Active Directory

Fundamentals. Configuration. Management

Windows Server

SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Have a Question?

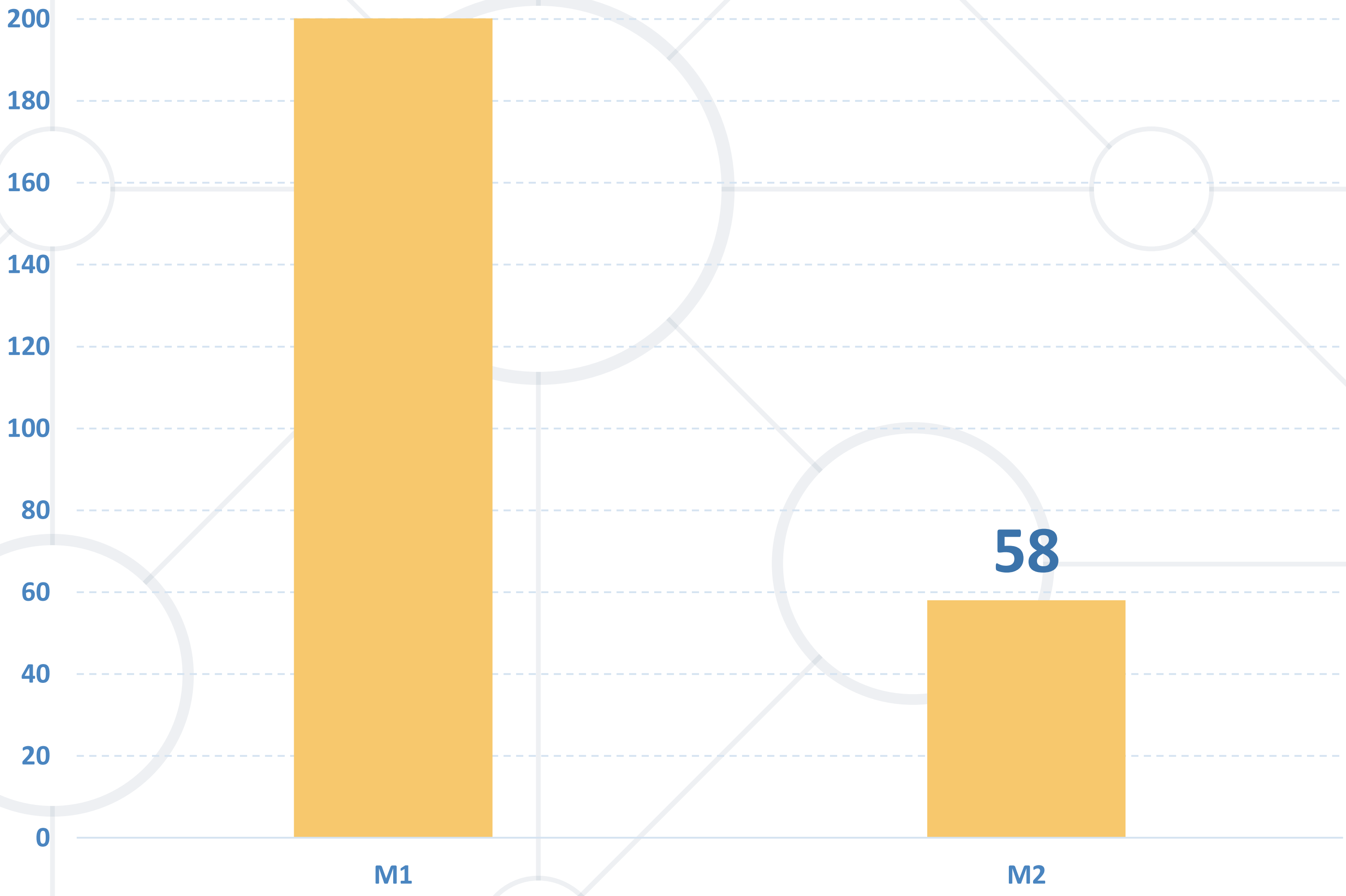
Software University

sli.do

#WSA

facebook.com/groups/
WindowsSystemAdministrationMarch2023/

Homework Progress



Submit M2 until 23:59:59 on 14.04.2023

Submit M3 until 23:59:59 on 21.04.2023

Previous Module (M2)

Quick overview

What We Covered

- Server roles and features
- Software management
- Services management
- Disk management
  - Storage Basics. RAID and Disk Types
  - File Systems. Management Tools
- Basic networking and Firewall

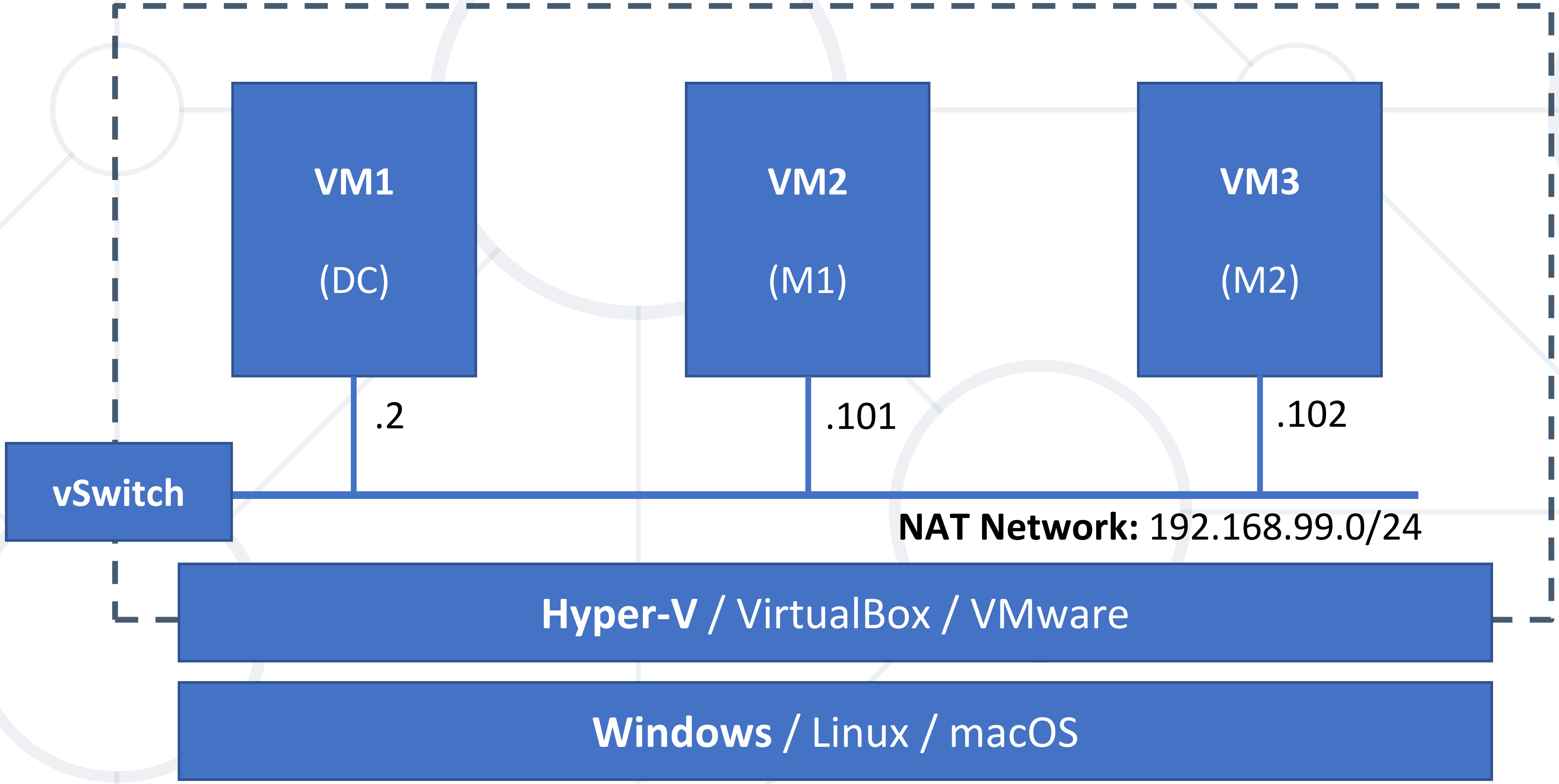
This Module (M3)

Topics

Table of Contents

1. Active Directory Fundamentals
2. Configuring Active Directory
3. Managing Active Directory

Lab Infrastructure



VM1

(DC)

VM2

(M1)

VM3

(M2)

.2

.101

.102

vSwitch

NAT Network: 192.168.99.0/24

Hyper-V / VirtualBox / VMware

Windows / Linux / macOS

Active Directory Structure

Domains. Trees. Forests

Before Active Directory

- **Workgroup**
  - Since 1980s
  - Group of PCs, same group name, shared resources
  - De-centralized
- **Domain**
  - Introduced with Windows NT3.1 in 1993
  - Centralized control through domain controllers
  - Microsoft implementation of centralized directory service

Active Directory

- Introduced with the release of **Windows 2000**
- Active Directory (AD) is Microsoft's network **directory service**
- It is used to create a domain
- Tracks and manages objects (**users**, **groups**, **computers**, …)
- Central repository for **querying**, **updating**, and **authenticating**
- AD infrastructure includes **Domains**, **Domain trees**, and **Forests**

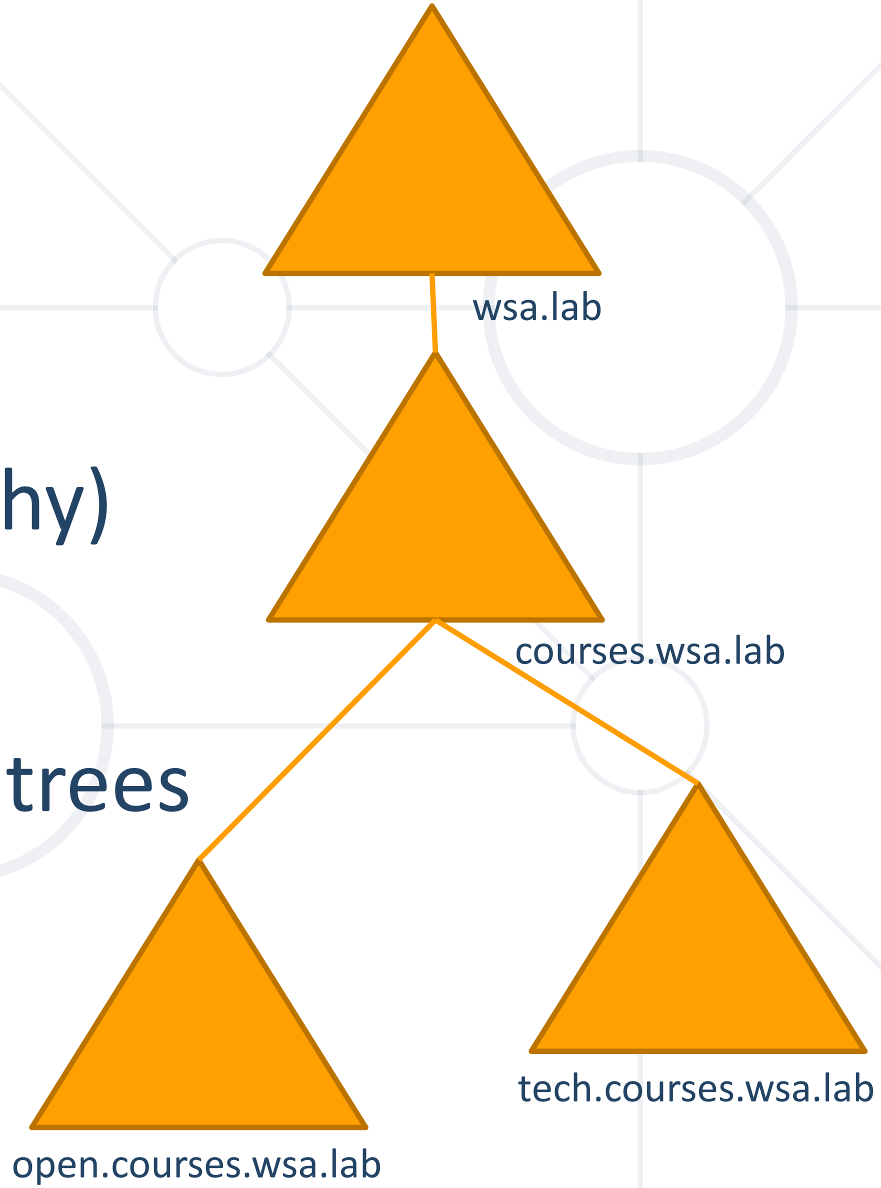
Active Directory Domains

- Could be part of a hierarchy
- Logical administrative container
- Contains objects
  - User accounts
  - Groups
  - Computers
  - Organizational Units
  - Built-in containers

wsa.lab

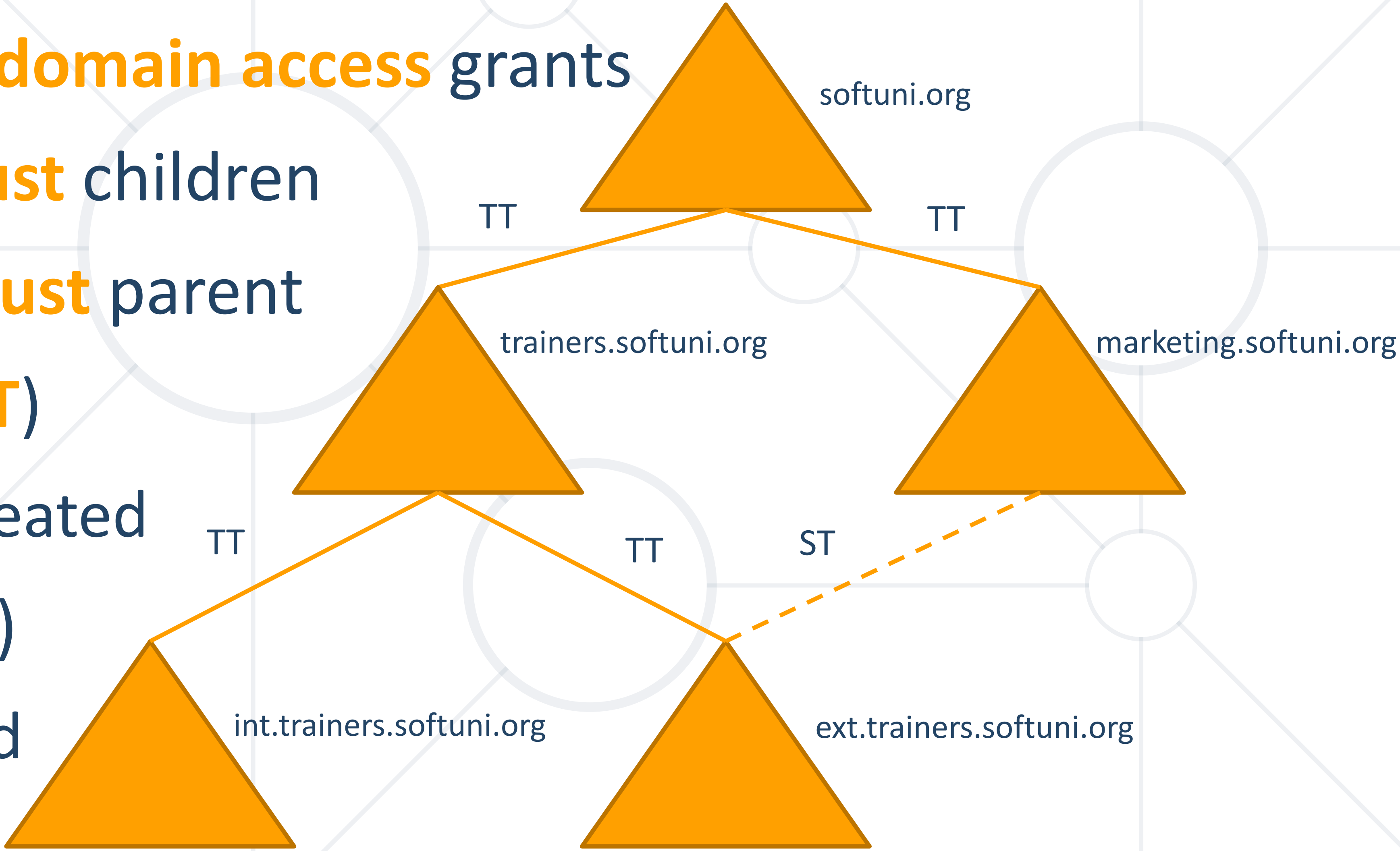
Active Directory Trees

- Group of domains
- Common schema and configuration
- Share same root namespace
- Organizational structure (logical hierarchy)
- Linked through **trusted relationship**
- Active Directory is a set of one or more trees



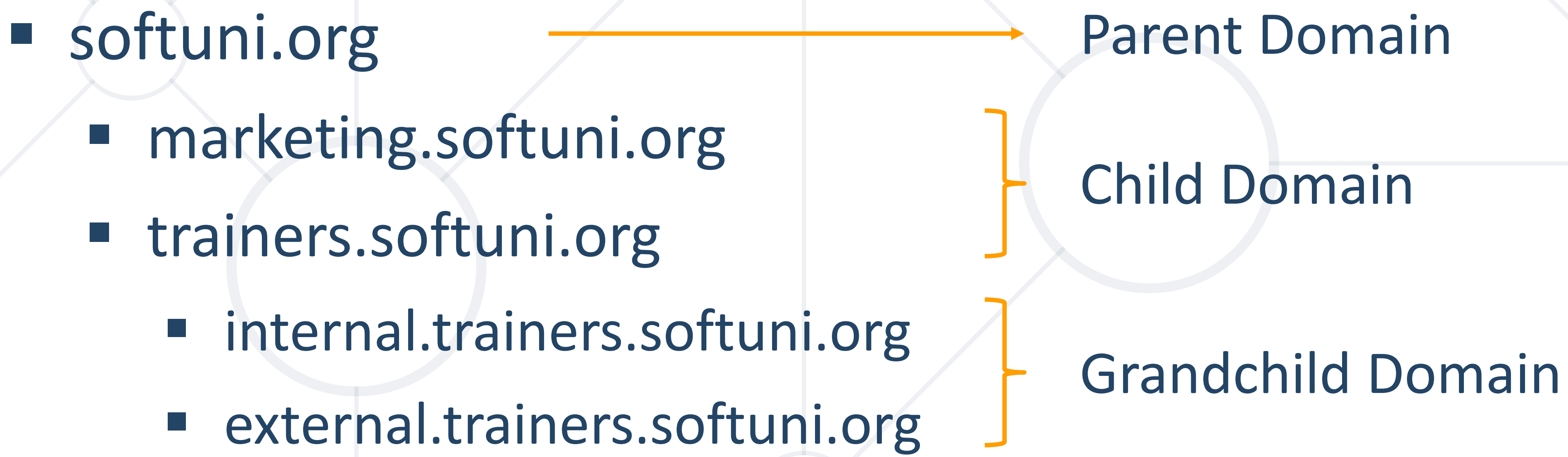
Trust Relationships

- Trust allows **inter-domain access** grants
- Parents **always trust** children
- Children **always trust** parent
- **Transient Trust** (**TT**)
  - Automatically created
- **Shortcut Trust** (**ST**)
  - Manually created



Namespace Hierarchies

- Organization hierarchy in AD can be represented by
  - Single domain and set of **Organizational Units** (OUs)
  - Multiple domains => **namespace hierarchy**
- For example



  - softuni.org
    - marketing.softuni.org
    - trainers.softuni.org
      - internal.trainers.softuni.org
      - external.trainers.softuni.org

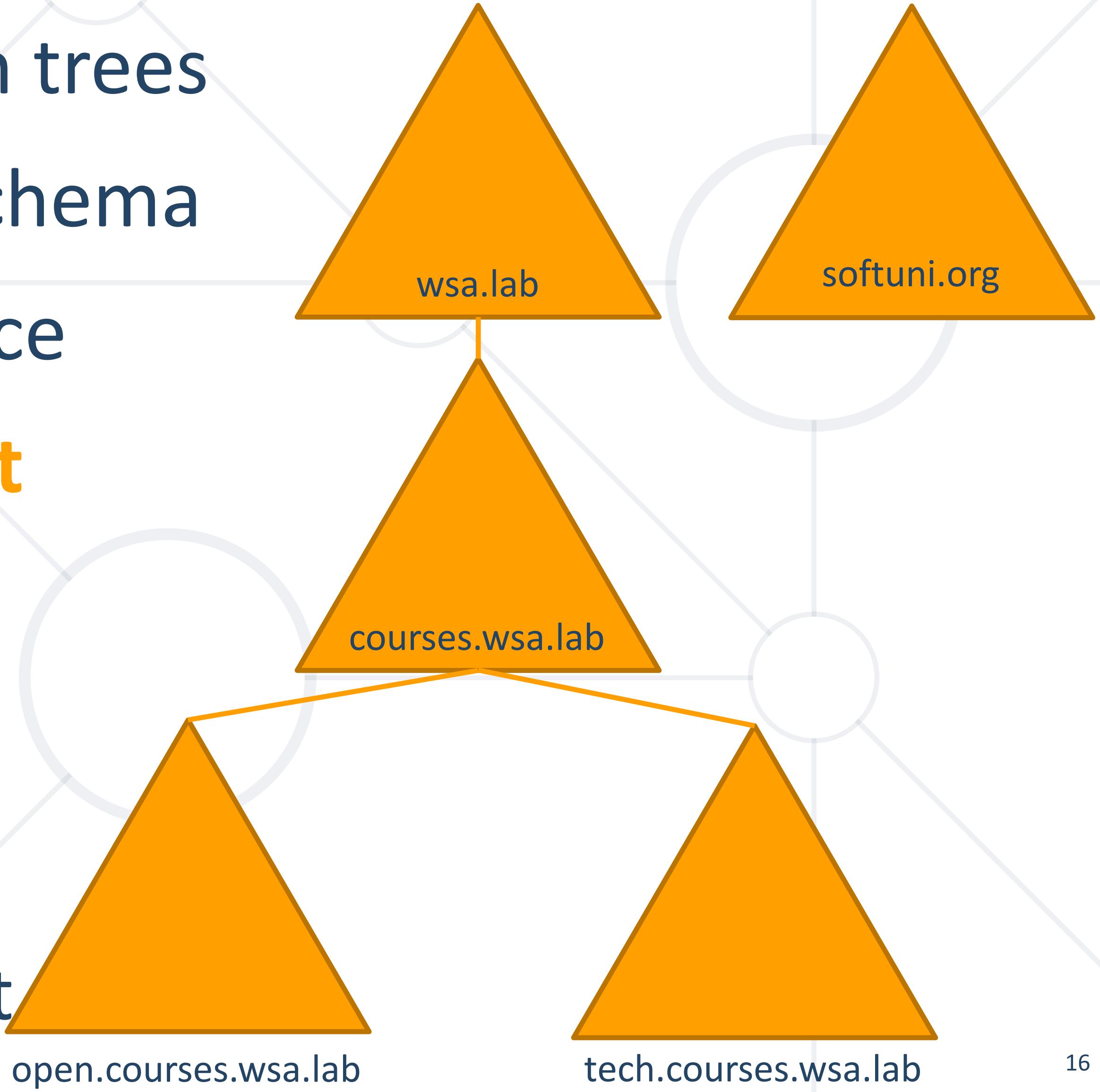
Parent Domain

Child Domain

Grandchild Domain

Active Directory Forests

- Collection of one or more domain trees
- Share same Global Catalog and schema
- Can have common root namespace
- **One domain**, **one tree**, **one forest**
- **Enterprise Admins** group
  - Controls all domains in the forest



Active Directory Structure

Domain Controllers. Supporting Servers

Active Directory Structure

- Logical architecture
  - Domains
  - Domain trees
  - Domain forests
- Physical architecture
  - Servers (domain controllers and supporting servers)
  - Sites

Domain Controllers

- Server that stores and manages a copy of AD database
  - Usually stored in **C:\Windows\NTDS\NTDS.DIT**
- Responsible for
  - User account provisioning
  - Logon processing
  - Resource access processing
  - Database replication

Domain Controller Roles

- **Domain Naming Master**
  - Prevents domains with same name; Single DC/Forest
- **Infrastructure Master**
  - Proper update of group changes; Translation; Single DC/Domain
- **Schema Master**
  - Only DC that can make changes to the schema; Single DC/Forest
- **Primary Domain Controller (PDC) Emulator**
  - Primary password change server; Single DC/Domain
- **Relative ID Master**
  - Assigns pools of RIDs to DCs; Single DC/Domain

Flexible Single Master Operation (FSMO)

Functional Levels*

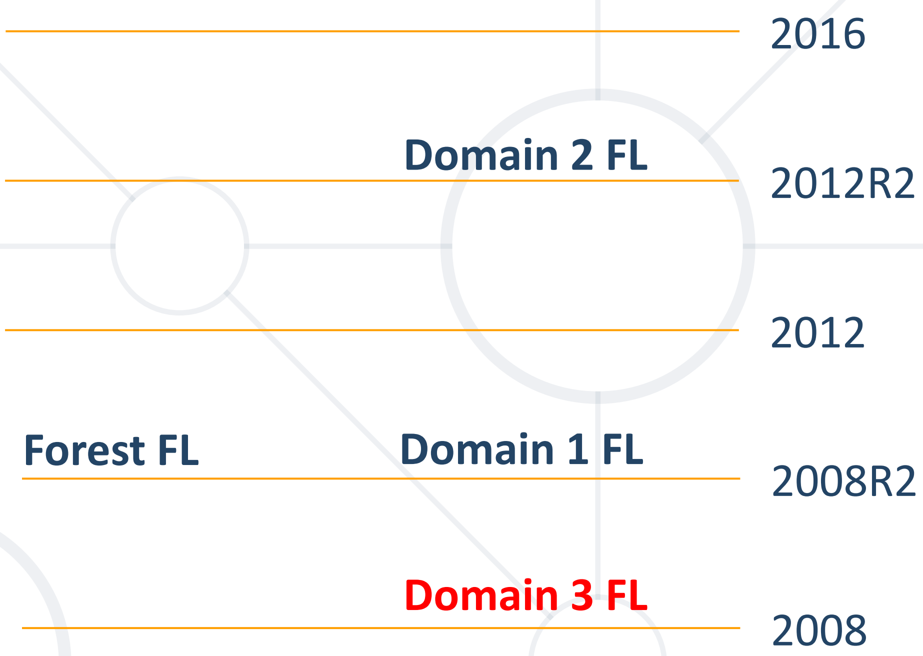
Software University

- **Domain Functional Levels (DFL)**
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - ~~Windows Server 2019~~

No such level

- **Forest Functional Levels (FFL)**

Applies also to forest



2016

Domain 2 FL

2012R2

2012

Forest FL

Domain 1 FL

2008R2

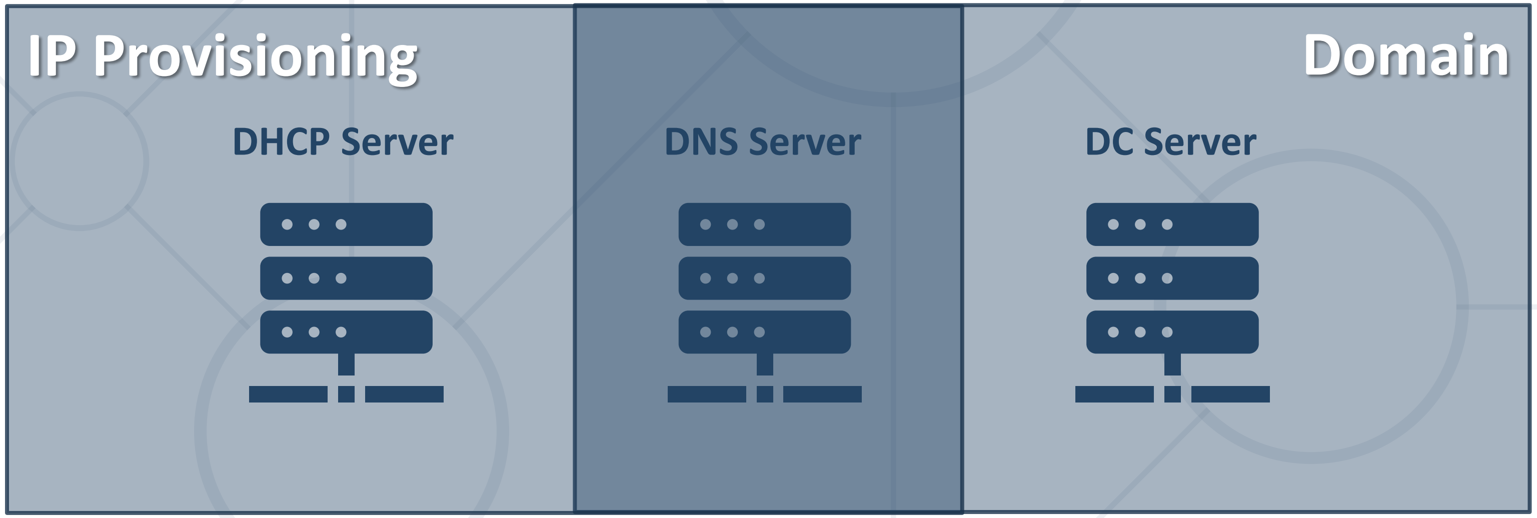
Domain 3 FL

2008

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels

Supporting Servers

- AD depends on
  - Name resolution for the network (DNS)
  - IP configuration for the clients (DHCP*)



- All roles can be installed on a single or multiple servers

Active Directory and DNS

DNS Overview

DNS Overview

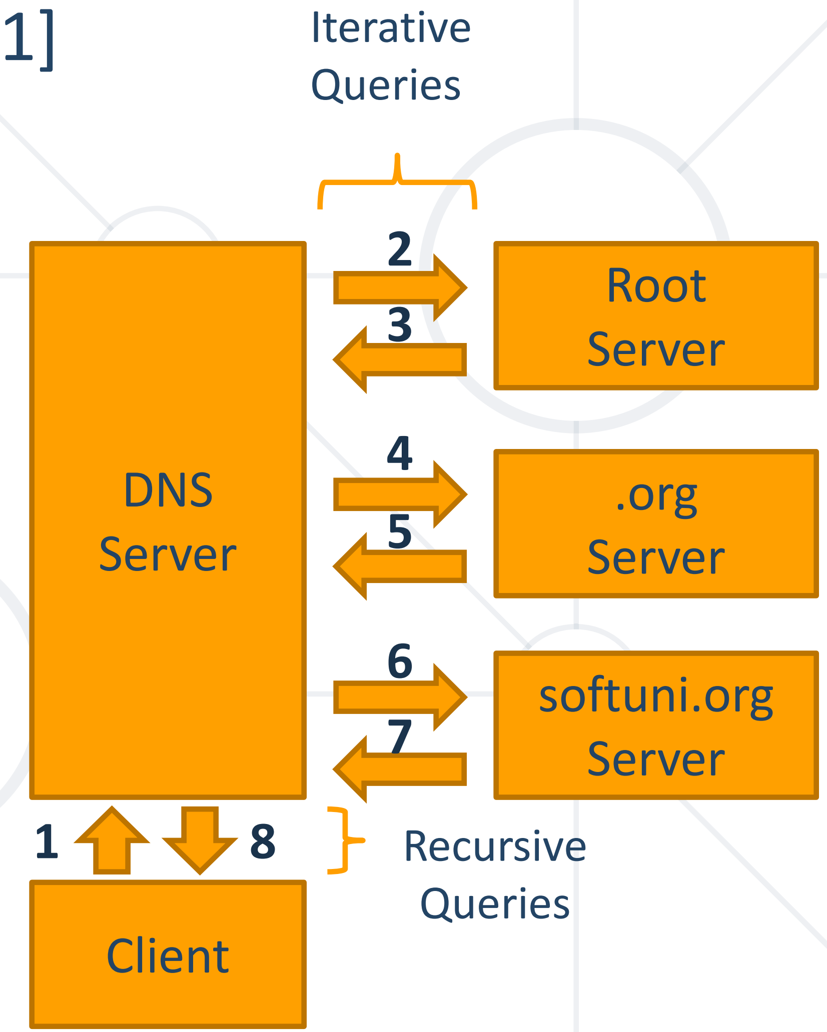
- **Hostname**
  - Character-based name (alias) assigned to machine
- **Fully Qualified Domain Name** (**FQDN**)
  - Combination of hostname and DNS domain name
- **Name server**
  - The DNS server that resolves hostnames to IP addresses
- **Hosts file**
  - Text file with hostname-to-IP address mappings. It overrides DNS and resides under **C:\Windows\System32\Drivers\etc\hosts**

DNS Name Resolution

- Methods
  - **Recursion**
    - DNS server does the job on its own
  - **Forwarding server**
    - The resolution task is outsourced to another DNS server
- Name queries
  - **Recursive** – returns either requested resource record or error
  - **Iterative** – returns best answer or referral

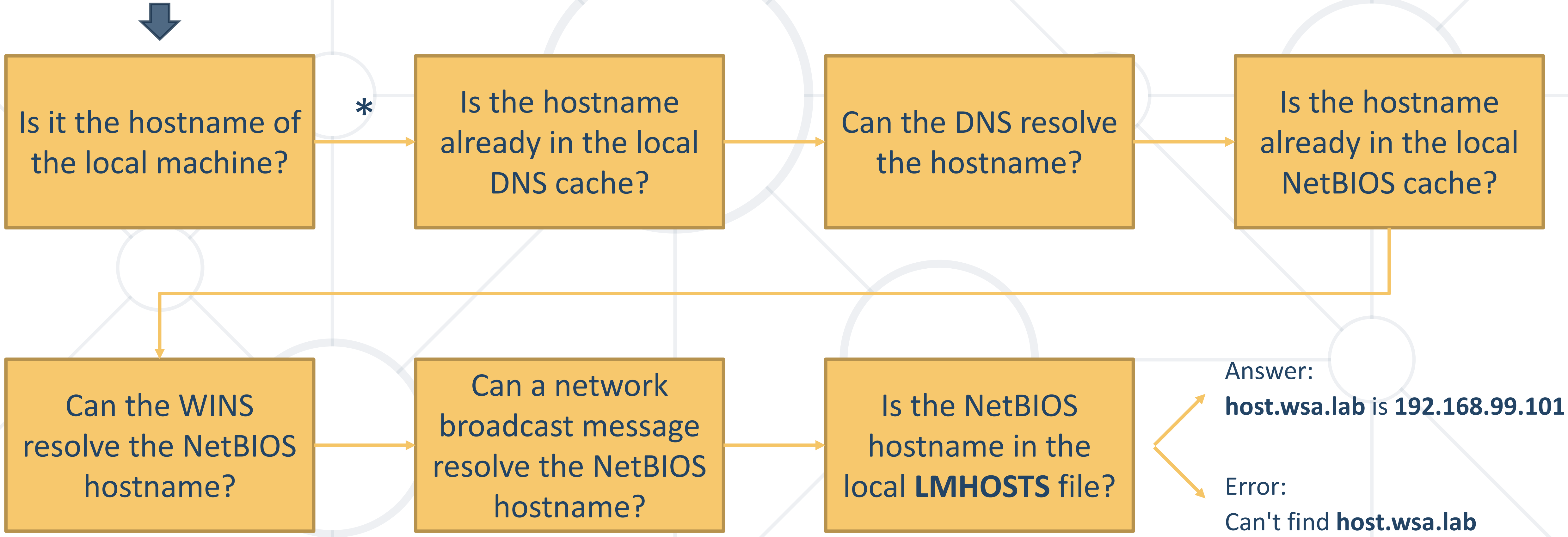
Process Flow

- Client requests name resolution (lab.softuni.org) [1]
- DNS server inspects its local database
- DNS server performs recursive lookup
  - Asks ROOT server for lab.softuni.org [2]
  - ROOT server returns reference [3]
  - Asks .org responsible for lab.softuni.org [4]
  - .org server returns reference [5]
  - Asks softuni.org responsible for lab.softuni.org [6]
  - softuni.org returns address [7]
- Returns answer to the client [8]



Windows Client Name Resolution

- **Who is host.wsa.lab?**



Is it the hostname of the local machine?

*

Is the hostname already in the local DNS cache?

Can the DNS resolve the hostname?

Is the hostname already in the local NetBIOS cache?

Can the WINS resolve the NetBIOS hostname?

Can a network broadcast message resolve the NetBIOS hostname?

Is the NetBIOS hostname in the local **LMHOSTS** file?

Answer:
host.wsa.lab is **192.168.99.101**

Error:
Can't find **host.wsa.lab**

* The contents of the **hosts** (C:\Windows\System32\drivers\etc\hosts) file are automatically loaded into the local DNS cache.

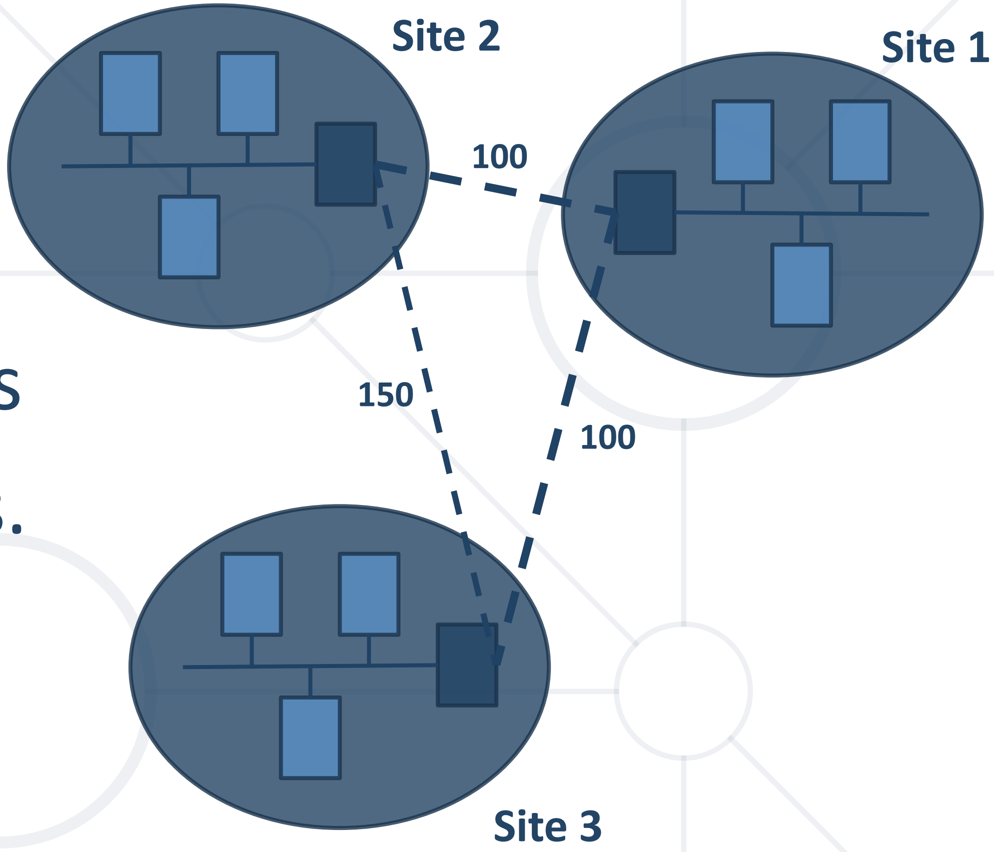
Basic DNS Record Types

- **Address (A)**
  - Translates domain name to specific IPv4 address
- **Address (AAAA)**
  - Translates domain name to specific IPv6 address
- **Canonical name (CNAME)**
  - Alias (secondary name) for an existing A or AAAA record
- **Mail Exchange (MX)**
  - Includes priority and mail exchange agent (references existing A, AAAA, or CNAME)
- **Start of Authority (SOA)**
  - Configured with the creation of the zone. Includes authoritative information
- **Name Server (NS)**
  - Delegates the authoritative name servers for a domain. Created during zone creation

Sites and Replication

AD Sites

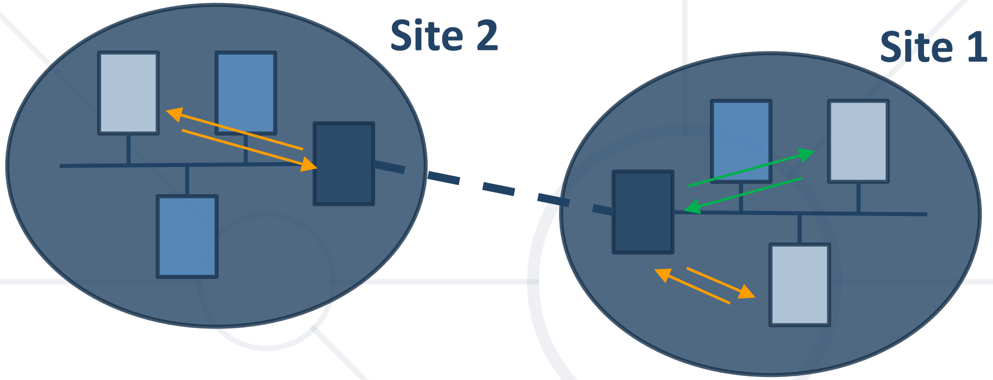
- Group of well-connected computers
- Sites consists of
  - **Subnets** – define sites.
    One site includes one or more subnets
  - **Site links** – connections between sites.
    Can be assigned cost
  - **Bridgehead servers** – servers on the either end of the site links



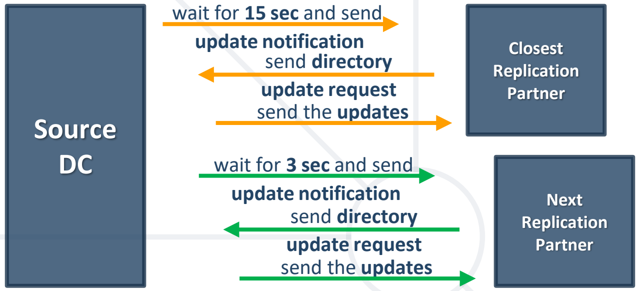
- Site is a collection of IP subnets specified to be part of a site
- Sites support single and multiple domain across sites

AD Replication

- It allows objects synchronization among multiple DCs in a domain
- Two methods
  - **Intra-site** (within AD site)
    - It is configured automatically
    - Knowledge Consistency Checker (KCC) process is responsible
    - Replication topology ensures max. three hops between two DCs
  - **Inter-site** (between AD sites)
    - Inter-Site Topology Generator (ISTG) determines bridgehead servers
    - We can control the schedule for replication



Intra-site (on change)



Source DC

wait for **15 sec** and send **update notification**

send **directory update request**

send the **updates**

Closest Replication Partner

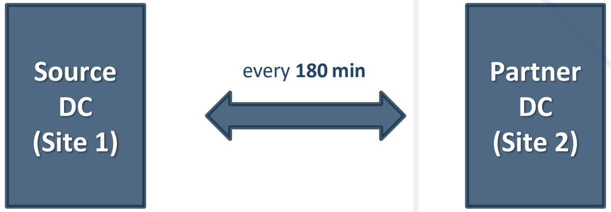
wait for **3 sec** and send **update notification**

send **directory update request**

send the **updates**

Next Replication Partner

Inter-site (periodically)



Source DC (Site 1)

every **180 min**

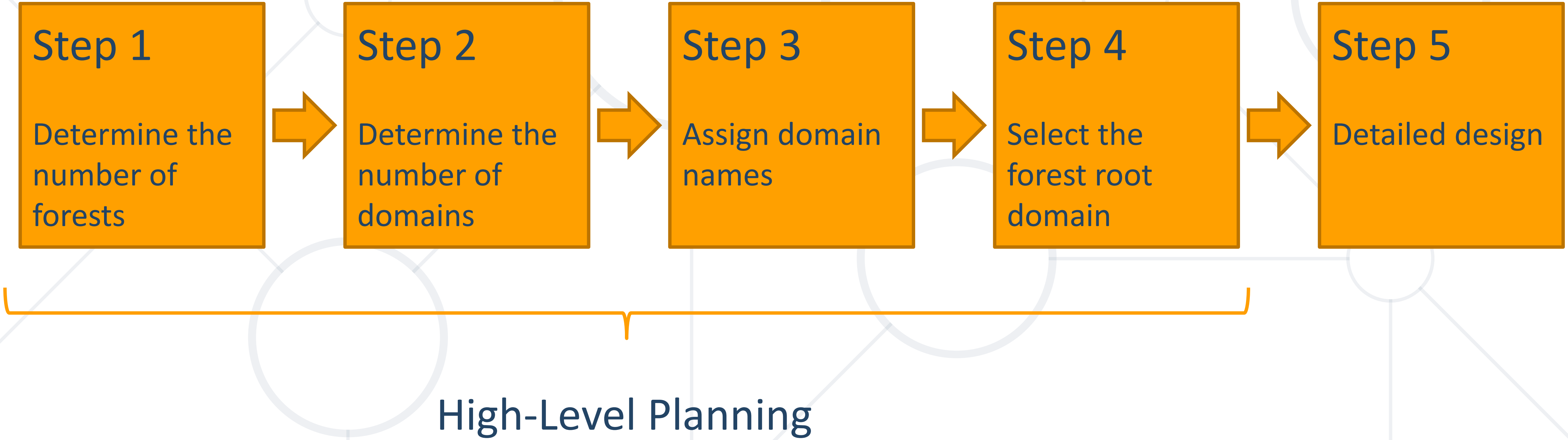
Partner DC (Site 2)

Time for a Break

Let's prepare our infrastructure for the next part

Planning Installation

Planning Process



Step 1

Determine the number of forests

Step 2

Determine the number of domains

Step 3

Assign domain names

Step 4

Select the forest root domain

Step 5

Detailed design

High-Level Planning

Detailed Design

- Organizational Units (OU)
- Determine the number of DCs
- Determine the placement of DCs
- Assign Global Catalog placement
- Select Operations Master role placement
- Planning site design

Organizational Units

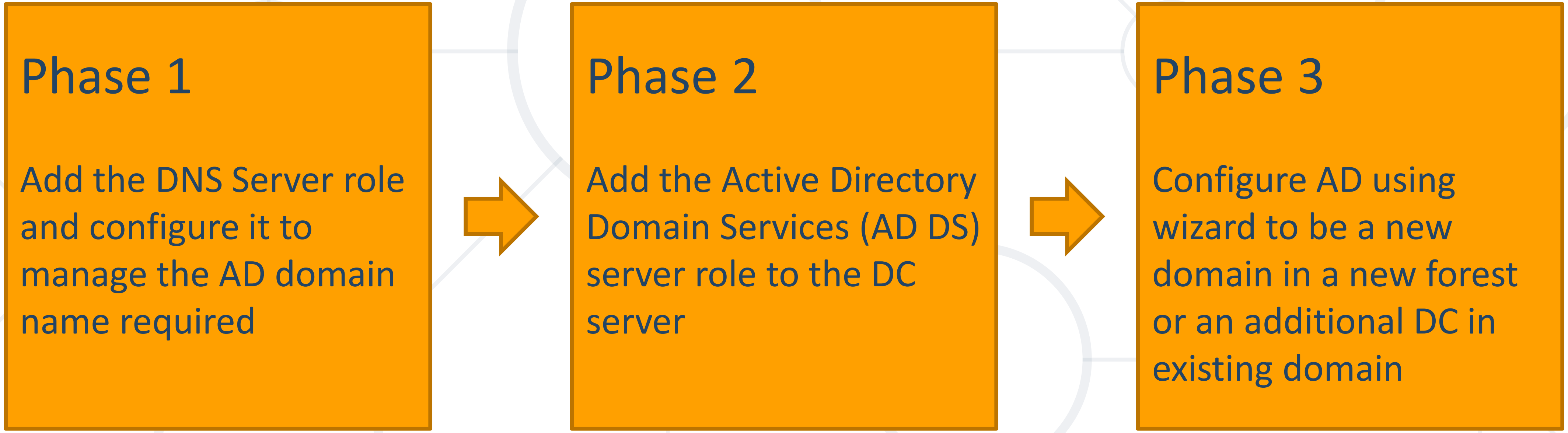
- Serve as container for users, computers, and other objects
- It can be used for
  - Administration Delegation
  - Group Policy Application
- The structure can be based on
  - Organization's hierarchy
  - Administrative needs alone
  - Mixed approach (organizational OUs + administrative OUs)

Operations Master Roles

- Roles can be spread amongst Domain Controllers
- Microsoft recommends simple Operations Master plan
- Recommendations
  - Single domain forest – all OM roles on the first DC installed
  - Multidomain, single-forest
    - All OM roles on the first DC in the root domain
    - All domain-specific roles on the first DC in each additional domain

Implementation

Typical Installation Process



Phase 1

Add the DNS Server role and configure it to manage the AD domain name required

Phase 2

Add the Active Directory Domain Services (AD DS) server role to the DC server

Phase 3

Configure AD using wizard to be a new domain in a new forest or an additional DC in existing domain

Implementation Options

- DNS could be installed as part of AD DS installation
- Installation could be done from GUI or PowerShell
- AD configuration
  - For 2008/2008 R2 is done with **dcpromo.exe**
  - For 2012+ there is a new wizard
- Configuration can be done with PowerShell
  - Module **ADDSDeployment**
  - Cmdlet **Install-ADDSForest**

PowerShell Way

```
# Windows PowerShell script for AD DS Deployment
Import-Module ADDSDeployment

Install-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainMode "WinThreshold" `
-DomainName "wsa.lab" `
-DomainNetbiosName "WSA" `
-ForestMode "WinThreshold" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

Practice: AD Installation

Live Demonstration in Class

Management Tools

Management Tools

- By their purpose
  - Architecture Management
    - Active Directory Sites and Services (**dssite.msc**)
    - Active Directory Domains and Trusts (**domain.msc**)
  - Object Management
    - Active Directory Administrative Center (**dsac.exe**)
    - Active Directory Users and Computers (**dsa.msc**)
- Both categories – CMD Shell and PowerShell (**ActiveDirectory**)

CMD Shell

- Get information

```
:: Query the domain for the current list of FSMO owners
C:\> netdom query fsmo
```

- Display specific objects

```
:: Display properties of the Administrator user
C:\> dsget user "cn=Administrator,cn=Users,dc=wsa,dc=lab"
```

- Find AD objects

```
:: List all domain computers
C:\> dnsquery computer
```

PowerShell – Retrieve Information

- Retrieve AD domain information

```
PS C:\> Get-ADDomain
```

- Retrieve information about forest

```
PS C:\> Get-ADForest
```

- Retrieve information about DC

```
PS C:\> Get-ADDomainController
```

- Retrieve the root of a directory server information tree

```
PS C:\> Get-ADRootDSE
```

PowerShell – Set Parameters

- Modify global parameters in the forest

```
PS C:\> Set-ADForest
```

- Set forest functional level

```
PS C:\> Set-ADForestMode
```

- Modify global parameters in the domain

```
PS C:\> Set-ADDomain
```

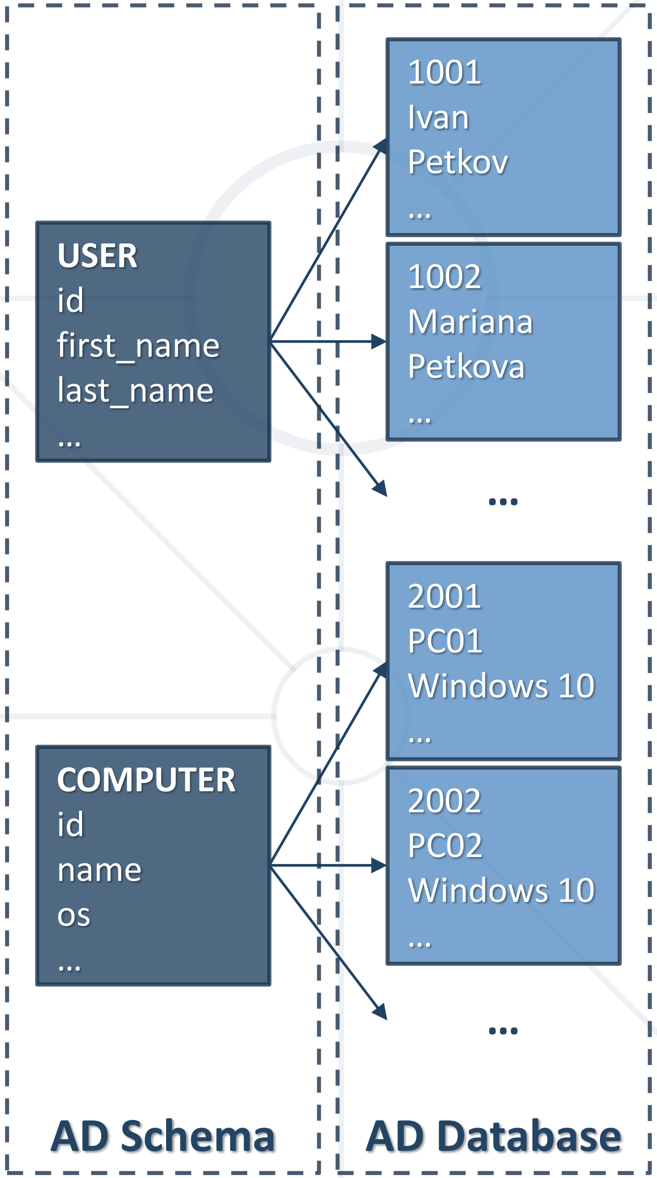
- Set domain functional level

```
PS C:\> Set-ADDomainMode
```

Active Directory Objects

Objects (1)

- Objects are **entities** that represent a resource which is part of the AD
- Each object is defined by a set of fields or **attributes**
- Attributes may include first name, last name, phone number, etc.
- Attributes are defined by the **object class** to which an object belongs
- Object classes and their structure are defined in the **AD schema**



USER
id
first_name
last_name
…

COMPUTER
id
name
os
…

1001
Ivan
Petkov
…

1002
Mariana
Petkova
…

…

2001
PC01
Windows 10
…

2002
PC02
Windows 10
…

…

AD Schema

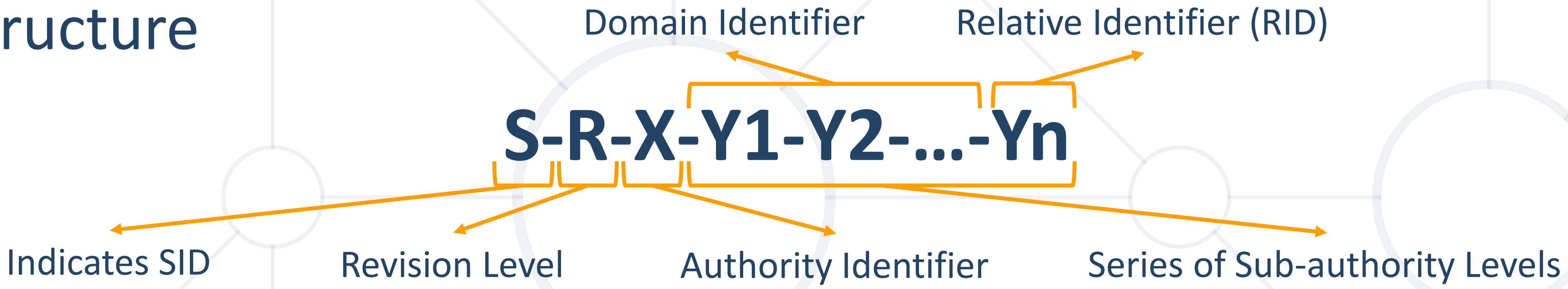
AD Database

Objects (2)

- Every object is identified by a **global unique identifier (GUID)** which is a **128-bit value**
- Some objects act as **security principals** and have additional identifier called **security identifier (SID)**
- Security principals are **authenticated** by the operating system
- Only **users**, **computers** and **groups** are security principals
- Security principals can be used to manage access to domain resources

Security Identifier (SID)

- Structure



Domain Identifier

Relative Identifier (RID)

S-R-X-Y1-Y2-…-Yn

Indicates SID

Revision Level

Authority Identifier

Series of Sub-authority Levels

- Built-in Example (Administrators Group)
  - **S-1-5-32-544**
- AD Example (Administrator Account)
  - **S-1-5-21-152261188-2570450788-2846045064-500**

https://technet.microsoft.com/en-us/library/cc962011.aspx

Well-known SIDs (1) *

- **S-1-1-0** (**Everyone**)
  - A group that includes all users, even anonymous users and guests
- **S-1-5-7** (**Anonymous**)
  - A user who has logged on anonymously
- **S-1-5-< domain >-500** (**Administrator**)
  - It is the first account created during operating system installation
- **S-1-5-< domain >-501** (**Guest**)
  - A user account for people who do not have individual accounts

https://technet.microsoft.com/en-us/library/cc978401.aspx

Well-known SIDs (2) *

- **S-1-5-11** (**Authenticated Users**)
  - A group that includes all users whose identities were authenticated when they logged on. Membership is controlled by the operating system
- **S-1-5-< domain >-512** (**Domain Admins**)
  - A global group whose members are authorized to administer the domain
- **S-1-5-32-544** (**Administrators**)
  - A **built-in group**. First member is the **Administrator**. The **Domain Admins** group is added to it when computer joins a domain. Its members **full control** over the system
- **S-1-5-32-545** (**Users**)
  - A **built-in group**. Initially, the only member is the **Authenticated Users** group

https://technet.microsoft.com/en-us/library/cc978401.aspx

Working With Computers

Manage Computers (1)

- GUI (dsac.exe)
- CMD Shell

```
:: Add workstation to a domain
C:\> netdom add /d:wsa.lab my-station

:: Join workstation to a domain
C:\> netdom join /d:wsa.lab my-station
/OU:OU=IT,OU=Workstations,DC=wsa,DC=lab

:: Remove workstation from domain
C:\> netdom remove /d:wsa.lab my-station
/ud:wsa\administrator /pd:password
```

Manage Computers (2)

- PowerShell

```
# Display information about computer or computers
PS C:\> Get-ADComputer MY-SRV
PS C:\> Get-ADComputer -Filter 'Name -like "*SRV*"'

# Create new AD computer object
PS C:\> New-ADComputer SRV-CORE
PS C:\> New-ADComputer -Name "DC-2" -Path "OU=Srv,DC=WSA,DC=LAB"

# Remove computer object from domain
PS C:\> Remove-ADComputer SRV-CORE

# Join or remove computer to/from a domain
PS C:\> Add-Computer -Domain WSA
PS C:\> Remove-Computer -UnjoinDomainCredential WSA\Administrator
```

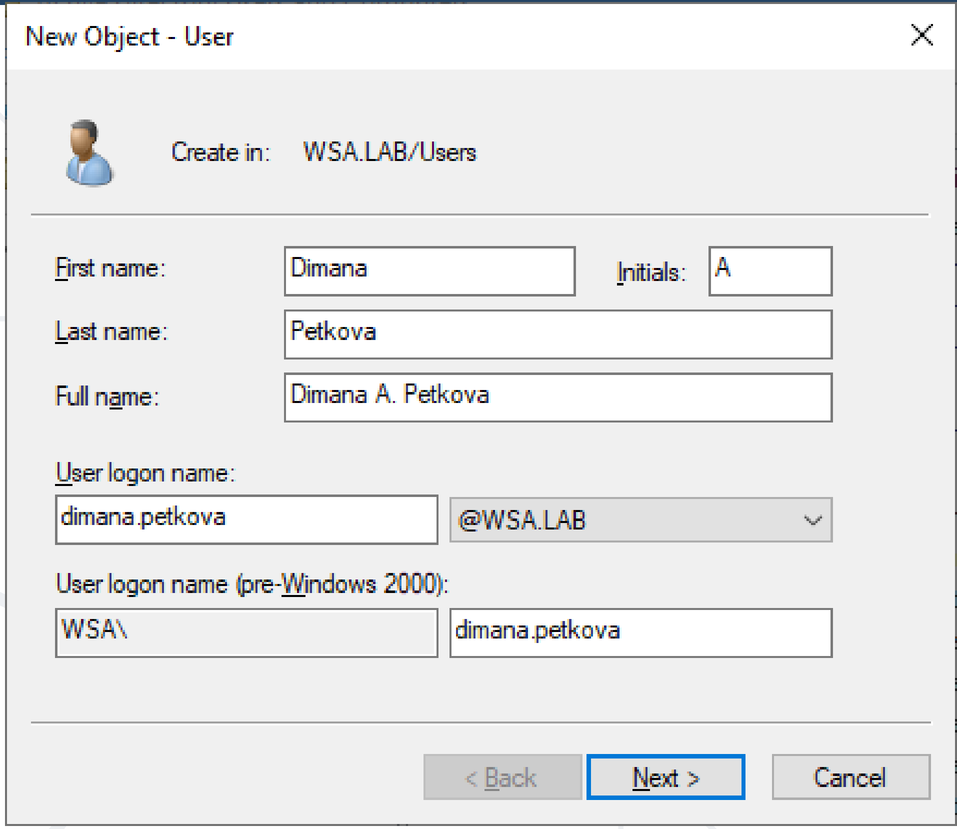
Working with Users and Groups

Users Accounts

- **Local Accounts**
  - Stored in a local database
  - Supported by client and server OS
  - Managed with GUI (**compmgmt.msc**), CMD Shell, and PowerShell
- **Domain Accounts**
  - Created and stored in the AD database
- Both have profiles (contain settings, specific files, etc.)

User Account Properties

- First name + Initials + Last name = **Full Name** (Name)
- User logon name + domain name = **User Principal Name** (UPN)
- User logon name (pre-Windows 2000) = **Security Account Manager** (SAM) **account name**



New Object - User

Create in: WSA.LAB/Users

First name: Dimana

Initials: A

Last name: Petkova

Full name: Dimana A. Petkova

User logon name: dimana.petkova @WSA.LAB

User logon name (pre-Windows 2000): WSA\ dimana.petkova

Manage Users

- PowerShell

```
# Display information about user or users
PS C:\> Get-ADUser Administrator -Properties *
PS C:\> Get-ADUser -Filter {Name -Like "*adm*"}

# Create new AD user object
PS C:\> New-ADUser -Name John -AccountPassword (ConvertTo-
SecureString -AsPlain "Password1" -Force) -DisplayName "John Smith" -
Enabled $true -GivenName John -Surname Smith -UserPrincipalName
john.smith@wsa.lab

# Remove user object from domain
PS C:\> Remove-ADUser John

# Set user object properties
PS C:\> Set-ADUser John -HomePage "http://softuni.bg"
```

Groups

- **Local Groups**
  - Stored in the local database
- **Domain Groups**
  - Stored in the AD database
  - **Security Groups**
    - Group that may be assigned permissions
  - **Distribution Groups**
    - Used for email lists and other purposes not requiring permissions

Domain (Security) Groups

- **Domain Local** (**DLG**)
  - Permissions to resources in the domain
  - Members - Same Domain (DLG); Any domain (GG,UG,UA)
- **Global** (**GG**)
  - Permission to any resource in the forest
  - Members - User Accounts (UA) and Global Groups from same domain
- **Universal** (**UG**)
  - Permissions to any resource in the forest
  - Members - Any domain (UG, GG, UA)

Manage Groups (1)

- PowerShell

```
# Display information about group or groups
PS C:\> Get-ADGroup "Domain Admins"
PS C:\> Get-ADGroup -Filter {GroupScope -Eq "DomainLocal"}

# Create new AD group object
PS C:\> New-ADGroup -Name "Help Desk L3" -SamAccountName HelpDeskL3 -
GroupCategory Security -GroupScope DomainLocal -DisplayName "Help
Desk L3 Staff" -Path "CN=Users,DC=WSA,DC=LAB" -Description "Members
of this group are Help Desk L3 Staff"

# Remove group object from domain
PS C:\> Remove-ADGroup HelpDeskL3

# Set group object properties
PS C:\> Set-ADGroup HelpDeskL3 -DisplayName "(L3) Help Desk"
```

Manage Groups (2)

- Avoid nesting groups at more than three or four levels
- Keep it simple. Complexity makes administration difficult
- Different group scopes allow different nesting options

```
# Display information about all group members
PS C:\> Get-ADGroupMember "Domain Admins" -Recursive

# Add group member
PS C:\> Add-ADGroupMember HelpDeskL3 John,Jane

# Remove group member
PS C:\> Remove-ADGroupMember "Domain Admins" John
```

Containers and OUs

Default Containers and OUs

- **Domain**
  - The domain itself
- **Built-in**
  - Contains default groups
- **Users**
  - Default location for newly created users and groups
- **Computers**
  - Default location for computer accounts
- **Domain Controllers**

Organizational Units

- Customizable containers
- Used to create hierarchy following our organization structure
- Can be used for **delegation**
- **Group Policy Objects** can be linked to different OUs
- Can contain
  - Other OUs
  - Regular objects - computers, users, groups, etc.

Practice: Active Directory in Action

Live Demonstration in Class

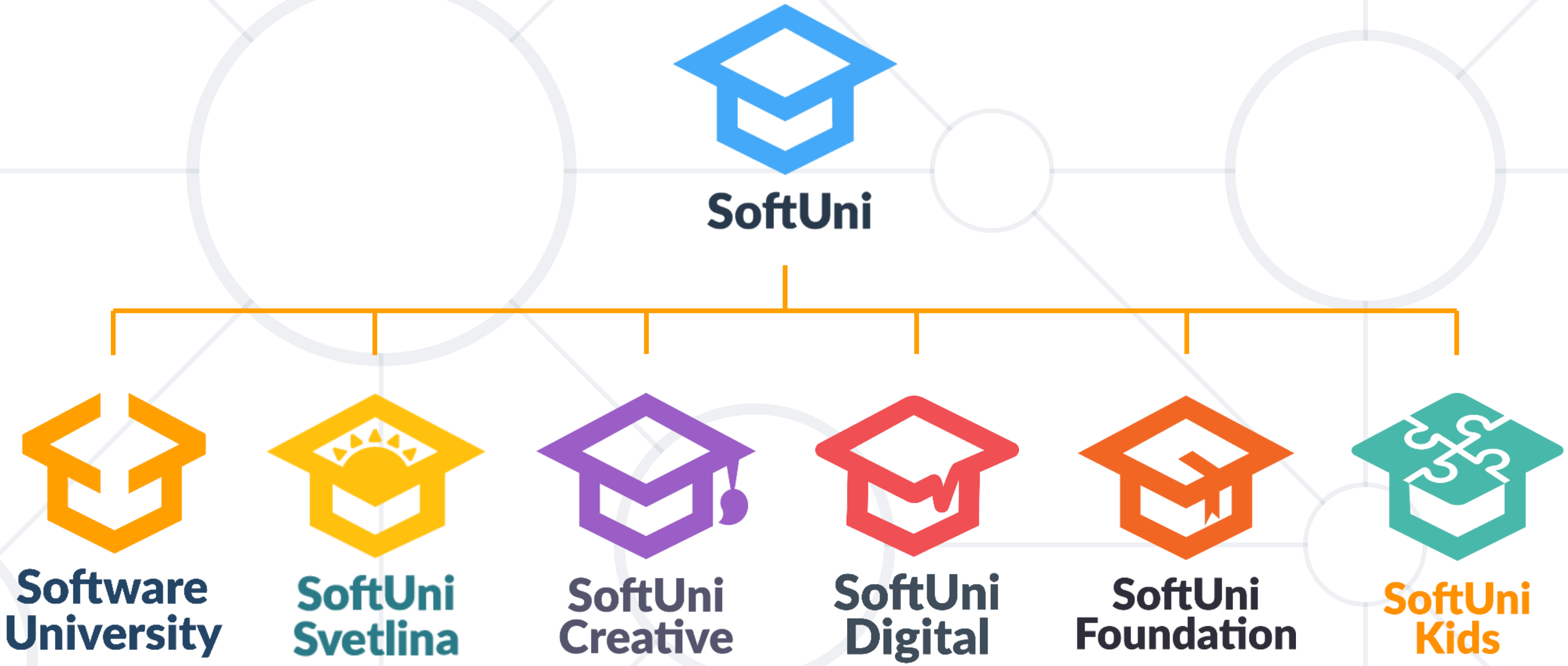
Summary

- Logical architecture - Domain, Domain Trees, and Forests
- Physical architecture - Servers (DCs and others) and Sites
- AD is supported by DNS and DHCP
- Organizational structure - OUs or Parent-Child Domains
- Replication is used within and between sites
- AD Implementation - High level + Detailed planning
- Implementation steps vary in Window Server versions
- There is plenty of AD management tools
- Typically, we will work with Computers, Users, Groups, a nd Organizational Units

Resources

- ADDSDeployment Module
  https://docs.microsoft.com/enus/powershell/module/addsdeployment
- ActiveDirectory Module
  https://docs.microsoft.com/enus/powershell/module/addsadministration

Questions?



SoftUni

Software University

SoftUni Svetlina

SoftUni Creative

SoftUni Digital

SoftUni Foundation

SoftUni Kids

SoftUni Diamond Partners

SCHWARZ

LIDL

Kaufland

SCHWARZ Produktion

pre zero

Coca-Cola HBC Bulgaria

POKERSTARS | CAREERS

Postbank

Решения за твоето утре

AMBITIONED

DXC TECHNOLOGY

SOFTWARE GROUP

Bosch.IO

INDEAVR

Serving the high achievers

DRAFT KINGS

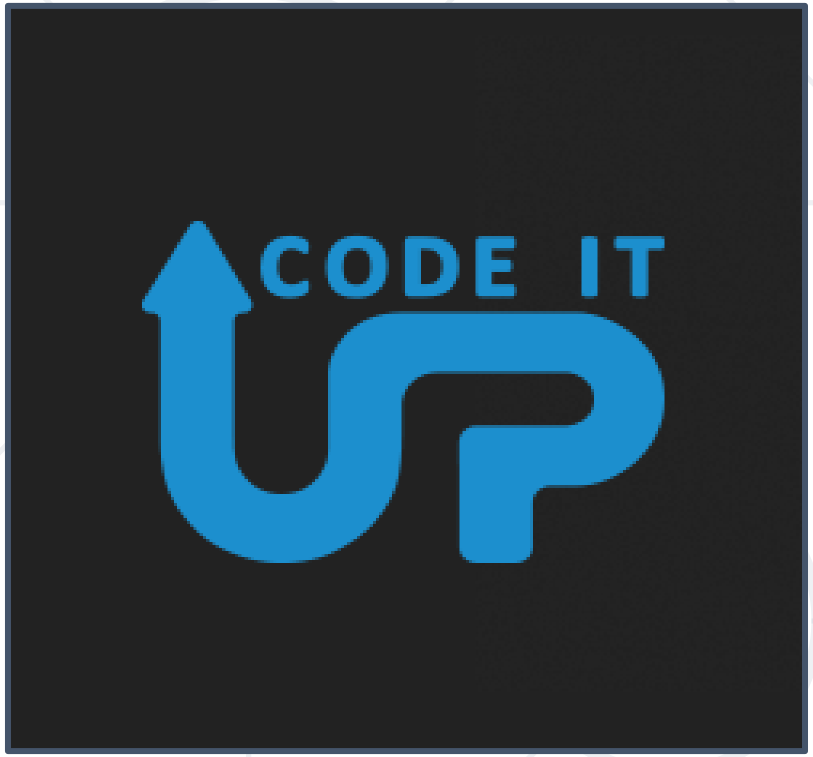
PHAR VISION

SmartIT

createX

SUPER HOSTING .BG

Educational Partners



License

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, softuni.org
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity
- Software University Forums
  - forum.softuni.bg