Server 2 – 📘 جزوه کامل

🟦 جلسه اولDNS –

DNS

- کار DNS: **تبدیل نام FQDN به IP**
- تبدیل IP به نام هم توسط DNS انجام می‌شود

IP Version

- IPv4 → 32 بیت
- IPv6 → 128 بیت

🏷️ نام در سیستم

دو نوع نام داریم:

- **NetBIOS**
- **FQDN**

NetBIOS

- حداکثر 16 کاراکتر (یکی رزرو شده)
- کاراکترهای غیرمجاز . و: _
- کاراکترهای مجاز - و: عدد
- Computer Name = NetBIOS

تبدیل NetBIOS به IP

1. LMHOSTS
   - دستی
   - لوکال روی هر سیستم

- ایراد: باید روی تک‌تک سیستم‌ها ست شود

2. **WINS**
   - سرور مرکزی
   - ثبت دستی اما یک‌جا
3. **Broadcast**
   - ارسال پیام در کل شبکه
   - ایراد:
     - ترافیک بالا
     - از Router عبور نمی‌کند

FQDN

- حداقل یک .دارد
- حداکثر 255 کاراکتر
- هر بخش جدا شده با .حداکثر 63 کاراکتر

ساختار:

HostName.DomainName.TLD

تبدیل FQDN به IP فقط با **DNS Server**

DNS Manager

Forward Lookup Zone

- تبدیل **نام** → **IP**

Reverse Lookup Zone

- تبدیل **IP** → **نام**

🧱 انواعZone

- Primary Zone
- Secondary Zone
- Stub Zone

Active Directory Integrated Zone

- فقط روی DC فعال می‌شود
- دیتابیس DNS با AD ادغام می‌شود

مزایا:

- امنیت بالاتر
- خطای کمتر
- ReplicationباForest

📄 رکوردهای پیش‌فرضZone

- **SOA**
- **NS**

رکوردها

- **A** → نام بهIPv4
- **AAAA** → نام بهIPv6

🧪 تستDNS

nslookup

DNS Cache

- پیش‌فرض: 1 ساعت

نمایش:

ipconfig /displaydns

پاک‌سازی:

ipconfig /flushdns

🟦 Secondary Zone

- Read Only
- وابسته بهPrimary Zone
- بدون Zone Transfer کار نمی‌کند

Zone Transfer

در:Primary

- To any server
- Only servers in Name Servers
- Only listed servers (امن‌ترین)

پورتDNS

- UDP 53 → پاسخ به کلاینت
- TCP 53 → Zone Transfer

📜 SOA

- هر 15 دقیقه Serial Number را چک می‌کند
- اگر Primary جدیدتر بودZone Transfer →
- Retryهر 10–15 دقیقه
- بعد از 24 ساعتInvalidate →

🟦 Stub Zone

- Read Only
- فقط SOA وNS
- کل رکوردها را نمی‌آورد
- برای پیدا کردن DNS مسئول Zone

روش کار:

- DNS می‌بیند Zone دارد ولی Stub است
- از NS می‌فهمد کدام DNS مسئول است
- سؤال را مستقیم می‌پرسد
- جواب را Cache می‌کند

🔁 Forwarder

- اگر DNS جواب را بلد نباشد
- می‌رود سراغ Forwarder
- جواب را Cache می‌کند

🏷️ CNAME (Alias)

- نام مستعار برای یک رکورد

🟦 جلسه دوم – DDNS

Dynamic Update

سه حالت:

1. None
   - هیچ‌کس نتواند ثبت یا تغییر دهد

2. Nonsecure and Secure
    - Joinباشد یا نباشد
3. Secure Only
    - فقط اعضایActive Directory

Zone Aging

- 5روز تمدید نمی‌شود
- بعد از تغییرIP
- 3روز فرصت
- در صورت عدم ارتباطInvalidate →

🟦 نکاتDNS

DNS vs WINS

- IPبهDNS → FQDN
- IPبهWINS → NetBIOS

🌍 GNZ (Global Name Zone)

- قابلیت مخفیDNS
- تبدیل NetBIOS بهIP
- پیش‌فرض غیرفعال
- نداردGUI

فعال‌سازی:

- CMD: dnscmd

- PowerShell: Set-DnsServerGlobalNameZone

بعد از فعال‌سازی:

- ساخت Zone به نام GlobalNames
- ساختCNAME
- حالا NetBIOS بدون .هم Resolve می‌شود

Cache Locking

- از Server 2016 به بعد
- پیش‌فرض فعال
- جلوگیری از تغییر رکوردCache

dnscmd /config /cachelockingpercent 100

100٪یعنی تا پایان TTL قابل تغییر نیست

SRV Record

- مشخص می‌کند چه سرویسی روی چه سروری است
- رکوردهای پیش‌فرض:
  - GC
  - Kerberos
  - LDAP
  - kpasswd

فرمت:

_Service._Protocol.Domain

مثال:

_GC._tcp.meschi.com

اولویت‌بندی

- Priority → عدد کمتر = اولویت بیشتر
- Weight → عدد بیشتر = اولویت بیشتر
- اول Priority ، بعد Weight
- اگر برابر Load Balancing →

🟦 جلسه سوم DNS – ادامه

Reverse Lookup Zone

- تبدیل IP به نام
- رکورد PTR

مثال:

192.168.1.0

→

1.168.192.in-addr.arpa

ساخت خودکار PTR

- هنگام ساخت A Record

⚙️ DNS Server Properties

Interface

- تعیین کارت شبکه‌های پاسخ‌دهنده

Advanced

- Disable Recursion

- Enable Round Robin
- Enable Netmask Ordering
- Secure Cache Against Pollution

Name Checking

- RFC
- Non-RFC
- Multibyte (UTF8)
- All

💾 Disk Quota

- در Windows 11
- محدودیت روی **درایو**

🗂️ FSRM

1. Quota

- روی پوشه
- Hard → اجازه عبور نمی‌دهد
- Soft → عبور می‌دهد + لاگ

2. File Screen

- جلوگیری از پسوند خاص
- Active → بلاک
- Passive → لاگ

3. Storage Report

- فقط گزارش

- حذف نمی‌کند

🟦 جلسه چهارم – DHCP

DHCP

- گرفتن IP
- فقط UDP

پورت‌ها:

- 67 → Server
- 68 → Client

سرویس‌ها

- DHCP Server Service
- DHCP Client Service

Authorize

- روی DC یا Domain
- حتماً باید در AD Authorize شود

📦 Scope

- محدوده IP برای کلاینت‌ها

🤝 DORA

- Discover
- Offer
- Request

- Ack

⏱️ Lease Time

- LAN → 8 روز
- Wireless → 8 ساعت
- BOOTP → 30 روز
- Multicast → 30 روز

🖥️ CMD

ipconfig /renew

ipconfig /release

⚙️ DHCP Options

- Server Options
- Scope Options
- Reservations

Options مهم:

- 003 Router
- 006 DNS
- 015 DNS Domain

🚦 Filters

- Allow

- Deny

⏳ T1 / T2

- T1 → 50٪ → تمدید از همانDHCP
- T2 → 87.5٪ → هر DHCP دیگر

DNS Tab 🧠 درDHCP

- ثبت یا آپدیت رکوردDNS
- مالک رکوردDHCP =

راه‌حل:

- دادن یوزر/پسورد
- عضویت در **DNSUpdateProxy**

🆚 BOOTP vs DHCP

- BOOTP:
  - Diskless
  - IPv4
  - دستی
- DHCP:
  - داینامیک
  - خطای کمتر

🔗 SuperScope

- ترکیب چند Scope با NetID متفاوت

📣 Multicast Scope

- ارسال به گروه
- Class D:

224.0.0.0 – 239.255.255.255

- پروتکلMADCAP :
- TTL = تعداد Router مجاز

🧯 High Availability

Split Scope

- 50/50یا 20/80

Built-in Failover

- فقط 2 سرور
- Active/Active
- Active/Passive

تایم‌ها

- MCLT
- State Switchover Interval
- پیش‌فرض: 60 دقیقه

🧩 User Class

- اعمال تنظیم شرطی

ipconfig /setclassid "Ethernet" pass

🧩 جلسه ۶ – IPv6

IPv6 🔹 چیست و چرا به‌وجود آمد؟

یکی از مشکلات IPv4 ، **تعداد کم آدرس‌ها** بود.
IPv6 برای حل این مشکل طراحی شد.

- آدرس‌دهی **128بیتی**
- تعداد IP برابر با **2به توان 128**
- نمایش به صورت **Hexadecimal**
  - شامل اعداد **0–9** و حروف **A–F**

🔹 ساختار IPv6

- هر **16بیت** با علامت : از هم جدا می‌شوند
- نسبت به IPv4 **سریع‌تر** است
- برای کار کردن **نیازی به اینترنت ندارد**

🔹 تفاوت‌های مهم IPv6

- **Broadcast ندارد**
- به‌جای آن **Multicast** دارد
  → به همین دلیل **پروتکل ARP ندارد**
- **IPSec اجباری نیست**
- **Anycast** دارد
  → یعنی کوتاه‌ترین مسیر تا مقصد انتخاب می‌شود
- **Mobility** دارد
  → بین گوشی، سیستم و... جابه‌جا می‌شوی ولی IP تغییر نمی‌کند

🔹 ساده‌نویسی IPv6

اگر **بیش از 8 صفر پشت سر هم** وجود داشته باشد، می‌توان آن‌ها را با :: جایگزین کرد.
⚠️ این کار **فقط یک بار** در هر IP مجاز است.

Prefix 🔹 در IPv6

در IPv6 چیزی به اسم **Subnet Mask** نداریم.
به‌جای آن از **Prefix** استفاده می‌شود.

مثال:
/64

- 64بیت اول **ثابت**

- بقیه بیت‌ها **متحرک**

برای ارتباط سیستم‌ها **بدون روتر**،
64بیت اول (از سمت چپ) باید یکسان باشند.

🔹 **دسته‌بندی آدرس‌های IPv6**

Global Unicast

- مشابه Public در IPv4
- امکان رفتن به اینترنت
- IPبا **2 یا 3** شروع می‌شود

Link-Local

- معادل APIPA در IPv4
- با **FE80**شروع می‌شود

Unique-Local

- شبیه Private در IPv4
- به اینترنت دسترسی ندارد
- با **FD**شروع می‌شود

Loopback

::1

IPAM – DFS Namespace – DFSR

🔹 **IPAM (IP Address Management)**

IPAMبرای **مدیریت متمرکز چندین DNS و DHCP** از طریق یک سیستم استفاده می‌شود.

- رول **IPAM**
  ❌ **هرگز** نباید روی:
  - DC
  - RODC
  - Additional DC
    نصب شود.

مراحل راه‌اندازی IPAM

1. بعد از نصب رول، **اولین گام ساخت Database** است.
2. برای ارتباط با سایر سرورها، اجازه‌ی ساخت **Policy**داده می‌شود.
3. برای اعمال Policy روی سرورها از دستور زیر استفاده می‌کنیم:

```
Invoke-IpamGpoProvisioning -Domain Meschi.com ...
```

4. بعد از اجرای دستور، **Group Policy** مربوطه روی DC ساخته می‌شود.
5. این GPO به‌صورت پیش‌فرض **غیرفعال** است، چون در بخش **Security Filtering** مشخص نشده به چه سیستمی اعمال شود.
6. باید **Computer Account** سرورهایی که قرار است این Policy را بگیرند، **دستی** به Security Filtering اضافه شوند.

🔹 Namespace (DFS Namespace)

Namespace فضایی است که **لینک پوشه‌های اشتراکی کاربران** داخل آن قرار می‌گیرد.

- رول مورد استفاده **DFS Namespace** :
- نصب رول:
  - نصب روی **یک سیستم** کافی است.

🔹 DFSR (Distributed File System Replication)

DFSR برای این استفاده می‌شود که **محتوای یک پوشه** روی تمام سرورهایی که عضو آن هستند، **همیشه یکسان** بماند.

- رول **DFSR** باید روی **همه سرورها** نصب باشد.
- به‌صورت پیش‌فرض:
  - **SYSVOL** با DFSR Replicate می‌شود.

انواع Replication

Multipurpose

- Replication بین **چندین سرور**

Data Collection

- Replication فقط بین **دو سرور**

🔹 Staging Folder

- هر فایلی که قرار است **Replicate** شود، ابتدا وارد **Staging** می‌شود و در صف قرار می‌گیرد.
- مسیر Staging را می‌توان از تب **Properties** تغییر داد.

🔹 Advanced (Deleted Files)

- در تب **Advanced**، پوشه‌ای شبیه **Recycle Bin** وجود دارد.
- فایل‌ها به‌جای حذف کامل، ابتدا به این پوشه منتقل می‌شوند.

🧩 جلسه ۷ – RAS & DHCP Relay Agent

🔹 RAS (Remote Access Service)

RASرولی است که **ویندوز سرور را به روتر تبدیل می‌کند**.

🔹 DHCP Relay Agent

به‌طور پیش‌فرض، **پیغام‌های Broadcast از روتر عبور نمی‌کنند**.
به همین دلیل سیستمی که بین آن و سرور DHCP یک روتر قرار دارد،
در حالت عادی **نمی‌تواند از آنDHCP ، IPدریافت کند**.

نحوه عملکردDHCP Relay Agent

- DHCP Relay Agentروی **سیستم روتر** نصب می‌شود.
- وقتی کلاینت پیغام **DHCP Discovery**ارسال می‌کند:
  - پیام به روتر می‌رسد.
  - اگر Relay Agent فعال باشد، روتر پیام را **Dropنمی‌کند**.
  - روتر پیام را به‌صورت **Unicast**به سرور DHCP ارسال می‌کند.

نقشGIADDR

- سرور DHCP از طریق فیلد **GIADDR (Gateway IP Address)**تشخیص می‌دهد:
  - درخواست از کدام شبکه آمده
  - و باید از **کدام Scope** به کلاینت IP بدهد

Upgrade & ADPrep

🔹 Upgrade

در ابتدای **Upgrade**، سیستم خطا می‌دهد که **Active Directoryباید آماده‌سازی شود**.
این آماده‌سازی **فقط از طریق Command Line** انجام می‌شود.

🔹 ADPrep

- ابزار **ADPrep**داخل پوشه‌ی support
- این پوشه در **ISOنصب ویندوز سرور جدید** قرار دارد.

برای اجرا، از طریق **CMD**به مسیر ADPrep می‌رویم و دستورات زیر را اجرا می‌کنیم:

```
cmd> adprep.exe /forestprep
```

```
cmd> adprep.exe /domainprep
```

با اجرای این دستورات، اکتیو دایرکتوری برای **Upgradeنسخه جدید ویندوز سرور** آماده می‌شود.