Welcome to the Domain

Active Directory

- Collection of various software systems used to manage fleets of Windows computers
- LDAP – Lightweight Directory Access Protocol. Contains user and device information
- KERBEROS – Single Sign On
- Group Policy – Manages permissions, settings and a slew of things via “polices”. This is the feature that cemented AD in business

Active Directory

- Has a steep learning curve and we cannot going to cover every aspect today.
- AD is one of the topics VERY much worth exploring further. If you can master AD that is one of the skills that will make you invaluable to a team.

Active Directory

- DNS – On a Windows Domain you MUST AD as the DNS server so the LDAP database can store all the information about you and your computer.
- DHCP – Also, handled by AD so the LDAP database can tract assigned IPs
- File Sharing – Server Message Block (SMB) and Network File Share (NFS)
- Email – Microsoft Exchange Server
- Many other roles

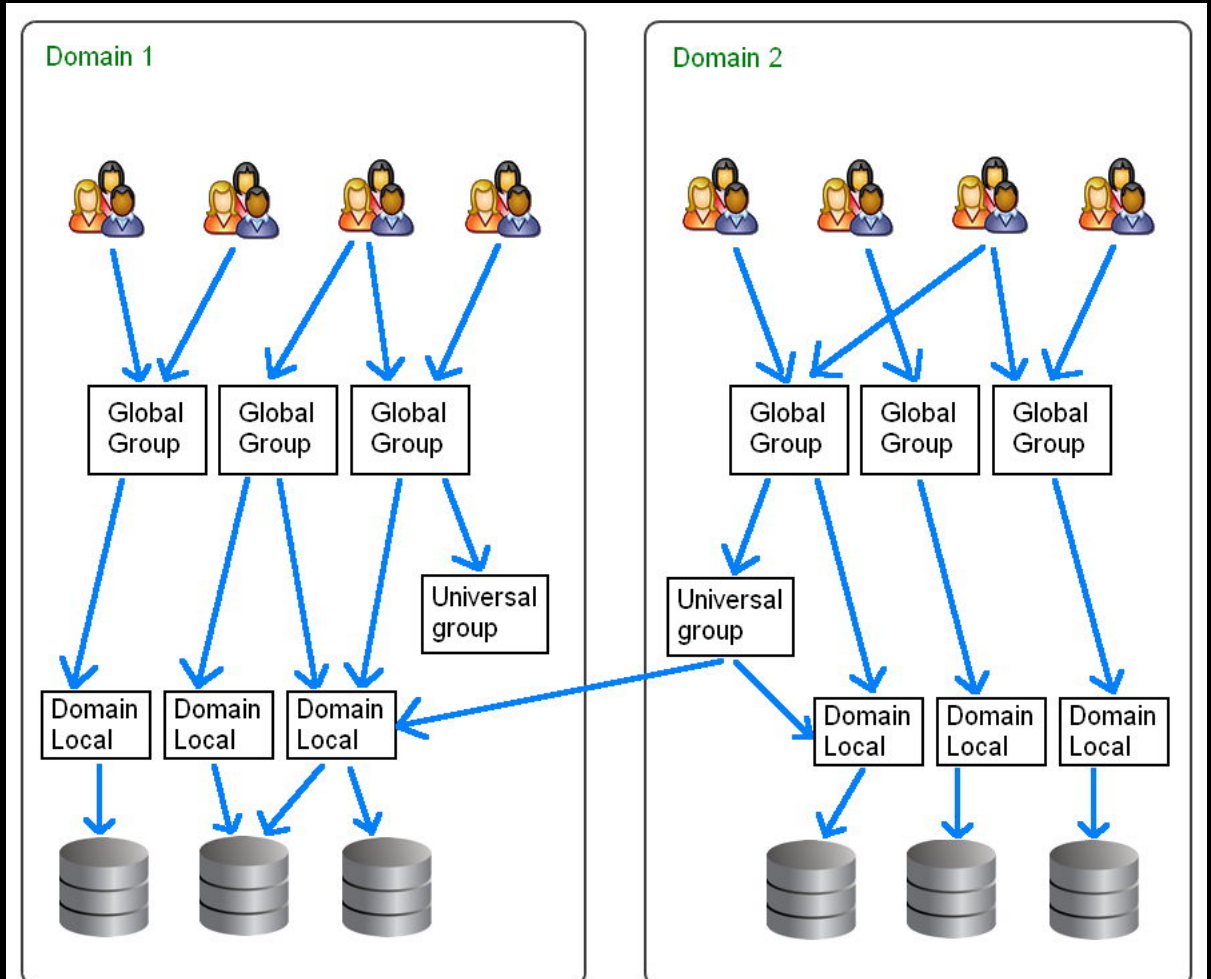
Active Directory Groups

Global Groups and Domain Local Groups only apply within a domain.

Universal Groups apply across domains

Notice no user directly connects to the resources. The groups they belong to inherit permissions and pass them down to the users

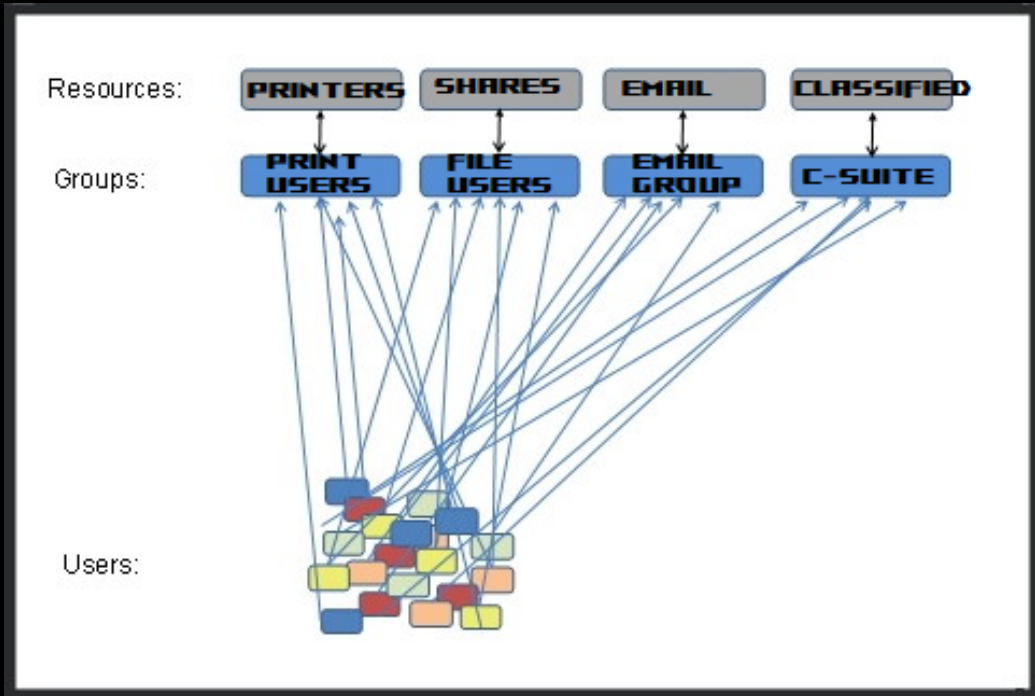
Domains use URI format

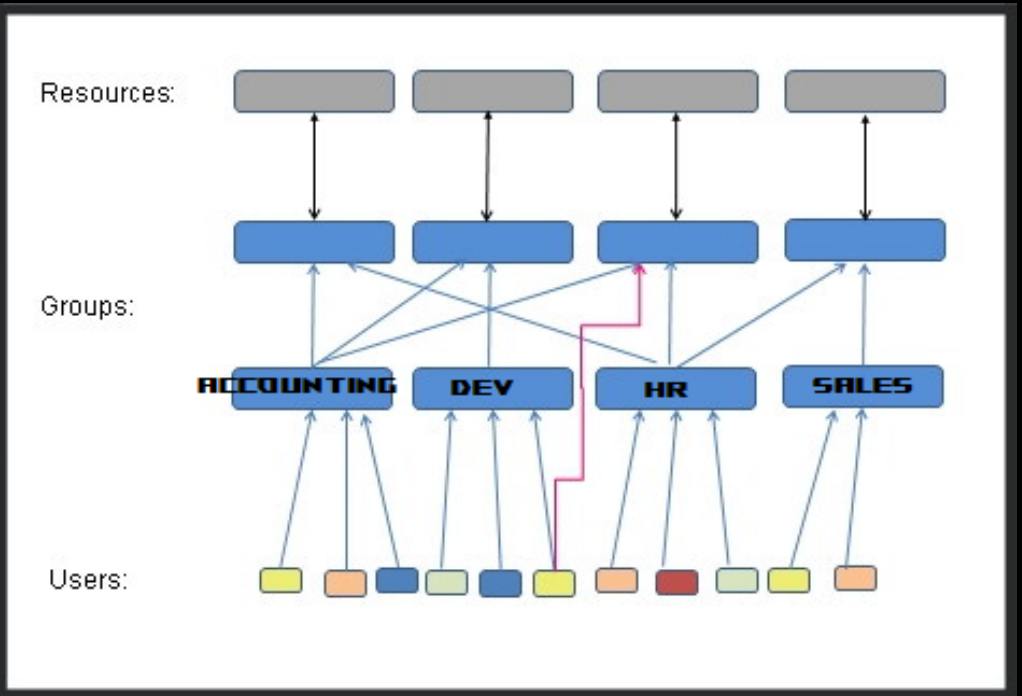


https://ss64.com/nt/syntax-groups.html

Active Directory

Nested Groups





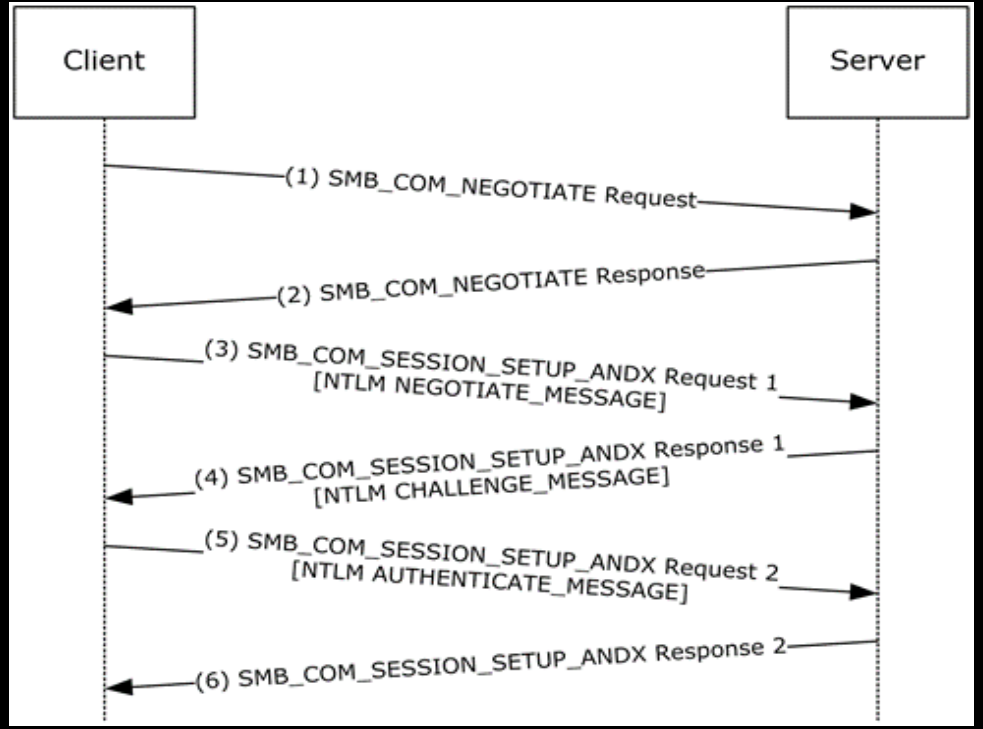
https://ss64.com/nt/syntax-groups.html

Domain vs Workgroup

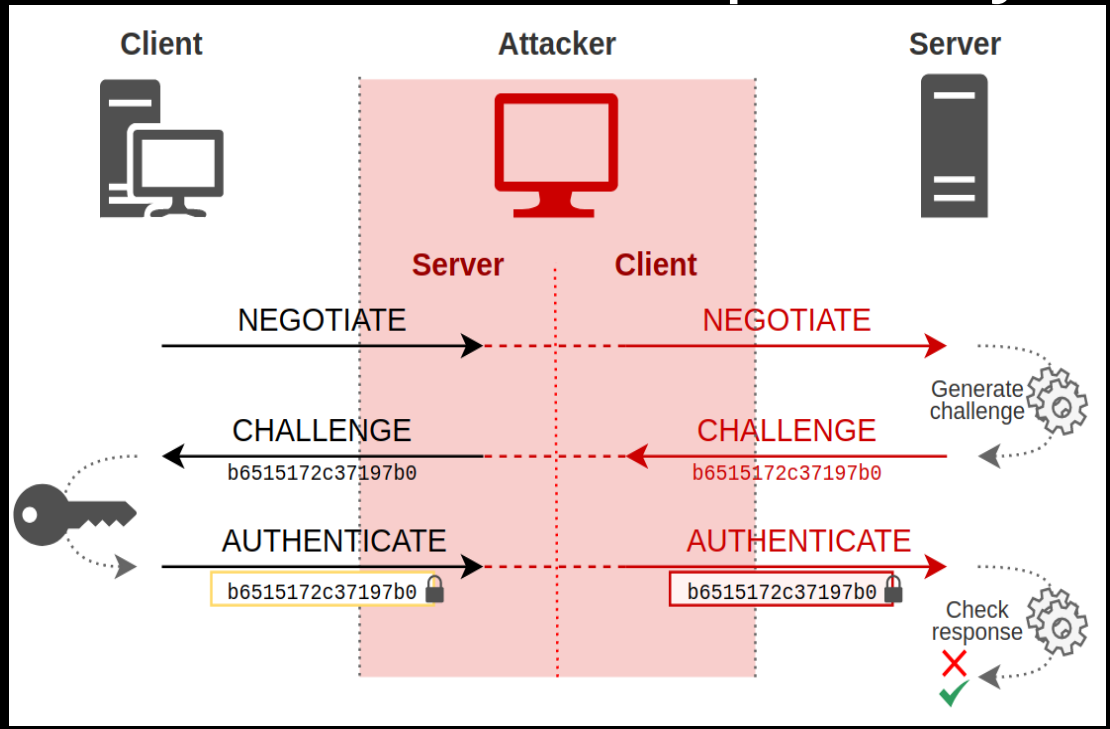
- Domains are managed by a centralized Domain Controller.
- Workgroup are ad-hoc groups of PCs with their own internal set of users and permissions
- Workgroups work ok-ish for a couple computers , but becomes VERY difficult to manage once you get over 10-ish computers

NTLMv2

Obsolete, but included for backwards compatibility

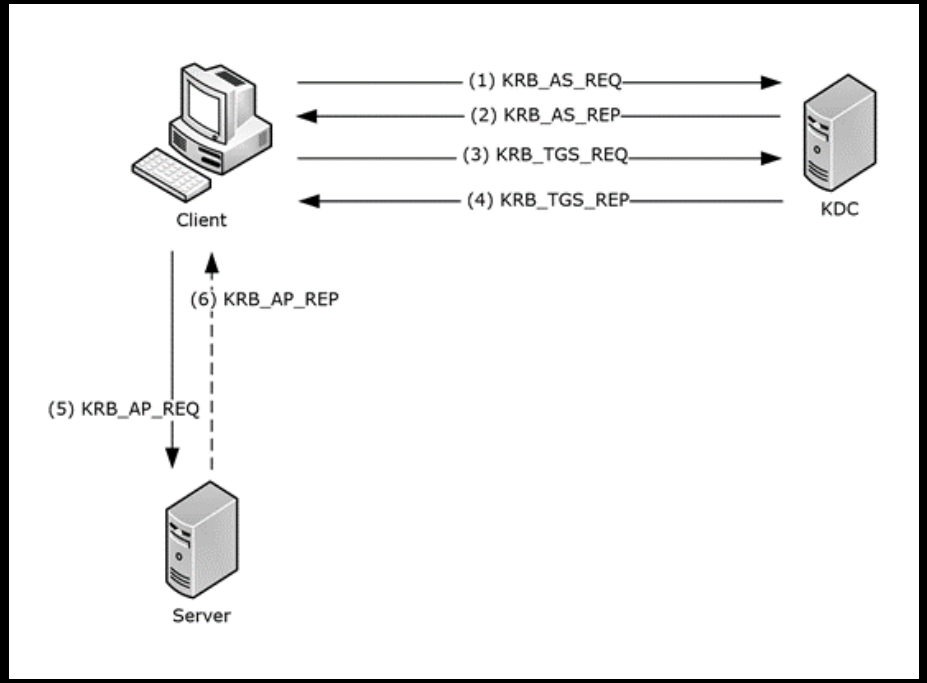


https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-nlmp/c083583f-1a8f-4afe-a742-6ee08ffeb8cf



https://en.hackndo.com/ntlm-relay/

Kerberos



(1) Request ticket-granting ticket (TGT)

(2) Grants TGT and Session Key

(3) Request Authorization for service

(4) Grants Resource Ticket and Session Key

(5) Request Service From Service Server

(6) Service Server Grants access

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/b4af186e-b2ff-43f9-b18e-eedb366abf13

NET Command

- Display a list of local users: net user
- Add a local user: net user <user_name> /add
- Delete a user: net user <user_name> /delete
- Reset a local password: net user <user_name> <password>
- Enable an administrator account: net user administrator /active:yes
- Run a command as an administrator: runas /user:<user_name> <program_name>
- Add a local user to a group: net localgroup <group_name> <user_name> /add
- Delete a local user from a group: net localgroup <group_name> <user_name> /delete
- Create a local group: net localgroup <group_name> /add
- Delete a local group: net localgroup <group_name> /delete