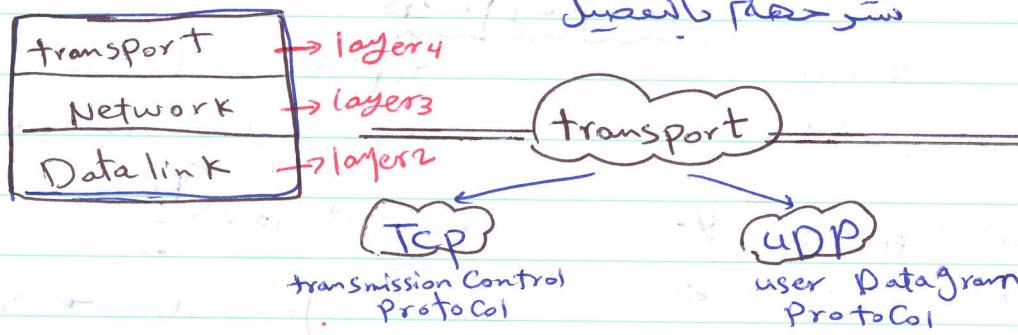


Track 2 Infra & Application

1 Introduction

- ① Network models $\xleftarrow{\text{OSI}}$ TCP/IP
- ② Routing $\xrightarrow{\text{simple}}$ static
 $\xrightarrow{\text{Dynamic}}$ Packet Filter
- ③ Nating
- ④ DHCP $\xleftarrow{\text{Relay Agent}}$ DHCP split $\rightarrow R_2$
- ⑤ DNS \rightarrow IIS
- ⑥ Network Policy Server \rightarrow application
 \rightarrow NPS \rightarrow NAP
- ⑦ Remote Access (VPN)
- ⑧ Demand Dial (VPN site-to-site)
- ⑨ IPsec
- ⑩ Clustering (NLB)
- ⑪ DFS Replication
- ⑫ Name Resolution
- ⑬ Windows Firewall
- ⑭ Windows media Services
- ⑮ IP v.6

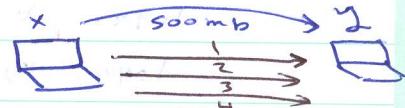


لكل حاجة متعلقة بالمهنة Port ينخرطوا فيه

HtP → 80
FtP → 21
Dns → 53
Dhcp → 67
Rdp → 3389

65535 port; 1023
0 → 1023
Standard port

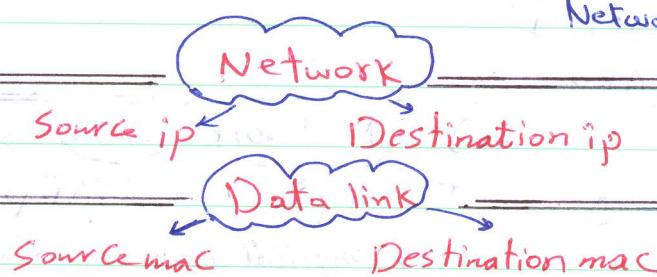
0 → 65535



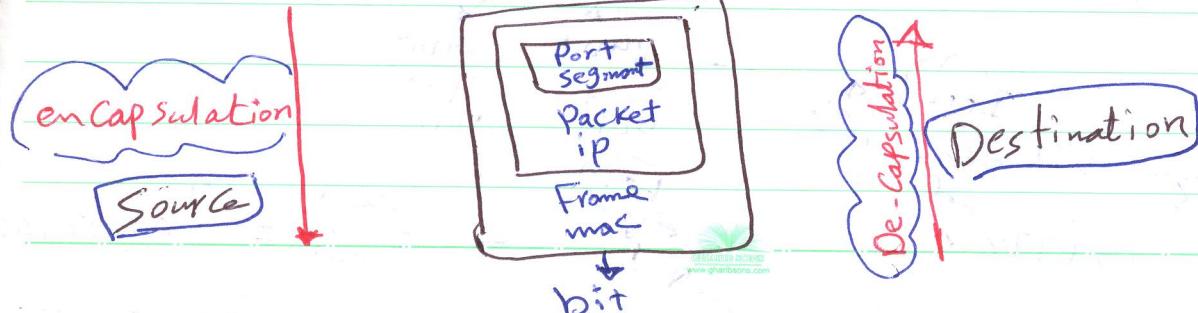
The diagram shows two hosts, 'Source' and 'Destination', connected by a cloud labeled 'Connection Oriented'. A blue arrow points from Source to Destination. Above the arrow, the text 'TCP' is enclosed in a box with a star, and '500 mb' is written below it. Below the arrow, the text 'Segment Header' and 'Sequence Number' is written. To the right of the Destination host, there is Arabic text: 'البيانات ترسل ب-segments' (Data is sent in segments), 'الكلمة الأولى في كل segment' (The first word in each segment), 'ويتم إثبات ذلك بـ-sequence numbers' (And it is confirmed by sequence numbers), and 'ويتم إثبات ذلك بـ-sequence numbers' (And it is confirmed by sequence numbers).

 UDP → Connection less

ما ينفعنا بمرة واحدة لازم نقطع data
Sequence Number و سط لكر و Segmant



کل ہائسٹر لے Layer 1 تک کل 140 Data نیں سامنہ کیا اسیاتھ اپلیکیشن کے الگ زادتے علیحدہ خرچ مانع کیا جاتے۔



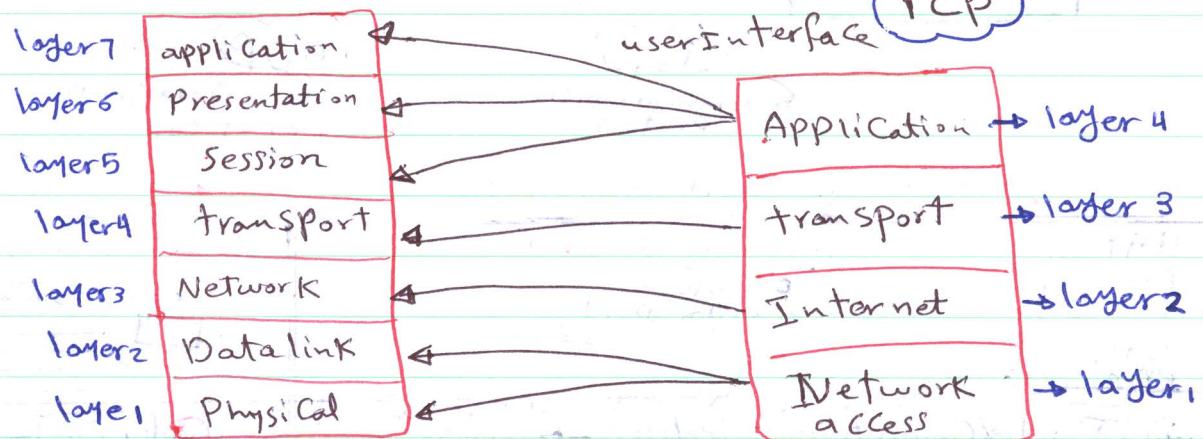
"3" TCP-IP ↗

OSI → 7 layers

conform module goes next ↓ and

TCP-IP → 4 layers

order of layer goes from top to bottom



Tcp / ip → 4 layers

① Application → layer 4

Ex : HTTP 80, Https 443, Ftp 21, , Ftps , Dns 53, Dhcp 67, Rdp 3389
telnet 23, windows port 25

application same as in Console / si

② Transport → layer 3

TCP, IP

③ Internet → layer 2

ip, NAT

④ Network access → layer 1

mac, IP SEC, ARP

① Network access → layer 1

A mac

B IP SEC

C ARP

A MAC

(media access Control) physical address hexadecimal 0-9 A-F

1 hexa = 4 bit

→ mac = 12 hexa = 48 bit

unique

Segment
Packet
Frame
bites

24bit
Vendor Oui
24bit
Host Hui

IEEE

mac address 48 bit / 6 byte

16777216

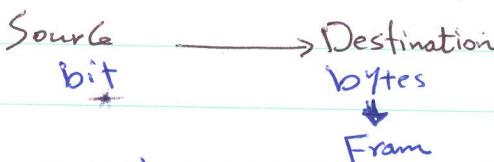
bit

mac / 12

$$\Rightarrow 2^{24} = 16777216$$

 LLC → local link Control

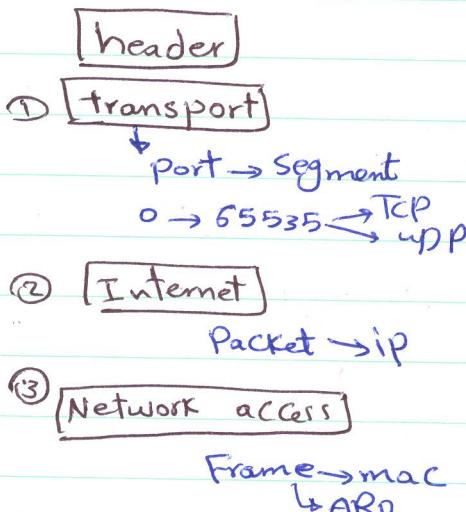
نحوں من والی bit bytes کا check ہے جو destin IP address کو broadcast کرے۔ LLC



(LLC) \rightarrow 8 bit \rightarrow 1 byte



لحوظات **Lab** مثلاً جهاز يعمل على بروتوكول Ping لذاً يكون عارف بالآدرس IP وعنه يعرف الآدرس mac بداعه بـ ARP protocol يحيط بالآلات بالمريخ او
C:\> arp -a ل查詢 ARP مثلاً تعرف الآدرس



• من ذكره : عدم جهاز غير (ARP) وسائل رجوع يار

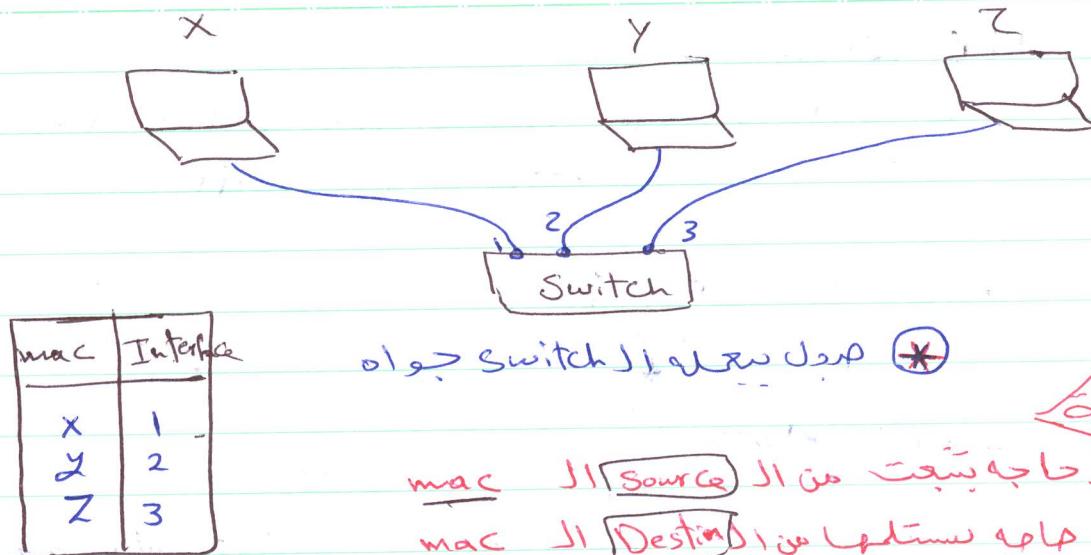
BroadCast

FF-FF-FF-FF-FF-FF

ملحوظہ: ARP II سے کل سرویس بیکارنے کا ایک Broadcast ہو جائے گا۔

فنهاد mac پیغام طبع دارد و درین پیغامها عنوان

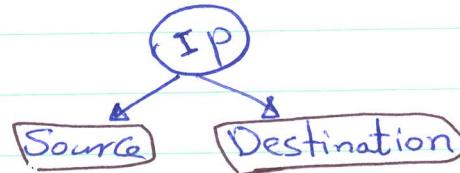
C:\>nbtstat -C Cache لحصيل الحالات التي تمها
-- يحفظها ٦٠٠ ثانية



layers Internet Data بعدها سنلاد

IP

NAT



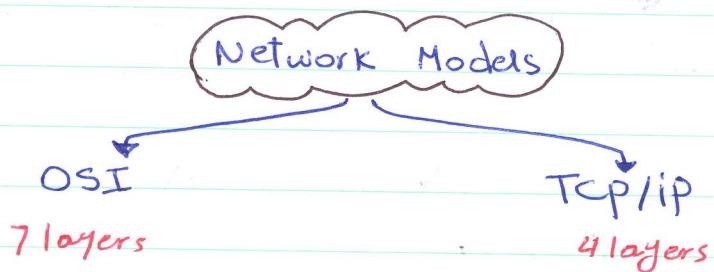
Decimal

Ex: 192.168.1.1 Decimal في بين ايجامات

binary في اخر 3 دخولة

5

"4" TCP-IP ②



Internet ← طبع الارقام لـ data الارقام

"Internet"

ip, NAT

IP

IP v4

IP v6

4 octet

— — — —

8 bit × 4

= 32 bit

$$\rightarrow \frac{1}{2} = 256$$

Decimal

IEEE

Class A

0 → 126

Class B

128 → 191

Class C

192 → 223

Class D

224 → 239 ↳ multicast [video conference, games]

Class E

240 → 255 ↳ experimental

IP

Private

LAN

Internal

Public

WAN

External

Class A $10.0.0.0 \rightarrow 10.255.255.255$

$0.0.0.0 \rightarrow 126.255.255.255$

Class B $172.16.0.0 \rightarrow 172.31.255.255$

$128.0.0.0 \rightarrow 191.255.255.255$

Class C $192.168.0.0 \rightarrow 192.168.255.255$

$192.0.0.0 \rightarrow 223.255.255.255$

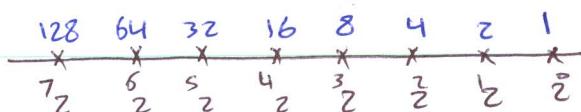
Host تجربة ملحوظة

Class A, B, C

Network ID
Common

Host ID
unique

التحويل من binary إلى decimal



192.168.1.1

255.255.255.0

11000000.1010000.00000001.00000001

11111111.1111111.1111111.00000000

Decimal

binary

bitwise
Anding

مطابقة subnetmask مع IP

192.168.1.1

Subnetmask

255.255.255.0

8 - 8 8 0

→ 192.168.1.1/24

Class A /8

Class B /16

Class C /24

Number of Host in every Class = 2^n

\boxed{N} = Number of Zero's in Subnet

$$\text{Class A}/8 = 2^n = 2^{24}$$

$$\text{Class B}/16 = 2^n = 2^{16}$$

$$\text{Class C}/24 = 2^n = 2^8$$

"5" Tcp - IP

كل ما ياتي في subnet تحتوي على اصناف كثيرة كلها كانت تتشيل أجهزة
أكبر وكلها زارت الواحد قلت عدد الأجهزة التي تتشيلها.

192.168.1.0

ال 0 هي ال Network ID يرمز لها IP

192.168.1.255

ال 255 هي ال Broadcast IP يرمز لها IP

255.255.255.0

ال 0 هي ال Host Subnet يرمز لها IP

(255.255.255.0)

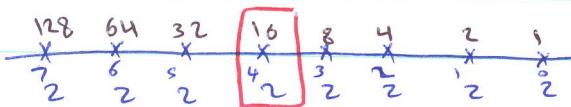
ال 255 هي ال Network Subnet يرمز لها IP

$$\textcircled{2} \text{ Number of Host} = 2^n - 2$$

Ex: 192.168.1.0

عاليزينة تتشيل 20 جهاز

ال 254 بتاعة default



$$\textcircled{1} \text{ Number of Host} = 2^n = 2^4 = 16$$

Subnet القديم 255.255.255.0

.....111111.111111.111111.00000000

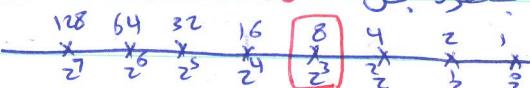
Subnet الجديد111111.111111.111111.11100000

255.255.255.240

كذا تتشيل 14 جهاز

Ex: 192.168.1.0

عاليزه تتشيل 8 أجهزة بين



New Subnet111111.111111.111111.11110000

255.255.255.248

Ex: 192.168.1.0 \leftarrow 1000 PC خاير نتية يشيل

1024	512	256	128	64	32	16	8	4	2	1
X	X	X	X	X	X	X	X	X	X	X

عدد المقدار

$$n=10 \rightarrow 111111.111111.1111100.00000000$$

$$255 \cdot 255 \cdot 252 \cdot 0$$

$$192.168.1.0 / 22 \rightarrow \text{الويمان}$$

Ex: 192.168.1.0 \leftarrow 64 PC

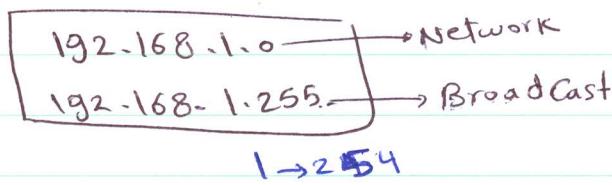
128	64	32	16	8	4	2	1
X	X	X	X	X	X	X	X

n=6

$$111111.111111.111111.11000000$$

$$255 \cdot 255 \cdot 255 \cdot 192$$

$$192.168.1.0 / 26$$



1 → 254

$$255.255.255.248 \leftarrow 8 \text{ PC}$$

192.168.1.0 \rightarrow Network كيبر من Network ID

192.168.1.7 \rightarrow Broadcast إلى

دافعلي كيشيل 64 جهزه

د5 الـ network الى بدها 1.8

د5 ستنهى بـ 1.0

لاب يكون رقم زوجي ويقبل القسمة على 8 قاعدة Network ID
لاب لا يكون رقم فردي ولا يقبل القسمة على 8 Broadcast

Ex:

$$192.168.1.0 \rightarrow 64 \text{ PCs}$$

$$255.255.255.192$$

$$192.168.1.0 / 26$$

Start \rightarrow 192.168.1.0

End \rightarrow 192.168.1.63

$$\text{Start} \rightarrow 192.168.1.0 \cdot 64$$

$$\text{End} \rightarrow 192.168.1.0 \cdot 127$$

Ex:

$$192.168.1.0 \rightarrow 3 \text{ PCs}$$

$$255.255.255.254$$

11

$$192.168.1.0$$

$$192.168.1.1$$

109

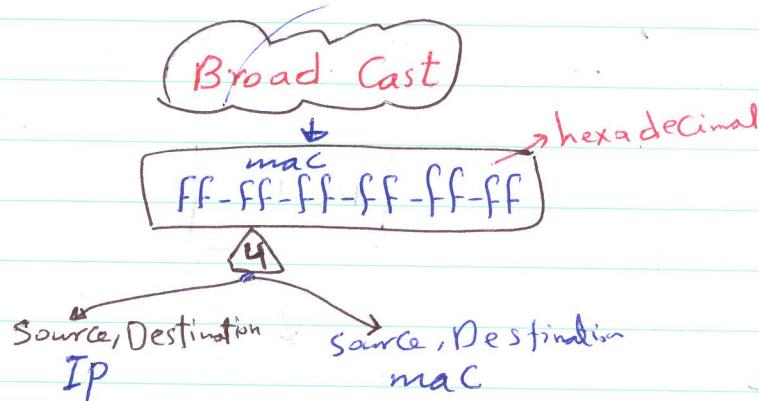
"6" TCP - IP 4

Ex. 10.0.0.0 /29

Subnet 255.255.255.248

→ 10.0.0.0

→ 10.0.0.7



Ex: 10.0.0.0 /8

10.255.255.255 بث播廣 Cast

Ex: 10.0.0.0 /29

Broadcast: 10.0.0.7

Sip	Dip	Smac	Dmac
10.0.0.1	10.0.0.7	FF-FF-FF-FF-FF-FF	

Ex: 192.168.0.1 /19

255.255.224.0

192.168.0.255

نخل اخر 255 octet

255.255.224.0

وندخل في الـ جيـه طـيـاعـوـصـل

أعـجـبـهـابـ 8190

Broadcast 192.168.33.31

192.168.1.1

192.168.2.1

Router دلـ حـاـيـشـوـقـوـثـ بـعـضـ عـسـتـاـ نـيـشـوـعـواـبـعـمـ لـارـمـ بـيـصـلـواـدـ

10.0.0.1

172.16.1.1

10.0.0.2

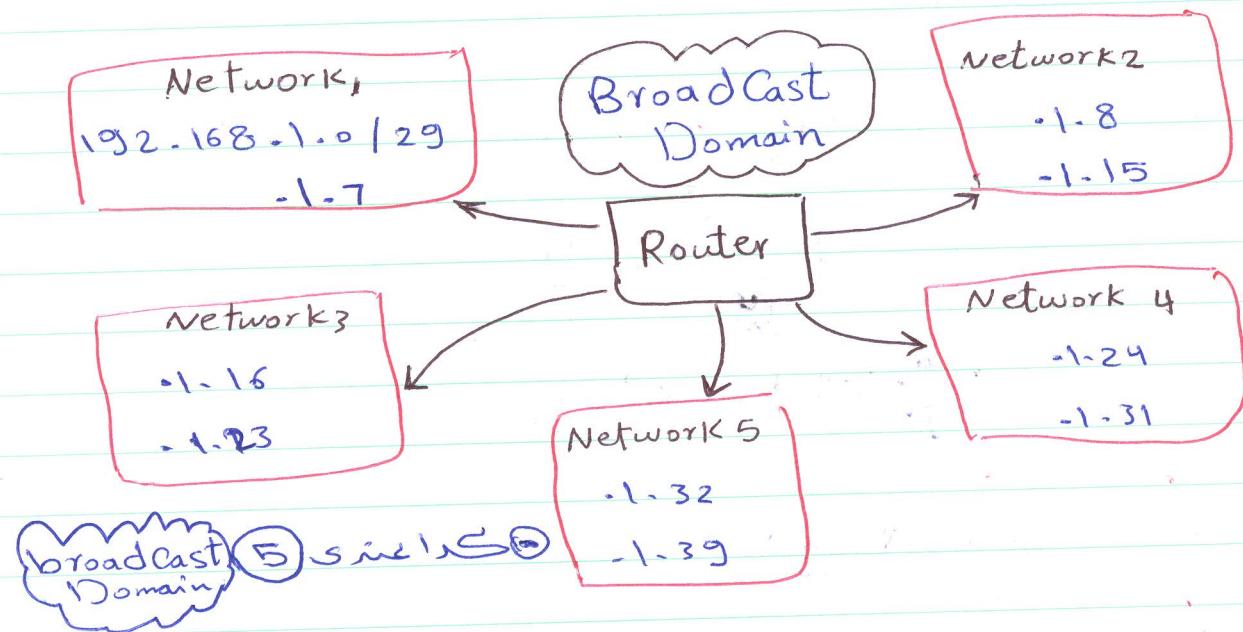
172.16.1.2

لازم ارتكب للراوتر 2 كادت مت

واحد من المعمليات range IP او first last IP

ملحوظة

Router يفهم الـ Default Gateway فقط لاحظ



فقط Router يعلم عن播送 (Broadcast) لأن Router لا يفهم播送

Collision Domain

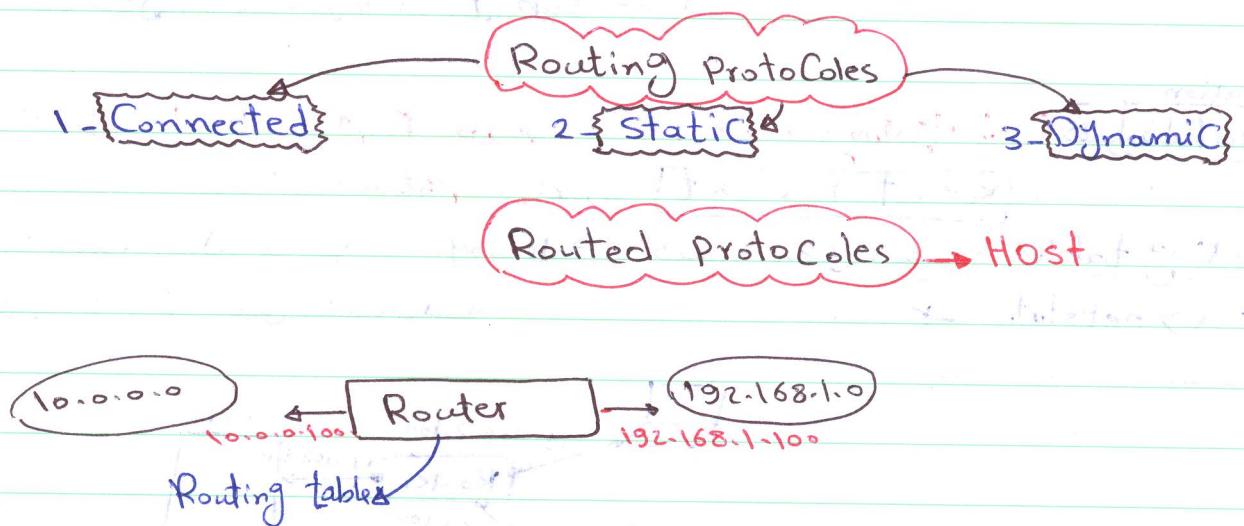
يتحقق من الـ Switch من سه Ports وبعضا

الوصول إلى Router يكون جوا Router (Broad Cast) فقط، لباقي الأجهزة فقط ولو عبارات كثيرة جداً أو Subnet يتعارض معه Router حيث أن المسندة إلى آخرين بخلاف Router تكون جوا المسندة إلى الآخرين (Broad Cast)

7) Simple Routing (Connected)

mac : Hop-to-Hop delivery

IP : End-to-End delivery



- ① **Broad Cast**
 - ↳ one-to all
- ② **MultiCast**
 - ↳ one-to many
- ③ **uniCast**
 - ↳ one-to one

Ping 2188 (TTL) time to live

Router its will of 1 second 128 times

Server is software Microsoft is Router is **Lab mode**

Hardware calls Cisco 6500

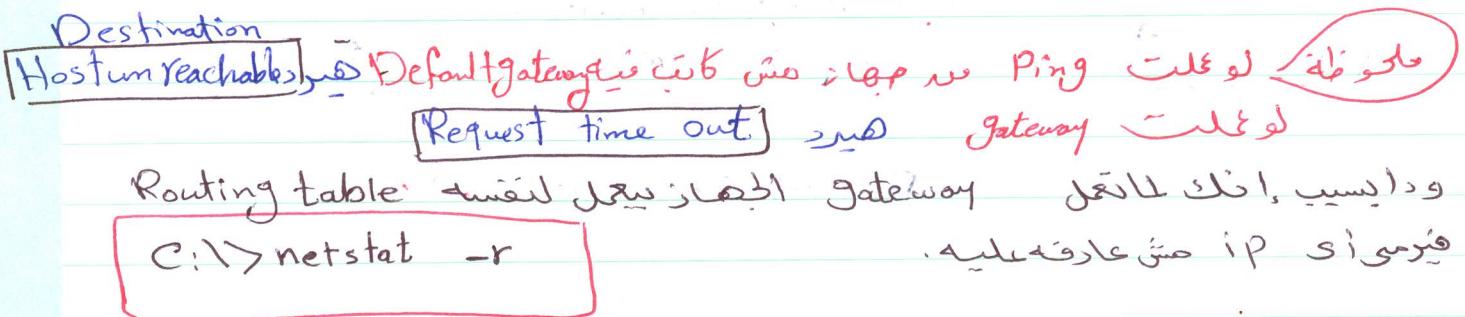
① 192.168.1.1

② 172.16.1.1

③ 192.168.2.1 وعاليزون سيرفوراينج

لوحة جهاز كل واحد من تلك لوحة

لعملت Ping من اي جهاز على الثاني من كمبيوتر لا الموقن
لكن كل واحد منهم في subnet مختلف



وادى بسيب انك لاتعلم gateway اليمار يتعل لفقطه gateway

C:\> netstat -r

عشان تخل جهاز روتراي VM لنضيف 3 كروت Network

ونحط عليهم 3 IP بناع المفاتح الواصمه بال Router

ونحط كل واحد على switch لوحة

ونوصل كل Client بال Switch بناء على IPاته

والموقع كما

ونخل Ping لكل Client بناء على IPاته

كل ما عانا جهاز فيه 3 كروت Network فيه Server اخلي

* Servermanager → Roles → add Roles → Next → Network policy and access services
→ Next → Next → Routing and Remote access services
 Remote access service
 Routing

→ Next → Install

→ administrative tools → Routing and Remote Access →

① Router (local) → Right Click → Configure and enable Routing and Remote access
→ Next → ② Custom Configuration → Next → LAN routing
→ Next → Finish → start service → Finish

رِيْكَارْدُو هَنْلَاقِي الْجِهَاد عَلِي لَمَسَّهُ
Routing table

C:\>netstat -r

9) `C:\> route print`

* تزوج بعده كل gateway وكل جهاز Client ينبع من gateway

→ Router أحدى أعمدة بنية وسیط الواقع كـ

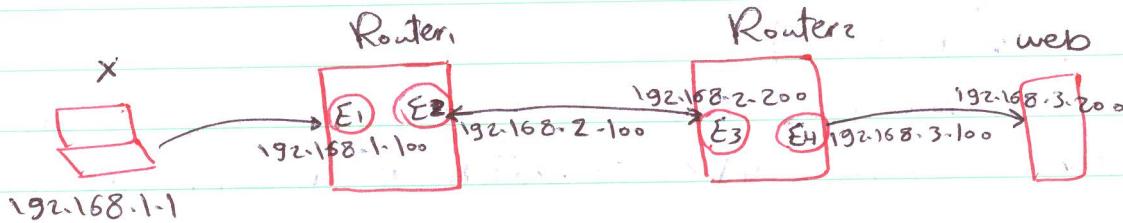
(C:\>pathping - 192.168.1.1)

Simple routing ↵

Connected

يعنى اللي واصل بي Cable مباشر مع ال Router

11.8 Static Routing



E₂ (E₁) فاهم السيناريو Router1

E ₁	192.168.1.0
E ₂	192.168.2.0

Router1

192.168.3.0

E₂

E₃

الخطيب العربي

Router2

E ₃	192.168.2.0
E ₄	192.168.3.0

Router2

192.168.1.1

E₃

E₂

R₁

E₁ → 192.168.1.100 (Vm₁)

E₂ → 41.1.1.1 (Vm₂)

Client₁

192.168.1.1 (Vm₁)

R₂

E₃ → 41.1.1.2 (Vm₂)

E₄ → 192.168.2.100 (Vm₃)

Client₂

192.168.2.1 (Vm₃)

R₁

E ₁	192.168.1.0
E ₂	41.1.1.0

R ₂	R ₂
E ₃	41.1.1.0
E ₄	192.168.2.0

نعمل في R₁ و R₂ على ping إلى الشبكة الداخلية بقائمة وكل سائقها.

(R₁)

admin tools → Routing and Remote Access → Router1 → Network Interfaces → إضافة الشبكات التي شاركها.

IPV4 → static Routes → New Static Route

Interface E₂ (41.1.1.1) قاعدة الروابط في الشبكة المترابطة

Destination 192.168.2.0 السبركة المقابلة

Network mask 255.255.255.0

Gateway 41.1.1.2 قاعدة الروابط في الشبكة الثانية

Metric 1 عدد الافتراضات



وکذلک راوتر اسین R₂

Interface E₃ 41.1.1.2

Destination 192.168.1.0

Network mask 255.255.255.0

Gateway 41.1.1.1

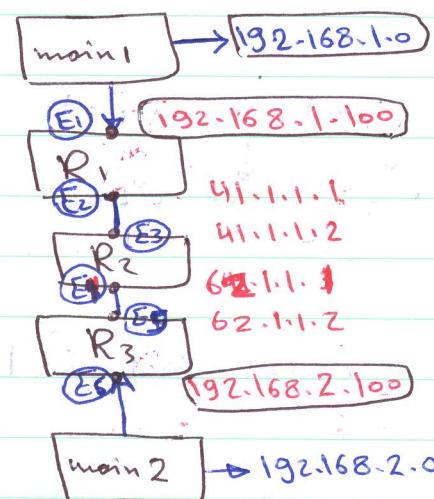
metric 10

من ای جهاز عاید جهاز ونچل Ping

TTL=126 (خطہ)

لوگوں کے طور پر Pathping کی طرف سے عاید مسافت تکمیل کر دیا جائے

C:\> pathping 192.168.1.1



لوگو صفت راوتر تالث +

نکل عاید IP جی R₂ کے ساتھ، اس 62.1.1.2

وں 4 عاید R₃ و R₂ کے ساتھ

وں 5 عاید E6 کے ساتھ
وں 5 main2

(R₁) static route جسے اسی طبقہ میں

Int E₁ (192.168.1.100)

Dest 62.1.1.0

mask 255.255.255.248

Gateway 41.1.1.2

Int E₃ (41.1.1.2)

Dest 192.168.1.0

mask 255.255.255.0

Gateway 41.1.1.1

Int E₅ (62.1.1.2)

Dest 192.168.1.0

mask 255.255.255.0

Gateway 62.1.1.1

Int E₁ (192.168.1.100)

Dest 192.168.2.0

mask 255.255.255.0

Gateway 41.1.1.2

Int E₄ (62.1.1.1)

Dest 192.168.2.0

mask 255.255.255.0

Gateway 62.1.1.2

Int E₅ (62.1.1.2)

Dest 41.1.1.0

mask 255.255.255.248

Gateway 62.1.1.1

"9" Dynamic Routing

Dynamic

Rip v1 Rip v2

broadcast multi Cast

Router 1 (Broadcast Interface) على (Rip v1) ينزل (Broadcast)

لـ (Rip v2) ينزل (multi Cast) لـ (Router 2) (Multi Cast Interface)

لـ (Rip v2) أورادوـر في طريـقة يـسـطـقـفـ السـيـكـةـ دـيـنـاعـةـ وـيـطـهـاـ فـيـ رـوتـنـجـتـابـلـ

Rip v1
Broad Cast

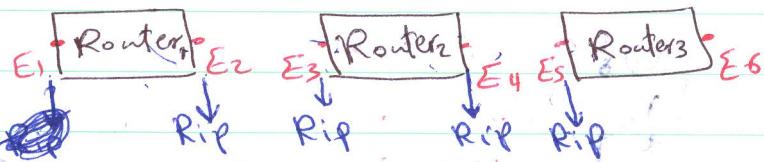
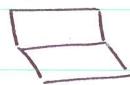
Rip v2
multi Cast

فقط ورد في طريـقة Router 1 16 بـسـحـرـكـ لـ Router 2 16 Routers 1 16 one-to-many Router 2 Routers 1 16 Passwords بـسـنـاـ اـنـ اـنـ عـاـيـزـهـاـ

Router 1 16 Router 2 16 Router 3 16

Authentication

Client



كل داوتر جـمـعـهـ رـاـوـتـرـاتـيـ بـسـخـدـهـ لـ الـ رـاـبـطـاتـ

R1

Static Route

الـ مـسـحـ

admin tools → Routing and Remote Access → IP v4 → General →
New Routing protocol → Rip v2 → OK

R1

• RIP → New interface → E2 (192.168.1.1) → OK

R2

• RIP → New interface → E3, E4

R3

• RIP → New interface → E5

دـيـ ping 192.168.1.1 -t

ping لـ اـنـ عـاـيـزـهـ اـنـ

General



operation mode:

Periodic update

كل مدة تحددها

auto static Rip ينقل المعرفات static new Route
لهم حصل تبديل الـ RIP

out going packet

Rip v2 multi Cast

[Security]

ip ونكتة IP → [add]

لو اضطرت دى

use neighbors in addition to broad or multi

Rip v2 broadcast

[Security]

Accept all routers

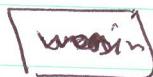
Accept in range Range المكتبة

• Packet Filter

Access Control List

Cisco في اسم

web



نحو معايير الأجهزة عن طريق حقل او



انتهاء Client من main لا يوصى غير web

Port 80
HTTP

65535 port على

ملحوظه ان الارقام المدخلة على E1 هي اتجاه traffic من routers الى الفاصل

لتحت الاوامر تفتح افلاطها على اول مخرج بعد الرور المدخل

بيانات مصدره - si على

Out bound , In bound

Routing and Remote access → IPv4 → General → E4

out bound → New → Source network

ip 192.168.2.0

mask 255.255.255.0

Destination

ip 192.168.1.6

mask 255.255.255.0

Protocol TCP

Source port

قافية

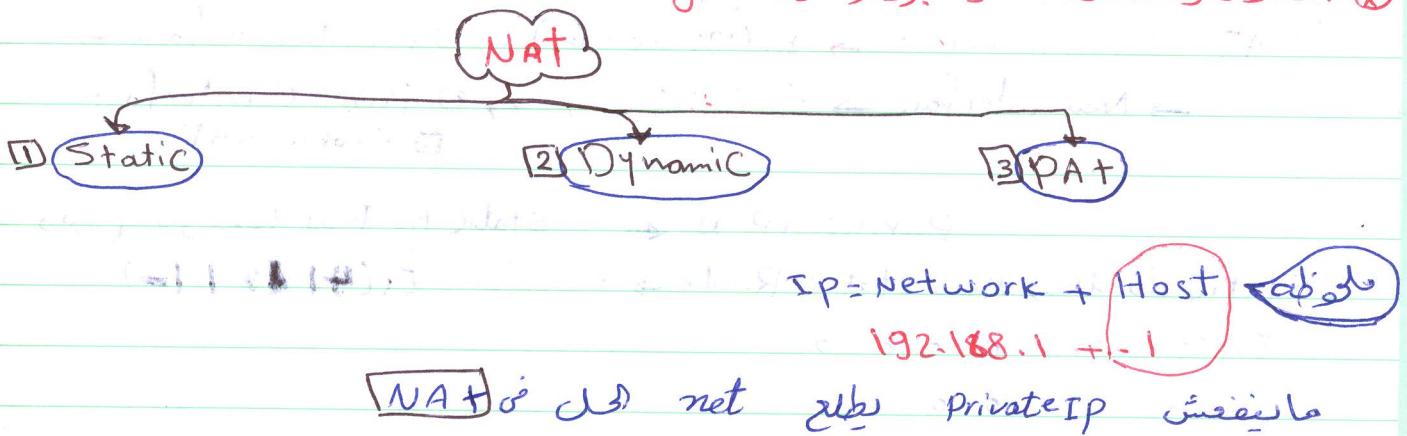
source port if true Destination 80 → OK

- Transmit all packets except those
- Drop all packets except those

نحو حقل مابه (80) نتحقق الموقع

(10) NatingNetwork address translation

* أي راديو أو مودم عليه بروتوكول الـ Nating

① Static NAT

كل جهاز لديه Private IP هشتريله Public IP

* 30 private \rightarrow 30 public

- 192.168.1.1 \rightarrow 62.1.1.1

- 192.168.1.2 \rightarrow 62.1.1.2

Security أو فيه مشكلتين
الكلفة عالية.

سلوكيات static 11

② Dynamic NAT

عبارة عن Pool public IP هشتريله Pool private IP ويتدلوا اتسواني

30 private \rightarrow 20 public

- 192.168.1.1 \rightarrow 62.1.1.1

- 192.168.1.30 \rightarrow 62.1.1.20

يستخدم في Exchange Server

يجا حل مشكلة الـ Security وقلل شوبة في الكلفة

③ PAT

Port address translation

Private IP 16777214 \leftarrow 1 Public IP عبارة عن

16777214 private \rightarrow 1 public

يسرحه الـ Public IP لـ private IP يرجع بالرد

يسخدم الـ Port لتثبيت الفرق بين الأجهزة

Subject.....

PAT II (نحو اولى) = "النحو الثاني"

Routing and Remote Access → IPv4 → General → New Routing protocol

→ NAT → OK

Private IP (نحو الثالث) →

NAT → New interface → E1 (192.168.1.100) → Ⓛ Private interface →

→ New interface → E2 (41.1.1.1) → Ⓛ Public interface

Enable NAT

Public IP II ← static Route (لخوفها للغوفها) ←

Static Route → New static Route → Interface E1 (41.1.1.1)

Destination 0.0.0.0

mask 0.0.0.0

Gateway 41.1.1.2

Metric 1 → OK

Static (نحو الثاني)

Public (نحو الرابع)

NAT → New interface → 41.1.1.1 → Ⓛ Public interface

Enable NAT

Real IP Range (نحو الخامس)

Address Pool → Add → Start 41.1.1.1
mask 255.255.255.248
End 41.1.1.7 → OK

Reservations (نحو السادس)

Private IP II (نحو السابع)

→ add → Reserve IP Public

41.1.1.1
For this Computer on Private network

192.168.1.1

Private IP II (نحو السادس) → Public IP (نحو الخامس) طريقة اولاً من بروتوكول IPSec Allow incoming session to this address

Private IP II (نحو السادس) → add → 41.1.1.2
Public IP (نحو الخامس)

192.168.1.2

Dynamic (نحو الثامن)

= Address pool → Add → Real IP II (نحو سابع)

NAT → Properties → address assignment

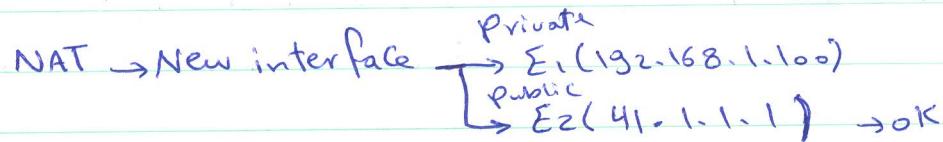
Automatically assign IP

IP address
mask

Private IP II (نحو سابع)

ملحوظة

في الحياة العملية مش بدليه Real IP لكن بدليه Private Router يفتح الـ Public بـ IP على الـ Router



E2(41.1.1.1) → Services and ports

web server http

◎ one this interface

Private ip 192.168.1.100

http://41.1.1.1

① كـ Client متصل

غير مسجل على الموقع الـ IP

دعشان الـ Security يعنى IP يفتح الـ Site

Remote Desktop Service و كذلك في

11) DHCP

« Dynamic Host Configuration protocol »

DHCP Server

• الـ Sub mask والـ ip والـ Gateway والـ DNS والـ domain name

- IP من Configuration بیدی لا جهز DHCP سی لابو

scope DHCP لازم رکونه کنند

Scope = IP Address Range, Subnet Mask

Install DHCP

Roles → add Roles → Next → DHCP Server

→ Next → 192.168.1.1 → Next → Domain DNS دار

→ @wins not required → Next → Scope خودا

Add → name [] Start [] End [] mask [] gateway [] IP address []

→ Next → \oplus Disable DHCP vs → Next →

❸ Use Current Credentials admin يَعْرِفُ بِنَا

Skip authorization → Install → Close

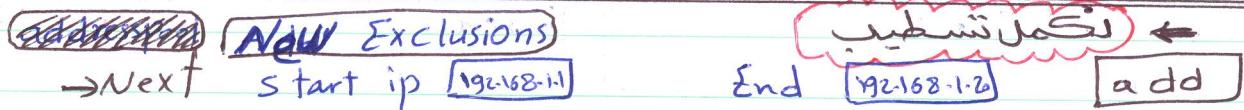
مثلاً DHCP استعمل بس هنّ هبيون غير ملائمه Scope على مرض انه معذبه شرط

IPV4 → New Scope → Next → Name [] → Next
Start ip [192.168.1.1]
End [192.168.1.254]
Length [24] ^{mask} _{دالة الماسك}
Subnet mask [255.255.255.0] → Next

لا جمجمة Subnetmask Scope ماني نفس ستحل تاني لأنّه تشيل او ولتحلها من جديد

DHCP ينفع فيأخذ IP من الـ Server والـ Printer وللـ Range كل جهاز من نطاق الـ DHCP يحصل على IP

كما أسلفنا، هنا سبب DHCP يعني نعرف الـ IP انه مایدش الـ Printers و الـ Servers و الـ Static يتوجه لـ جهاز لأن دول أناه خلود



الـ Range هو مساحة طرد

→ Next → Leased Duration IP مدة الإيجار

Days Hours minutes
 → Next

① Yes, I want Configure options → next

Default Gateway → add → next

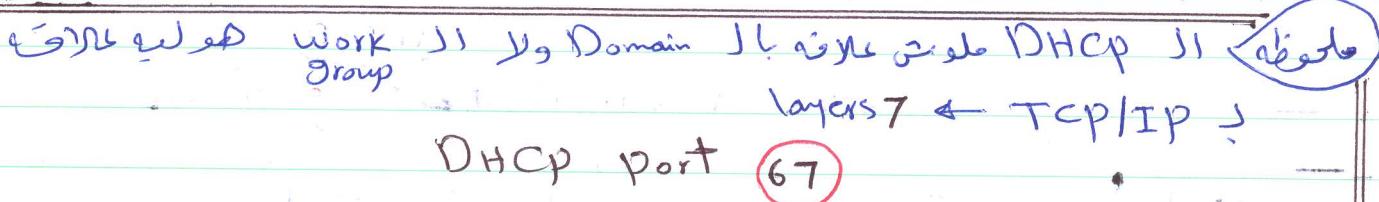
DNS → next → next → ② Yes, I want activate scope
→ Next → finish

Scope II IPv4 كتبت
ويندرأ تشغلي اولاً DHCP

admin tools → DHCP → IPv4 → Scope → Properties
الـ Range هو جزء من mask ينبع منه
• address pool لـ IP الذي ينبع فيه New Exclusion
• scope options DNS Options التي تخصيصها
• Address leases الـ lease التي تأخذ IP منه وتحتفظ بها

③ لورقة على الـ Client وتحت Client obtain automatic

DHCP هي بروتوكول IP الذي يأخذون منه
وهو يعتمد على الفضاء المخصوص به



لأنه في المتصفح في الـ browser \rightarrow back ground message \rightarrow Client

ادخل ما دار \rightarrow Client \rightarrow obtain automatically IP address

1 Discover message

S port	1024	D port	67
SIP	??? 0.0.0.0 switch	DIP	??? 255.255.255.255 broadcast
Smac	Client	Dmac	??? FF-FF-FF-FF-FF-FF

لحوظة يتعاون DHCP هنا ممكن ما يتردش عليها .
دخل ما دار مع Floating IP يوصل switch طبخت FF-FF-FF-FF-FF-FF
لكل العقدات يستلمهم المايند DHCP يرد عليه؟ يرد اد

2 Offer \leftrightarrow DHCP Server

S port	67	D port	1024
SIP	192.168.1.1 يتابع او DHCP	DIP	192.168.1.255 يعطي Range 11 no broadcast
Smac	DHCP	Dmac	FF-FF-FF-FF-FF-FF switch no ok broadcast

لحوظة كل DHCP يعرف اد Client انه موجود واللى عايزه

يكتبه وبرضنه يكون

3 Request \rightarrow Client

Sport	1024	Dport	67
SIP	0.0.0.0	DIP	255.255.255.255 Broadcast
Smac	Client	Dmac	FF-FF-FF-FF-FF-FF

ويطلب DHCP اد IP يطلب Client اد لـ لحوظة

4 ACKnowledgment \leftrightarrow DHCP Server

Sport	67	Dport	1024
SIP	192.168.1.1	DIP	IPclient
Smac	DHCP	Dmac	Client

TCP و IP \rightarrow Client اد DHCP اد لـ لحوظة

IPV4 → Right Click → **Display statistics**

تحليل الرسائل

و عدد الطلبات و هي جدول احصائيات .

للحظة DHCP يبحث لا يجد Client لجر ٠.١ من مدة الایجار لسؤال

لتحدد لا يجد لا يجدهم ؟ NC طلب message

لو DHCP لفقي اطلبها : معمول يستعمله بعد ٠٨٧٥٪ من مدة الایجار لسؤال database لتحقق هل يجيئ على طرد مامدة الایجار لخلص لومردىش للمساحة من العداد

DHCP ملحوظة عسان نسخه Client نعسان البيانات الى ما ذهابه

C:\> IpConfig /all

DHCP ip عسان يلغى الایجار

C:\>ipConfig /release

عسان يحدد الایجار

C:\> ipConfig /renew

ملحوظة

لوقت لا يقدر كذا من هيتشي

DHCP بتابع او Folder لمعايير الشروق

C → windows → system32 → dhcp → log

فت برائته و تحريره والـ ip الذى وزعها

طهارى كل action اتقل يجهز DHCP log

ملحوظة عڪر ابنت ip طهار لوجهه خرس ياخذه علىه بجهه بجز حته وقت السؤال

IPV4 → **Reservations** → **New Reservation**

Reserv. name [] اسم اجهزة

ip address 192.168.1.136

Mac address [] ازى اعرف mac اجهزة

GDHCP CCGetmac لـ IP 192.168.1.2 من برزاج بصيغه, LLC /u administrator /p 123 /w سورد

→ add

1. Ping 192.168.1.2

2. arp -a صحيحة الـ IP

2. getmac /s 192.168.1.2

/u administrator /p 123

• حسان نسبت ip لكيذا جهاز مع بعضه ينتمي إلى

reservation

DHCP.bat

netsh dhcp server scope 192.168.1.0 add

reservedip 192.168.1.25 000CG92C86 → mac

وكتبتها لكيذا جهاز وتغير ip وار

Alternate Config

لولبات المطلوب . ① obtain automatic

② userConfig & DHCP لـ IP دا

IP []

(APIPA)

③ Automatic private ip address

Class B

169.254.0.0 → 169.254.255.255

دارجات المجزئات IP، DHCP، بياخرته Range

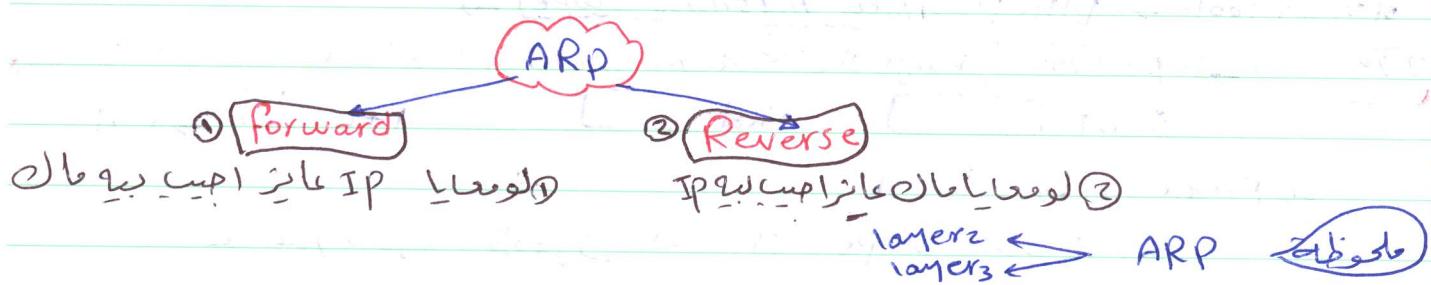
Range في APIPA تعرف نظام بعضها البعض في

المخططة الـ Class B واحد و Class A مع بعضهم

* جهاز على عرض دقائق يبعث رسالة Discover لـ DHCP لـ

الـ DHCP (ستعمل هياكله من ip)

4.12. DHCP ②



ملحوظة : يفتح امثلة كثيرة على DHCP Scope حتى لا يكون على نفس Subnet اهم حاجة ماركت لنفس ال Range || Range ||

Ex:

5 Cope, 192-168-1-1 192-168-1-30 mask 255.255.255.0

Scope2 192.168.1.33 192.168.1.61 8J

لوازا mask مفتوحة کدا حش ڪيڠ اعمل Scopez

و لكن لو خلصتها كرادامي Scopei $255.255.255.224$ كا هي نفع عساناً قفلت

اتى network فى Scop2 و network is Scop1 فهذا ينبع من mask II

255.255.255.244 Scopz C mask 111

لتحق المهم مفهـس دكتـوى scope جواها .

Scope options: Scope will decide options like Ex: Router

Server Options: SCOps will take care of option like Ex: DNS

الخطوة ١١ DHCP سوچ ١٣ من ١١ الى راهن همها نفته

من الـ Range بـنـاـءـها يـعـنـي كـارـتـ الـ net~work بـنـاـءـها مـنـ الـ Range بـنـاـءـها

Super Scope

Scope لیکن اس سطح فنی کذا

admintools → DHCP → IPv4 → Right Click → New SuperScope → Next → None

→ Scope الـ λ \rightarrow Next

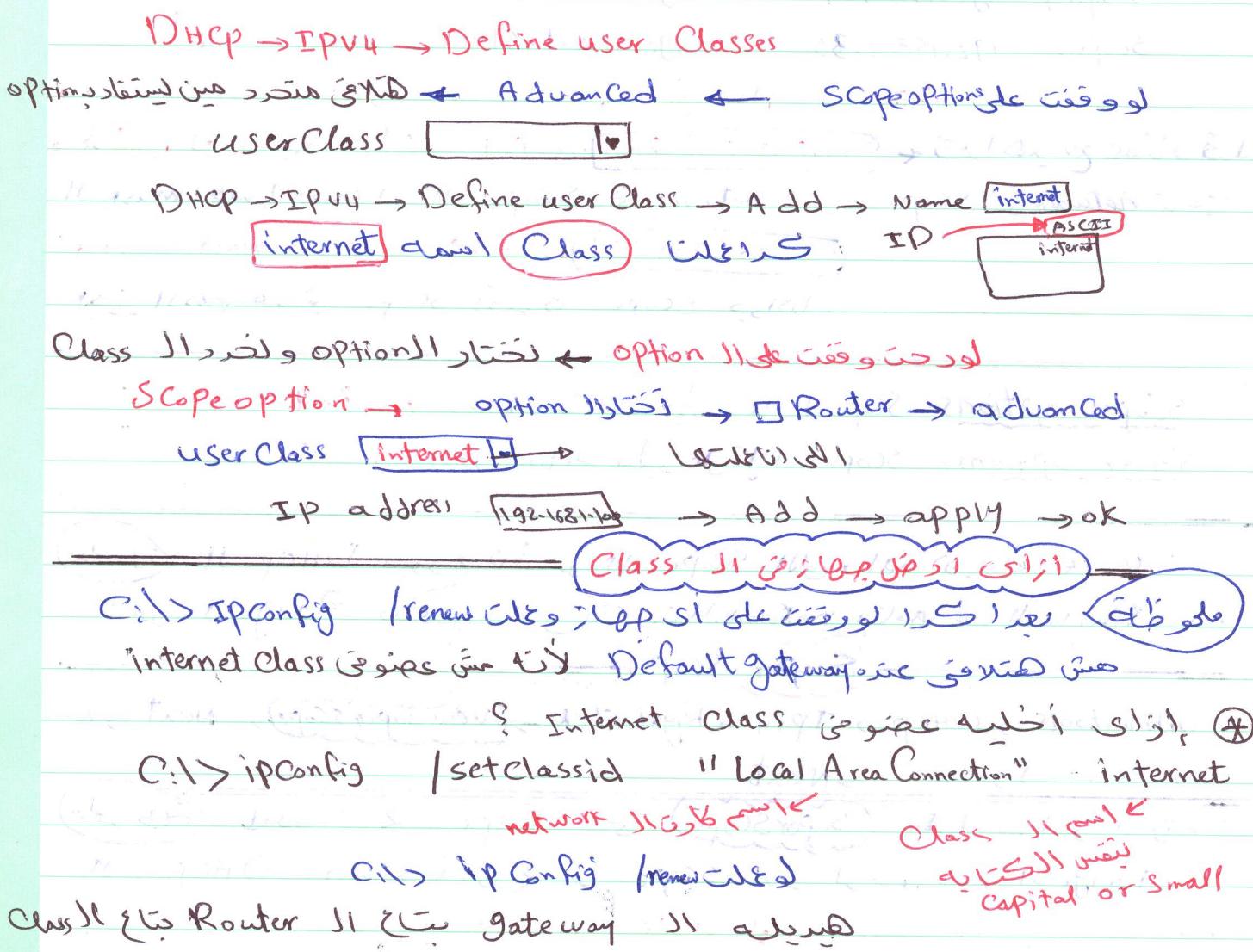
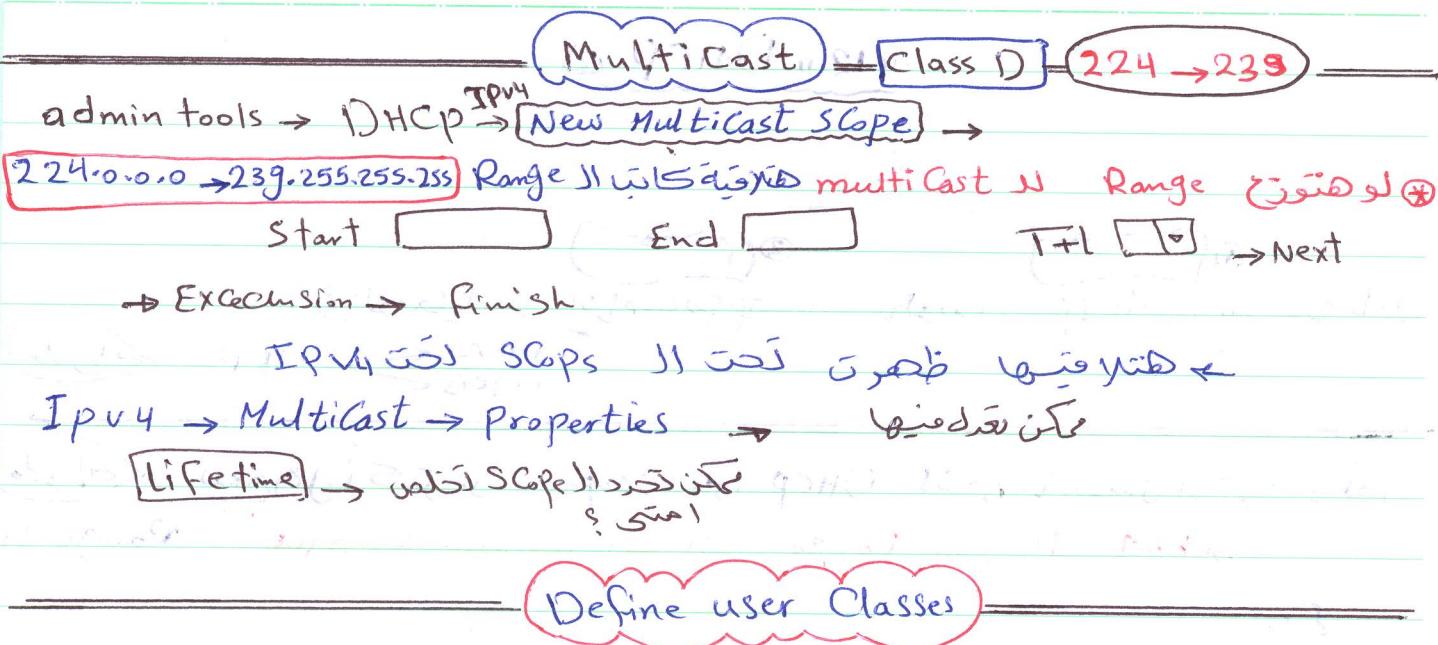
SuperScope میں Scope 2 ball کا نام دخال کر دیا گی

نـ DHCP يـ بـسـدـ زـيـونـجـ مـهـنـ لـوـمـقـنـ لـفـسـ الـاـنـ

و کار یافی طلاک کر جهاز من Scope لومدره یافی هش همیستوف فاعلیت

وهي تحدد نطاق DHCP من سُقُن الوجهة التي تُدار Scope.

• Indo Range II



و من همیشه نلتانی

نوع ایجاد خل کذا جهاز في Class
 Class.bat → ipconfig /setclassid "Local Area Connection"

Intent

GP → net چنطه گوئی on active directory user and group
 GP → Script → Startup → Class.bat ورخ

Define Vendor Class

نوع ایجاد هسته معرفی +

Proxy
Gateway
Firewall

عسان اطلع هست Net Firewall

Firewall
Client

Server بدل

DHCP

1 IPv4 → Define vendor Class → Add → Name TMG
 IP TMG → OK

2 Client نجذب عسان تغون ال

IPv4 → Set predefined options → Configure options →

option Class TMG

add → Name TMGclient

Datatype String

Code 081

آخر حسم بعد (B) Builtinoptions → OK

Value

String: http://192.168.1.100:8080/WPAD:8080

TMG پسخ

TMG Client شاید تحریک او Capital O تحریک

Scope options

Configure option → Advanced → Vendor Class TMG

→ Apply → OK

که المی سنبه علیه هسته

ملحوظه Reconcile لوقتی علی ال لفیضها Client هسته رکنیلیزه Verify

ملحوظه DHCP error پسخ سخاله طالع مطلبی IPV4 یعنی علی المی سنبه

میکنی در منه اتفاق علی ال scope داخل

C → windows → system32 → DHCP → backup

DC-ABC.COM → Right Click → backup →

DC-ABC.COM → Restore →

ملحوظه لفتح اتمل backup N

server N RestBackup فرماتیزه

DHCP N backup بدل

"13" DHCP Split & Relay AgentDHCP split 2008 R2

• نعمل ad balance بين DHCP Server ② دخل لهم حماية ونعمل
حماية عسان ما ييقاشر ادخل كلهم على واحد ويبيوزعوا بينهم وبين بعض
50-50 , 80-20 , 70-30

DHCP1 1-127

DHCP2 128-254

Discover message

المسكلة الـ 11 الجهاز يجل IP انتهى واحد

فقط هيرد ؟

هيرد الاسرع منهم وهو الذي هيديتني IP
المسكلة لمعامل Reservation طهاز من **DHCP1**
والأسرع كان Reservation بـ Range من IP **DHCP2** فيهديلة

DHCP1, DHCP2 انتانجل الـ Reservation على مشترك بين

Ex: DHCP1 1-127 DHCP2 117-254

Reservations من 117-127 هوا ديك

في كل 1 IP هييفهم و DHCP2 هييفهم

DHCP Split

2008 R2

2008 R2

لمعايير DHCP يتآثر عن DHCP الثاني في الرد على المدى على نفسه

Scope → properties → advanced → Subnet delay 2 ms

كل ما هو متصل بالBroadcast غير بعد المدة دي *

• لابد الاتيني يكون له نفس النسخة 2008 أو 2008R2

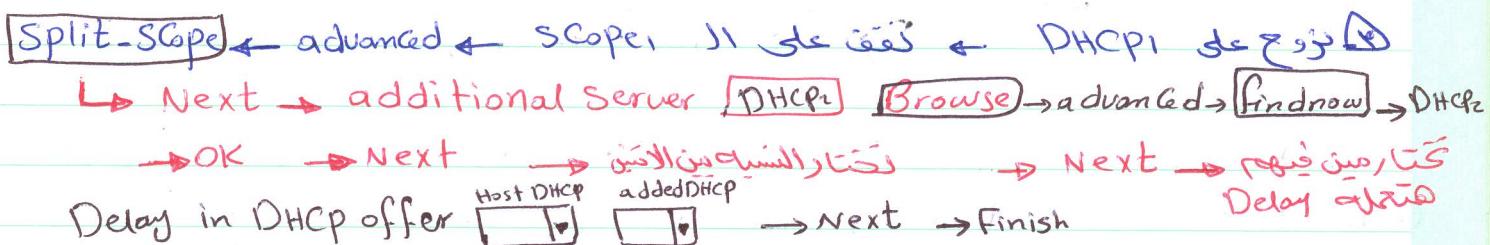
ولازم الـ 2 يكونوا في نفس الـ domain أو في نفس الـ workgroup

عنان يشوفوا بعض

التطبيق العملي

• سطبل او DHCP على Server1 بالطريقة العاديّة

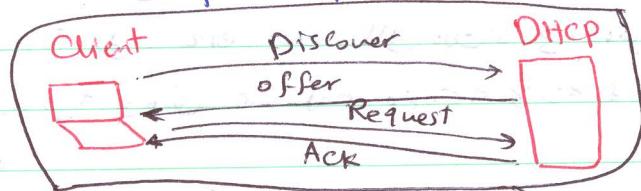
• سطبل او DHCP على Server2 الى معاه في نفس المجموعات workgroup أو domain بالطريقة العاديّة وعش هنديله Scope لأنّه هيامن من DHCP بالمسيّه الذي هندرد لها.



* لو دخلت على DHCP2 اصنافت و Scope هنلاقي DHCP2
 يقع الا DHCP1 موجودين عنده و كذا Reservation si
 هنوصل ل DHCP2 وعش هنديله لأنّ جهاز برهنه.

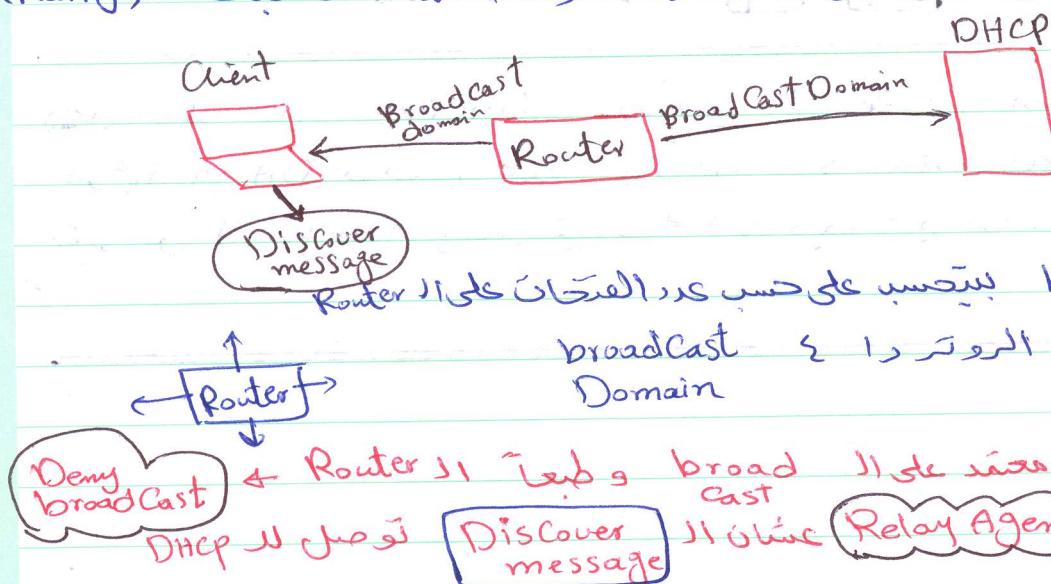
• Relay Agent •

"IP helper Address" → Cisco

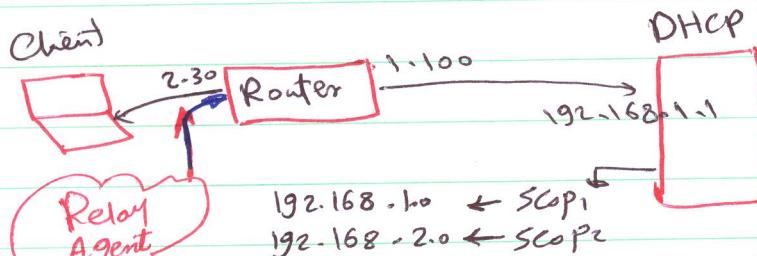


الخطوة الأولى عن طريق Client

للحظة Client لا يخزن IP على نفسه (Range) ويكون على نفس subnetmask ونفس network address Switch لا يخزن على نفسه DHCP لذا عليه عادة على نفسه



طبعاً DHCP لا يعطي IP من Scopes ② لو انتي Relay Agent
طبعاً DHCP لا يعطي IP من Scopes ① لو انتي Router
طبعاً DHCP لا يعطي IP من Scopes ③ لو انتي Client



طبعاً DHCP لا يعطي IP من Scopes ① او ادار ما يسمعها Relay Agent
طبعاً DHCP لا يعطي IP من Scopes ② او ادار ما يسمعها Relay Agent
طبعاً DHCP لا يعطي IP من Scopes ③ او ادار ما يسمعها Relay Agent

طبعاً DHCP لا يعطي IP من Scopes ④ او ادار ما يسمعها Relay Agent

Uni Cast

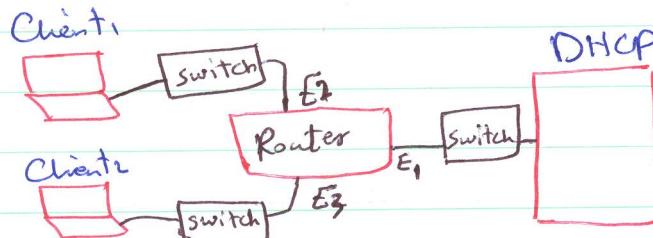
Relay Agent (ا) ملحوظة

Relay Agent

automatic مسند على Router si (ا)

لقد Router 15 على بعد 16 Hop

Relay agent



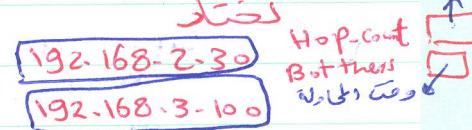
التطبيق العملي

نحو جهاز Router (ا) من خارج Router 3 clients

- Switch ① (a) DHCP متصل مع IP 192.168.1.100 ← E1
- Switch ② (a) Client متصل مع IP 192.168.2.30 ← E2
- Switch ③ (a) Client متصل مع IP 192.168.3.100 ← E3

Client متصل بـ E3 (a) E2 (a) Relay Agent (ا) نشفل الا

- administrative tools → Routing and Remote access → General → new Routing Protocol
- DHCP Relay Agent → OK
- DHCP Relay agent → Right Click → New interface →



? DHCP Server (a) بين Router (a) Relay agent (ا) ملحوظة

- IPv4 → DHCP Relay agent → Right Click → Properties →

Server address [192.168.1.1] [add]

ادم بـ IP DHCP Server

192.168.1.0
192.168.2.0
192.168.3.0

Scope ③

* مثلاً هنعمل في DHCP Server

الغرض لـ كل Client (a) يتصل به DHCP Server (a) range من IP (a) renew و release

عن IP (a) Scope (a) التي تخصه (a) من IP (a) يتبعه.

لـ وصلت خـ اـ دـ مـ نـ عـ لـ لـ فـ لـ (a) DHCP (a) Switch (a) range من IP (a) DHCP (a) Scope

«14» Network Access Protection

Network policy service (NAPS) → NAP

2008 جدیدہ حصہ *

Discover message $\xrightarrow{\text{Install NAPS}}$ ~~لذى يطلب~~ من DHCP Server التعبير عن NAPS

1- Servermanager → add Roles → next → Network policy and access Service → next → Net work policy Server → Install → Close

- admin tools → Network policy Server → Network access protection →

Windows Security Healthy
الجهاز الذي يتعارض مع قواعد التأمين على أجهزة عمان
 Remediation Server

NPS (local) → Configure NAP → DHCP → Machine Groups → Remediation → Help N

Local NPS (NPS) **لوباتير اسل** **NAP** **DHCP Server** **الخدمات المتاحة**

ادخل IP **Next** **RADIUS Clients** **ادخل IP** **Next** **DHCP Scope** **ادخل IP** **Next** **Machine Groups** **ادخل IP** **Next** **Remediation** **ادخل IP** **Next** **Help N**

الى جانب مفهوم Defaut Windows security health

كما ذكرنا سابقاً، لاستبعاد جميع الأخطاء

⑥ Deny full network access to NAP

لواطها: صنف حظيم على الشرط

مسئان اطعنهما واعرف ادا Client

admin tools → gp management → Default Domain policy → edit → Comp Config →

Windows setting → Network access protection → NAP Client Configuration →

Enforcement Clients → DHCP Quarantine Enforcement Client → Enable → ok

نافذة لتنشيل الـ NAP Service

CompConfig → windows setting → security setting → system services → Network access protection agent
 Define Automatic → Edit security → network limited user role → add →
 Domain users
 Start/Stop service

عنوان المتصفح Client IP على شكله أولاً

C:\> netsh nap client show state

كذا المفترض يعني أن دور NAP فهمه أولاً

DHCP على NAP لتنشيل الـ NAP ②

لو عايز تطبقها على كل IP Client لغير على الـ NAP

IPv4 → Properties → Network Access protection → Full Access
 Restricted Remediation
 Drop Client لوعن طبيعته
 Role من داخل IP

لو عايز تطبقها على Scope واحدة فقط

Scope → Right click → properties → Network Access → Enable security
 Use default NAP profile
 Use custom profile

لو عايز تطبقها على Scope كلها، أو على المجموعات فقط

لو عايز اضبط الـ NAP وربطه مع الأجهزة التي في Domain ③

CompConfig → policies → admin templates → window Components → security Center → Enable

DHCP mac address لعوايز تمنع أو تسمح بطبع ما يطبع

DHCP filters

Enable (اختيار)

admin tools → DHCP → Filters → Allow → Right click → New filter →

Mac address []

→ Deny → new filter

طبع ما يطبع من مكتبة

طباعة → add filter to → allow → deny

ip ip لـ network لـ طباعة → deny أو allow

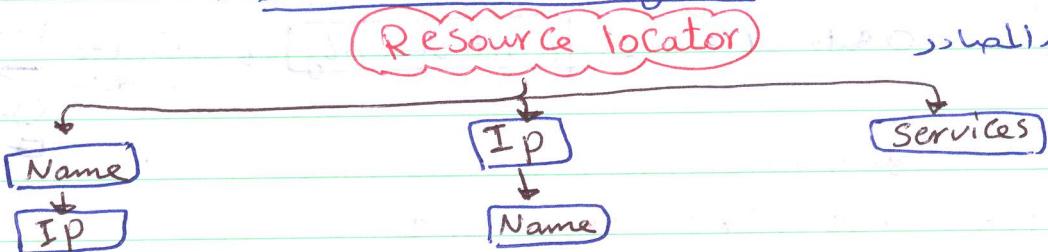
mac FF-FF-FF-FF-FF-FF & Deny

or permit

طباعة network لـ طباعة بناءً على جهوده ← allow

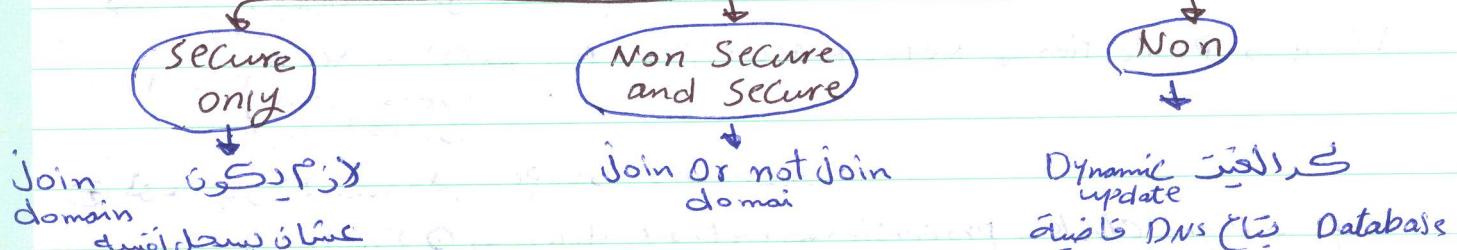
„15.“ DNS

"Domain Name System"



٤ الاجهزه يعملا ببيان تعرف DNS

Dynamic update



نامه دارای لازم و تابع Domain نامه داری هست

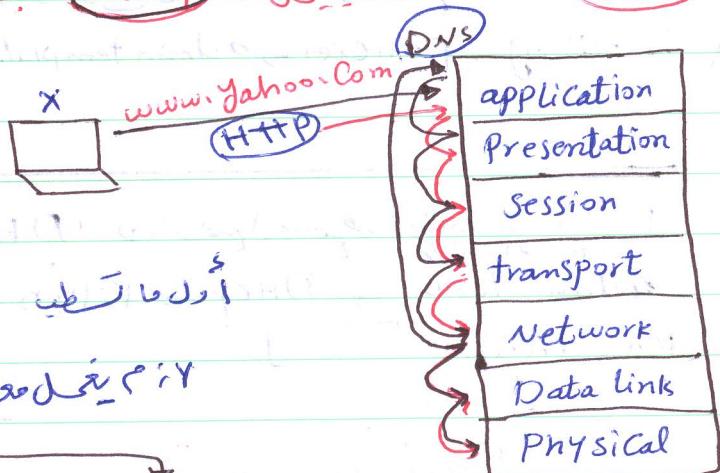
Relay

جذب DNS 51

dit zijn dingen

DNS → application

layers → port 53



بعملها أتوهار با رسنها با Forw

Forward lookup Zone

L10o Name → IP

Reverse
Lookup Zone

Ques IP → Name

ملحوظة اي جهاز joinDomain اول ما تدخله ال DNS بيروح سيرجع نفسه

الوهابية جوا DNS الموصى به مرحلتين [١] اظهار سجل على نفسه

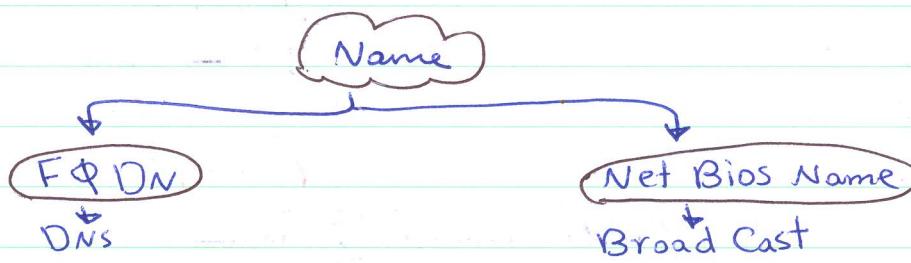
my Comp → Properties → more → Primary Drs []

→ Primary DNS |

Secure

→ Non Secure
and Secure

محلوظات لو دخلت على الصفحه بناء IP بناء Client ال واخترت من كَت ودخلت DNS هنلامي كَت Register this in DNS
 ← معنى الاختيار ادا الجهاز يسجل نفسه في ال DNS لو شلت الاختيار دا هو اهيرق دحصل على ال Data DNS لكن يعني معلومه في ال DNS عنه.



مكتوب

لكل جهاز يسجل نفسه في DNS \leftarrow Record \leftarrow DNS \leftarrow يكون المسجل فيه
 لا Cache يتابع اطلاعه الى سائل عليه الـ DNS والـ Cache دائمته ساعه
 مسجل على سائل الـ DNS عن نفس اطلاعه دائفي ينزل فيها في الـ Record يتابعه
 \leftarrow Cache \leftarrow سلسلة تقبل الـ Cache

admin tools → DNS → view → advanced

dc → properties → Time to live (ttl) [] → Cache ^{one}
[] → Cache ^{one}

اسم انجمن
Record

• Cache الوعاء الخلفي

C:\> ipconfig /flushdns

Client Server

Client

Server

Properties → Secure on

DNS Service Enabled

IPs → advanced → STG Register

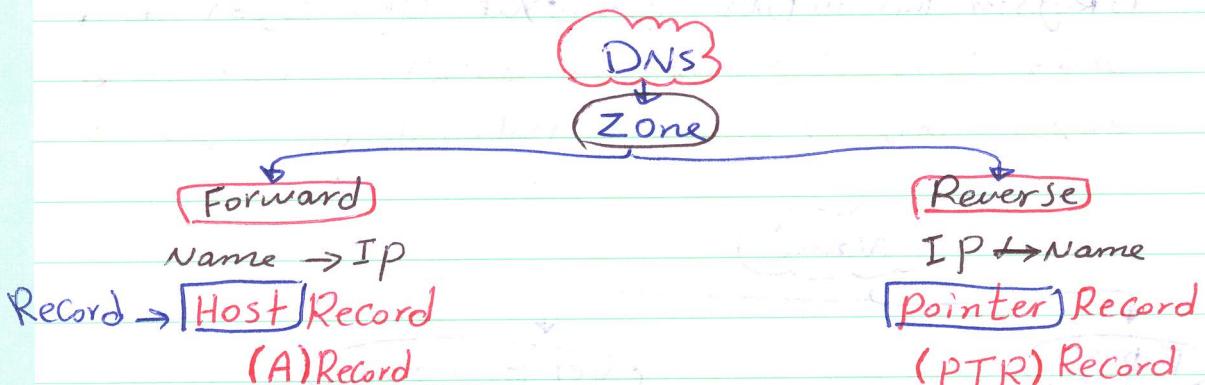
لوعایر Record معنی مخالش Cache

Record JI selected → DC → Properties → time to live (ttl)

Cache چیزی کیا ہے؟

C:\> ipconfig /flushdns

سونی مارکٹ

((16)) DNS (2)Create Reverse Zone

Reverse Lookup Zone → Right Click → New Zone → Next → Primary Zone
 → Next → Next → IPv4 → Next → Network ID [192-168-1]
 → Next → Allow only secure → Finish

هذه هي الخطوات لـ Reverse Lookup Zone

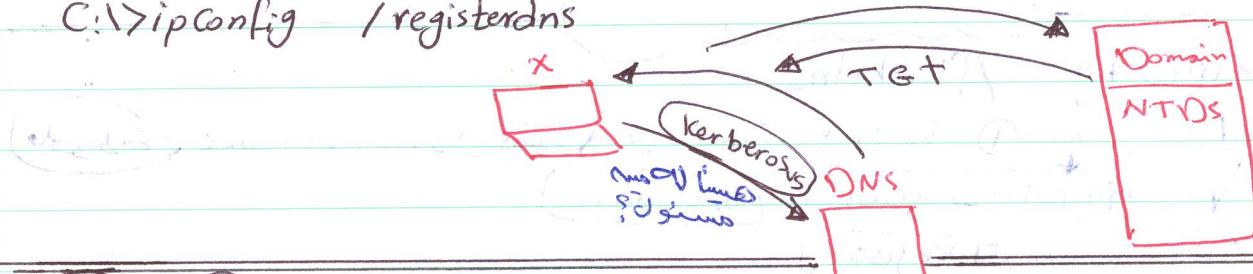
- على الشبكة

مخطوطة

Reverse Forward محوظة
 Reverse طلب: لا يجده في المدخلات فسيسجل لفترة مرتين فهو
 Restart manual

لوعاية تختلف

C:\>ipconfig /registerdns



Broadcast domain Client من كل DNS من محوظة

موقعه لـ DNS من صور ادخل على Client الـ IP's الواقع

C:\>ping -a 192.168.1.1

تحليل اسم الـ IP

C:\>nslookup
 > 192.168.1-2

تحليل اسم الـ Domain Controller

نطليه الـ IP

تحليل الـ IP

Reverse
Lookup Zone

لـ DNS

• لوعاير اعل Record طهار و سکان نیعل

Reverse
lookupZone
Record

- ⑥ Forward lookup Zones → New Host → Name ⚡ Create associated (PTR)
Reverse ⚡ forward ⚡ ایندیکات فروراکٹ

مکتوظہ کیوں اسے Services سجل اور DNS جو انہیں پہنچاتے

Forward lookup Zones → ABC.Com → TCP → Service ای جہاز سے یہ

مسئلته هي DNS ← ينفع لسجل كل بقى الأسماء
أو بقى IP ← IP

```

graph LR
    FZ[Forward Zone] --> DNS[DNS]
    DNS --> Aging[Aging]
    Aging --> SSSR[Scavenging state resources]
    SSSR --> LRU[Least Recently Used]
    SSSR --> DS[Delete]
    DS --> Aging
    DS --> LRU
    
```

لكل يوم ، يطرد المهاجر بعد 14 يوماً ويرثي
وكل يوم بعد سبع تابع صدره
تحل محله كاربيت ميسورة

[Integration] مراجعة DHCp المعايير

DHCP → Scope [192.168.1.0] → Properties → DNS → Enable DNS Dynamic

DNS is also configured via DHCP. It is dynamically updated.

لما نطلب DHCP اولاً نختار checkbox (Always dynamically update IP)

Discard Aand PTR Record
when leased deleted

فلكيًّا) بين عرض الـ DHCP وأخيراً صدر عنه على الـ DNS أنه يجري تجربة منه

DNS خوادم معرفی کننده IP & default جایز

Active directory users and groups → users → Dnsupdate

(members) → Add → Server (Container)
Dhcp (ابعاد) → Object type (Computer)

Dynamic update DNS DHCP Client
not Request updates

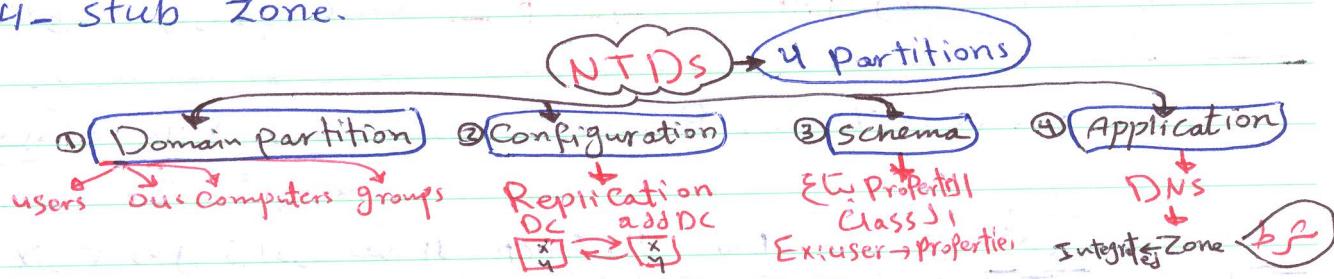
R2 Go on step 3 Name protection →
DNS will ask to database to check the DHCP 31 user Configure

بُرْطَانِيَّا لِلْأَسْمَاءِ الْمَتَّكِّرِ وَالْمُنَعَّصِ وَالْمُوَلَّقَاتِ هِيَ سَاحَةٌ .

"17" DNS (3)

Zone Type

- 1- Integrated Zone. (Default) → افضل
- 2- Primary Zone.
- 3- Secondary Zone.
- 4- Stub Zone.



NTDS ينكرن Integrated Zone من application و Partition (5) نجارة مكان دا ملحوظ

ملحوظة مكان دا DNS في المسند

C → windows → system32 → dns

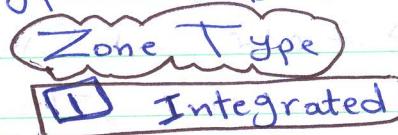
من هنلاص فيها لـ database في NTDS

من حالاته تكون Integrated Zone لكن لو زوي تانية تكون DNS في ABC.com.dns

Integrated Zone → NTDS

any other type → DNS

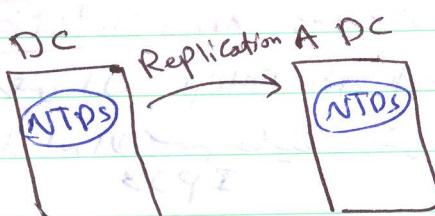
مثلث



A. Stored in active directory (NTDS)

NTDS في Replication لـ DNS من يفتح اعلى DNS من يفتح اعلى Replication

من يستغلوا مع بعض لكن واحد يستغل ما يقع الثاني في يستغل DNS (2) sites (4)



Primary domain من لو ادا additional domains

ملحوظة Replication على مستوى DCs لـ NTDS فقط

يبقى اذا DNS مكتوب مكتوب DNS او NTDS في Integrated Zone

(B) • Replication:

النهايات تكون متحركة في NTDS

(C) • Active Directory DataBase and DNS server in the Same Server.

Domain Controller دلائل، من الممكن لـ DNS Server أن يكون متصلاً

(Available only if Dns server is a domain Controller)

(D) • Supported SECURE ONLY

(secure or non secure, None) (only NT4)

(E) • Support Security

Integrated Security, Zone Properties (لوحة خواص) (المنفذ)

Delegate to Zone (المنفذ) (Zone delegation) (المنفذ) (Security) (المنفذ)

Control

Zone type

1- Integrated:

Stored in active

2- Primary:

Data Base local in Server

win → system32 → dns
هذا مكتبة DNS

3- Secondary:

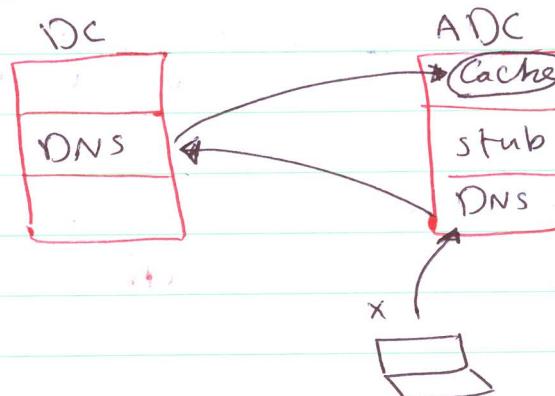
Read only → help Disk فتحة add service → Secondary DNS

ما يجري هنا هو إضافة خدمة DNS على سيرفر آخر

4- Stub:

Server to Server

بيانات DNS بين المواقع



Stub: Record ملخص فني

ولو اتّصلنا بـ Stub بـ Direct Query بـ DC DNS

Client will go to Cache (الخادم) و DC (الخادم) (الخادم) (الخادم)

Cache (الخادم) (الخادم) (الخادم) (الخادم)

Subject.

• أنتو بستخدم الـ Primary Zone

• لما تكون عند افرادين بينهم مصادقة Data غير منفردة في كل دى
 يجعل Primary DNS بتاعة كل فرع متكرر في database بتاعة
 على الفاصل بين المسئلتين التي هي بيستفيد بياني الميزات.

اطل

Router
Packet Filter

عمل على كل Integrated Zone
Integrated Port 53 لذلك يقاد خصائص الملفات
Replication ومن ثم يعادلوا

Secondary Zone

additional Domain

بس المكونات الـ Primary DNS بتاع الـ Default فالباقي الثاني
لهم ذات المكونات وعاليات امورها Integrated secondary
سيتم معالجتها.

اطل اعمل من NTDS II و DNS II Primary zone ← P DNS
هبيك في add DC فالعكس add DC لا ايه الا لو ادوك
هذا غير DNS فهبيك منه قاعدة Create و اعمل من حسوبة
Secondary zone

اطل كل دلائل

Next ← DNS من هبيك او addDC
DNS مايلد او active directory addDC هبيك
و نابطه او addDC من هبيك او addDC

Servermanager → add Role → DNS Server → Next → Install

DNS → Forward lookup Zones → new zone → next → Secondary zone → Next

Zone name ABC.Com → Next → IP 192.168.1.1 → Next → Finish
domain الـ primary

اطل Zone نزلت عليها

نزول الـ Domain الرئيسي و توافق على الطلب

ABC.Com → Properties → Zone transfers → Allow Zone transfer
Only to server listed to Name server

← add

←

Name Servers

او

Only the Following Server

← addDNS و نزول IP جتناه ← Edit
abc.Com → Right click → transfer from Master

فيكون كل حاجة على الـ master بس هي يعرف بعد

(144)

ABC.Com → [] -tcp → Kerberos + 3

ممكن تو اجهت لومها؛ عايز دخل join من هيرف بيل domain
 Read add مسنان DNS Record only

Primary DNS دوكمه لجها و هما بيعمل join domain
 Integrated ← primary دوكمه join Record دعيين بيعمل join

* إزاي بتسم عملية Replication د

أى حاجة بتسم جوا DNS بـ serial number و مكانه لـ authority

ABC.Com → properties → start of authority → Serial number

Primary DNS

اللة اللي بيروح يطلع فيها بروح ساند نبا الـ Refresh interval
 لـ DNS وقع، لـ time Refresh تبع المدى
 Expires after

لـ Client و عايز المرق ديانات الـ DNS

C:\> nslookup

> Set type=soa تجيبيك بـ soa

> abc.Com

> Set type =ns ممكن DNS بـ ns

> abc.Com توصل من ضلال

Stub Zone

add Domain نقق

admin tools → Dns → Forward Zone → NewZone → Next → Stub Zone → Next

Zone name abc.Com → Next → Next → IP 192.168.1.11 → Parent DNS → Next → Finish

abc.Com → properties → TTL ممكن تسرد Cache بـ stubZone

abc.Com → properties → TTL

ملحوظة هامة

اولاً سيد Ping على جهاز يسوي ع ر DNS بسيوفه عنده في ال Records لذلك يعرفه طبعاً انا اكتب اسم موقع هيومن ديجي واسم الموقع من موجود DNS في ال Record

اولاً لوجهة Real DNS في حالة ان المعلومات من DNS

admintools → DNS Server → DC → Forwarders → Edit → IP 8.8.8.8 → apply
 كل الـ DNS الى انا كابنه واقع كـ Root hints
 DNS → DC → Forwarders → Root Hints

User root hints if no forwarders are available

جاء

→ DC → properties → advanced → BIND Secondaries
 bindry Secondary ← Linux بناءً على Linux اول ما add DNS على

هذا دns مكتبة داخلية → properties → Monitoring → A simple query

A recursive query
 لـ DNS عن ماجد برا

test نعمل على امر دخول testName

ملحوظة . لـ Client نحن ابرم ما تـ الـ DNS دخل عليها سـ خارج

C:\> ipconfig /displaydns

يـ نـ لـ المـ وـ اـ قـ الـ دـ خـ لـ عـ لـ يـ

لـ Client اـ طـ عـ هـ اـ حـ

C:\> ipconfig /displaydns > C:\x.txt

هـ نـ لـ اـ مـ عـ لـ مـ لـ فـ مـ لـ اـ جـ بـ لـ كـ المـ وـ اـ قـ الـ دـ خـ لـ عـ لـ يـ

١٩) DNS - IIS (٤)

Servermanager → add role → Web Server (IIS) → Next → Next → Install
 admin tools → IIS manager → Default website → Right Click → Stop

Sites → Add website → Physical path → IP address Port
 Site type http https http
 SSL Certificate Site name Yahoo
 or type http Hostname → OK

Sites ملحوظة

الملحوظة على من قدر الموقع

Yahoo → Default Document → add → Name → Yahoo.html → OK

website على domain

Internet Explorer to http://192.168.1.254

لابد من عاشرة تربط DNS بـ IIS

Server.abc.com Server ملحوظة يفتح الناس سهل بـ Server.abc.com
 بناءً على ما يحصلون في طيارة العجلة دينياً بـ DNS الموقع من الذهاب

IIS → DNS ربط

لود ملحوظة Records بـ ABC.Com ← DNS بناءً على الاجماع

admin tools → DNS → ABC.Com → New Alias (C Name) →

Alias name www

Fully Qualified domain name Server Browse
 IIS ← server بـ Records

Site على www Client لـ http://www.abc.com

ملحوظة لـ A صناعي الموقع من باسم domain

Forward lookup zone → New zone → Next → Next → to all DNS on domain → Next →

Zone name ABC-EG.com → Next → Don't allow Dynamic update → Next → Finish

بـ الموقع

بعد عملت اد Zone طريقة مختلفة لها خطوات

ABC-EG.Com → New Alias (CName) → Aliasname [www] → FQDN [ABC.Com] → Browse → OK
كتابات الماكينة على جهاز Server record

لارتكب عن اداة المفروض [http://www.abc-eg.com]

Client

الstrukts اللى رباعي اجز مساطس بتعل القائمه

IIS → sites → add website → sitename [vodafone] physical path [C:\inetpub\wwwroot]

Type [Web Site] IP [192.168.1.254] Port [90] → OK
هذا يعني نفس الماكينة التي وافت الايport على نفس الماكينة

→ Default Document → add → Name [vodafone.html] → OK

لورى عن اداة Client المفروض دلوقت وكيف اداة IP بتاع اداة

Portgo على اللى واحد 80 اداة لوعايز ادخل على الايport على الايport المفروض على اللى واحد 80

http://192.168.1.254:90/

طبعاً دايماركت على اداة DNS

vodafone المفروض على اداة Zone

Newalias (CNAME) → Alias name [www] → FQDN [www.vodafone.com] → Record [DNS] → Browser → OK
كتابات الماكينة على جهاز Server record

→ OK

site IP نفس الماكينة [192.168.1.254] Port [80]

← Editesite binding

Hostname [www.vodafone.com]

عرض site اول وربط برضه اداة Hostname

ديكته بنفس الماكينة IP وPort

اللى [192.168.1.254] المفروض على اداة Client

واهذبته المواقعين من هيفن ورادا ورادا (نقطة الاتصال)

وادا اللى بيعمله + Tedata ← Service provider

Domain [ETisalate]

Server [ETisalate.Com] ← DNS المفروض على اداة Zone

Zone name [ETisalate.Com] ← DNS المفروض على اداة Zone

FQDN [Server ABC.Com] → Browse ← www Alias name

Server [ABC.Com] ← add website ← sites ← IIS ← زر عرض

Site name [ETisalate] Physical Path [ETisalate]

فول المفروض وتبقي نفس الماكينة IP وPort

Host name [www.ETisalate.Com] → OK

OK ← Name [ETisalate.html] ← add ← default document

IIS 11 لا ينزل على جهاز ويعمل كنطاق join domain group & Builtin & domain active directory IIS - I Users

القولدر بناءً على website كذا كل يوم على صورتين

لعماءِ دايل لوجين pass user Basic Authentication Windows Authentication

IIS 11 Service صوراً Basic Authentication Windows Authentication

Roles → IIS → add Role Services → Security

Basic Authentication
 Windows Authentication

→ Next → Install

لورقة على أي website هنا في authentication صاف

(لاستثناء) Basic Authentication Windows Authentication

له لواد user موجود في SAM file

website وحيث تدخل على website anonymous

لـ Disable

متى يفتح.

لورقة Client وحيث دخلت في Basic

هذا يفتح صفحة دخول و

لـ folder security حفظ الموقع

(Virtual Directory) website يفتح مع نفسه

تقع على الـ website نفسه الموقع الذي يديره يفتح معه الـ alias

Vodafone → add Virtual directory → Alias mcitp Physical path

Default Document → add → mcitp.htm → OK

لواد Client كـ http://www.vodafone.com

* لواد افتح الموقع الـ alias http://www.vodafone.com/mcitp/mcitp

لواد web في فتح او صيانته فعاليات الموقع site

صفحة ذاتي . نعمل هنود، فيه الصفحات التي يديرها (وهي عليها)

DNS Zone IIS ونظام المواقع

Subject.....

DNS خي Hostname \leftarrow Ftp \rightarrow موقع نقل ن

جوا ٥١ DNS مياد zone newHost لعن DNS

Name [application] IP [192.168.1.254] \rightarrow Next

[ftp://application.abc-eg.com] Client

موقع نقل ن \leftarrow Ftp
Redirect
ويمكن برقم application على

مكان نقل ftp لكل شركه تستوفى الى يخصها بس
user active director المعرفه active directory المعرفه
user name folder المعرفه active directory المعرفه
اسم او login جنباً
جهاز لوعنهي كل شركه حمل لكل شركه user من اجل
users folders في نفس اساسى كل FTP folder

مزود لا \leftarrow Ftp user isolation \leftarrow Ftp web

① user name directory \rightarrow ok

دلونت لا اول user يقع على جهاز يكتبه myComputer

[Ftp://192.168.1.254] \rightarrow username
Password

* لا زم يكون لقى اول user و اذ صلاحيته في add Ftp Authorization في اول ما يدخل على Ftp

المحظوظة ممكن تحدى يتقدل كم يوم من الايام وحيط قدراته upload

Download

IIS \rightarrow Sites \rightarrow Ftp \rightarrow Ftp logging \rightarrow schedule

maximum size upload or download default 20mb

Hostname بضمه موقع نقل Ftp

20) Name Resolution

- ① **Cache** المراحل التي يمر بها Client
Client → DNS → Cache → Client
- ١) Host Name = FQN 255 Character
- ٢) Net Bios Name = 15 Character
- ٣) **DNS** لو اتجهت مسأله DNS موجوده في DNS بيرجع لها
- ٤) **Hosts File** C:\windows\→system32\→drivers\→etc\→hosts
كان قبلها DNS كان يصنف فيه المواقع
manual & Name, IP كان يصنف فيها المواقع
- ٥) **Wins** window internet name Service
كان قبلها DNS لو اتجهت له wins سيعبر عن wins
- ٦) **BroadCast** Broadcast من يفتحه
- ٧) **LM Hosts** windows → system32 → drivers → etc → LM Hosts, SAM
IP, Name → SAM وتنقل Rename
انه يتغير كل يوم في NetBIOS
- ٨) **FQDN** IP Interface → advanced → WINS → Enable LM Hosts lookup

مخطوطة لعمليات تشغيل بثحache

C:\>nbtstat -C -R لعمليات تلقي ال Cache

DNS لعمليات تشغيل Cache

C:\>ipconfig /Displaydns
C:\>ipconfig /Flushdns لعمليات فحص Cache

BroadCast لعمليات الغى حظوة

Scope ID لعمليات الغى Scope ID، اعاده لوغيرها ان defautl

من هم ينفعونا يعني .

Run → regedit لعمليات على ال Client

HKEY_LOCAL_MACHINE\→System\CurrentControlSet\→Services\NETBT\parameters\→New\→Stringvalue\→ScopeID\→value data [n]

ClassID (نحوه لثبات رسمية) ونحوه Client ينبع على ال value data [m] → ok

ونجد ال جهاز قد دخل للتنبوع يعني Restart

مخطوطة لـ DHCP على هذا الجهاز بخلاف ClassID

IPv4 → Scope options → Configure option → 47 NetBIOS Scope ID

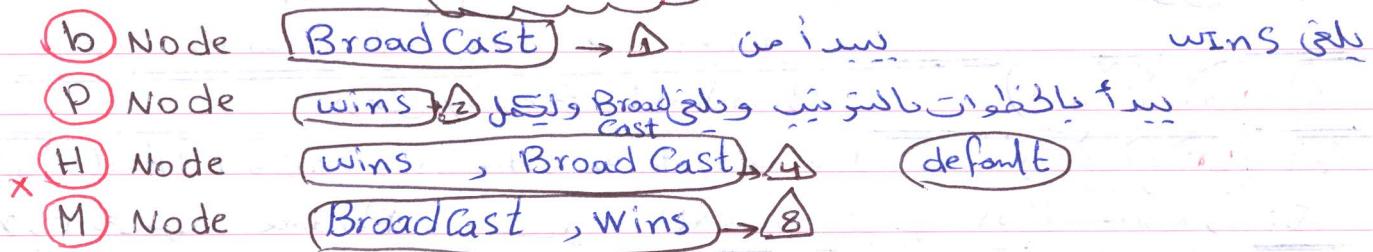
String value [h] → كل الـ domain من 11 هم ينتمون إلى Scope

فقط Broadcast ClassID 11 Class [h]

مخطوطة الطها: الذي لديه domain ID معرفته ديكلم

ClassID مخطوطة

Node Type



Run → Regedit → HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services

→ NetBT → parameters → New → String value → NodeType → 1,2,4,8

DHCP يفتح ورحمة نعرف ما عن طريقة

Scope options → Configure option → 46 WINS/NBT NodeType

Byte [1,2,4,8] → OK → apply

كل type ليه رقم معين

WINS

NetBIOSName على نفس الـ IP DNS 192.168.5.98 و 5.99

Server manager → Features → add features → WINS Server → next

الجهاز متصل بـ WINS فنambah في Install

IP Interface

WINS Client

Advanced → WINS → add → wins Server [192.168.5.98] → add

admin tools → WINS → Active Registration → New static mapping

Computer name [] netBIOS scope [] IP [] → OK → apply

لوحة Display هتترى الجهاز مسجل نفس IP مرات

Subject:

DNS WINS ملخص المحتوى

DNS manager → ABC.Com → Right Click → properties → WINS →

use wins Forward lookup WINS هو المدى يبحث عن DNS

ip [192.168.1.200]

Don't Replicate record

Replication

WINS في كل ما يكتب داخل DNS = كنتم من

Search Filter ملخص المحتوى

WINS → Active Registry → Display Records → Filter records → find now

Active Registry → Import LMHostsfile → تحرير المحتوى

→ verify Record name → Record تجربة

WINS من الدليل

ملحوظات

WINS → Replication partners Replication WINS 2 دليل

→ New replication

→ properties → push Replication

Replicate كل دليل ينفرد بـ

At service startup

When address changes

→ Pull Replication

Start time كل وقت معين

→ Advanced

Replicate لـ WINS لـ WINS Add

لـ WINS

DC [192.168.1.200] → Display statistics ملخص المحتوى

→ scavange database لـ WINS لـ WINS

→ properties → Backup Browse لوحة تحكم

→ interval → Renew DNS وقت ابراهيم 24 hours

→ Database verify

→ advanced Enable burst handling

WINS لـ WINS update

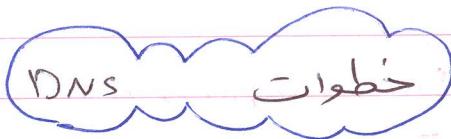
0.10w 300

Medium 500

High 1000

(FQDN) Host Name Hosts file DNS

NetBIOS Name WINS, Broadcast, 1M Host
DNS & Record CLE



① Cache

② DNS Database

③ WINS

Net BIOS Name

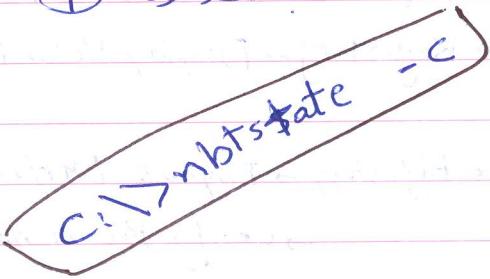
④ سيرفر

① Cache

② WINS

③ Broad Cast

④ LM Host

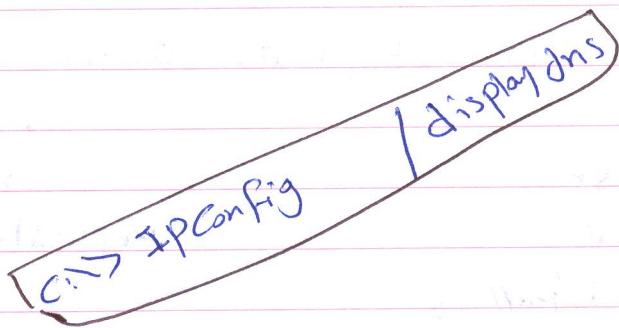


Host Name FQDN

① DNS

② Host File

③ Cache



IP Interface & Client لورڈ لاب

advanced → wins → Disable NetBIOS over TCP/IP

Network places لورڈ عایز مکانات

سے لورڈ کیتی جائیں

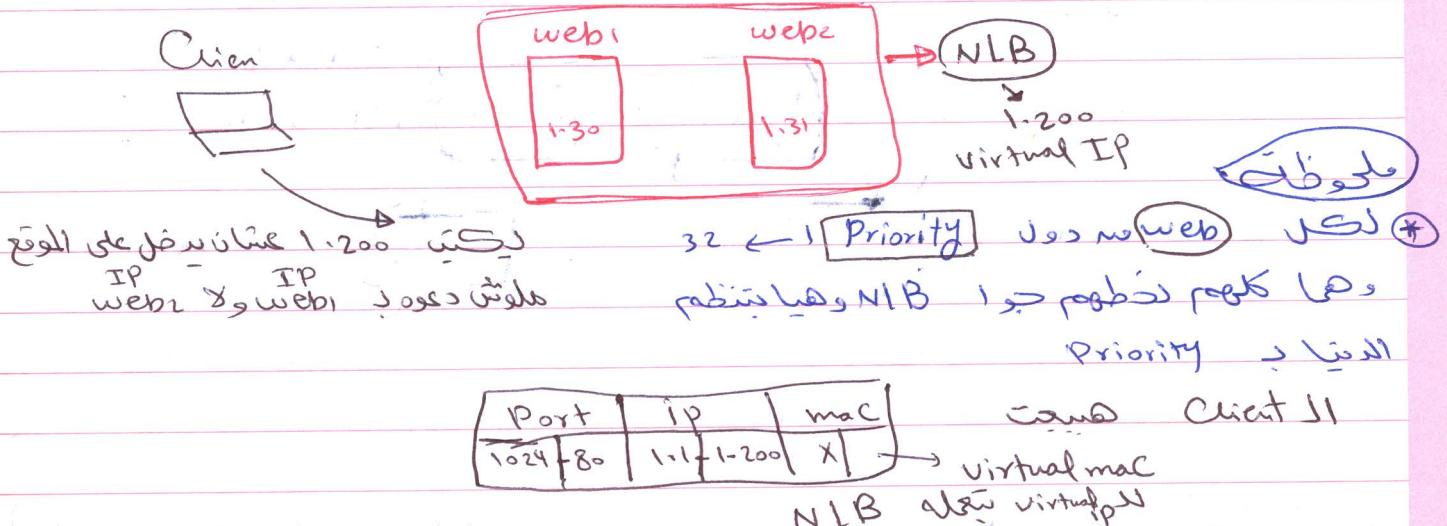
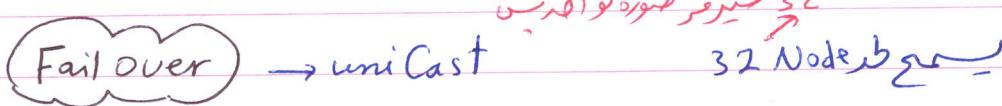
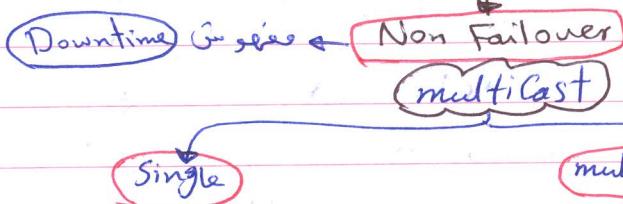
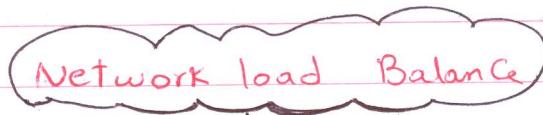
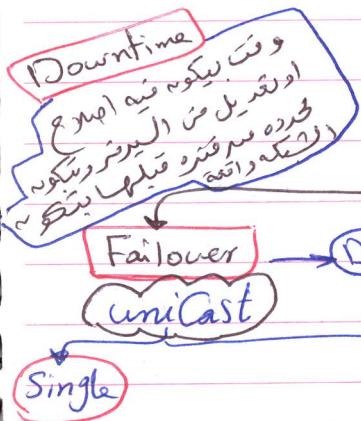
« 21 » Clustering ①

« Network load Balance »

« H/A High availability »

يُعمل من كل أثنين لوعاء وقع الناتج ينتقل مكانه في حالة الفشل additional DC Domain Controller

كل المواقع العالمية يتصل بالـ Network load Balance على الناتج المترافق لـ failover



virtual mac يخلي او mac يخلي كل IP failover
Priority
ويختار الذي تردد عليه على نفس IP

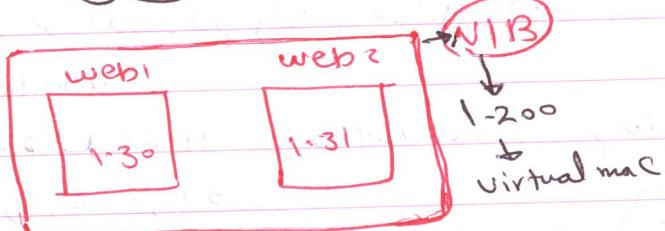
كما انت انت تكتب 1.200 على اي الى priority
① الى priority
web1 IP 1.30 الواقع في failover
web2 IP 1.30 الواقع في failover

الحوسبة سترخيم ال Failover في Hardware

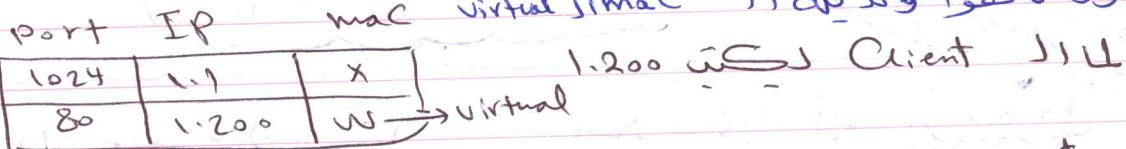
دالا لافتة

Non failover

→ Non Downtime



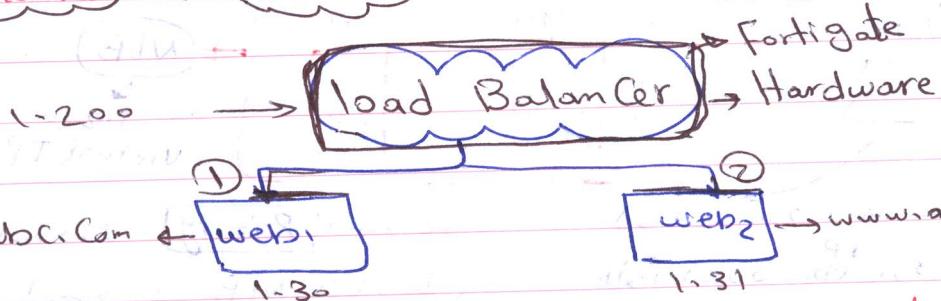
فيما يلي بناءً على mac وال web لكن تسبّب لكل virtual mac في



الـ Request هيدر (Header) يحمل priority بين الماكين web1, web2
ولم ينفع الثاني لكن لو الماكين web1 يحمل priority أعلى منه في
الـ multiCast هيدر ولم ينفع الثاني. لذلك هو priority
microsoft technique

Load Balancer and Device

الحوسبة على ما يستخدمها



* الوجهة 1.200 لـ Request من www.abc.com تذهب إلى web1 ومره يمررها web2 أو limit concurrent requests لـ web2

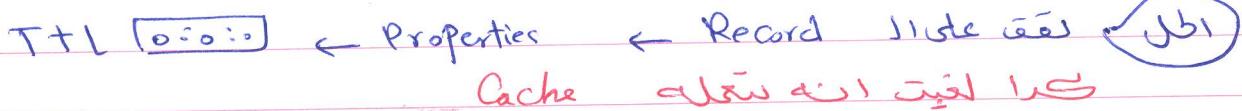
Round Robin

الحوسبة من DNS من ماحمله سنه في الأسماء
لوجعلت لها ونوى Record ^{Host} Enable ينقى الأسماء مرره يمررها
على الأولى ومره يمررها على الثانية بين هنوا حمله سنه في الـ
Cache one Cache Client يبعد عن جهاز الـ

Round Robin ترتيل الدور

DNS → dc.abc.com → properties → advanced → Enable Round Robin

النقطة التي هي اجهتنا الـ Cache



الـ DNS هي من صرحتنا هى الموقع واقع ملوش دعوه هو اـ IP سيعمل بين نـ دعوه

التطبيق الحالي

١ عندنا جهاز في IIS Server متـ عليهم ونـ جواهم كل واحد منهم Folder بـ الموقع ونـ لهم كل واحد موقع

٢ IP www وكل واحد يـ على DNS في Record بـ الموقع فيه .

٣ Client على اـ كـ موقع صـ عليه على الموقع دارمه عليه على اـ كـ

Application si

state less

دـ لا يتغير في حالـ

load balancer يستـ فيـ

web1

1-2

لويدـ

مـ دـ

وـ قـ

منـ

كتـ

الـ

state full

دـ يـ تـ حـ مـ سـ

علـهـ عـ سـ انـ يـ حـ كـ

DFS Replication

web1

web2

2

1

web1

2

web2

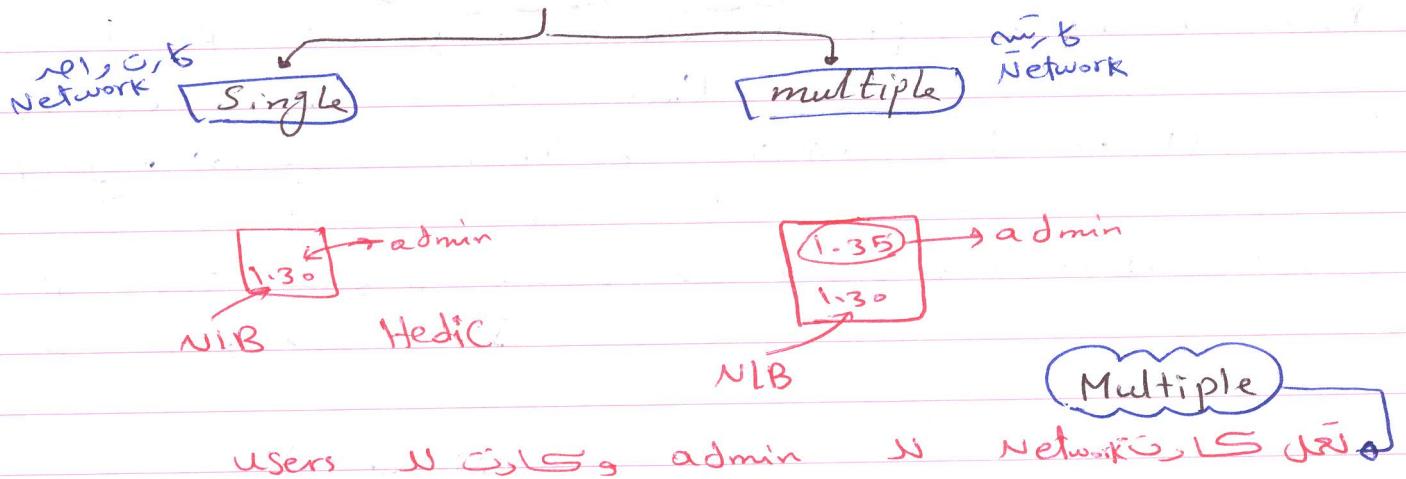
1

اـ تـ حـ مـ فـ عـ

فـ عـ تـ حـ لـ

Subject.....

Failover



" 22 " Clustering & DFS Replication

التطبيق العادي

نعمل على إنشاء Server Cluster و نترك عليهم IIS واحد مسوّع

① IP 192.168.1.30

② IP 192.168.1.31

نزرع NLB في web1, web2

Server manager → Features → add → Network load Balancing

مستغل مع application stateless

web2 في web1

admin tools → Network load Balancing → Network load Balancing → Right Click → New Cluster → Host IP [192.168.1.30] → Next → Priority [1]

Retain suspended state لو حصلت على دليل و رعي لـ web2 أو لـ web1

→ Next → add → IPv4 [192.168.1.200] → OK → Next

Virtual كذا نعمل على web1 لو اتيت بـ 80 web → Finish

web2 نزرع

admin tools → Network load Balancing → Network load Balancing → Right Click →

Connect to existing →

web1 من

Network load balancing → 192.168.1.200 → Right Click → add Host to Cluster →

Host IP [192.168.1.31] → Connect → Next → Priority [2] → Next → Finish

web1 edit binding → Edit → IP [unassigned] ← web1, web2 في IIS

web1 مدخلته 192.168.1.200 لوكيل Client

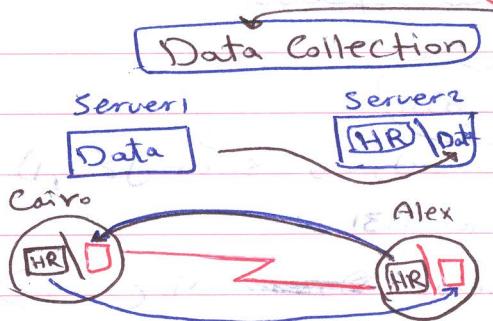
web2 يواجه موقعه على

web2 هو child of web1 أو web1 هو parent of web2

DFS Replication ← service ← لنة عزم شحنة

مدونة

DFS Replication



multi purpose

server1 server2

Data Data

نحو المفهومين

يتحقق ذلك من خلال الاسم و يقين الـ path

نوع لشغيل لوحدها من ٤٠٪ DFs Replica II (لحوظة)

التبيّن العلوي Data Collection

Server manager → Roles → add → File services → Next → Distributed File Systems →
→ Next → Create Name space later → Next → install

8. admin tools → DFS management → Replication → New Replication group →

① Replication data Collection → Next → Name
Server → Domain abc.com → Next

Name Browse → Next → local path HR Browse

السيرفر الذي عليه الملف Name Browse → target folder Test Browse
Replicate السيرفر الذي نريد نقل معه

٢١ HR داوم هنكلت (asm) Test لحق دلختنی هیبعی

→ Next → ⚡ Replicate bandwidth  → Full  new, up date

④ Replicat specific days schedule (مواعيد محددة)

→ Next → Create

Test → HR

* اول مرہ بی لازم تھا۔

DFS → Replication → Server → ^{check} HR → Connections → ~~File~~ web → Replicate
Now

وَكُلُّ اِعْجَاجٍ كُلُّمْ لَحْنٍ وَاحِدٍ فِي هُمْ سَامِعٌ لِلَّهَمَّ.

Multi Purpose

DFS Replication

النوع الثاني من

Admin tools → DFS management → Replication → New Replication group

④ Multiple purpose Replication group → Name [webRepl1] Domain [] → Next
add → [web1, web2] → Servers [الخطي] [النقطي] [الشبكي]
Replicate → Next → ① Full mesh كله مرتبط
→ Next → ② Bandwidth full →
Primary member [web1] → Next → add [] → Path ()
Path
→ Next → [web2] → Edit → ③ Enable [web1] Browse → Yes
زنده [web2] ←
→ Next → Create → Close

Replicate now ← Connection

أول صر فرضه نعم على الفوادر ←

لجعل موقع حديثي website وديكون بالفولدر الذي مهتم عليه Replicate

IIS → add website → Name [web] → [Browse] [Cancel] IP [not assigned]

المفهومي يظهر التعديل في web

لوعاریستا کے ادھل علی کل دا 1 مرد IP بتائدا

Share folder dc DFS Replica di nts obiecto

DFS → Replication → New group → Name **IT** → Next → add → server ^{now!} ②

→ Next → Full mesh → Next → primary [web1] . Path [c:\IT] → ok

Next → Edit → Enable path C:\IT → OK → Next → Create

٤) نعمل Share للمعذرة الذي على web ونعمل كذلك المغولز على web

Replicate now uses DFS to do this

192.168.1.200 \ mapNetwork Client \ \!؟

Replicate J - 5 min

GL Namespace

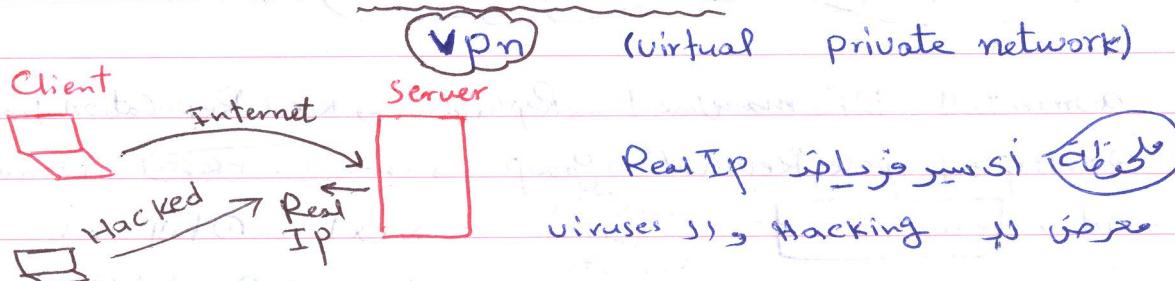
DFS Namespace

DFS management → Name spaces → New Name Space → ~~Name~~ **Set** Server [web] → next.

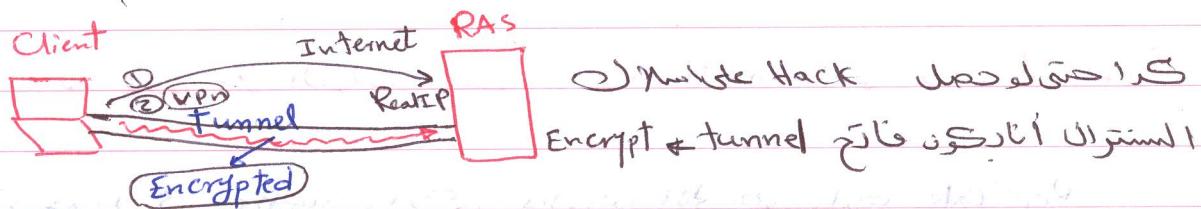
→ Name Sale → Next → Create

DFS management → A.B.C.Com\Sales → New Name Space → Browse [web]
server

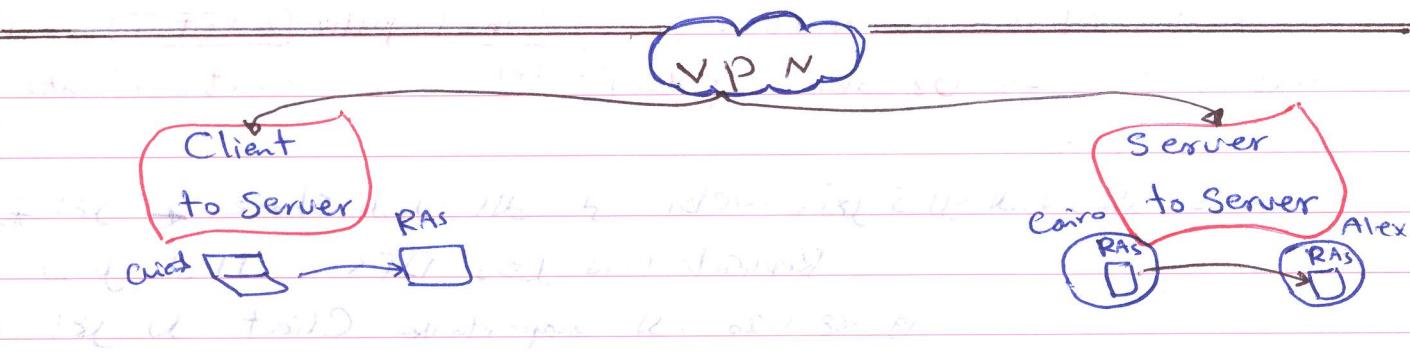
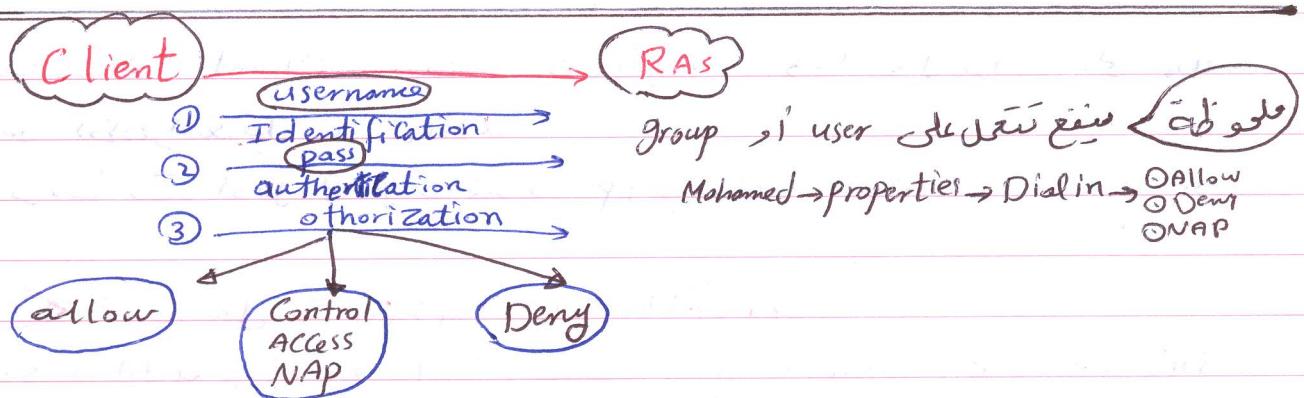
(23) Remote ACCESS



اتصل (Call) لوصن من الانترنت على الشبكة التي
يس فيها ما يحصل احتراق اسلك الانترنت
بواسطة (through) vpn عن طريق (via)



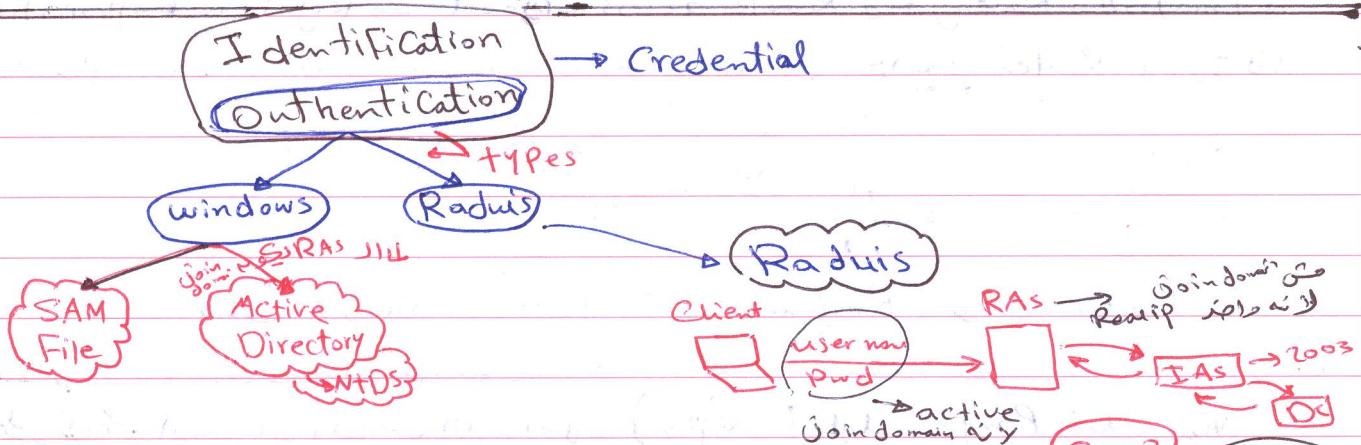
لذلك من يتحقق يدخل على موقع (Client) يعطيه data من الموقع



اتصل (Call) لاحق (ملحوظة)
لذلك إذا كان هناك (Client) يطلب (Request) (ملحوظة)

Tunnel Type	
PPTP Point-to-Point 2003 Microsoft Protocol Supported all Port 1723	L2TP 2003 Supported 2000, xp UDP Port 500 TCP Port 1701 Encrypted
SSTP 2008 Site-to-Site Port 443 Encrypted	Internet Key Exchange IKEv2 R2 mails Port 443 Encrypted

tunnel type JSI 128 port يُفتح RAS ← Server ملحوظة اول ما تقول
 Ports 11 وتفقد باقي 11 وتفقد عددي ناس على هندهم
 انته تجربه انته انته (الربع)



als IAS ← ubiq user, pass على RAS 11 6 قم (ابو)
 domain 11 user, pass 11 يسخن Join domain ويكون den Server
 RAS 11 يقدر و Authorisation 11 يقدر على domain 11
 (ابو)

IAs 2008 دخلوا 11 IAs لغوا (2008) وينجح لفون خطوات Nps

Authentication type methods

Windows

Radius

CHAP → unix (non microsoft) ← CHAP

ms CHAP → Not Support (xp, vista, 7) ← ms CHAP

ms CHAPv2 → Support all microsoft (اقوى نوع) ← ms CHAPv2

EAP → Smart Card ← EAP

PAP → Not encrypted ← PAP

النطاق المفتوح

1- نعمل RAS Server ونعمل Client من حبيبات التي همJoindomain

62.1.1.1 ونعمل Real IP على الباقة الدافعة 192.168.1.100

IP ليس هنليل Not Joindomain من حبيبات التي همJoindomain كأنه طالع في Client 11-2

[IP 62.1.1.2] mask [255.255.255.0]

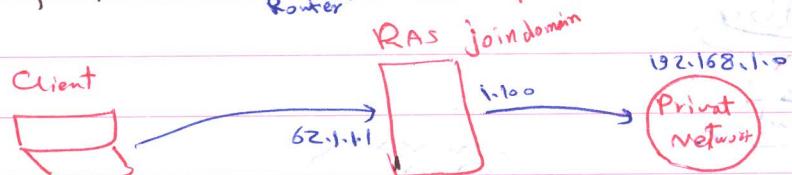
2- نزول لـ RAS من اتصال Service 11 سحب RAS Server

Server manager → Roles → add Role → Next → Network policy and access services

Routing and Remote → Install

admin tools → Routing and Remote access → Router → Right click → properties →

IPv4 Router (استغراء Router) IPv4 Remote access Server (استغراء RAS)



لذلك لا يرى RAS

مخطوطة الصحن او النسخة المفتوحة (VPN) مختلفة عن

10.10.10.0 مان يدخل كل الصالات 8 بت لونته 11

لكن لو تأتي بقى اعلى Filter وارد كلها

ادخل ادوات RAS او VPN او IP address #

هذا يفتح بـ Remote access

⇒ Router → Ports → Right click → properties → Ports

Remote access (inbound) maxport [] يمكن تعدد عالي

⇒ Router → Properties → Security → authentication

Windows [] authentication methods []

PAP, EAP

⇒ static address → add [10.10.10.1] end [10.10.10.10]

او IP المفتوحة التي تجرب

DHCP, DNS هي لـ Network Adapter internal []

internal [] internal []

DNS [] RAS []

„24“ Remote Access 2

٤- دلوقت يبدأ التطبيق الفعّال الثاني من authorization

RAS
join domain

Control Access NAP
Allow with NAP Control

١- نزوع على RAS Server على NPS

Server manager → add Roles → Network policy and access → Network policy ser...

→ Next → Install

admin tools → Routing and Remote access → Router → Properties → Security

admintools → Nps → policies → Network policies → New → Policy Name [vpn]

① type **VPN Dial up** → Next → add → **Condition** → **add** →

فهي تتبعها ل羣組 machine groups ل羣組 windows group

- location تقدیر، نقشه
- Day and time شرط، لوقت للدھول

- Operating system ترتيب الأجهزة
- Authentication typechap, pap, mschapv2

- Calling StationID تم تعيينه .
- NASport هو IP DSL طبق روابطها .

→ Next → ② Access granted لوحظ افعى معاينا سرطان

☒ Disconnect after idletime لغرسن، تاوس

Disconnect Session time [60]

allow access only number ل使用者只可输入数字

→ Next → Next → **Setting** also see 2.5

IP-Filter → Destination network 192.168.1.1

النحو الآخر Encryption

- IP Setting → Ⓛ Server setting determin Ip

→ Next → Finish

3.0.8.1 - VPN / Law / Policy

→ Next → Finish

UPN Game Policy (بایگانی) ۴

مشروع N - user

mSarhan → properties → Dial in → Control access through NPS → apply → ok

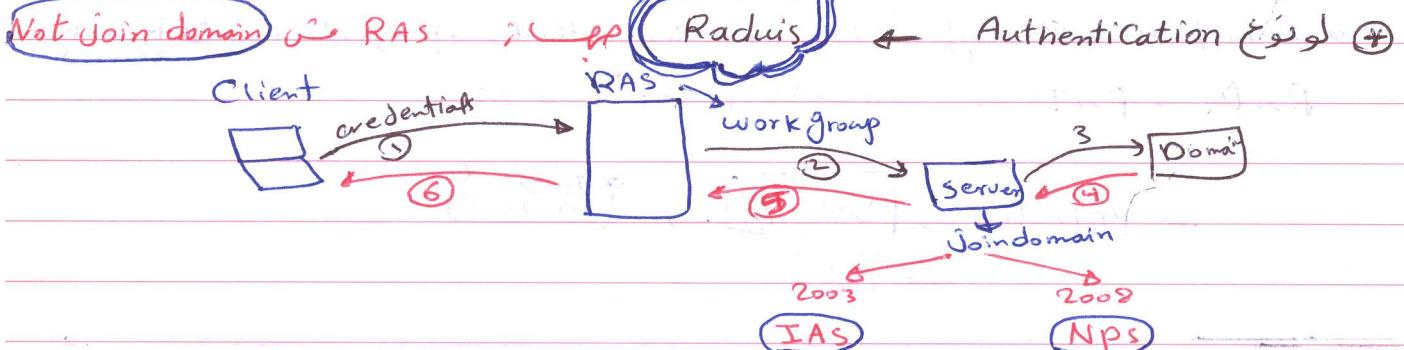
الشروط والبنود التي يقبلها المستخدم من قبل المستخدم

لعمليات احکام فی Client II بن Browsing

VPN properties → setting → ip Filters → + Destination 192.168.1.0

الاگی هنری علی بیخ website

Protocol TCP
Source port _____
Destination 80



دیکار لوار RAS اینکه Network را Hack کند

Joindomain نیز می‌باشد

التحقیق الجدی

- نزدیک RAS و نتیجه نماید
- DC Joindomain همیکو سروری
- NPS نتیجه نماید

Servermanager Roles → add →

admin tools → nps → RADIUS Client → Configure RADIUS Client

RADIUS Clients → New → Friend name 192.168.1.100 DNS 192.168.1.100

Shared secret [] Confirm [] NPS, RAS پسورد را بذکروا بعد از نتیجه نماید → OK

4- نزدیک RAS نزدیک NPS

Router → properties → Security → authentication Provider RADIUS Authentication → Configure → NPS Server
Servername 192.168.1.1 Shared Secret [] Password [] NPS Server

Account Provider RADIUS
Logging → add → Servername 192.168.1.1 → Change secret

NPS Server de la چشم Condition لوقت

Allow access → Dialin → user نماید - 0

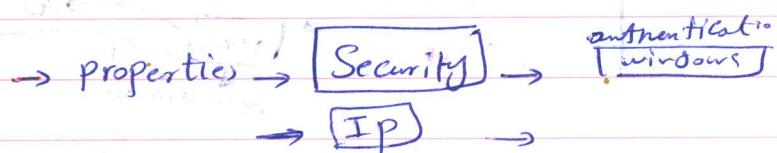
RAS

و NPS Server و authenticate جلسات الـ RAS

نفترض نسخة 2003 مع المطارات، نفتح

IAS

(RAS) (Remote access Service)

admin tools → Routing and Remote access → Router → properties → Remote access Service
Router → ports → بروتوكول L2TP, PPTP

نفترض NAP يعمل على Condition لعام 2003 في لمحات

Router → Remote Access policy → New Remote Access policy RAS

→ Next → Name [VPN] → Next → Groups → Next → Groups

ونختار المطرادات عارض

RADIUS (Radius Client) (Windows) ربط اتصال (RADIUS) لـ RAS

Control panel → Add/Remove Programs → Network Services → Details →

→ Internet Authentication Service → OK → Next → Finish

admin tools → Internet Authentication Service → RAS

Radius Client → New → Friendly name [192.168.1.100] → Next → Password
DNS [192.168.1.100]

RAS نزاع

Router → properties → security → Radius → Configure → Add →

Server name [] → IP IAS Server → OK

IAS

Via authentication need المعنون (public)

Client-to-Server

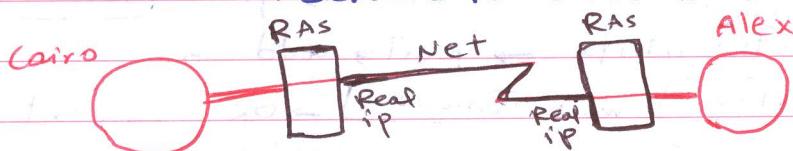
VPN (Virtual Private Network)

Site-to-Site

الموجهات (routers)

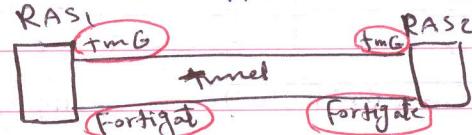
"25." Demand Dial (vpn Site-to-Site)

« Server-to-Server »



الخطوة ② الفرز بين استانسات RAS أو انتقال RAS

Encrypted tunnel يحتوي على بعدهم RAS ② JUN Router



Vpn site to site

demand dial

Persistent Connection

الاتصال وفتح الاتصال يعني اتصال من

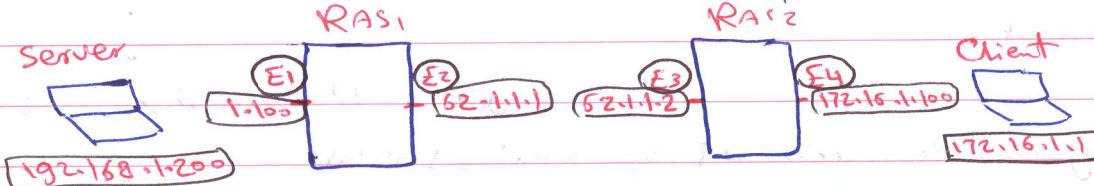
فترة مطولة Connectin ②

ستحث على طلب وفتح متصفح بـ http://www.google.com

Connectivity ④ حفظها او لا access

التطبيق العالمي

Not join domain عنوان IP راس ② JUN Router



RAS ① طرق السيرفر لـ Client ②

Realip → internal ip كاريبي ② اي RAS, a server ③

Routing and Remote up

Server manager → Roles → add → next → Network policy and access service → Next

Routing and Remote access services → Next → Install

فقط على درجة دخول قاتلين ② Firewall

admin tools → Routing and Remote access → ① RAS → Right Click →

Configure and Enable Routing → Next → ② Custom → Next → ③ Demand dial Connection

RASi is exits

Network interface → New Demand dial interface →

④ RASi → properties → ① LAN and demand dial routing
② Remote access server
IPN

① RAS1 → Network Interface → New Demand Dial Interface → Next → Name [Connect to alex] → Next → ② vpn → Next → ③ Automatic → Next → ipname [62.1.1.2] → Next
 Router ← RAS 11 چیزی که
 ④ Route ip packets on this interface → Next → add →
 Destination [192.168.1.10] mask [255.255.255.0] → OK → Next →
 user [RAS] Domain [] pass [12345] Confirm [12345]
 چیزی که RAS2 11 چیزی که سامانه دیگر را
 Connect to Alex (gant interface هدایتی
 این مرا فهمیدم چیزی که RAS2 چیزی که user 11 شد
 Local users and groups → RAS → Properties → Dialin → ⑤ Allow Access → Apply
 چیزی که RAS2 چیزی که user چیزی که مغایض ایجاد کردی RAS, چیزی که نظری
 Properties چیزی که Pass چیزی که RAS, چیزی که نظری
 ⑥ Allow access → Dialin چیزی که
 ⑦ vpn & Demand Dial & Configure later چیزی که RAS2 چیزی که
 ↳ Next → Finish

Network Interface → New Demand Dial → Name [Connect to Cairo] → Next
 → ⑧ vpn → Next → ⑨ Automatic → Next → IP [62.1.1.1] → RAS1 11
 → Next → ⑩ Route ip packets → Next → add →
 Destination [192.168.1.10] mask [255.255.255.0] → Next → user [RAS] pass []
 → Next → Finish

website چیزی که Domain چیزی که ترددی
 Server manager → Roles → add → ⑪ IIS → Next → Install →
 چیزی که نظری چیزی که Site چیزی که ایجاد کردی
 Admin tools → IIS → Default, stop → add web site → name [www.web]
 Physical path [کتابخانه] [] → IP [192.168.1.200] → OK → Default Document
 add → Name [-htm] → OK
 چیزی که RAS چیزی که المفهوم رسمی چیزی که Default چیزی که نظری
 Default gateway [192.168.1.100] → OK

RAS Alex چیزی که Default gateway چیزی که Client N چیزی که
 Default gateway [192.168.1.100]

چیزی که RAS چیزی که RAS چیزی که Ping - ok

Domain 11 to Ping & Client 11

Ping 192.168.1.200 -t

(1) → Remote access & RAS2 or RAS1 to RAS2 or RAS1

IP (1) IP (2) IP (3) IP (4) IP (5) IP (6)

Disconnect RAS1, RAS2, RAS3 & Interface to 11

Q Static pool → ipv4 → Properties → RAS to RAS2 or RAS1

Start [10.10.10.1] End [10.10.10.10] Adapter [192.168.1.100] → OK

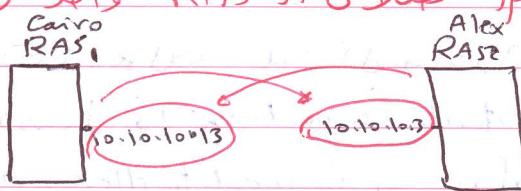
RAS2 → Forward

Start [10.10.10.11] End [10.10.10.20] → OK

IP (1) to IP (2) to Connect RAS1 to RAS2

Connect & Interface to 11

IP (4) to RAS1 to ipconfig cmd 11 to 12



10.3 & RAS2, 10.3 يخرب RAS1 على Connect RAS1 to RAS2

NAT (نجل) RAS2, RAS1

RAS1 → IPv4 → General → New interface → Routing protocol → NAT → OK

IPv4 → NAT, RightClick → New interface → 192.168.1.100 → O private → OK

New interface → Connect to alex → External IP → OK → O public

Enable NAT

RAS2 → General → New Routing protocol → NAT → OK

NAT → New interface → Internal → 172.168.1.100 → O private

→ New interface → Connect to Cairo → O public & Enable NAT → OK

Ping (لوكات)

Replay (الجهاز) Domain 11 Client 11

Cmd C:\> pathping 192.168.1.200

0 Client 172.16.1.1

dest IP 11

1 RAS 172.16.1.100

& RAS 11

2 10.10.10.1 tunnel 11

3 DC 192.168.1.200 DC 11

طبعاً لو مت Client || Domain || or site

<http://192.168.1.200>

سيوفه

ملحوظة

ملحوظة) Connect Client || NAT ركست || على || Domain

كل Clients الذي همروا من على RAS

بـ vpnIp || IP داير

Domain دلوقت يفتح درفل || Client ||

لوكرا || Data Security tunnel ملحوظة

ملحوظة) اللى كنت بتحلها Demand Dial او اتصال داير, لعاليين تغيره لا اتصال داير

RAS → Network Interfaces → Connect to Alex → properties → options → Persistent Connection

+ كذا يفضل الاتصال بيتم علطول

"26" Ip Sec

layer 2

Transport mode

Protocol

Tunneling mode

VPN

① Policy

② Rule tun, trans, L2L③ Filter Port

④ Action

Permit Negotiate Block



للوصول إلى البيانات Encrypt Data
للوصول إلى المنشآت IPsec values
رسائل IPsec

نحو IPsec
نحو IPsec
نحو IPsec
نحو IPsec
نحو IPsec

التطبيق الثاني

Local IPsec على سطح المكتب

admin tools → gp management → Default Domain policy → Edit →

ComplConfig → windows setting → security setting → Ip security policy →

Create Ip security policy → Next

الطريقة الثانية

Run → mmc → file → add/remover snap → Ip Security → add → ① Local Comp
→ finish → OKIp security policy → Create Ip security policy → Next → Name **HTTP** → Next →

Next → Finish

Policy ①

Rule ②

Rules → add → Next → ① this rule doesn't specify a tunnel → Next →

② All network Connections → Next →

Filter ③

Ip Filter list → Add → Name **HTTP** → OK → Next → ④ mirrored match, packet
→ Next → Source **Any IP** → Next → Destination **My IP** → Next →
select Protocol type **TCP** → Next → ⑤ From any port → ⑥ To this port
Next → Finish → OK

Subject.

Date.

لوبيتهم او مانعهم من حفظها IPsec

Add → Next → Name [] → permit → Next →

Action

عمل ②

 New filter Action → Next → Finish → OK

هذا يعني ارسال Policy ظهر ونفع لها

HTTP → Right click → Assign →

③ نرحب بـ Client IP ١٩٢.١٦٨.١.٢٠٠
 نرحب على المتصفح زيستي
 Permit لفتح وافز website

لورممعت غيرنا من ١١ Policy

HTTP → Right click → properties → HTTP → Filter Action → Block →
 Apply → كـ المفترض قفلت Port 80
 Assign و بعد ما نفتحها unassign ← Policy ونعمل

لورممعت ١١ IP تابع من هيفتح Client

لـ المتصفح
 ④ Negotiate security

④ Negotiate

Accept unsecure Comm, but انت ابغاه سالم اساله
 لـ المتصفح انت خاصهم IPsec انت IPsec فـ IPsec

Add وحيث

البيانات التي قد اتصال لا رقم يدخل integrity and Encryptionاظهار البيانات التي قد اتصال بـ integrity only

Custom

Apply → OK

Assign ونعمل ← و بعد ما نفتحها

Allow Fallback unsecure Comm. if Secure Can't establish source of the secure connection
 اذا امكنني من ادخال

Client وحيث ادخل عن ١١ Negotiate ← Action

من المفترض ان يدخل لكن لو عملت Reply + Pingحافة Port 80 فقط لـ المتصفح ادخل Filter Ping

نقطة على الـ (Protocol Pings)  **Protocol Pings** 

ممكن سطحب ||| telnet ||| على Server من Features

Features → telnet Client → Next → Install =
 telnet Server

admin tools → Services → telnet → automatic → apply

⑦ ۱۱ client ۱۲۳

Cp → admin tools → program and Features → Turn windows features →
 telnet Client telnet Server → OK

Cp → admin tools → Services → telnet → automatic → OK

Cmd → C:\>telnet 192.168.1.200 Server 1 [Is Cmd de ciso]

لوچیت علی Policy و مدلات میں ایک Server کی عملیات

① HTTP → Edit → protocol → Select protocol (TCP)

① to this part [23]

* نوعية ادخال Client || no telnet

لورقت مارکیز فایل unassign گیرنده Policy ۱۱ از Server می‌گیرد

ملحوظات لوقتیں اے Policy II اے OHTP اے Properties کے

authentication methods → Kerberos → Edt → Use Certificate ~~use in site~~

مشروع Client N ← Client Side نسخة العميل IPsec

Run → mmc → IP Security Policy → add → Local Computer → P

IP Security policies → Create IP security policy → Next → Name → Next →

Finish [Policy](#) [Timeline](#)

Das ist die zweite Übung mit einer Form. Sie ist eine sehr einfache Rechtschreibung.

Add → Next → ⚪ rule doesn't specify tunnel → Next → ⚪ All network Connection
Filter

→ Next → add → Name [any IP] → Add → Next → Source address [TCP]

→ Next → Destination address [] → Select protocol []
Next : From any port → to this port [] → next → Finish

Action Jai

① Telnet → Next → Add → Name [] → Next → ② Negotiate security
 → Next → ③ Do not allow unsecured communication → Next →
 ④ Integrity and encryption → Next → Finish → ⑤ New filter action
 → Next → ⑥ Active Directory (Kerberos v5 protocol) → Next → Finish
 Assign or unassign (جامعة)
 (جامعة) لـ telnet Server (لـ telnet Client)

لـ telnet Client (لـ telnet Server) لـ IPsec (لـ IPsec Client)
 (لـ IPsec Client) لـ telnet Client (لـ telnet Server) (لـ IPsec Client) (لـ IPsec Client)

telnet من هيئه لـ unassign ← Policy (لـ telnet Client)
 IPsec (لـ IPsec Client) بـ من هيئه

لـ telnet Client (لـ telnet Client) (لـ IPsec Client) (لـ IPsec Client)
 Http → Edit → Authentication methods → Kerberos → Edit →
 ⑦ Use this string [hii] → OK → assign و unassign (لـ telnet Client (لـ telnet Client))

لـ telnet Client (لـ telnet Client) (لـ IPsec Client) (لـ IPsec Client)
 Policy → Properties → ⑧ telnet → Authentication methods → Edit →
 ⑨ Use this String [hii] → OK → Apply → assign or unassign (لـ telnet Client (لـ telnet Client))

لـ telnet Client (لـ telnet Client) (لـ IPsec Client) (لـ IPsec Client)
 Group policy (لـ IPsec Client) (لـ IPsec Client) (لـ IPsec Client) (لـ IPsec Client)

Admin tools → Active Directory users and groups → New → On → Name [server] → OK
 Admin tools → Gp management → ABC.Com → Default Domain policy → Create gp → Name → IPsec

IPsec → Edit → Policies → window setting → Security setting → IP Sec policy →
 Create IP Security Policy → Next → Name [] → Next → Finish →

Rules → Add → Next → ⑩ this rule don't specify → Next → ⑪ All network → Next
 add → Name [RDP] → Add → Next → Next → Source address [my IP] → Next
 Dest [my IP] → Next → Select protocol [TCP] → Next → ⑫ to this [3389]
 → Next → Finish → action [Jai Filter] (لـ Jai Filter)

⑬ RDP → Next → ⑭ Edit → ⑮ Permit connection → Next →

" 27 " RDP WEB (Session Host)

طريقة تخلی كل clients الى في المستكمة يدخلوا على برنامج مستطبي على الـ Server
احسن ما اسطبه على كل جهاز لوحدة بس Microsoft من طريقة Internet Explorer

❶ يجي في شرطين للموضوع دا :

- active directory Server على Service غيره
- license Client his Service || Install اجل اجل اجل

ملحوظة لو ان اسرع انت عندي بطيئة وبحل لـ Download من على Server سرعه هو افالله

١٠٥ الملفات التي يطلبها لو انت انت سريع عندي وبحل Download من على Server من يطلب برخصه او بصيغه بصيغه يطلب عسان استدعاء البيانات في الـ Server

١٠٦ اولاً و بعد ذلك ١٠٧ هي البرامج التي غير الناس تدخل عليها Service

الخطيب الاهلى

Certificate Services من هنا

١- رختارا servermanager على activedirectory وبحل على Remote Desktop Service

Server manager → Roles → add → Next → Remote Desktop Service → Next →
 Remote Desktop session Host → Next → Next → Require Network level authent.
→ Next → Configure later ^{١٢٠ يوم} → Next → groups رختارا Add →
Next → Audio and video
 Audio recording redirection
 Desktop composition → Next → Install → **Restart**

١٠٧ اصحاب معاهدات **Remote webaccess** من هنا Client

• Roles → Remote Desktop Service → add → Remote Desktop webaccess → Add Requirements → Create self signed certificate
Admin tools → Remote Desktop Services → Remote App Manager → add Remote Application
→ Next →

Local Group اول ما تفتحه على Local Services يسيطر **Lab** على **TS group**

Server manager → Configuration → Groups → TS webaccess Computer → Add → **Local Group**
→ Apply → OK

❷ Remote App manager → Refresh → Distribution RD **Local Group** اول ما تفتحه

* سحب أي برنامج يقع على الـ **RD Server**

admin tools → Remote App manager → add → Next → Microsoft word → Next → Finish

IP Server RDP

http://192.168.1.200/rdweb Client

هذا خط على سطح المكتب RDP

↳ Rightclick → Run add-on → Run application

username abc\halil

Password -----

Public → Sign in

هذا ظهر البرنامج الذي أتى بفتح Microsoft Word

اضغط عليه ونختار Connect

User abc\halil

Pass ----- → OK

هذا يعمل وبعد حين هذل من البرنامج فتح معاك وستعمل عليه عادي على الرفع

من أن البرنامج من متجرنا Client

نواختها على الأصل (ملحوظة)

Remote App Deployment Setting → RD Gateway

ل睿连接 Client

Remote Desktop Connection → options → advanced → setting → use RD Gateway

Servername 192.168.1.200 → RD webserver → OK → Connect → user -----

Pass -----

هذا يعني دخول على vpn ← Server

Client لتوفرها على رخصة Microsoft

RD App

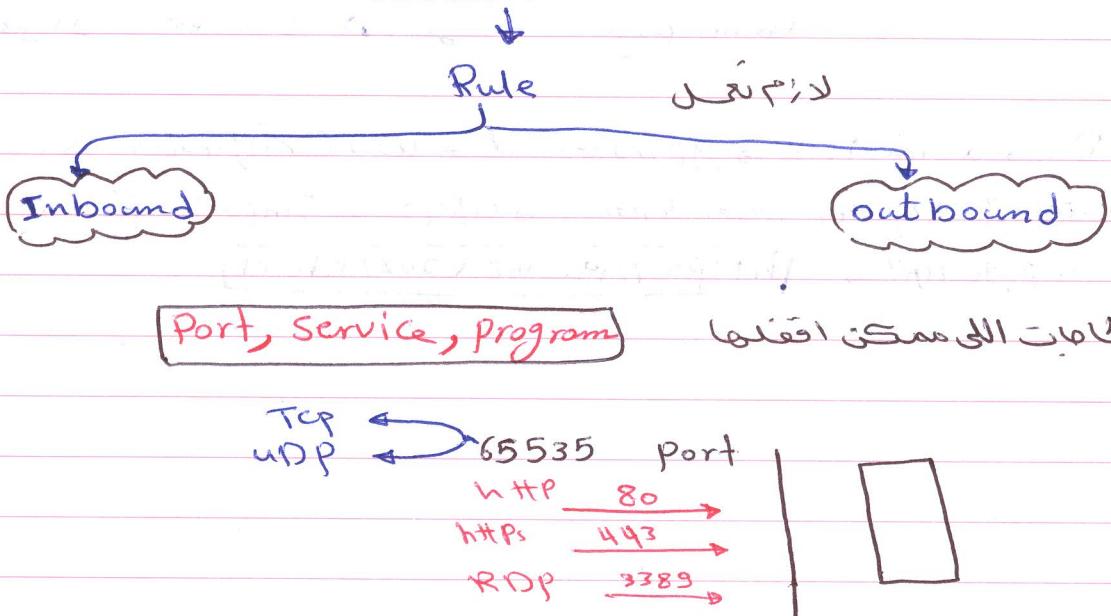
ملحوظة العائد من طرف

جكى سار اى Client او gp اى اى Explorer ىا يقى

نيدخل علطول على اى Server Home page اى اى

DC → admintools → gp management → User Configuration → policies →
 Internet Explorer maintenance → URLs → Import URLs →
 Home page URL → <https://192.168.1.202/rdweb>

1128) Windows Firewall



ملحوظہ لوگو ایڈیٹر اور Firewall ممنوع و افضل منہ حسابات رجسٹریشن فلٹر؛ اسے port80 website کا

Windows Firewall → advanced setting → Inbound → New Rule →

① port → ② TCP ③ Specific port [80] → Next → ④ Block → Next
→ Next → Name [HTTP] →

Rule هنلاین خودت ای Inbound Rules لو ضبط

لوار Client website میں کوئی محتوا نہیں
اوہ Rule وغیرہ کا Disable کر دیا جائے

للوصول إلى المخدمات عن بعد (Remote Desktop) على جهاز الكمبيوتر، افتح متصفح الويب واتصل بـ "3398" من خلال بروتوكول "Port Forwarding".

windows Firewall → Advanced Setting → Inbound → New Rule →

① predefined Remote Desktop → Next → Remote Desktop → Next →

① Block → finish

windows Firewall → Advanced → Monitoring → Link Log

Outbound & Inbound

ملحوظة ان الوجهات Server من خارج شبكة ولكن بفضل علىه IPSec

"29" Virtualization

Hyper V

اى سى 2008

جديد حى

* لوجىنىسى امكانيات استئناف سيرفرات كثيرة ببترى سيرفر واحد
او كامبيوناته عاليه وانزل عليهه كل ما برقى network ويعين انزل عليه
Bridge واحلى كارت الـ vm ware

vm → Setting → Network Adapter → Bridge

⇒ Replicate physical network

ممكن يوصله اى سى 2008 رى او من virtual pc
بس اى سى 2008 رى بيتم دعمها support لها ويعين اى سى 2008

Enable

ملحوظة

لوجىنىسى امكانيات على vm ware

Processors → Virtualize Intel VT-x
 Virtualize CPU Performance

كارديت الـ vmware

* فى طباعة الملفات ببترى server وتحل server 2008
رسالة فى BIOS ويعين كارد على HyperV
بتاح اى
Vmware و HyperV
العزم بين

Network يعرف اى حجز كارت HyperV
اول ما طبع يفتح اى كلام virtual PCs

الخطىء المدى

Server manager → Roles → Add Roles → Hyper-V → Next → local area
→ Install → Restart

 local area

admin tools → Hyper-V → New → virtual machine → Next → Name [Fileserver] →
Next → memory [512MB] → Next → [local area] → Next → location [Browse]
C → users → Administrator → my Document → C [هذا يكتب]
الاخير خطوة عوائى غير

الخطىء

 Size [127 GB] Create a virtual Hard Disk
Name [vhd]

Next →

② Install operating system later → Next → Finish

admintools → Hyper-v Manager → File Server → Right Click → Start
 لورقة على وملفات

File Server → Snapshot → Now → Connect
 دليل (دليلاً) على معاير
 تفاصيل

Hyper V manager → Virtual Network manager → New virtual network →

External → هاتجرا كارت الـ Net للمكائن → add → لختار الكارت

Internal Shared & Net كارت الشبكة المترابطة

Private Switch يتابع الـ Hyper servers وغير

Edit Disk ملحوظة ممكن نتعالى او File Server ونختار من المعنين او FileServer بناها او Setting او على او لختار HardDisk → Add → لختار نوعية

«30» windows Media Service 2008

لوعندى video وعابرات ملائمه Share عسان كل الشركات تجعل
بس محظى هيعنى ليقدم ولا يأخذ **BroadCast** **On Demand**
عليه قد امو طرفيتين **1** وقت الطلب الوقت اللي صنطبه فيه العميل **2**

لابد من اسفله Role بايام **Windows media Player** **Roles** **microsoft** من

لابد من **64** **32** بيعي كل واحد يستطع **Version** **②** لوي برنامج نازل منه على سنتها فقط

التطبيق العام

١) نصب البرنامج بالطريقه العادي وبعد ما ادخل على **Roles**

Servermanager → Roles → add → Streaming Media Service → Next
→ Next → windows media Server → Next → Realtime streaming protoc (RTSP)
→ Next → Management tools
 IIS management Console
 IIS management scripts
 Management service → Next → Install
 Port 554 media
 Port 80 Hypertext transfer protocol (HTTP)

admin tools → windows media services

admin tools → windows media services (web) → SSL Secure

Https Port 443 Secure

admin tools → IIS → Sites → windows media administration → Edit binding →
Edit → Ipaddress

بـنـدـحـظـ أـنـهـ حـتـىـ هـتـغـيـرـ غـيرـ لـوـعـتـ

IIS → Node2 → Server Certificates → Create self sign Certificate

Name **media**

لتحمل

اللى أنا عملتها

Type **HTTPS** **IP unassig** SSL Certificate **media** → OK

Port 8080 | Remove

admin tools → windows media service (web) → Enable SSL للتوصي

ترجمة لوصوتنا

admin tools → windows media services → publishing points →

add publishing point (wizard) → next → Name Media الى الالى
الى اسعار user connect
هاجمه بنتداح على قناته وعاليه التردد تجده (*) مروج
→ Next → ① Encoder (livestream) مروج دانه و معاير التردد تجده
→ Next → ② Broadcast → Next → ③ MultiCast مروج دانه و معاير التردد تجده
→ Next → HTTP:// لو ملئي بجودة ملفات عاليه الملاحة
و كل واحد يخلص بيأس الاس بعده

④ Play list

Play

لو ملئي بجودة ملفات عاليه الملاحة

و كل واحد يخلص بيأس الاس بعده

⑤ Broadcast يتحقق يوم الا user يتحقق بغيره ولا يأمر

⑥ On-demand تعرف قدم و تأم مروجها روتات اللي شفري معندها

→ Next → ⑦ Unicast

⑧ MultiCast

Enable unicast rollover → Next

⑨ New playlist

⑩ Existing playlist defalut هو موجهات عووهات

يتزفهم كت لنه الوسيط Wmpub vmroot

→ Next → Add media → Browse كتار الفيديو

One File

لو هستغل على ملف واحد

Files

ارك حاليه فديو موجود مدخل معاه اللي بعده بدوره واصل

→ Next →

ركمل عادي

⑪ Broadcast → Next → ⑫ MultiCast → Next → ⑬ New playlist

→ Next → Add media → Browse → لختا، ملف، wmv → Select File → -ASF

Add → OK → Next → Next → Loop الفديو يكرر ويعاد

Shuffle لعرض عشوائي

→ Next → Yes, enable logging → Next

→ Next → ⑭ Create a .nsf file → Finish

→ Next → ⑮ MultiCast information and announcement

Automatically Create web page - web server لتحته افتحه افتحه

⑯ MultiCast information file mediaplayers لتحته افتحه افتحه

- Next → Add → [Browse] → Add → OK
 → Next → Yes, enable logging For this multicast
 URL [http://node1.abc.com] → Next →
 → Next → @ web Server [http://node1.abc.com] ادخل user و password connect general
 → Next → Next → @ NO → Next → Finish

win Server گوئیں من بایو windows media player ۱۱ دھوکہ

درج کریں

Servermanager → Features → add Feature → Desktop Experience
 (Add Required) → Next → Install

media service اپلود کریں outcast client دھوکہ لے لیں
 http://node2.abc.com/media کام کریں media اپلود کریں

service ۱۱ اپلود کریں Client ۱۱ اپنائیں لے لیں
 Servermanager

admin tools → windows media services → Announce → لے لیں
 Client ۱۱ اپ، Copy لے لیں

۱۱ کھٹکے Client ۱۱ اپنائیں

Client ۱۱ اپنائیں on demand لے لیں
 من صورت میں اپنائیں Broadcast لے لیں

Advertising

windows media player → Advertising → use wallpaper لے لیں
 صورت میں اپنائیں (فائدہ)