اليوم الثاني والثلاثون: IPv6 - الجزء الثاني

رأس IPv6 (IPv6 Header)

رأس IPv6 أبسط بكثير من رأس IPv4. بينما رأس IPv4 يحتوي على 12 حقلاً مختلفاً ويتراوح حجمه من 20 إلى 60 بايت، رأس IPv6 ثابت الحجم (40 بايت) ويحتوي على 8 حقول فقط. هذا التبسيط يسرع معالجة الحزم في الموجهات لأن كل حزمة IPv6 لها نفس حجم الرأس (40 بايت)، مما يسمح بمعالجة أسرع في العتاد (Hardware).

حقول رأس IPv6:

1. Version (4 بت): دائماً 6 (0110). هذا يحدد أن هذه حزمة IPv6.

2. Traffic Class (8 بت): مشابه لحقل ToS في IPv4. يستخدم لتحديد أولوية الحزمة (QoS).

3. Flow Label (20 بت): حقل جديد في IPv6. يسمح بتحديد تدفق معين (Flow) من الحزم التي تحتاج معاملة خاصة (مثل VoIP). الموجه يتعرف على التدفق من هذا الحقل ولا يحتاج إلى فتح الرأس بالكامل.

4. Payload Length (16 بت): طول البيانات (Payload) بالبايت، بعد الرأس الأساسي. لا يشمل الرأس الأساسي نفسه.

5. Next Header (8 بت): يحدد نوع الرأس التالي (مثل TCP = 6، UDP = 17، ICMPv6 = 58). في IPv4، هذا الحقل يسمى Protocol. في IPv6، يمكن أن يكون الرأس التالي رأساً إضافياً (Extension Header) أو بروتوكول طبقة النقل.

6. Hop Limit (8 بت): مشابه لـ TTL في IPv4. ينقص بمقدار 1 عند كل قفزة. عندما يصبح 0، يتم تجاهل الحزمة. تم تغيير الاسم من TTL إلى Hop Limit لأنه أكثر دقة (TTL كان يقاس بالثواني نظرياً ولكن عملياً كان يقفزات).

7. Source Address (128 بت): عنوان IPv6 للمصدر.

8. Destination Address (128 بت): عنوان IPv6 للوجهة.

ما تم إزالته من IPv4: تم إزالة حقل IHL (لأن الرأس ثابت الحجم 40 بايت). تم إزالة حقل Identification و Flags و Fragment Offset (نقل التجزئة إلى Extension Headers). تم إزالة حقل Header Checksum (لأن الطبقة الثانية وطبقة النقل تقوم بفحص الأخطاء). تم إزالة Options (نقلت إلى Extension Headers منفصلة).

تغيير مهم: لا يوجد Checksum في رأس IPv6. هذا يعني أن الموجهات لا تحتاج إلى إعادة حساب الـ Checksum عند كل قفزة (كما كانت تفعل في IPv4). هذا يسرع عملية التوجيه بشكل كبير.

Extension Headers: بدلاً من حقل Options في IPv4، يستخدم IPv6 رؤوساً إضافية (Extension Headers) توضع بين الرأس الأساسي ورأس طبقة النقل. أمثلة: Hop-by-Hop Options Header (0)، Routing Header (43)، Fragment Header (44)، Destination Options Header (60)، Authentication Header (51)، Encapsulating Security Payload (50).

ICMPv6 - Internet Control Message Protocol for IPv6

ICMPv6 هو إصدار IPv6 من ICMP. ولكنه أكثر من مجرد ICMP مع عناوينICMPv6. IPv6 يدمج عدة وظائف كانت منفصلة في IPv4. رقم بروتوكول ICMPv6 هو 58 (في حقل Next Header).

وظائف ICMPv6: الإبلاغ عن الأخطاء (مثل Destination Unreachable، Time Exceeded)، التشخيص (Ping باستخدام Echo Request/Reply)، والوظيفة الأهم: NDP (Neighbor Discovery Protocol).

NDP هو قلبNDP. IPv6 يحل محلIPv4 (ARP) وأيضاًIPv4) (ICMP Router Discovery وجزء من DHCP. NDP يستخدم خمسة أنواع من رسائل ICMPv6:

1. Router Solicitation (RS) - النوع 133: يرسله الجهاز (Host) لطلب معلومات من الموجه المحلي (اكتشاف الموجه). يرسل RS إلى عنوان All Routers (FF02::2).

2. Router Advertisement (RA) - النوع 134: يرسله الموجه (Router) استجابة لـ RS أو بشكل دوري (كل 200 ثانية افتراضياً). يحتوي RA على معلومات التوجيه: البادئة (Default Gateway Link-Local، Prefix)، وهوامر SLAAC و DHCPv6. يرسل RA إلى عنوان All Nodes (FF02::1).

3. Neighbor Solicitation (NS) - النوع 135: مشابه لطلب ARP في IPv4. يرسله جهاز لمعرفة عنوان Link-Layer (MAC) المرتبط بعنوان IPv6 معين. يرسل NS إلى عنوان Solicited-Node Multicast للجهاز الهدف.

4. Neighbor Advertisement (NA) - النوع 136: استجابة لـ NS. يحتوي على عنوان MAC للجهاز المرسل. يرسل NA كـ Unicast إلى الطالب.

5. Redirect - النوع 137: يرسله الموجه لإعلام الجهاز بأن هناك مساراً أفضل إلى وجهة معينة (مشابه لـ ICMP Redirect في IPv4).

NS/NA - استبدال ARP

في IPv4، عندما يريد جهاز معرفة عنوان MAC لجهاز آخر في نفس الشبكة، يرسل طلب ARP (بث إلى FFFF.FFFF.FFFF). في IPv6، هذا يتم عبر NS و NA.

كيف يعمل: عندما يريد الجهاز A معرفة عنوان MAC للجهاز B (الذي يعرف عنوان IPv6 الخاص به)، يقوم A بحساب عنوان Solicited-Node Multicast للجهاز B. هذا العنوان يتكون من البادئة FF02::1:FF00:0/104 مع آخر 24 بت من عنوان IPv6 للجهاز B. A يرسل NS إلى هذا العنوان المتعدد البث. B يستقبل NS (لأنه مشترك في هذه المجموعة المتعددة البث) ويرد بـ NA مباشرة إلى Unicast (A) يحتوي على عنوان MAC الخاص به.

مزايا NS/NA على ARP: لا يوجد بث (Broadcast) - كل شيء عبر Multicast. هذا يعني أن الأجهزة في الشبكة التي لا تشارك في هذه العملية لا تتأثر. هذا يحسن الأداء خاصة في الشبكات اللاسلكية. أيضاً، NS و NA هما جزء من ICMPv6، مما يعني أنهما محميان بالأمان (IPSec يمكن استخدامه).

SLAAC - Stateless Address Autoconfiguration

SLAAC هي ميزة قوية في IPv6 تسمح للأجهزة بتوليد عنوان IPv6 خاص بها تلقائياً دون الحاجة إلى خادم DHCP. هذا يجعل الشبكة "جاهزة للتوصيل والتشغيل" (Plug and Play).

كيف تعمل SLAAC:

الخطوة 1: عندما يتصل الجهاز بالشبكة ويفعّل IPv6، يقوم بتوليد عنوان Link-Local تلقائياً (FE80:: مع EUI-64).

الخطوة 2: الجهاز يرسل RS (Router Solicitation) إلى FF02::2 لطلب معلومات التوجيه.

الخطوة 3: الموجه (Router) يرد بـRA (Router Advertisement). يحتوي RA على: بادئة الشبكة (Prefix) مثل DB8:1:1::/64:2001، طول البادئة (Prefix Length)، الـ Default Gateway (عنوان Link-Local للموجه).

الخطوة 4: الجهاز يأخذ البادئة من RA ويضيف EUI-64 الخاص به (أو عنوان عشوائي للأمان - Privacy Extensions) ليكون عنوان IPv6 الكامل. مثلاً: DB8:1:1:211:22FF:FE33:4455:2001.

الخطوة 5: الجهاز يقوم بـDAD (Duplicate Address Detection) للتأكد من عدم وجود جهاز آخر يستخدم نفس العنوان. إذا كان هناك تعارض، يولد عنواناً آخر.

ميزة SLAAC: لا حاجة لخادم DHCP، إدارة أقل، مناسب للشبكات الصغيرة والمتوسطة. عيب SLAAC: لا يوفر معلومات إضافية مثلDNS Server addresses (بشكل افتراضي). إذا كان RA يحتوي على خيارات DNS، يمكن لـ SLAAC توفيرها.

DHCPv6

في DHCP، IPv6 يعمل بشكل مختلف. يوجد نوعان من DHCPv6:

النوع الأول:Stateless DHCPv6. هذا هو الأكثر شيوعاً. يستخدم مع SLAAC. الجهاز يأخذ عنوان IP من SLAAC (من RA)، ويستخدم DHCPv6 فقط للحصول على معلومات إضافية مثلDNS Servers و Domain Name. لا يعطي DHCPv6 Stateless عناوين IP. يجب ضبط RA على أن M (Managed Address Configuration) = 0 و O (Other Configuration) = 1.

النوع الثاني:Stateful DHCPv6. هذا مشابه لـ DHCP في IPv4. الخادم يدير عناوين IP ويعطيها للأجهزة. يجب ضبط RA على M = 1. في هذه الحالة، الجهاز لا يستخدم SLAAC، بل يحصل على عنوانه بالكامل من DHCPv6.

```
! تكوين Stateless DHCPv6 (SLAAC للعنوان + DHCPv6 الأخرى للمعلومات)
Router(config)# ipv6 dhcp pool DHCPv6_POOL
Router(config-dhcpv6)# dns-server 2001:4860:4860::8888
Router(config-dhcpv6)# domain-name example.com
Router(config-dhcpv6)# exit

Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ipv6 address 2001:DB8:1:1::1/64
Router(config-if)# ipv6 nd other-config-flag
Router(config-if)# ipv6 dhcp server DHCPv6_POOL

! تكوين Stateful DHCPv6 (عنوان IP + معلومات)
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ipv6 address 2001:DB8:1:2::1/64
Router(config-if)# ipv6 nd managed-config-flag
Router(config-if)# ipv6 dhcp server DHCPv6_POOL
```

أوامر IPv6 الأساسية على Cisco

لتكوين IPv6 على أجهزة Cisco، نستخدم أوامر تبدأ بـ `ipv6`. الأمر `ipv6 enable` يفعل IPv6 على واجهة ويولد عنوان Link-Local تلقائياً. الأمر `ipv6 address` يعين عنوان IPv6 للواجهة.

```
! تفعيل IPv6 تمكين التوجيه (على الموجه)
Router(config)# ipv6 unicast-routing

! تكوين واجهة مع عنوان ثابت
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ipv6 address 2001:DB8:1:1::1/64
Router(config-if)# ipv6 enable
Router(config-if)# no shutdown

! تكوين واجهة مع EUI-64
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ipv6 address 2001:DB8:2:2::/64 eui-64
Router(config-if)# ipv6 enable
```

لاحظ: الأمر `ipv6 unicast-routing` ضروري لتفعيل التوجيه IPv6 على الموجه (بدونه، يعمل الموجه كـ Host وليس كـ Router). هذا الأمر يجعل الموجه يرسل RA ليعلن عن نفسه كموجه للأجهزة المتصلة.

التحقق من تكوين IPv6

```
Router# show ipv6 interface brief
GigabitEthernet0/0   [up/up]
    FE80::211:22FF:FE33:4455
    2001:DB8:1:1::1
GigabitEthernet0/1   [up/up]
    FE80::211:22FF:FE33:4456
    2001:DB8:2:2:211:22FF:FE33:4456

Router# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

C   2001:DB8:1:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:1:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2001:DB8:2:2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:2:2:211:22FF:FE33:4456/128 [0/0]
     via GigabitEthernet0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

ملاحظة مهمة: تذكر دائماً تفعيل `ipv6 unicast-routing` على الموجه حتى يعمل كموجه IPv6. بدونه، لن يرسل الموجه RA ولن تتمكن الأجهزة المتصلة من استخدامه كـ Default Gateway. SLAAC هي إحدى أجمل ميزات IPv6 لأنها تجعل إعداد الشبكة أسهل بكثير.