IR.3504 Convergent Services and Technologies

IP Network Basics

Sofiane Imadali, PhD <sofiane.imadali@orange.com>

Summary

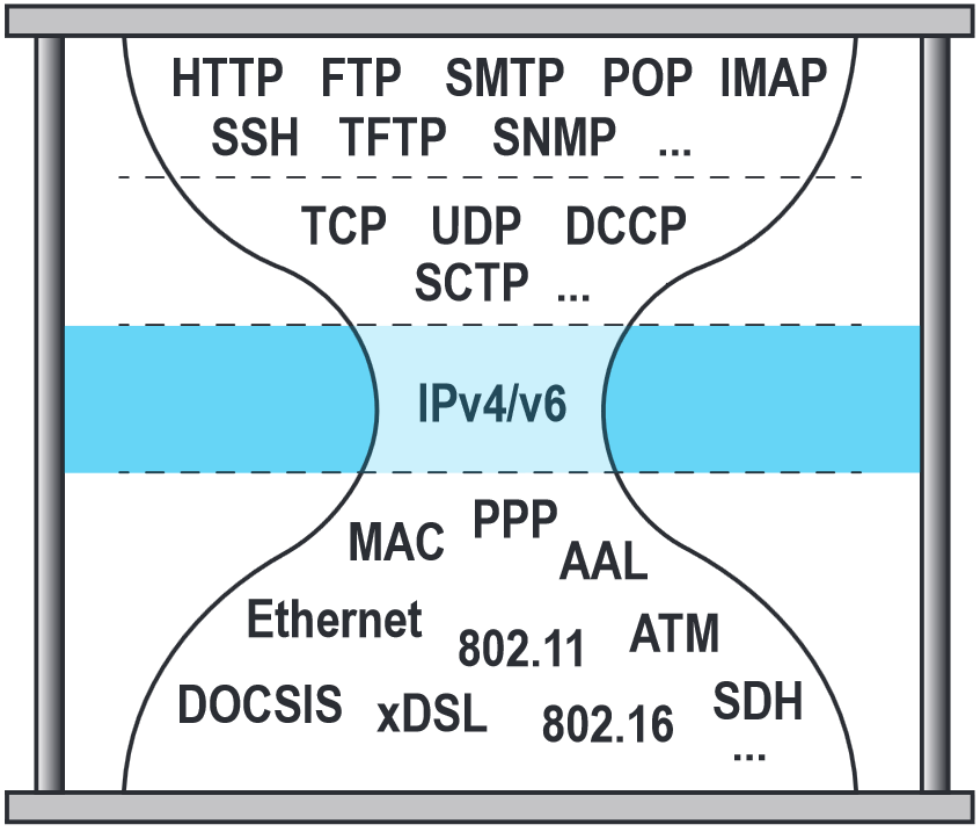
At the end of this talk, you should be able to answer the following questions:

- What happens (protocols, messages exchanged, entities, programs) when I first connect my PC to a network ?
- What happens when I send a message to be routed somewhere ? (ping, traceroute, http)
- What are the networking tools/programs you would use to diagnose a non-responding website, local service, a database connection ?
- How do I build my own IPv6 address based on a prefix that I know ? Do I need to be connected to the Internet to have a globally-scoped address ?

➢ **Some of the information, tests and experiments that we do are present in: https://github.com/sofianinho/training (the network folder)**

OSI model

		Example
7	Application	Web Application
6	Presentation	HTTP
5	Session	80
4	Transport	Transmision Control Protocol (TCP)
3	Network	Internet Protocol (IP)
2	Data Link	Ethernet
1	Physical	CAT5



IP is the universal part

Some IP basics (1/2)

- **Usage : Internet, Intranet, Extranet**

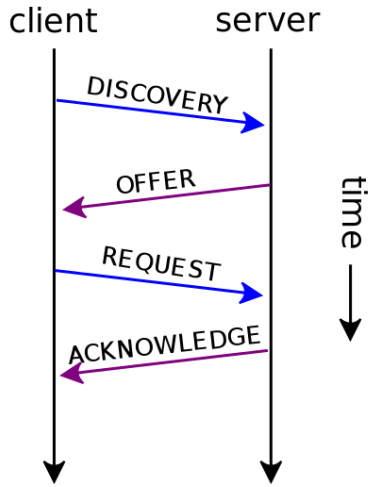
- **Single IP Address for every machine.**
  - Possiblity to add multiple adresses thanks to virtual interfaces (labels, dummy kernel module of linux)
  - Example: 192.168.0.1
- **A general rule of thumb: One interface has a unique address, assigned for a certain duration.**
  - The exceptions arise when you want services with failovers
- **IP Network Role :**
  - Information transfer

Some IP basics (2/2)

- **An IP address MUST be unique in a network**
  - The case when multiple hosts are provided with the same address is called “an address collision” or “a duplicate address”
- **RFC 2131 Dynamic Host Configuration Protocol (DHCP)**
  - Every IP stack (meaning every OS) is provided with an implementation of DHCP
  - A DHCP Server gives a lease for a network configuration to a host

DHCP options
53: 2 (DHCP Offer)
1 (subnet mask): 255.255.255.0
3 (Router): 192.168.1.1
51 (IP address lease time): 86400s (1 day)
54 (DHCP server): 192.168.1.1
6 (DNS servers): • 9.7.10.15, • 9.7.10.16, • 9.7.10.18

DHCP offer example



DHCP protocol classic exchange

IP Addresses

- **Allows addressing machine *interfaces* and communication between them.**
  - The IP address (v4 or v6) is for an interface and not a host.
- **255 possibilities for every byte (with some restrictions) → there are 4**

- **Some of them are private, RFC 1918**
  - These addresses allows communication in a private domain, without any risk of conflict with public addresses

    - 1 A Class :

      10.0.0.0 to 10.255.255.255

    - 16 B Classes :

      172.16.0.0 to 172.31.255.255

    - 255 C Classes :

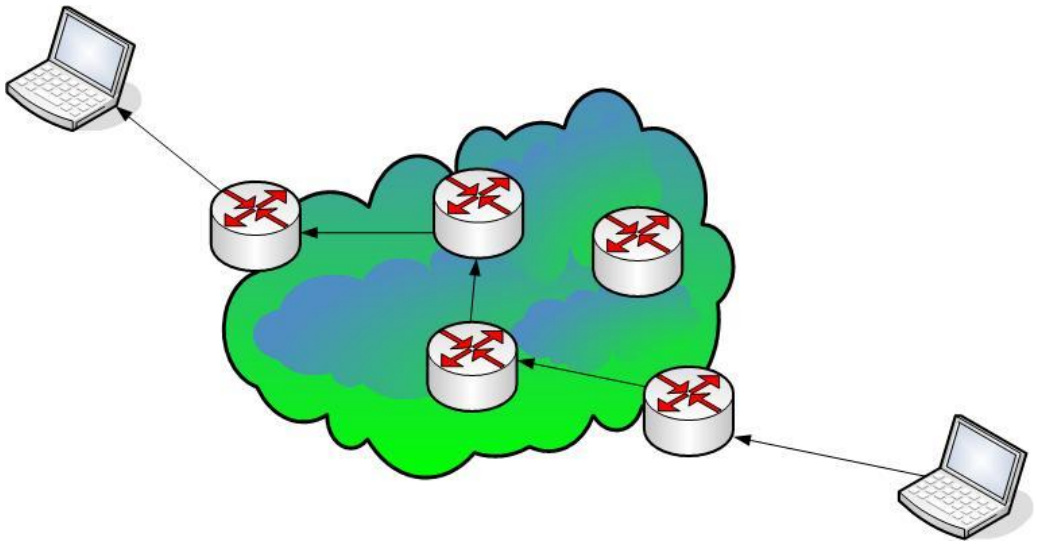
      192.168.0.0 to 192.168.255.255

Special IP Addresses (RFC 6890)

Address Block	Present Use	Reference
0.0.0.0/8	"This" Network	RFC 1122, Section 3.2.1.3
10.0.0.0/8	Private-Use Networks	RFC 1918
100.64.0.0/10	Shared Address Space	RFC 6598
127.0.0.0/8	Loopback	RFC 1122, Section 3.2.1.3
169.254.0.0/16	Link Local	RFC 3927
172.16.0.0/12	Private-Use Networks	RFC 1918
192.0.0.0/24	IETF Protocol Assignments	RFC 5736
192.0.2.0/24	TEST-NET-1	RFC 5737
192.88.99.0/24	6to4 Relay Anycast	RFC 3068
192.168.0.0/16	Private-Use Networks	RFC 1918
198.18.0.0/15	Network Interconnect Device Benchmark Testing	RFC 2544
198.51.100.0/24	TEST-NET-2	RFC 5737
203.0.113.0/24	TEST-NET-3	RFC 5737
224.0.0.0/4	Multicast	RFC 3171
240.0.0.0/4	Reserved for Future Use	RFC 1112, Section 4
255.255.255.255/32	Limited Broadcast	RFC 919, Section 7 RFC 922, Section 7

IP Principles

- **Principle : message exchanges (TCP, UDP, ICMP, etc) through Routers Networks**

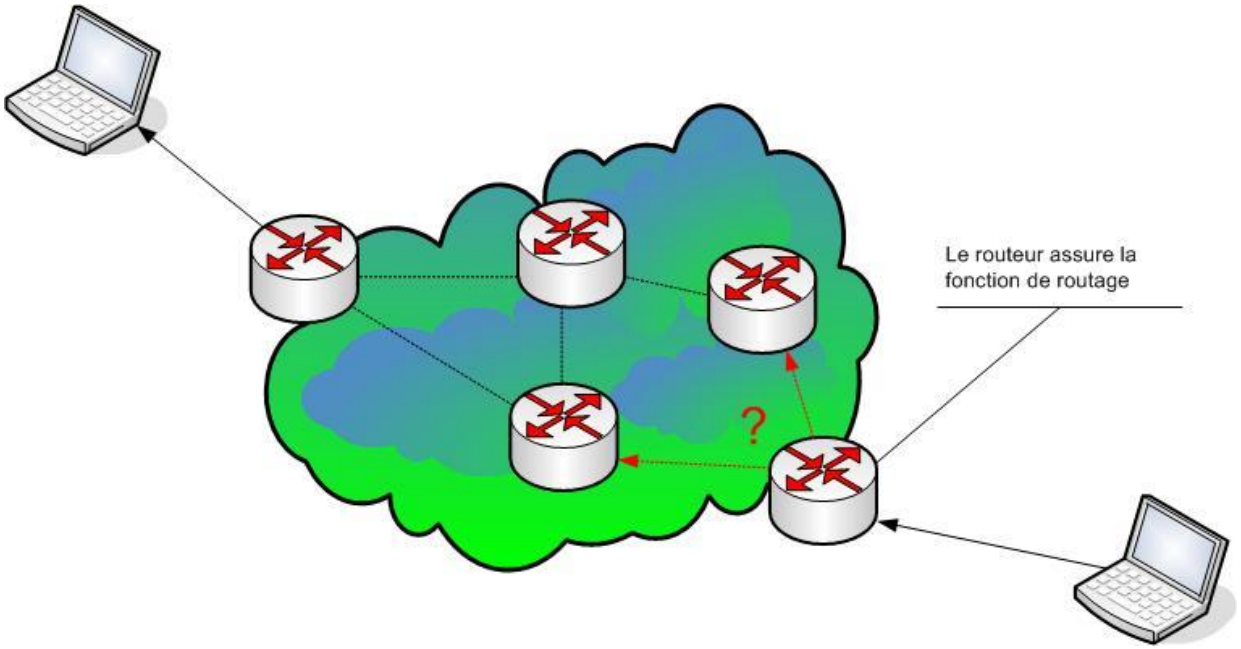


- **No result Guaranty: Best effort**
- **Jitter**
- **Every packet journey is determined by the Network: can change during the span of some seconds/minutes**

Tell me a story…

- What happens (protocols, messages exchanged, entities, programs) when I first connect my PC to a network ?
- What happens when I send a message to be routed somewhere ? (ping, traceroute, http)
- What are the networking tools/programs you would use to diagnose a non-responding website, local service, a database connection ?
- How do I build my own IPv6 address based on a prefix that I know ? Do I need to be connected to the Internet to have a globally-scoped address ?

Routing



- **Notion :**
  - Gateway
  - Routing: static, dynamic or default mode
- **Routing protocol:**
  - BGP, OSPF, EIGRP, RIP, etc

IP Packet

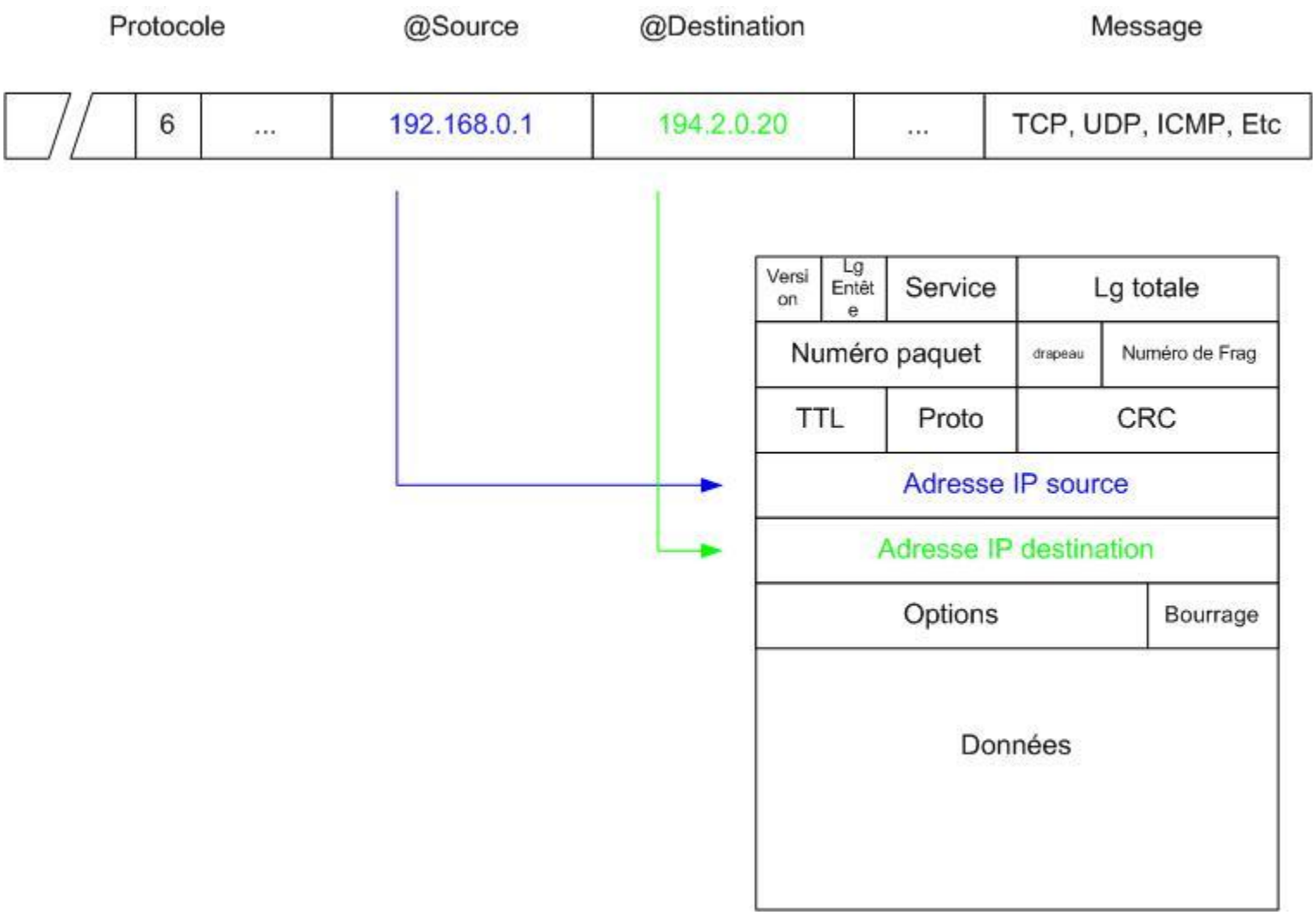
- **IP Packet length and size are variable**

- **All messages UDP, TCP, etc. are encapsulated into IP Packet**

IPv4 Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

IP Packet

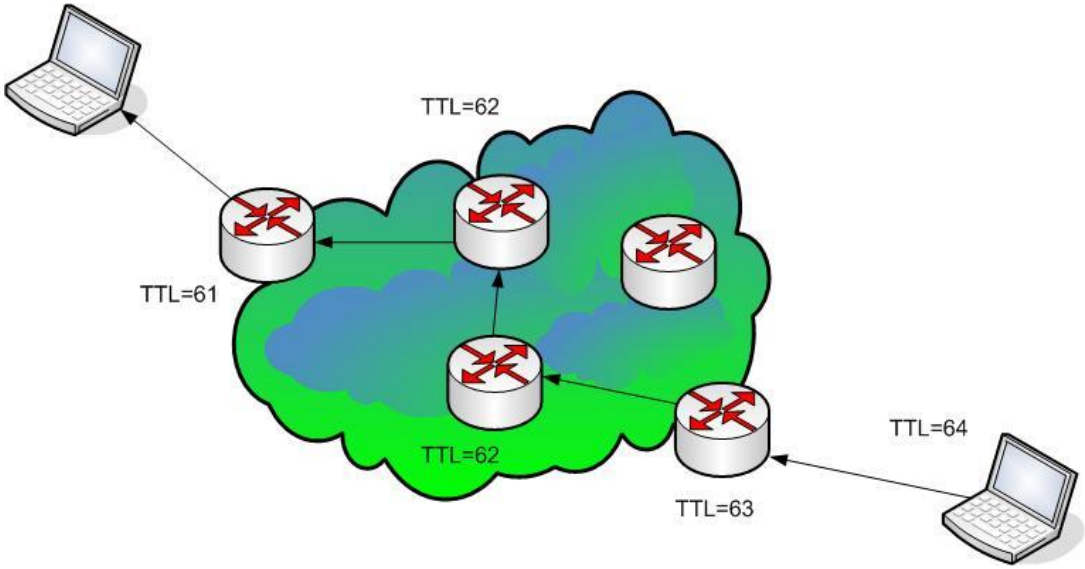

Protocole
@Source
@Destination
Message
6
...
192.168.0.1
194.2.0.20
...
TCP, UDP, ICMP, Etc
Version
Lg Entête
Service
Lg totale
Numéro paquet
drapeau
Numéro de Frag
TTL
Proto
CRC
Adresse IP source
Adresse IP destination
Options
Bourrage
Données

IP Headers

- Source Address ex: 192.168.0.1
- Destination Address ex: 194.2.0.20
- Protocol (TCP=6, UDP=17, ICMP=1)
- TTL
- Length
- Checksum
- Data (Message TCP, UDP or ICMP)
- Pour la fragmentation (DF, MF, Offset)
- Some well known protocol numbers:

Protocol Number	Protocol Name	Abbreviation
1	Internet Control Message Protocol	ICMP
2	Internet Group Management Protocol	IGMP
6	Transmission Control Protocol	TCP
17	User Datagram Protocol	UDP
41	IPv6 encapsulation	ENCAP
89	Open Shortest Path First	OSPF
132	Stream Control Transmission Protocol	SCTP

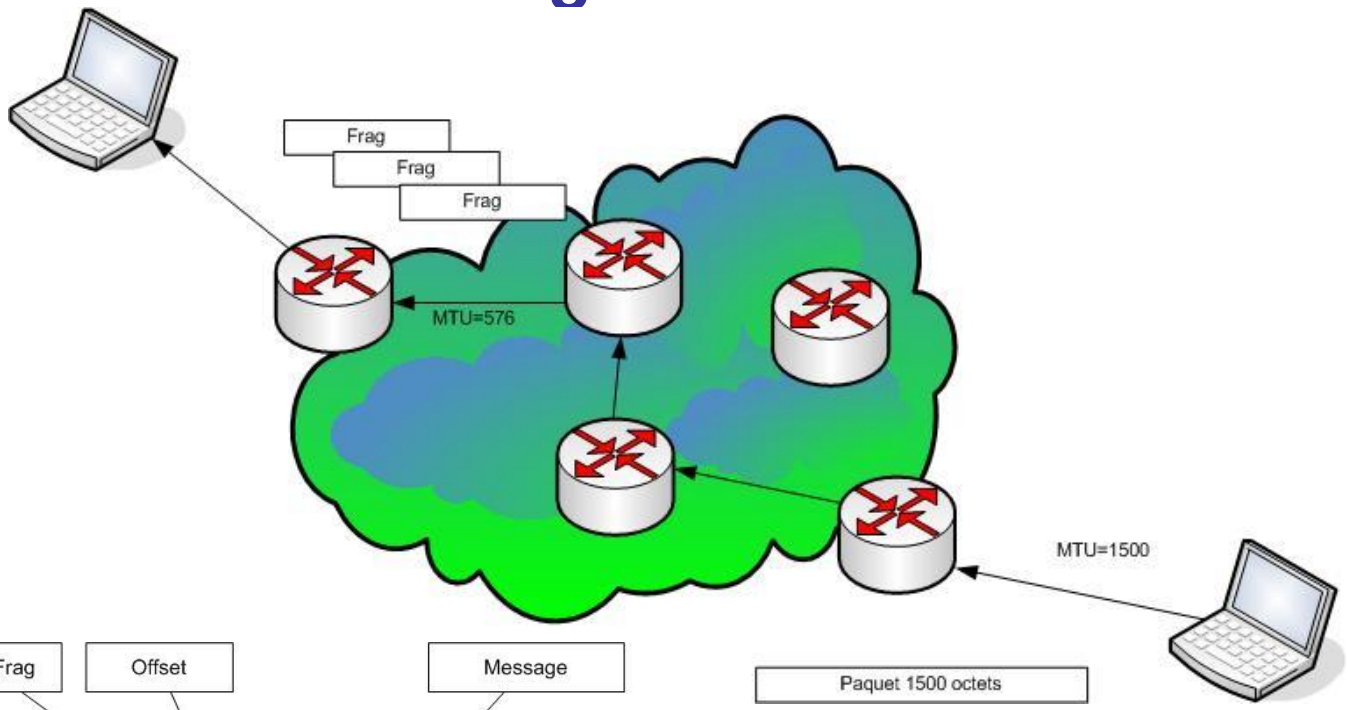
TTL

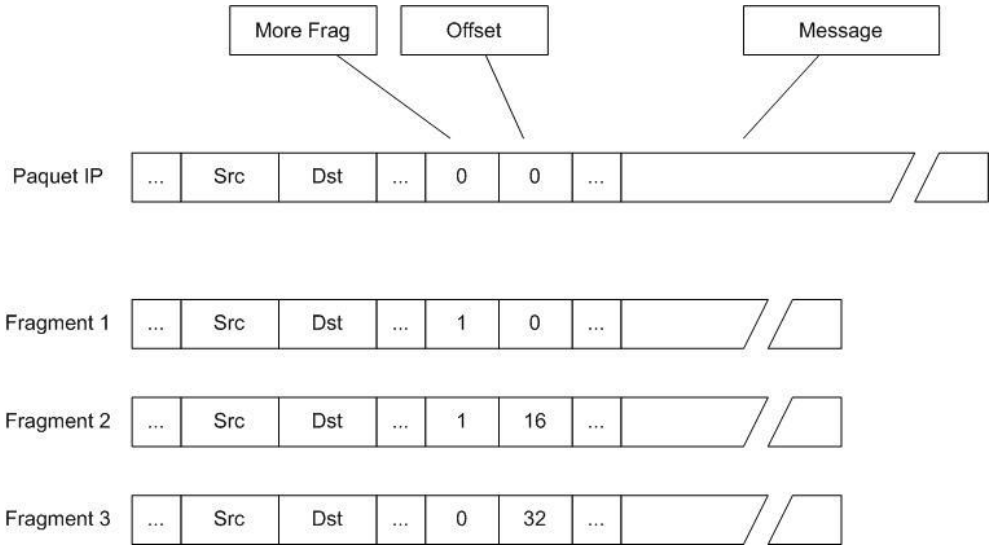


- **IP Packet Lifetime**
  - Hop number

```
U:\>ping 194.2.0.20

Envoi d'une requête 'ping' sur 194.2.0.20 avec 32 octets de données :

Réponse de 194.2.0.20 : octets=32 temps=64 ms TTL=55
Réponse de 194.2.0.20 : octets=32 temps=64 ms TTL=55
Réponse de 194.2.0.20 : octets=32 temps=64 ms TTL=55
Réponse de 194.2.0.20 : octets=32 temps=73 ms TTL=55

Statistiques Ping pour 194.2.0.20:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 64ms, Maximum = 73ms, Moyenne = 66ms
```

IP Fragmentation





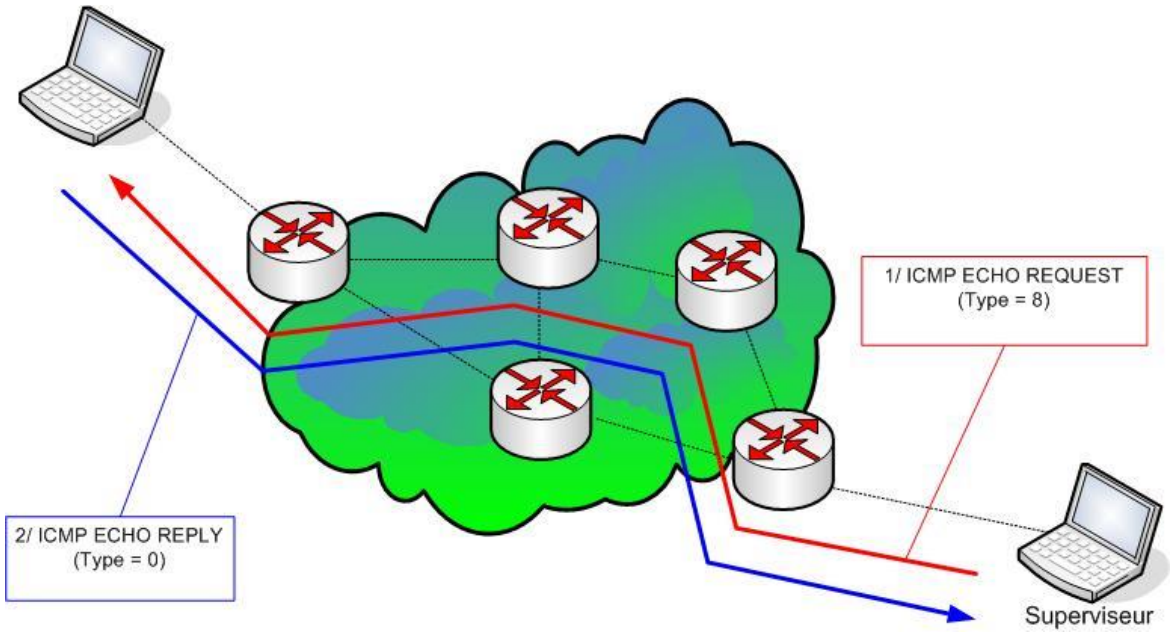
Tell me a story…

- What happens (protocols, messages exchanged, entities, programs) when I first connect my PC to a network ?
- What happens when I send a message to be routed somewhere ? (ping, traceroute, http)
- What are the networking tools/programs you would use to diagnose a non-responding website, local service, a database connection ?
- How do I build my own IPv6 address based on a prefix that I know ? Do I need to be connected to the Internet to have a globally-scoped address ?

ICMP – Internet Control Message Protocol

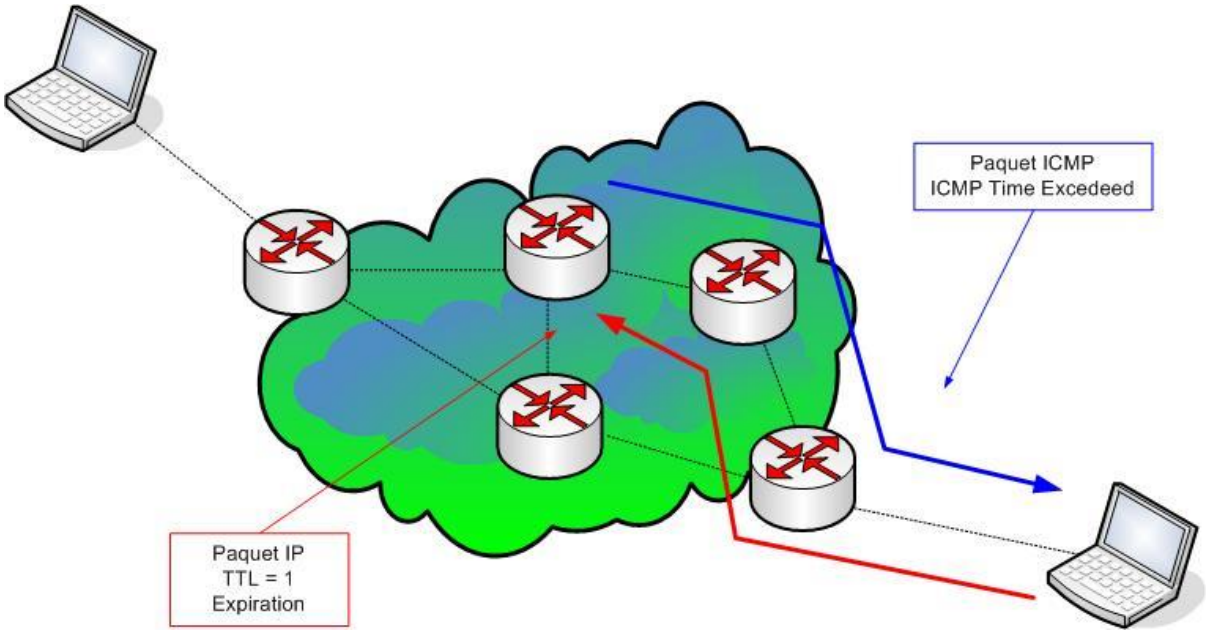
- **Used to carry error and control messages.**
- **Main service : « ping »**

- **Example : « ping » features**

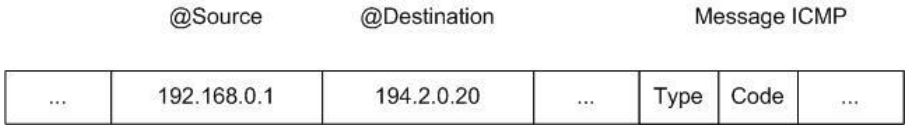


ICMP – Internet Control Message Protocol

- Not only to verify machine access.
- It allows retrieving relevant information : application port closed; network or machine unknown by router; TTL expiration, etc….
- Example TTL expiration :



ICMP – Internet Control Message Protocol



Exemples de valeurs du champ Type:

0 Réponse Echo

3 Destination non accessible

4 Contrôle de flux

5 Redirection 8 Echo

11 Durée de vie écoulée

12 Erreur de Paramètre

13 Marqueur temporelle

14 Réponse à marqueur temporel

15 Demande d'information

16 Réponse à demande d'information

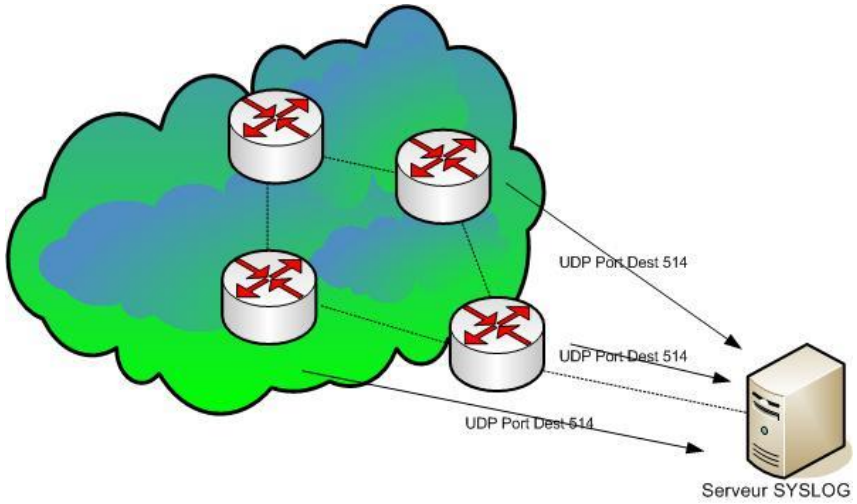
Type : 3
Code : 0 à 15
Message : destinataire inaccessible
Le code dépend de la cause du problème, respectivement :

- 0 : le réseau n'est pas accessible
- 1 : la machine n'est pas accessible
- 2 : le protocole n'est pas accessible
- 3 : le port n'est pas accessible
- 4 : fragmentation nécessaire mais impossible à cause du drapeau (*flag*) DF
- 5 : le routage a échoué
- 6 : réseau inconnu
- 7 : machine inconnue
- 8 : machine non connectée au réseau (inutilisé)
- 9 : communication avec le réseau interdite
- 10 : communication avec la machine interdite
- 11 : réseau inaccessible pour ce service
- 12 : machine inaccessible pour ce service
- 13 : communication interdite (filtrage)
- 14 : priorité d'hôte violé
- 15 : limite de priorité atteinte

UDP – User Datagram Protocol

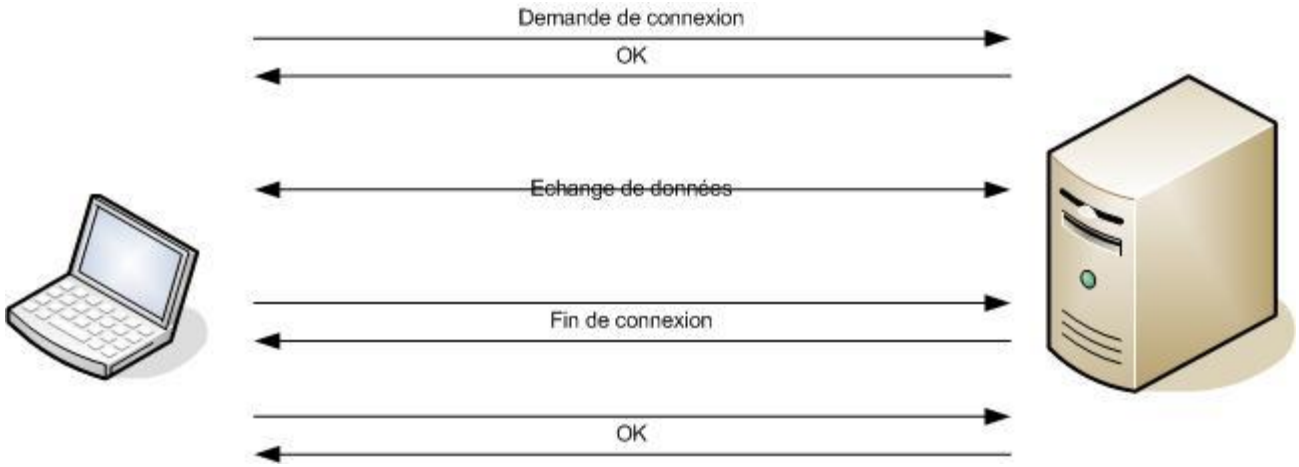
- Simple transmission between 2 IP machines.
- Non connected mode : no acknowledgment
- Unsecured transport mode (checksum from upper layers).
- BUT : very fast transmission

- Example UDP transmission (Syslog = events planning):



TCP – Transmission Control Protocol

- **Port notion (Source & destination)**
  - telnet 23/TCP, smtp 25/tcp, http 80/tcp, etc…..
- **Session Notion**
  - Retransmission of non-acknowledged packets
  - Unique Sequence number for every TCP Packet
  - Connection Establishment way
    - Flag Notion (SYN, ACK, FIN, RST, etc…)

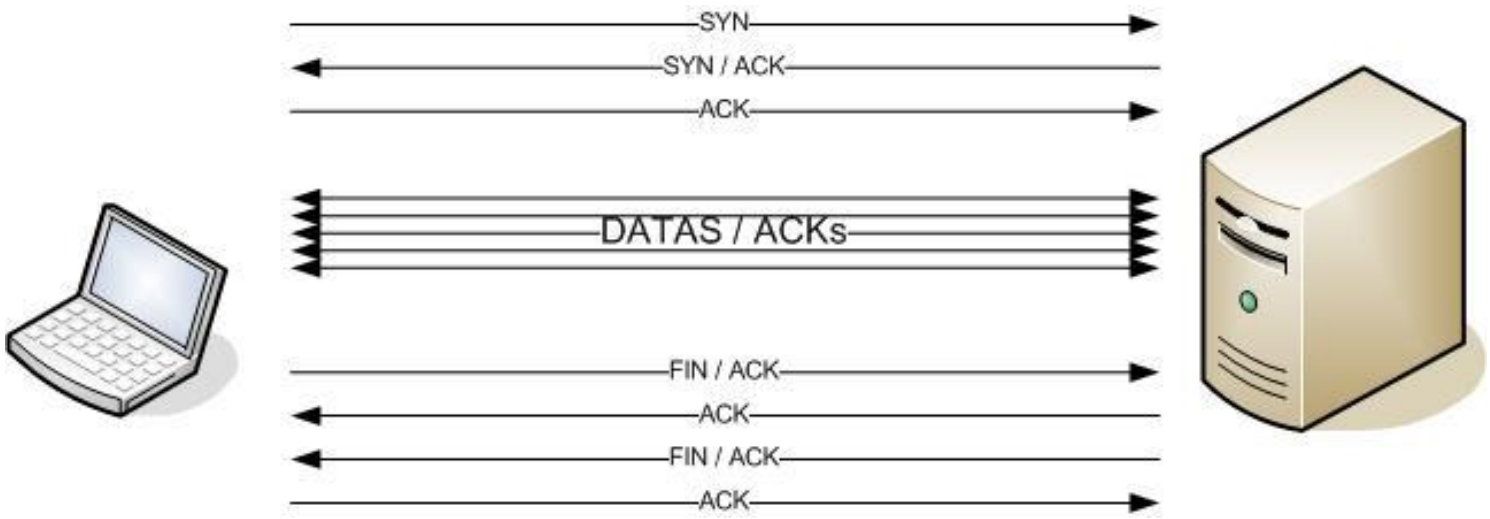


TCP – Transmission Control Protocol

- **Main TCP headers :**
  - Source Port
  - Destination Port
  - Sequence Number
  - Flags
    - SYN Establish connection
    - ACK Packet Acknowledgment
    - RST Reset session
    - FIN End Session
    - PSH Prevent temporary storage
    - URG Indicate emergency
  - Checksum (Integrity Control)
  - Data

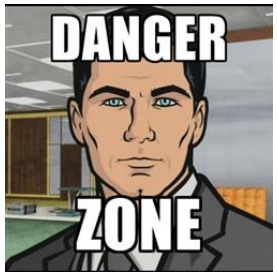
TCP – Transmission Control Protocol

- **TCP Session :**



The modern IT/Network engineer toolbox

- Know the content of /proc/sys/net and /sys/class/net, the structure and meaning of the files
  - An example experiment, cat 10 > /sys/class/net/eth1/mtu, and then do a "curl google.com", put the 1500 inside the mtu and see if it works
- Scapy*
- Wireshark, tshark, tcpdump**, packetbeat***
- nmap, etherape
- Curl (and its library libcurl, the origin story of everything worthy in the networking community)
  - Listen to: http://podcast.sysca.st/podcast/4-curl-libcurl-future-web-daniel-stenberg/
  - Read on: https://daniel.haxx.se/blog/



- Ettercap: Man in the middle attacks
- Medusa: network login with brute force
- Yersinia: known vulnerabilities in network protocols
- Anything here: https://tools.kali.org/tools-listing

*https://phaethon.github.io/scapy/api/usage.html
**https://www.wired.com/2012/05/van-jacobson/
***https://www.elastic.co/fr/products/beats/packetbeat

Applications internet

- **Application list used over the Internet**

Applications utilisant TCP		Applications utilisant UDP	
N° Port	Applications	N° Port	Applications
80 / 8080	Worl Wild Web (HTTP)	53	Domain Name Server (DNS)
443	HHTP over TSL/SSL (HTTPS)	113	Authentification Service
20 / 21	File Transfert Protocol (FTP)	123	Network Time Protocol (NTP)
23	Telnet	514	Syslog
119	Network News Transfert Protocol (NNTP)		
25	Simple Mail Transfert (SMTP		
110	Post Office Protocole V3 (POP3)		
66	Oracle SQL Net		
1352	Lotus Notes		

- **Link to TCP & UDP Ports**

DNS – Domain Name Server

- **Over Internet or Intranet, servers are often referenced by URL, and not their IP address, not easy to remember**
  - Easy to remember
  - More flexible : allows to change IP address, without any configuration of all users

- **From all over the world, any user shall retrieve the IP address of a server from its URL. This feature is called Domain Name Server (DNS)**

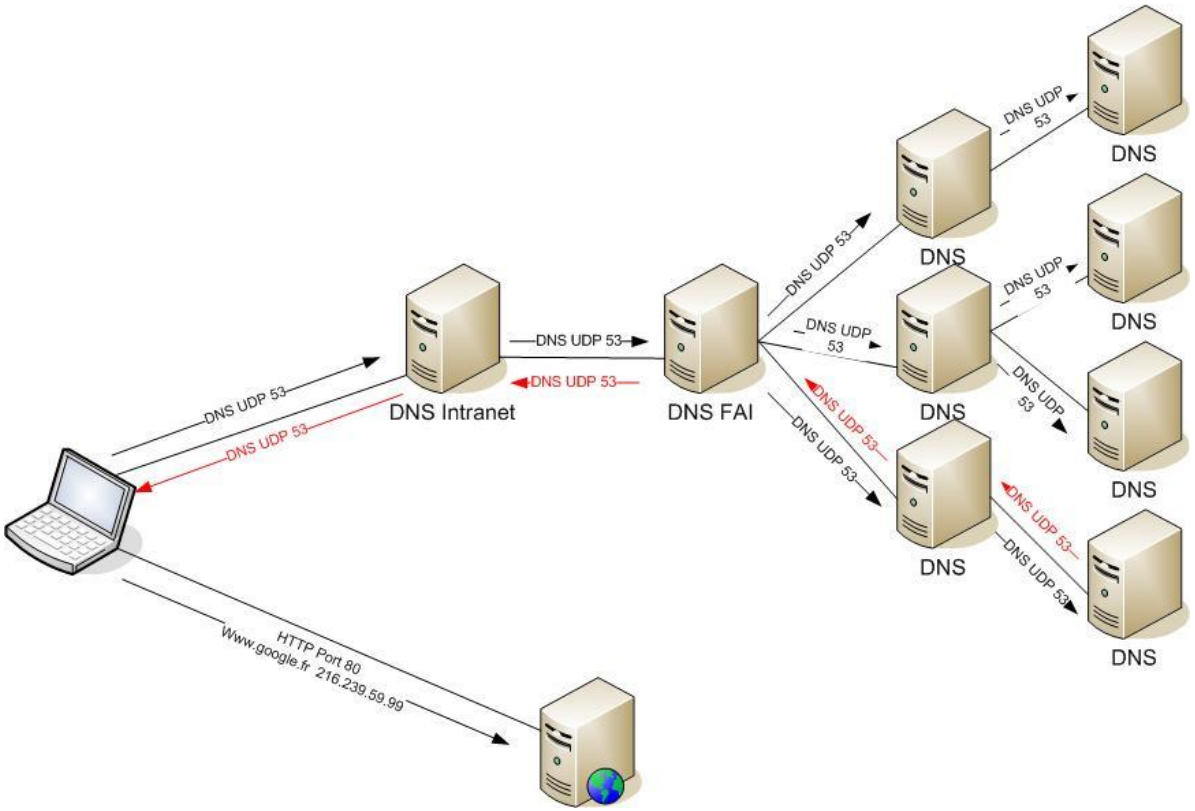
- **URL is composed of several hierarchical zones :**
  - Ex: www.google.fr
    - Zone **www** in zone **google** in zone **fr**

DNS – Domain Name Server

- **A Domain Name (DN) is an identifier registered in proprietary organization (Registrar) which makes sure it is unique**
- **To store an DN, user must describe on main DNS**
- **This description is :**
  - Domain Name = zone (ex: **google** under zone **fr**)
  - NS field = IP addresses DNS of parent zone
  - TTL field = Lifetime of domain information
  - MX field = reception server of sent messages to DN
  - For each under-zones of this domain, A field = server @ IP
    - Ex: www A 212.35.125.165 Web Server domain
- **DNS replicate registration of Domain Name, optimizing URL resolution delay. DNS knows a replicated Domain Name is called a secondary DNS.**

DNS – Domain Name Server

- **DNS resolution is performed with IP requests (UDP port 53). Request is forwarded from zone to zone, up to one DNS is answering.**



Tell me a story…

- What happens (protocols, messages exchanged, entities, programs) when I first connect my PC to a network ?
- What happens when I send a message to be routed somewhere ? (ping, traceroute, http)
- What are the networking tools/programs you would use to diagnose a non-responding website, local service, a database connection ?
- How do I build my own IPv6 address based on a prefix that I know ? Do I need to be connected to the Internet to have a globally-scoped address ?

NAT – Network Address Translation

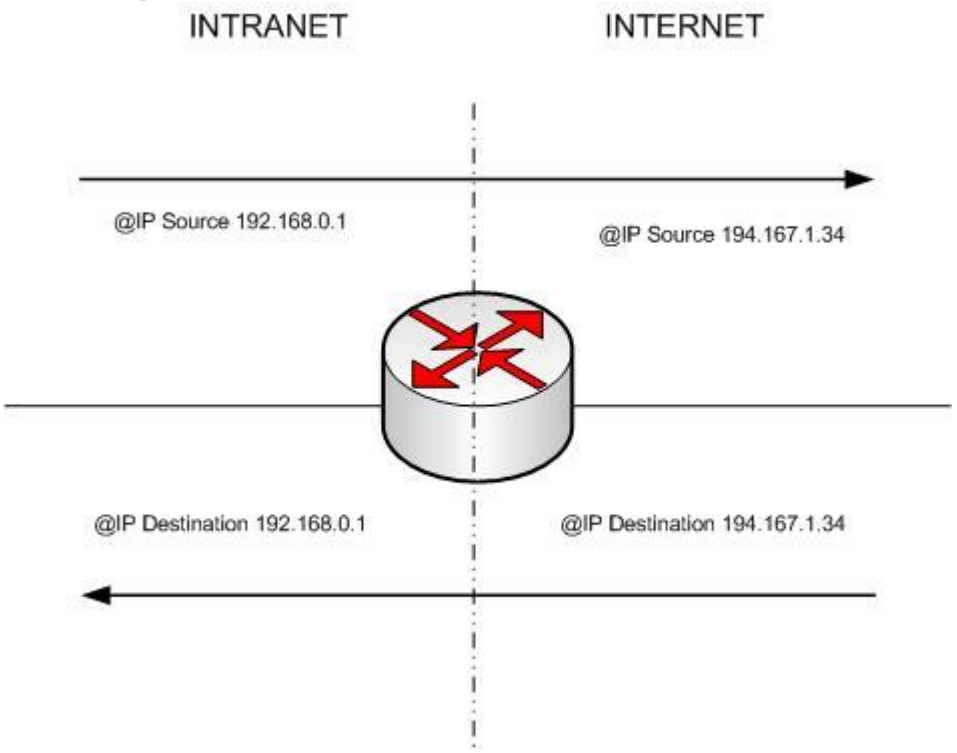
- **IP Address translation mechanism, used mainly to interconnect Internet to Intranet (public IP addresses to reserved private addresses).**

- **This feature can be implemented on the Internet access router, or on the Firewall.**

- **There are 3 address translation modes :**
  - Static NAT
  - Dynamic NAT : PAT
  - Port redirection

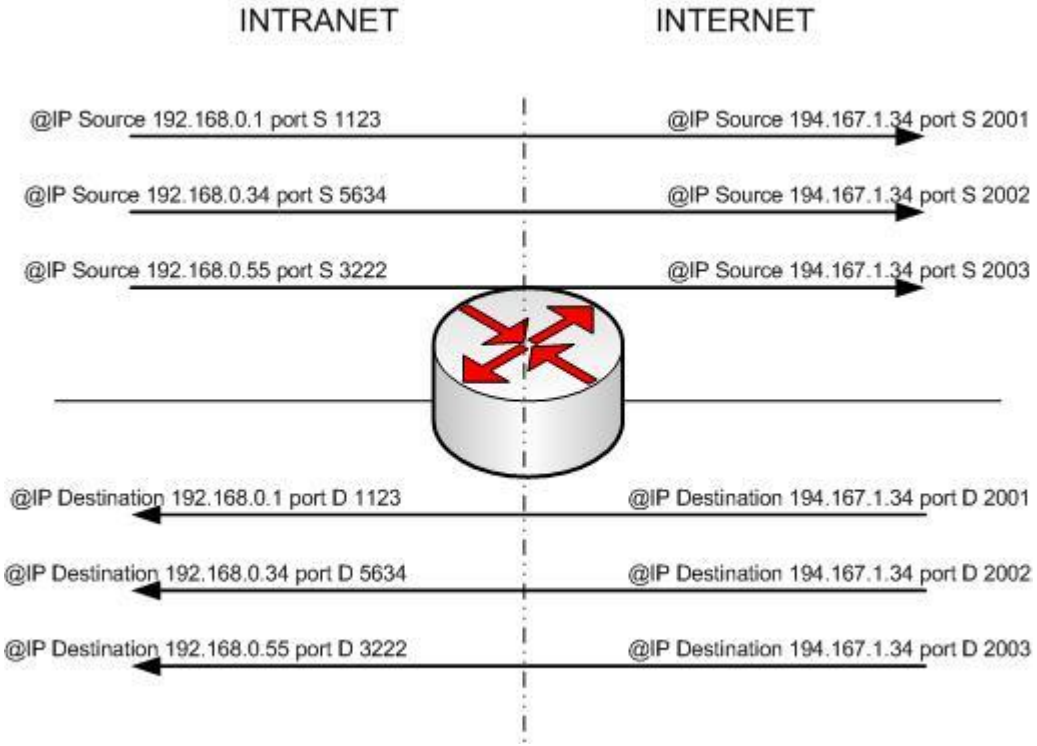
NAT – Static NAT

- **This feature allows private to public address correspondence.**
- **This feature is mainly used when administrator has enough public IP addresses to address private servers (SMTP, WEB, PROXY, etc…)**



NAT – Dynamic NAT

- This feature allows private to public address correspondence.
- This feature is mainly used to allow Internet access for worker of an enterprise. Source port is modified to isolate the flow and to redirect to the regular IP address.



Some IPv6 basics (1/2)

- **Usage : Internet, Intranet, Extranet**
- **First drafts in 1996, called ngIP back then**
- **Had a lot of difficulties to become the default version due to resistance, legacy, technical problems and lack of luck**
- **Multiple IPv6 addresses per interface!**
  - Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
  - Can be compressed to: 2001:db8:85a3::8a2e:370:7334
- **128 bits for one address. That's a lot!**
- **IPv6 address scopes :**
  - Local: ::1/128, fe80::/10. Associated with interfaces.
  - Unique Local addresses (ULA): fc00::/7 (globally scoped)
  - Globally scoped: e.g. 2001::/32, 2002::/16 (6to4)

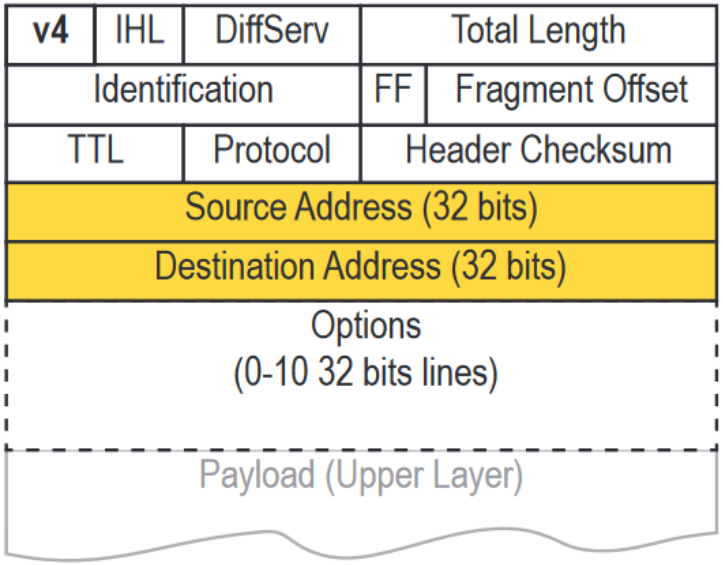
Some IPv6 basics (2/2)

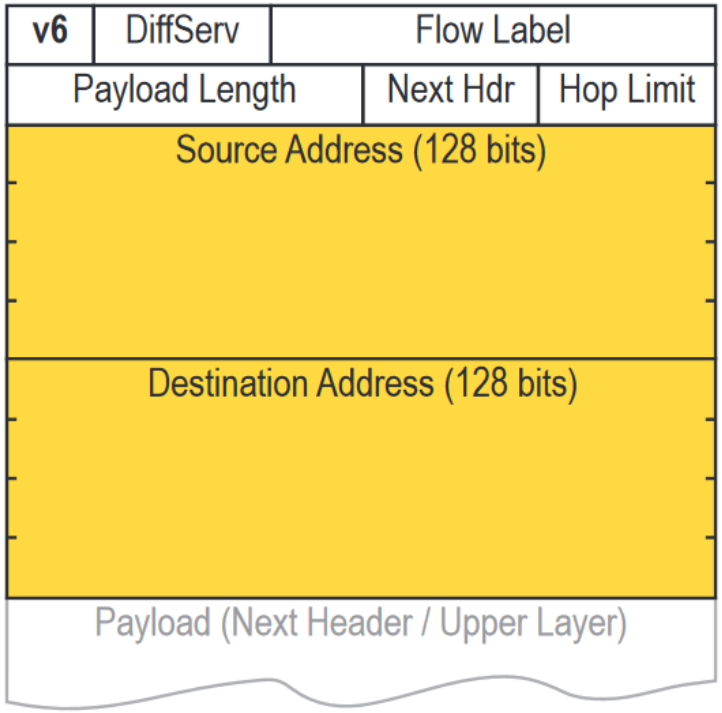
- **An IPv6 address MUST be unique in a network**
  - RFC 4861 Neighbor Discovery is the default IPv6 addressing protocol implemented in every stack
    - You need to "hear" a Router Advertisement with a Globally-scoped prefix
    - Create the Interface ID part using the MAC (deprectaed) or generating an random IID
    - Combine them and associate it to the interface
  - RFC 3315 Dynamic Host Configuration Protocol (DHCP) version 6
    - Not every IPv6 stack is provided with an implementation of DHCPv6

      At least at the beginning…
    - A DHCPv6 Server gives a lease for a network configuration to a host
    - Functions more or less the same as v4 DHCP, with some changes…

IPv6 Addresses

- **Allows addressing machine *interfaces* and communication between them.**
  - The IP address (v4 or v6) is for an interface and not a host.
- **16 bytes for an address**





Tell me a story…

- What happens (protocols, messages exchanged, entities, programs) when I first connect my PC to a network ?
- What happens when I send a message to be routed somewhere ? (ping, traceroute, http)
- What are the networking tools/programs you would use to diagnose a non-responding website, local service, a database connection ?
- How do I build my own IPv6 address based on a prefix that I know ? Do I need to be connected to the Internet to have a globally-scoped address ?