FSMO (OPERATIONS MASTER ROLES)

In a forest, there are five FSMO roles that are assigned to one or more domain controllers. The five FSMO roles are:

Schema Master:

The schema master domain controller controls all updates and modifications to the schema. Once the Schema update is complete, it is replicated from the schema master to all other DCs in the directory. To update the schema of a forest, you must have access to the schema master. There can be only one schema master in the whole forest.

Domain naming master:

The domain naming master domain controller controls the addition or removal of domains in the forest. This DC is the only one that can add or remove a domain from the directory. It can also add or remove cross references to domains in external directories. There can be only one domain naming master in the whole forest.

Infrastructure Master:

When an object in one domain is referenced by another object in another domain, it represents the reference by the GUID, the SID (for references to security principals), and the DN of the object being referenced. The infrastructure FSMO role holder is the DC responsible for updating an object's SID and distinguished name in a cross-domain object reference. At any one time, there can be only one domain controller acting as the infrastructure master in each domain.

Note: The Infrastructure Master (IM) role should be held by a domain controller that is not a Global Catalog server (GC). If the Infrastructure Master runs on a Global Catalog server it will stop updating object information because it does not contain any references to objects that it does not hold. This is because a Global Catalog server holds a partial replica of every object in the forest. As a result, cross-domain object references in that domain will not be updated and a warning to that effect will be logged on that DC's event log. If all the domain controllers in a domain also host the global catalog, all the domain controllers have the current data, and it is not important which domain controller holds the infrastructure master role.

Relative ID (RID) Master:

The RID master is responsible for processing RID pool requests from all domain controllers in a particular domain. When a DC creates a security principal object such as a user or group, it attaches a unique Security ID (SID) to the object. This SID consists of a domain SID (the same for all SIDs created in a domain), and a relative ID (RID) that is unique for each security principal SID created in a domain. Each DC in a domain is allocated a pool of RIDs that it is allowed to assign to the security principals it creates. When a DC's allocated RID pool falls below a threshold, that DC issues a request for additional RIDs to the domain's RID master. The domain RID master responds to the request by retrieving RIDs from the domain's unallocated

RID pool and assigns them to the pool of the requesting DC. At any one time, there can be only one domain controller acting as the RID master in the domain.

PDC Emulator:

The PDC emulator is necessary to synchronize time in an enterprise. Windows 2000/2003 includes the W32Time (Windows Time) time service that is required by the Kerberos authentication protocol. All Windows 2000/2003-based computers within an enterprise use a common time. The purpose of the time service is to ensure that the Windows Time service uses a hierarchical relationship that controls authority and does not permit loops to ensure appropriate common time usage.

The PDC emulator of a domain is authoritative for the domain. The PDC emulator at the root of the forest becomes authoritative for the enterprise, and should be configured to gather the time from an external source. All PDC FSMO role holders follow the hierarchy of domains in the selection of their in-bound time partner.

In a Windows 2000/2003 domain, the PDC emulator role holder retains the following functions:

- Password changes performed by other DCs in the domain are replicated preferentially to the PDC emulator.
- Authentication failures that occur at a given DC in a domain because of an incorrect password are forwarded to the PDC emulator before a bad password failure message is reported to the user.
- Account lockout is processed on the PDC emulator.
- Editing or creation of Group Policy Objects (GPO) is always done from the GPO copy found in the PDC Emulator's SYSVOL share, unless configured not to do so by the administrator.
- The PDC emulator performs all of the functionality that a Microsoft Windows NT 4.0 Server-based PDC or earlier PDC performs for Windows NT 4.0-based or earlier clients.

This part of the PDC emulator role becomes unnecessary when all workstations, member servers, and domain controllers that are running Windows NT 4.0 or earlier are all upgraded to Windows 2000/2003. The PDC emulator still performs the other functions as described in a Windows 2000/2003 environment.

At any one time, there can be only one domain controller acting as the PDC emulator master in each domain in the forest.