TCP/IP Adressing - Public IP VS Private IP

ال Public IP: هو IP عام ومميز على مستوى الأنترنت وبنستخدمه عشان نعرف جهاز أو خدمة تقدر توصلها بشكل مباشر من خلال ال Internet

ازاي يقدر احصل على Public IP

- في جهة دولية اسمها IANA مسئولة عن إدارة ال IPs على مستوى العالم
- ال IANA مش بتديك ال IP بشكل مباشر
- ال IANA بتوزع بلوكات IPs ضخمة على هيئات إقليمية اسمها RIRs امثلة ← ARIN امريكا الشمالية، AFRINIC افريقيا
- بعد كدا الشركات الكبيرة اللي زي AWS بتقدم طلبات ال RIR وتاخد عناوين IP
- مثلاً AWS بتمتلك بلوك ذي 3.0.0.0/8 بيكون مسجل بأسم AWS
- لما بتعمل VM أو EC2 وتطلب Public IP مش بتروح كل مرة تستأذن IANA هي مخصصة ليك بلوك IP بتاعك بالتالي بشكل تلقائي ال EC2 بتاخد IP
- البلوكات هي عبارة عن Range IP ← 3.0.0.0/8
- دلوقتي أي عناوين بتبدأ ب 3 بتبقى بتاعتك مثلاً ← 3.0.0.1 , 3.1.5.10

ليه مفيش منظمة تانية؟ لأن هيحصل تضارب بسبب الجهتين والانترنت محتاج جهة واحدة بس تدير ال IP Adressing

CS Scanned with CamScanner

TCP IP Addressing Public vs Private

ال Private IP هو IP بنستخدمه جوا شبكات خاصة ومش بيوصل بشكل مباشر بالإنترنت ومش محتاج مؤسسة عالمية تديره

ليه ال Private IP اتعمل ؟

- زمان مع IPv4 عدد العناوين حوالي 4.3 مليار ودا عدد قليل جدا مقارنة بعدد الموبيلات والسيرفرات واللابتوبات لو كل جهاز خد Public IP العناوين هتخلص بسرعة
- طلعت بقى فكرة ليه كل الأجهزة جوا البيت أو الشركة تاخد Public IP بالتالي كل الأجهزة تاخد Private IP والراوتر يبقى عنده Public IP واحد، ودا اللي وفر مليارات الـ Public IP يعني أي: ← الراوتر بياخد Public IP وعندي موبيل ولابتوب و Smart TV و Playstation كلهم واخدين Private IP وكل الأجهزة دي متوصلة بالراوتر اللي طالع على الإنترنت بالـ Public
- الراوتر نفسه بيعمل حاجة اسمها (NAT)
- الراوتر ياخد الـ Packet اللي طالعة ويبعتها للمكان المناسب
- ال NAT مهمته يشوف ال Private IP ومش مسموح يطلع على الإنترنت قبل ما ال Req يطلع يتحول لـ Public IP بتاع ال Router ويبعت ال Req للجهة المحددة مثلا google ولما جوجل ترد عليك هترد عليك على ال Public IP اللي انت بعت منه ال Req ساعتها ال Router هيستقبل ال Response أو الرد
- ال NAT هنا هينفذ مهمة تانية لما بيستقبل الرد بيكون اصلا عنده NAT Table بتتعمل لما انت تشغل service معينة بيتعمل Rule وتشغل الخدمة هتنشئ Rule مؤقتة لحد لما تخلص اللي انت عايزه وتقفل الـ service بيتكتب في ال NAT Table لو جه رد من خلال الـ service ابعته الي ال Pub IP الخاص بال Router والموجه الي ال Priv IP الخاص

Scanned with CamScanner

TCP IP Adressing - Public + Private

يبقى كدا الـ NAT مسؤولة عن

① Address Translation ← لما بتفهم كل IP بتاع مين
ولما تستبدل الـ Priv IP بالـ Pub IP وتعيد نفس العملية
وهي بتاخد الرد من الـ Service ويوجه الرد للـ Pub IP
وبعدها لل Priv IP المناسب

② NAT Table ← أول لما بتعمل اتصال جديد يبدأ يحط
الـ Rules المناسبة

Priv IP ← تابع عالي ← Pub IP

- ولما الـ Service ترد يرجع عالي الـ Pub IP
- ساعتها الـ NAT تبص في الجدول وتعرف ان الرد
لازم يروح لل Priv IP اللي طلع منه الـ Req واتعمل
ليه Rule جوا الـ NAT Table

الـ Router هو اللي بيبعت الـ Req على الأنترنت

يبقى كدا

- Routing ← يحدد الترافيك يروح فين ويمرره من الشبكة
- NAT ← يترجم العناوين و يحتفظ بالـ IPs في NAT Table

Scanned with CamScanner

TCP/IP Addressing Public + Private

RFC1918 IP Ranges ← في Ranges محجوزة للاستخدام الداخلي
فقط ودا بنحن الوثيقة اسمها RFC 1918
واتفق العالم كله على القاعدة دي ← أي عنوان يقع داخل
الرينجات دي لا يتم توجيهه إلى الأنترنت
وهما ← 10.0.0.0/8 و 172.16.0.0/12 و 192.168.0.0/16

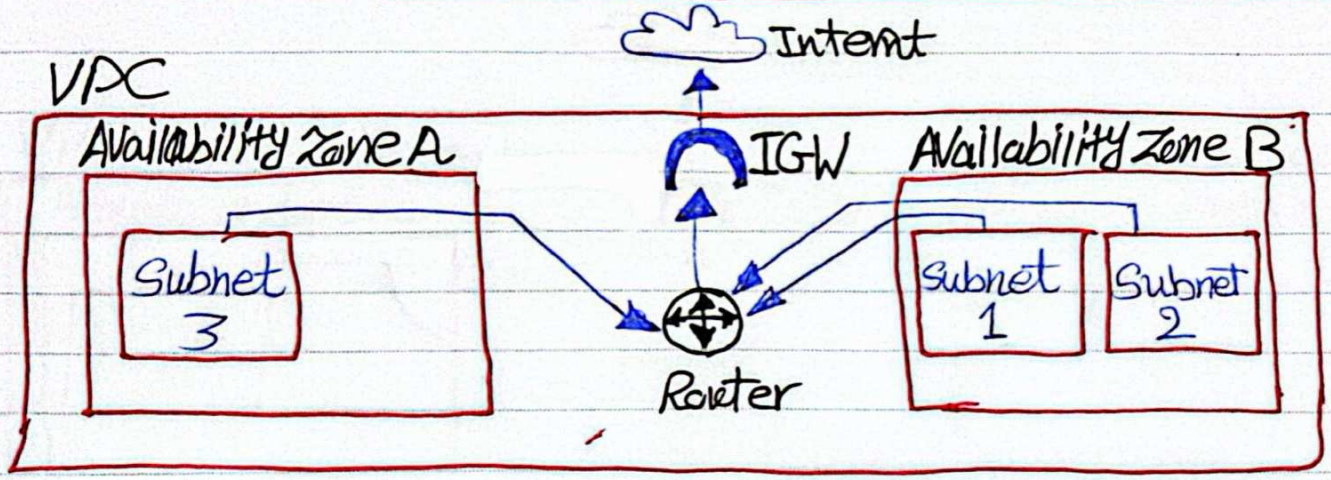
كل الـ Routers الحديثة من Cisco وغيرهم من الشركات
طبقوا المعايير القياسية للأنترنت

تقدر تكرر الـ Priv IP في أكتر من شبكة عادي لأنه داخلي
ومش بيطلع على الأنترنت ولو عايز تطلع عالأنترنت
ساعتها الـ NAT هيتعامل ويطلعك بالـ PubIP بتاع الـ Router
اللي مش بيتكرر فالعالم كله

الرينجات دي جزء من الـ IPV4 وزيها زي أي IPV4
الفرق بس في الرينجات دي محجوزة للـ Private وتقدر تكررها
ودا كان التوفير الحقيقي في عدد الـ IPs

Scanned with CamScanner

Public Subnet + Private subnet in a VPC



ال Subnet عشان تكون Public بيتحقق شرطين

1. تكون موجودة جوا VPC موجود فيها IGW
2. ال Route Table لازم يكون فيها

Subnet#3

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-12345

- ال Destination يعني ال IP بتاع المكان اللي خارج الشبكة يعني زي Google أو facebook

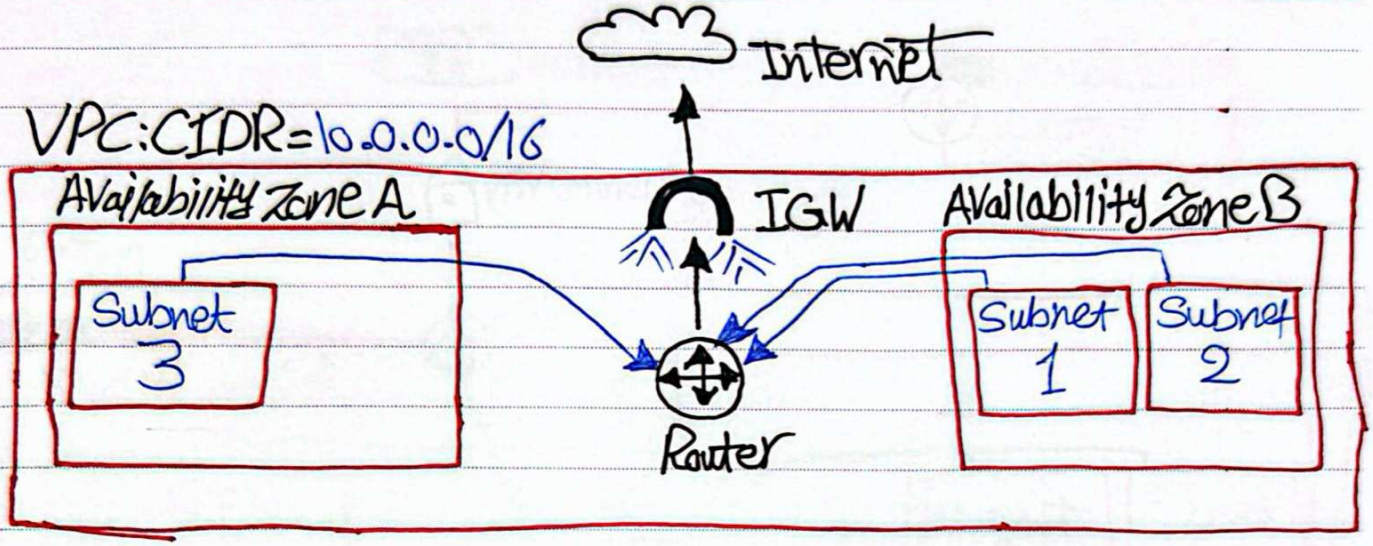
0.0.0.0/0 ← معنى بقى ال Destination اللي محطوط بقول لل Subnet تقدر تروح لأي Destination فالعالم لأني مش محدد هي هتطلع على ال Internet على أي بالظبط انا مخليها Global مفيش أي شرط أو bit ثابتة تحدد شبكة معينة

يعني أي مفيش أي شرط أو bit ثابتة تحدد شبكة معينة

- 10.0.0.0/16 معناها أول 16 Bit لازم يكونوا ثابتين يعني لازم أي IP يبدأ ب 10.0
- 192.168.1.0/24 معناها أول 24 Bit لازم يكونوا ثابتين يعني لازم يبدأ ب 192.168.1
- 0.0.0.0/0 معناها؟؟ مفيش معنى لوجود شرط اصلاً بالتالي هو مطلوب يقارن كل الـ Bit و اصلاً مفيش بالتالي مفيش شرط يبقى عدد ال Net Bit المطلوب للمطابقة هو Zero بالتالي أي عنوان IP هيطابق ال Route دي

Scanned with CamScanner

Public Subnet + Private Subnet in a VPC



الـ Private Subnet بتكون local على مستوى الـ VPC
لو عايز ابعت أي Trafic من خلال الـ Route داخل الـ VPC فقط

subnet 1,2

Destination	Target
10.0.0.0/16	Local

- بقول ان كل الـ Subnet اللي جوا الـ Range دا Local طيب أي هوا الـ Range دا هوا الـ VPC CIDR
- الـ Data بتاعة Sub1,2 بتقول تواصل داخلي جوا الـ VPC حتى لو موجود IGW مفيش الـ Entry اللي تخليني استعمل الـ IGW

Scanned with CamScanner

TCP/IP ADDRESSING – PUBLIC IP vs PRIVATE IP (COMPLETE ARCHITECTURE)

IP is a logical address used to identify devices or services and enable communication over the Internet.

IP TYPES

- **Public IP** : Reachable over the Internet.
- **Private IP** : Not reachable directly from the Internet.

1) INTERNET & PUBLIC IP

IANA

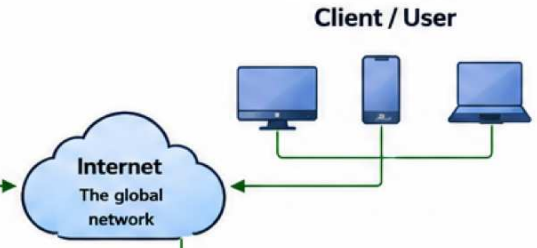
IANA is the global authority responsible for IP address allocation.

Public IP Ranges

Example of public IP block owned by AWS

3.0.0.0/8

Used in AWS regions (e.g., EC2, VPC, ELB, etc.)



PRIVATE IP RANGES (RFC1918)

These ranges are reserved for private networks and not routed on the Internet.

10.0.0.0/8	172.16.0.0/12	192.168.0.0/16

You can use any block from the above ranges.

In this example we use: **10.0.0.0/16**

We can expand the VPC by adding a Secondary CIDR.

Example: **172.16.0.0/16** (up to 4 secondary CIDR blocks).

WHAT IS NAT?

NAT (Network Address Translation) allows devices in a private network to access the Internet using a Public IP address.

HOW IT WORKS?

1- Device in Private Subnet sends a request to the Internet.

2- Request goes to the NAT Gateway.

3- NAT Gateway replaces the source Private IP with its Public IP.

4- Traffic goes to the Internet.

5- Response comes back to the Public IP of the NAT Gateway and the NAT Table maps it back to the original Private IP.

VPC (VIRTUAL PRIVATE CLOUD)

CIDR: 10.0.0.0/16

Internet Gateway (IGW)

Public Subnet (Example)

CIDR: 10.0.1.0/24

NAT Gateway (Managed)

Public IP: 3.0.0.10

Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

Private Subnet (Example)

CIDR: 10.0.2.0/24

Private Instance

Private IP: 10.0.2.10

Private DB

Private IP: 10.0.2.20

Private Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT GW

3) ROUTING

- Every VPC has **Route Tables** that determine where traffic is sent.
- Local route for VPC CIDR → local
- Internet route → 0.0.0.0/0 → IGW (Internet Gateway)

4) NAT RULES

- Outbound traffic → only via NAT Gateway.
- Inbound traffic from the Internet to Private IP is not allowed unless using Port Forwarding or specific services.

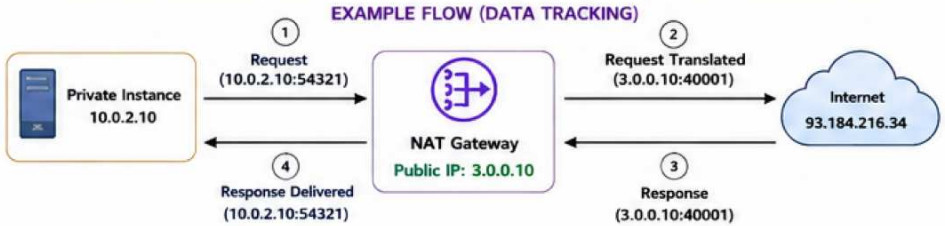
5) PROTOCOLS SUPPORTED

All protocols depend on IP, such as: TCP, UDP, ICMP (with TCP), etc.

NAT TABLE (INSIDE NAT GATEWAY)

Private IP:Port (Inside)	Public IP:Port (Outside)	Destination IP:Port (Internet)	Protocol	State
10.0.2.10:54321	3.0.0.10:40001	93.184.216.34:80	TCP	ESTABLISHED
10.0.2.20:56789	3.0.0.10:40002	8.8.8.8:53	UDP	ESTABLISHED
....	....	....	....	....

EXAMPLE FLOW (DATA TRACKING)



6) CIDR & VPC EXPANSION

You can add up to 4 Secondary CIDR blocks.

VPC

Primary CIDR	:	10.0.0.0/16
Secondary #1	:	172.16.0.0/16
Secondary #2	:	192.168.0.0/16
Secondary #3	:	100.64.0.0/16
Secondary #4	:	192.0.2.0/24

Used to scale the network in the future.

SUMMARY

- ✓ Public IP → reachable from the Internet
- ✓ Private IP → used inside private networks
- ✓ NAT → allows private devices to access the Internet
- ✓ Route Table → defines network paths
- ✓ 0.0.0.0/0 → default route to the Internet

TCP/IP Addressing – Public IP vs Private IP

الـ IP هو عنوان منطقي يُستخدم للتعرف على جهاز او خدمة وتحديد موقعها بشكل مباشر من خلال الـ Internet

IP Types

- **Public IP** : عنوان عام يمكن الوصول إليه من الانترنت
- **Private IP** : عنوان خاص غير قابل للوصول من الانترنت مباشرة

1) Internet & Public IP

IANA

الجهة المسؤولة عالمياً عن توزيع عناوين الـ IP

Public IP Ranges

مثال على بلوك مملوك لـ AWS

3.0.0.0/8

تستخدمه AWS في مناطق

مثل EC2 , VPC , ELB

Client / User

المستخدم النهائي

Internet

شبكة الإنترنت

Private IP Ranges (RFC1918)

هذه النطاقات خاصة وغير قابلة للتوجيه عبر الإنترنت

10.0.0.0/8	172.16.0.0/12	192.168.0.0/16

ملاحظة:

يمكن استخدام أي بلوك خاص من الثلاثة

في هذا المثال نستخدم : 10.0.0.0/16

ويمكن لاحقاً توسيع الـ VPC ← Secondary CIDR

(حتى 4 بلوكات ثانوية) مثل : 172.16.0.0/16

VPC (Virtual Private Cloud)

CIDR: 10.0.0.0/16

Internet Gateway (IGW)

Public Subnet (العامة)

CIDR: 10.0.1.0/24

NAT Gateway

Public IP: 3.0.0.10

Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

Private Subnet (الخاصة)

CIDR: 10.0.2.0/24

Private Instance

Private IP: 10.0.2.10

Private DB

Private IP: 10.0.2.20

Private Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT GW

ما هو الـ NAT ؟

الـ NAT يسمح للأجهزة داخل الشبكة الخاصة بلستخدام Internet من خلال عنوان Public IP واحد فقط.

كيف يعمل ؟

1- الجهاز داخل الـ Private Subnet يرسل طلب للإنترنت (سيرفر خارجي).

2- الطلب يذهب إلى الـ NAT Gateway

3- الـ NAT بترجم الـ Source Private إلى الـ Public IP به.

4- السيرفر الخارجي برد على الـ Public IP

5- المجمع يعيد الرد إلى الـ Private IP المطلوب بناء على NAT Table .

3) Routing

- (الخاصة) VPC الـ VPC الى الموجود بقرأ Table ويحدد الوجهة.
  - إذا الوجهة داخل الـ VPC ← local
  - IGW أو الوجهة ، 0.0.0.0/0 ← يرسل إلى IGW أو.

4) NAT Rules

- الـ Outbound Traffic على الـ NAIs فقط.
- Inbound من الإنترنت الـ Private IP (إلا من خلال Port Forwarding مسموح غير أو الأنواع الخاصة).

5) البروتوكولات التي يدعمها (5)

يدعم كل البروتوكولات التي تعتمد على الـ IP مثل: TCP , UDP , ICMP (مع القيود TCP)

NAT Table (Inside NAT Gateway)

Private IP:Port (Inside)	Public IP:Port (Outside)	Destination IP:Port (Internet)	Protocol	State
10.0.2.10:54321	3.0.0.10:40001	93.184.216.34:80	TCP	ESTABLISHED
10.0.2.20:56789	3.0.0.10:40002	8.8.8.8:53	UDP	ESTABLISHED
....	....	....		

مثال على تدفق البيانات

Private Instance 10.0.2.10

1 Request (10.0.2.10:54321)

NAT Gateway Public IP: 3.0.0.10

2 Request Translated (3.0.0.10:40001)

Internet 93.184.216.34

3 Response (3.0.0.10:40001)

4 Response Delivered (10.0.2.10:54321)

6) CIDR الـ VPC (CIDR Expansion)

يمكن إضافة حتى 4 بلوكات Secondary CIDR

VPC

Primary CIDR	10.0.0.0/16
Secondary #1	172.16.0.0/16
Secondary #2	192.168.0.0/16
Secondary #3	100.64.0.0/16
Secondary #4	192.0.2.0/24

تستخدم لتقسيم الشبكة أو التوسع للمستقبل

ملخص سريع

- ✓ Public IP ← للوصول من الموجود
- ✓ Private IP ← عنوان استخدامي داخلي
- ✓ الـ NAT يسمح للخاصة بالوصول للإنترنت
- ✓ الـ Route Table تحدد مسار الترافيك
- ✓ 0.0.0.0/0 هو Default Route