TD RNG 2

B.Stévant

En-tête des protocoles IP

istic IPv4 Header

0	-	-		-	-	۰.	
C	0	n	C	e	р	L	ь

F	а	C	0	n	
Δ	d	ld	200	se	5

Addresses

Protocol

IPv6 Header IPv6 Header IPv6 Extensions ICMPv6

Associated Protocols & Mechanisms

IPv6 & DNS

Integration

Programming IPv6 Applications

Ver.	IHL	DiffServ		Packet Length
	Iden	tifier	flag	Offset
Т	Checksum			
	_	Source	Address	
		Destinatio	n Address	
		Opt	ions	
	-	Lay	er 4	



istic IPv6 Header

Concepts					
Facts on Addresses	0	7	15	23	31
Addresses					
Protocol	6	DiffServ		Flow Label	
IPv6 Header IPv6 Header		Payload Length	_	Next header	Hop Limit
IPv6 Extensions ICMPv6					
Associated Protocols & Mechanisms			Source	Address	
IPv6 & DNS					
Integration			Destinatio	on Address	
Programming IPv6					
Applications			Layer 4 or	extensions	

Adresses IPv6

istic Addressing Space Utilization

Concepts

Facts on	
Addresses	0000::/8 Reserved by IETF [RFC4291]
Addresses	0100::/8 Reserved by IETF [RFC4291]
Addresses	0200::/7 Reserved by IETF [RFC4048]
Notation	0400::/6 Reserved by IETF [RFC4291]
	0800::/5 Reserved by IETF [RFC4291]
Addressing scheme	1000::/4 Reserved by IETF [RFC4291]
Address Format	2000::/3 Global Unicast [RFC4291]
Kind of addresses	4000::/3 Reserved by IETF [RFC4291]
	6000::/3 Reserved by IETF [RFC4291]
Protocol	8000::/3 Reserved by IETF [RFC4291]
Associated	a000::/3 Reserved by IETF [RFC4291]
Protocols &	c000::/3 Reserved by IETF [RFC4291]
Mechanisms	e000::/4 Reserved by IETF [RFC4291]
wiechanisms	f000::/5 Reserved by IETF [RFC4291]
IPv6 & DNS	F800::/6 Reserved by IETF [RFC4291]
II VO & DIVO	fc00::/7 Unique Local Unicast [RFC4193]
Integration	fe00::/9 Reserved by IETF [RFC4291]
-	fe80::/10 Link Local Unicast [RFC4291]
Programming	fec0::/10 Reserved by IETF [RFC3879]
IPv6	ff00::/8 Multicast [RFC4291]
Applications	

Whttp://www.iana.org/assignments/ipv6-address-space





fe80

C	\sim	n	~	0	n.	Fc.
~			~	C		LS

Facts on Addresses

Addresses

Notation Addressing scheme

Address Format Kind of addresses

Protocol

Associated Protocols & Mechanisms

IPv6 & DNS

Integration

Programming IPv6 Applications

Global Unicast Address:

3	45	16	64
001	Global Prefix	SID	Interface ID
	public topology given by the provider assign	local topology ed by network er	link address ngineer auto or manual configuration
Link-	Local Address:		
10	54		64

link address auto-configuration

Interface ID



0...0

istic Other kind of addresses : ULA (RFC 4193)

Concepts

Facts on Addresses

Addresses

Notation Addressing scheme Address Format Kind of addresses

Protocol

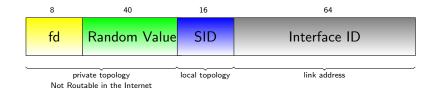
Associated Protocols & Mechanisms

IPv6 & DNS

Integration

Programming IPv6 Applications

- Equivalent to the private addresses in IPv4
- But try to avoid same prefixes on two different sites:
 - avoid renumbering if two company merge
 - avoid ambiguities when VPN are used
- These prefixes are not routable on the Internet
- Unique Local IPv6 Unicast Addresses:



 $W_{http://www.sixxs.net/tools/grh/ula/}$ to create your own ULA prefix.

(cc) BY-SA

©G6 Association

November 8, 2013

47 / 155

Auto-configuration

Concepts

Facts on Addresses

Addresses

Protocol

Associated Protocols & Mechanisms

Neighbor Discovery

Path MTU discovery DHCPv6 DHCPv6 Stateless Configuration DHCPv6 Statefu Configuration Stateless vs Stateful

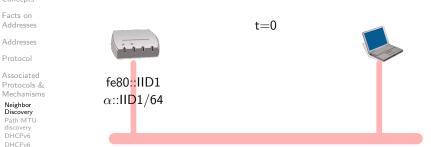
IPv6 & DNS

Integration

Programming IPv6 Applications



CC BY-SA

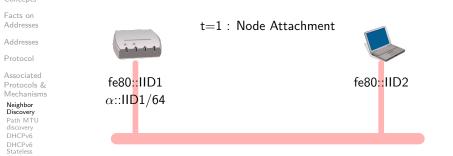


DHCPv6 Stateless Configuration DHCPv6 Stateful Configuration Stateless vs Stateful

IPv6 & DNS

Integration

Programming IPv6 Applications Time t=0: Router is configured with a link-local address and manually configured with a global address (α ::/64 is given by the network administrator)



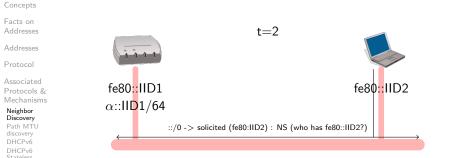
Host constructs its link-local address based on the interface MAC address

Applications

DHCPv6 Stateful Configuration Stateless vs

IPv6 & DNS

Integration Programming IPv6



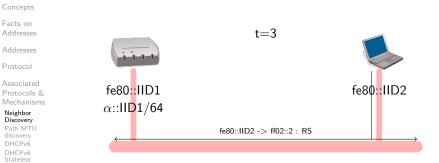
Host does a DAD (i.e. sends a Neighbor Solicitation to query resolution of its own address (tentative): no answers means no other host has this value).

DHCPv6 Stateful

Stateless vs

IPv6 & DNS

Integration Programming



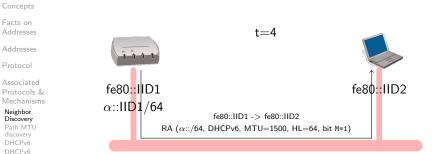
Host sends a Router Solicitation to the Link-Local All-Routers Multicast group using the newly link-local configured address

DHCPv6 Stateful

Stateless vs

IPv6 & DNS

Integration Programming IPv6



Router directly answers the host using Link-local addresses. The answer may contain a/several prefix(es). Router can also mandate hosts to use DHCPv6 to obtain prefixes (statefull auto-configuration) and/or other parameters (DNS servers...): Bit M = 1.

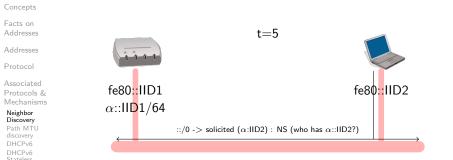
DHCPv6 Stateful

Stateless vs

IPv6 & DNS

Integration

Programming IPv6



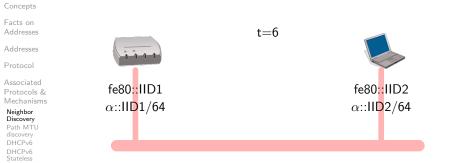
Host does a DAD (i.e. sends a Neighbor Solicitation to query resolution of its own global address: no answers means no other host as this value).

DHCPv6 Stateful

Stateless vs

IPv6 & DNS

Integration Programming IPv6



Host sets the global address and takes answering router as the default router.

DHCPv6 Stateful Configuration Stateless vs

IPv6 & DNS

Integration Programming IPv6

istic Address Lifetime

Concepts				
Facts on Addresses				
Addresses				
Protocol				
Associated Protocols & Mechanisms Neighbor Discovery Path MTU	allocation			
discovery				
DHCPv6 DHCPv6 Stateless Configuration	Tentative	Preferred	Deprecated	Invalid
DHCPv6 Stateless	Tentative → DAD ← →	Preferred Valid	Deprecated	Invalid
DHCPv6 Stateless Configuration DHCPv6 Stateful Configuration Stateless vs			Deprecated	Invalid
DHCPv6 Stateless Configuration DHCPv6 Stateful Configuration Stateless vs Stateful			Deprecated	Invalid

(cc) BY-SA

Sécurité



Security issues with Neighbor Discovery

Concepts

- Facts on Addresses
- Addresses
- Protocol
- Associated Protocols & Mechanisms

IPv6 & DNS

Security

Neighbor Discovery Security Firewalls

Integration

Conclusion

From an attacker point of view, IPv6 attacks are:

- **Difficult** from remote network:
 - Scanning IPv6 network is hard (2⁶⁴ addresses)
 - May use random IID instead of MAC-based IID (if needed)
 - No broadcast address
 - Remote attacks would mainly target hosts exposed through the DNS
- Easy from local network:
 - Neighbor Discovery is basically not secured (see SEND later)
 - Attacks inspired by ARP flaws + new attacks
 - Implementations not (yet) heavily tested

Attacker toolkits already available !

See http://www.thc.org/thc-ipv6/





Facts on Addresses

Addresses

Protocol

Associated Protocols & Mechanism

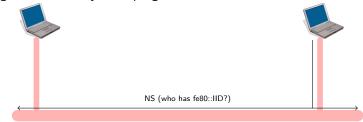
IPv6 & DNS

Security

Neighbor Discovery Security Firewalls

Conclusion

Neighbor Discovery Snooping



Host uses Neighbor Discovery notably in these two cases:

- To get the link-layer information (typically the MAC address) of another host (ARP-like)
- To verify address uniqueness (DAD)



Concepts

Facts on Addresses

Addresses

Protocol

Associated Protocols & Mechanism

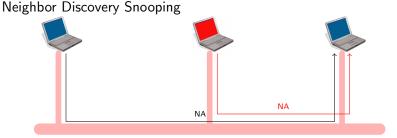
IPv6 & DNS

Security

Neighbor Discovery Security Firewalls

Integration

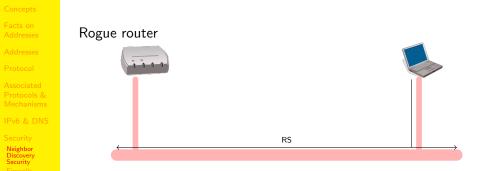
Conclusion



An attacker on the LAN can perform an attack by responding to ND messages

- ARP-like: Claim to be a given host on the LAN => Man in the Middle
- DAD: Claim to have any address asked for on the LAN => Deny of Service





Integration

Conclusion.

Host uses the Router Solicitation to get the address of the exit router and the prefix used on the LAN.



Concepts

Facts on Addresses

Addresses

Protocol

Associated Protocols & Mechanism

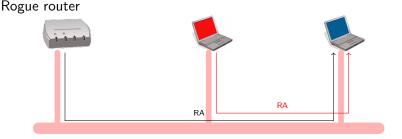
IPv6 & DNS

Security

Neighbor Discovery Security Firewalls

Integration

Conclusion



An attacker on the LAN can perform an attack by responding to RS messages

- Claim to be the exit router => Man in the Middle
- Claim to route another prefix on the LAN => Deny of Service



Example: Interface during an IETF meeting

- Facts on Addresses
- Addresses
- Protocol
- Associated Protocols & Mechanism
- IPv6 & DNS
- Security
- Neighbor Discovery Security Firewalls
- Integration
- Conclusion

en3: flags=8863:UP, BROADCAST, SMART, RUNNING, SIMPLEX, MULTICAST> mtu 1500 inet6 fe80::223:6cff:fe97:679c%en3 prefixlen 64 acopeid 0x6 inet6 2002:8281:1c8c:d:223:6cff:fe97:679c prefixlen 64 autoconf inet6 2002:c15f:2011:d:223:6cff:fe97:679c prefixlen 64 autoconf inet6 fec0::d:223:6cff:fe97:679c prefixlen 64 autoconf inet6 2001:df8::24:223:6cff:fe97:679c prefixlen 64 autoconf inet6 2001:df8::24:223:6cff:fe97:679c prefixlen 64 autoconf inet6 2002:8281:1ccb:9:223:6cff:fe97:679c prefixlen 64 autoconf inet6 fec0:9:223:6cff:fe97:679c prefixlen 64 autoconf inet6 fec0:9:223:6cff:fe97:679c prefixlen 64 autoconf ether 00:23:6c:97:67:9c media: autoselect status: active supported media: autoselect



Solutions to mitigate or prevent attacks?

Concepts

Facts on Addresses

Addresses

Protocol

Associated Protocols & Mechanisms

IPv6 & DNS

Security

Neighbor Discovery Security Firewalls

Conclusion

Prevention of attacks:

- SEND (Secure Neighbor Discovery)
 - IETF proposed solution: RFC 3971 (note: too complex to deploy for an average site!)
 - Use signed ND messages, with a trust relationship
- Level-2 Filtering
 - Filter ND on switch port (ex. only one port allowed to send RA)
 - A few switch still implements it ... (Cisco ?)

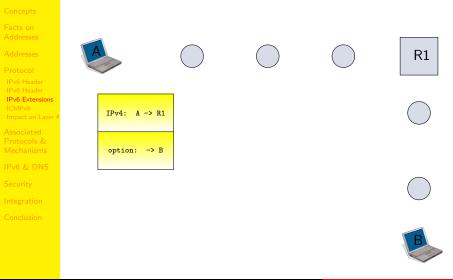
Detection of attacks: ndpmon

- Similar to ARP-watch
- Detect Snooping and Denial of Services
- http://ndpmon.sf.net

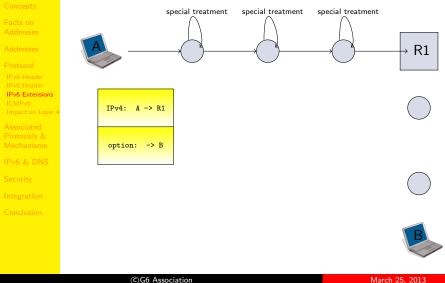
Routage par la source

 Utilise l'extension d'en-tête « Routing » de type 0, contenant tous les points à traverser avant d'arriver à la destination













Addresses

Addresses

Protocol IPv6 Header IPv6 Header IPv6 Extensions ICMPv6 Impact on Laver 4

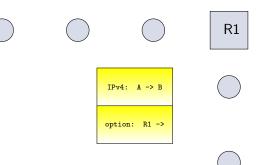
Associated Protocols & Mechanisms

IPv6 & DNS

Security

Integration

Conclusion









Facts on Addresses

Addresses

Protocol IPv6 Header IPv6 Header IPv6 Extensions ICMPv6 Impact on Layer

Associated Protocols & Mechanisms

IPv6 & DNS

Security

Integration

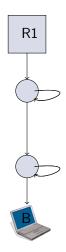
Conclusion



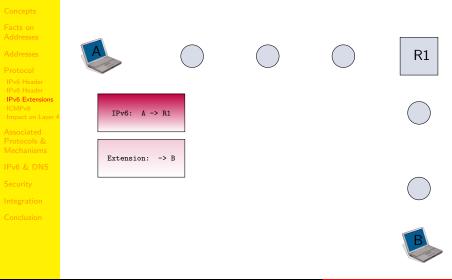
 \bigcirc

(

IPv4: A -> B
option: R1 ->





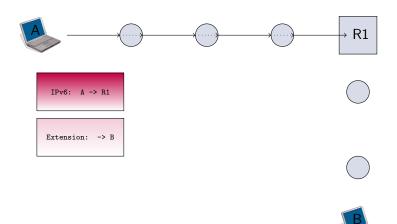






Facts on Addresses

- Addresses
- Protocol
- IPv6 Header IPv6 Header IPv6 Extensions ICMPv6
- Impact on Layer
- Associated Protocols & Mechanisms
- IPv6 & DNS
- Security
- Integration
- Conclusion





Concepts

Facts on Addresses

Addresses

Protocol IPv6 Header IPv6 Header **IPv6 Extensions** ICMPv6 Impact on Laver 4

Associated Protocols & Mechanisms

IPv6 & DNS

Security

Integration

Conclusion

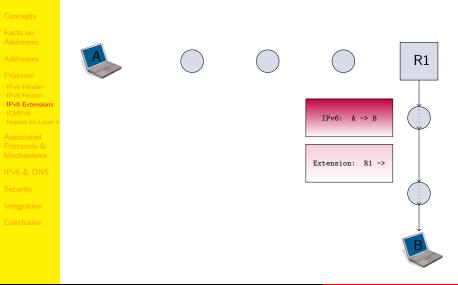


R1 is the destination, packet is sent to Routing Extension layer which swaps the addresses and forwards the packet.



R1

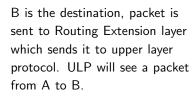


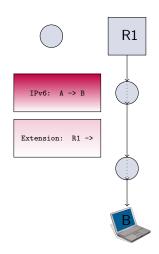




- Concepts
- Facts on Addresses
- Addresses
- Protocol IPv6 Header IPv6 Header IPv6 Extensions ICMPv6 Impact on Layer 4
- Associated Protocols & Mechanisms
- IPv6 & DNS
- Security
- Integration
- Conclusion







Routage par la source

- Problèmes de sécurité :
 - Contournement de règles de pare-feu
 L'extension de routage peut contenir une adresse
 qui n'est pas dans le même plan de sécurité que
 l'adresse de destination du paquet
 - Amplification d'attaque, type DoS
 L'extension de routage peut spécifier des allerretour entre 2 nœuds, surchargeant les liens

Voir http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf