test communications. All flowing over the same physical network this virtualization hides the actual physical network capacity while still meeting your organization's security requirements.

- There are four components of the network virtualization of the IDEN:
  - **VLAN (Virtual LAN)** - Each virtual network switch is a hypervisor component providing virtualized network resources to a virtual server. These virtual network interfaces are called VNICs and the VNIC is the network resource that a virtual server can use to access the IDEN. A name and a numeric VNIC identifier are required to define a VNIC.
  - **VSWITCH (Virtual Switch)** - The virtual switch is a hypervisor component that provides virtual network connectivity to a virtual server. The VSWITCH can connect to multiple VLANs simultaneously.

- The combination of the VLAN and VSWITCH allows the virtual server to have its own virtual MAC address.

- The virtual network is shared by all members of the ensemble.

This virtual network is shared by all members of the ensemble, and it is accessible to all members of the ensemble. At this level of the data path, the virtual servers can connect to the physical NIC (which has a virtual MAC address).

All this virtual data is managed by the ensemble management firmware cooperating with the hypervisors.

- The operating systems running in the virtual servers see the VNIC as a real network interface into a real network.
- They don’t need to be aware of the virtualization, but are able to utilize the virtualized resources.
- Virtualized components contain the VSWITCH definitions and VNICs that are contained in the VSWITCH.
- There is no IP address associated with the virtual server.

Connecting to the existing customer data network to the IDEN

- The factory TAP (Test Access Port) adapter is responsible for establishing a physical connection to the existing customer network data to the IDEN.
- The physical connection to the INM (aka the OAM) is established through the BladeCenter channel interface and the BladeCenter B2I port.
- The BladeCenter B2I port is connected to a zBX BladeCenter Hub. The BladeCenter Hub is connected to the zBX Bulk Power Hub.

- The initial TAP adapter is assigned a TAP ID 0x01 (for the zBX Bulk Power Hub). This TAP ID is connected to a zBX BladeCenter Hub (and then to a zBX BladeCenter).
- The connection to the zBX Bulk Power Hub is identified in the serial console to the BladeCenter.

- Each virtual server is assigned an IP address and then connected to the internal network of the ensemble.

* The virtual servers need IP addresses assigned just as they would as real servers on a real network.
* The IP addressing scheme is not defined in the network virtualization because it is a layer-3 function, which is built on top of the layer-2 structure and is the client’s responsibility to choose an IP addressing scheme appropriate for each of the VLANs on the IDEN.
* Either IPv4 or IPv6 (preferred) addressing can be used, depending on the OS capability of the virtual servers.