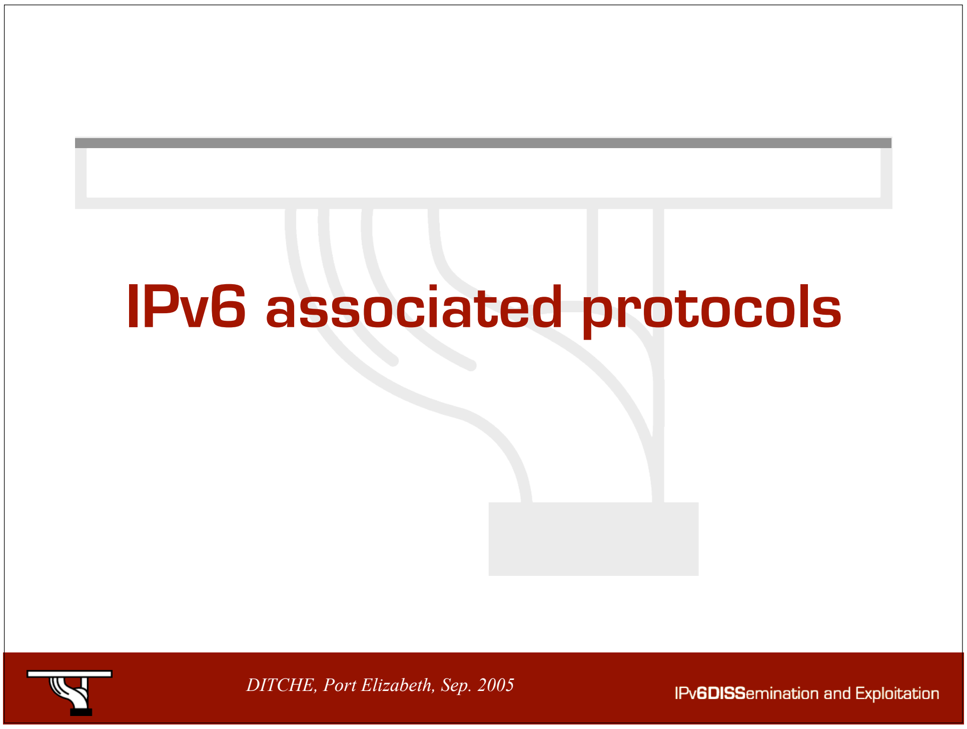
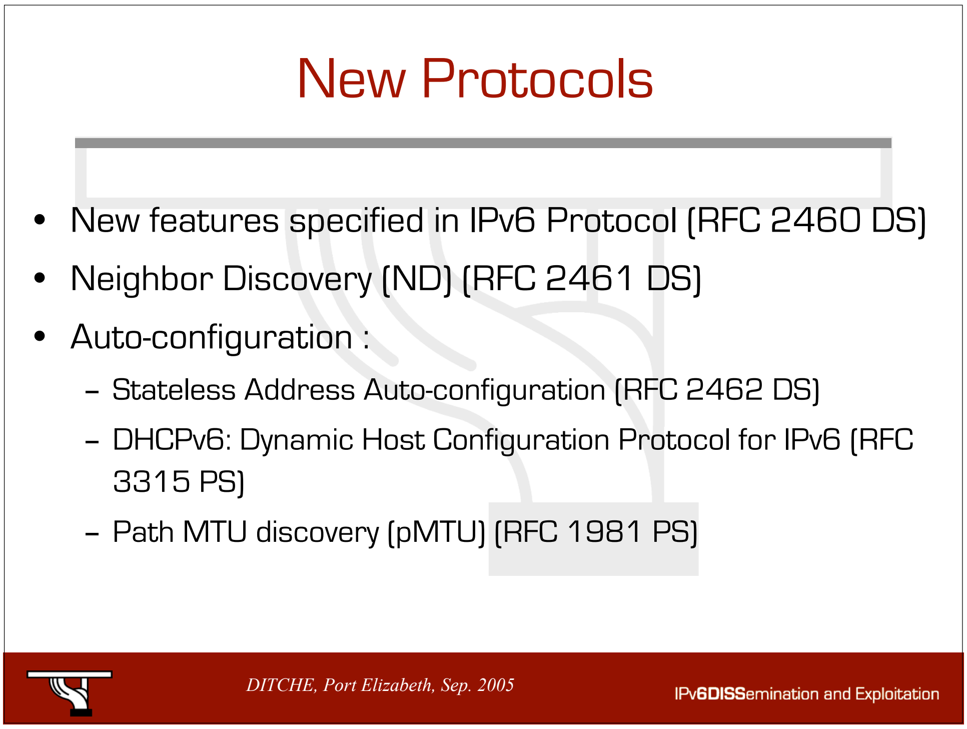
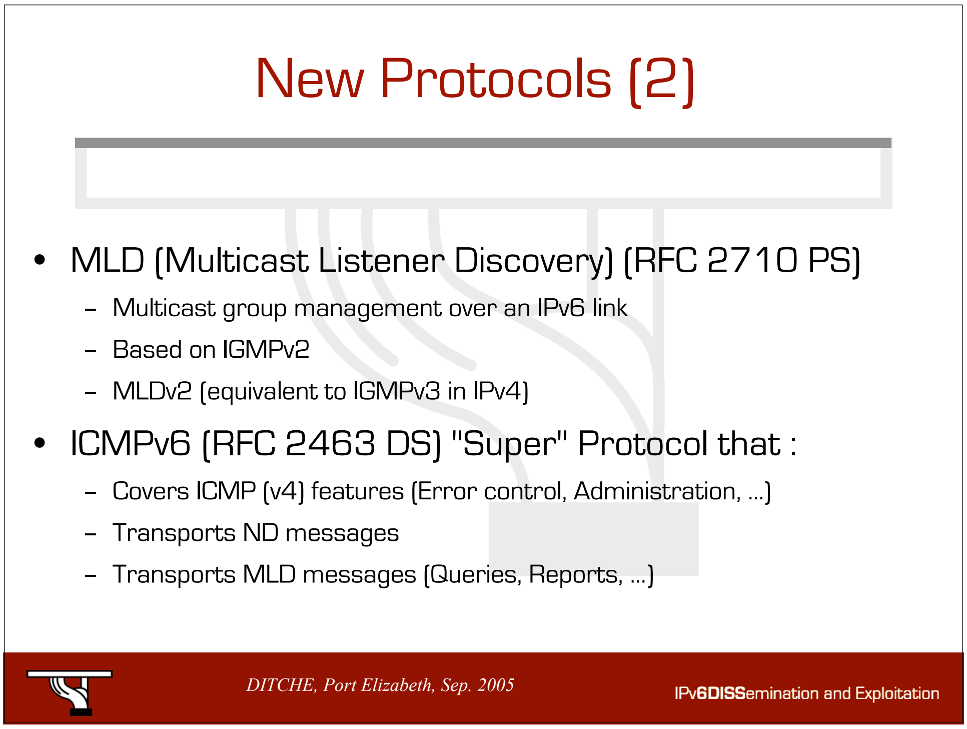


IPv6 associated protocols



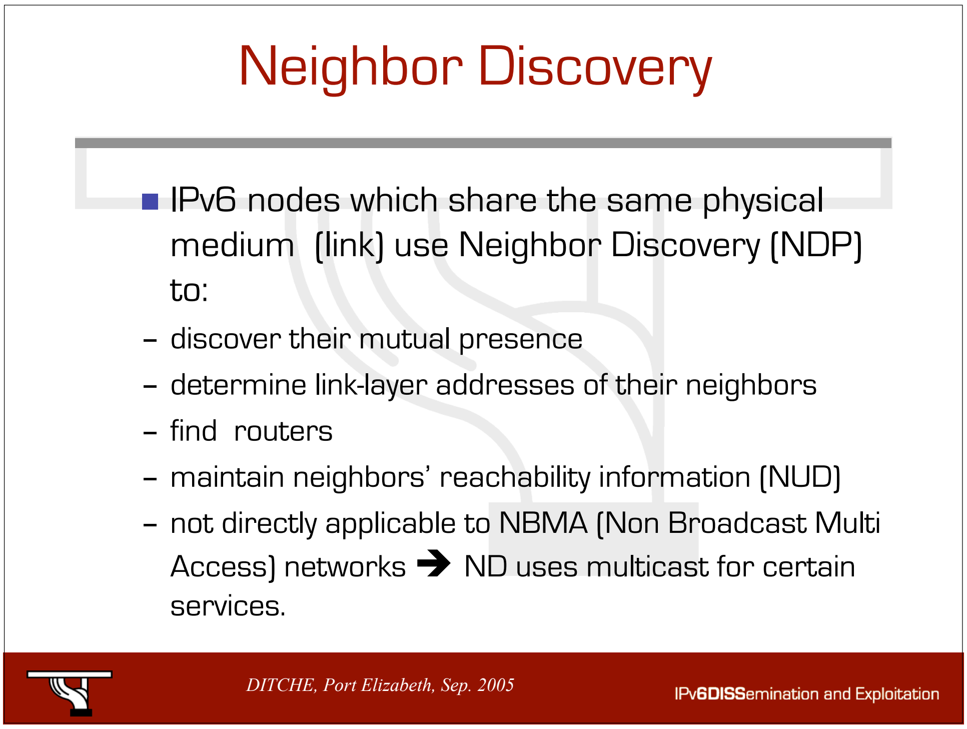
New Protocols

- New features specified in IPv6 Protocol (RFC 2460 DS)
- Neighbor Discovery (ND) (RFC 2461 DS)
- Auto-configuration :
  - Stateless Address Auto-configuration (RFC 2462 DS)
  - DHCPv6: Dynamic Host Configuration Protocol for IPv6 (RFC 3315 PS)
  - Path MTU discovery (pMTU) (RFC 1981 PS)



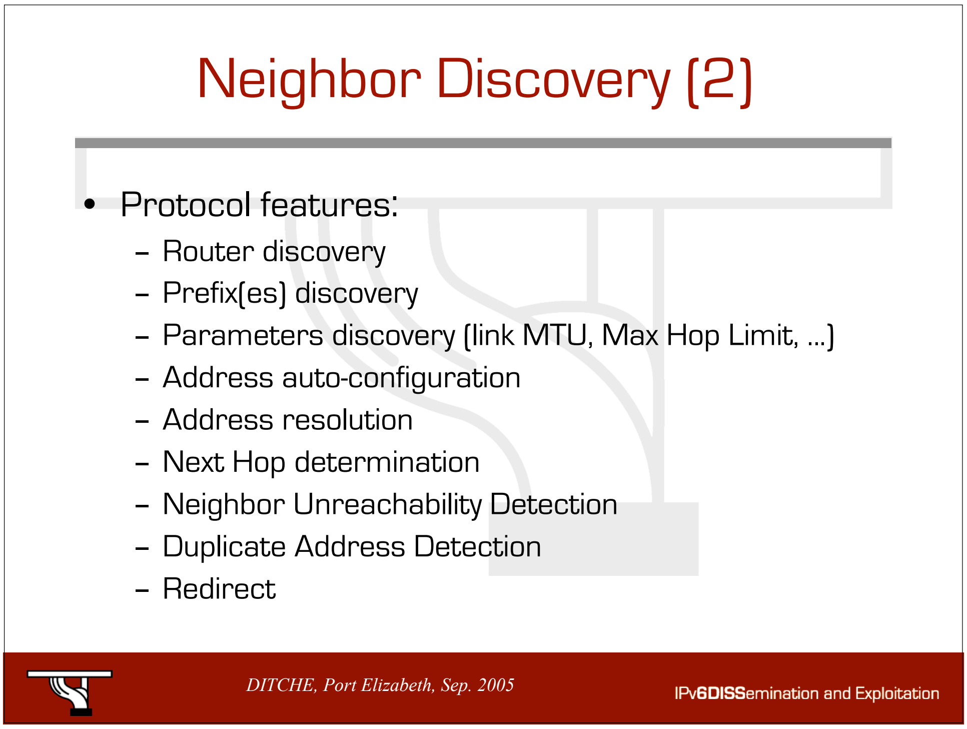
New Protocols (2)

- MLD (Multicast Listener Discovery) (RFC 2710 PS)
  - Multicast group management over an IPv6 link
  - Based on IGMPv2
  - MLDv2 (equivalent to IGMPv3 in IPv4)
- ICMPv6 (RFC 2463 DS) "Super" Protocol that :
  - Covers ICMP (v4) features (Error control, Administration, …)
  - Transports ND messages
  - Transports MLD messages (Queries, Reports, …)



Neighbor Discovery

- IPv6 nodes which share the same physical medium (link) use Neighbor Discovery (NDP) to:
  - discover their mutual presence
  - determine link-layer addresses of their neighbors
  - find routers
  - maintain neighbors' reachability information (NUD)
  - not directly applicable to NBMA (Non Broadcast Multi Access) networks ➔ ND uses multicast for certain services.

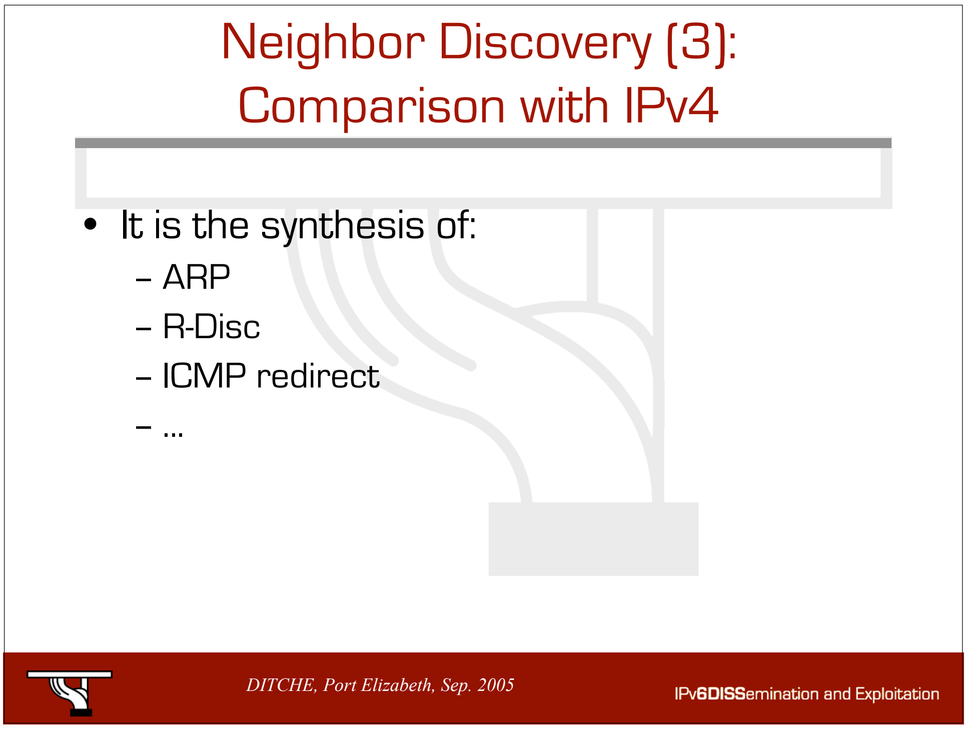


Neighbor Discovery (2)

- Protocol features:
  - Router discovery
  - Prefix(es) discovery
  - Parameters discovery (link MTU, Max Hop Limit, ...)
  - Address auto-configuration
  - Address resolution
  - Next Hop determination
  - Neighbor Unreachability Detection
  - Duplicate Address Detection
  - Redirect

DITCHE, Port Elizabeth, Sep. 2005

IPv6**DISS**emination and Exploitation

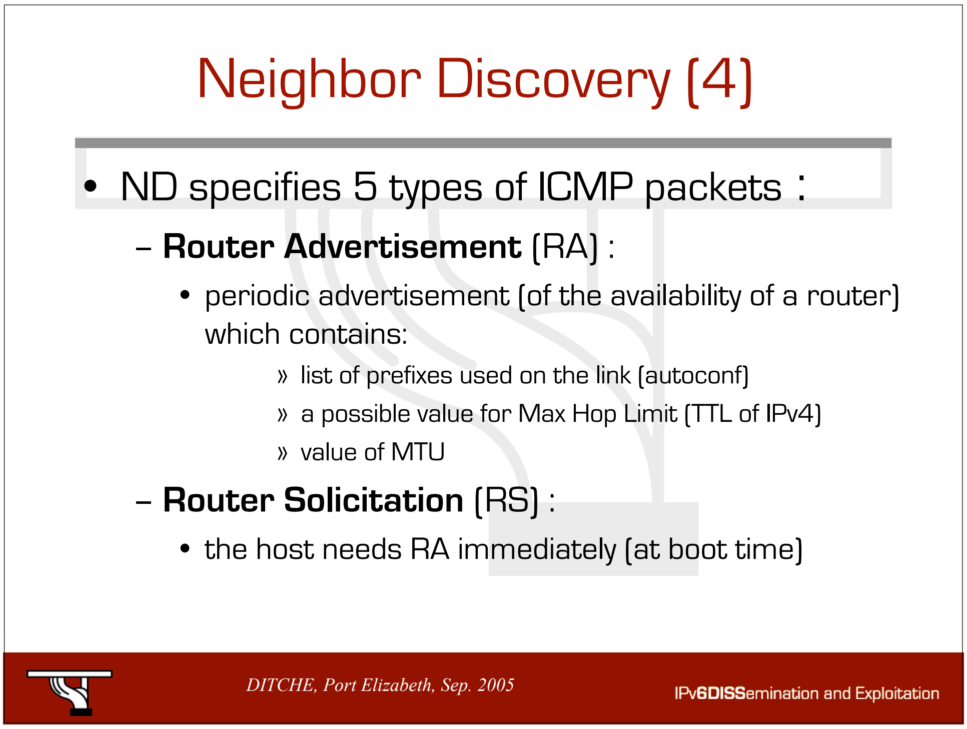


Neighbor Discovery (3): Comparison with IPv4

- It is the synthesis of:
  - ARP
  - R-Disc
  - ICMP redirect
  - ...

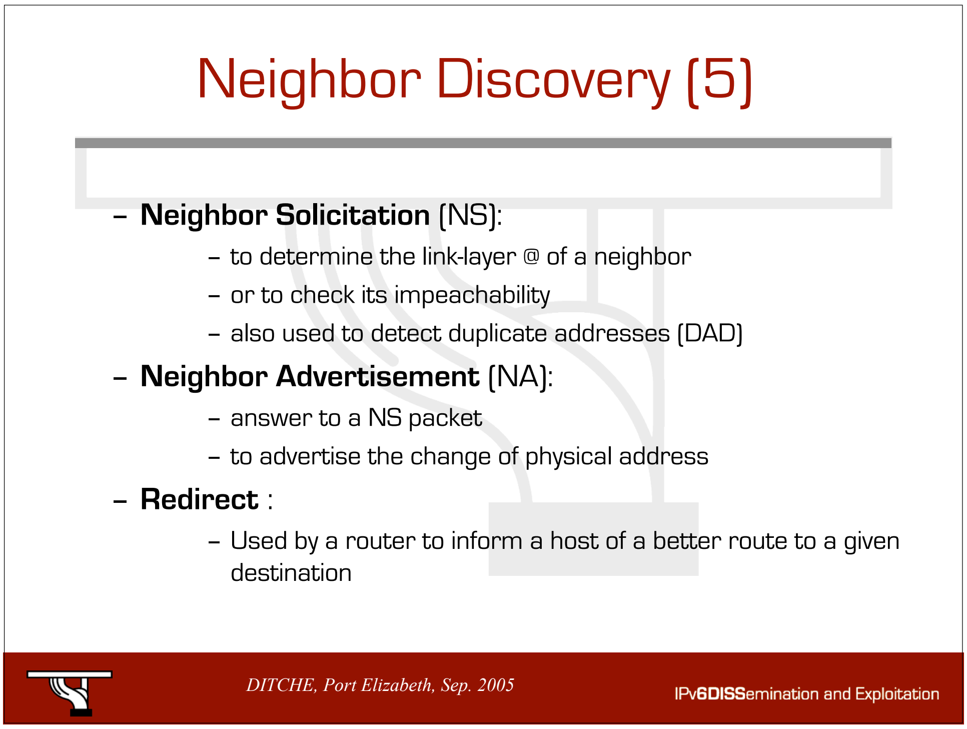
DITCHE, Port Elizabeth, Sep. 2005

IPv6**DISS**emination and Exploitation



Neighbor Discovery (4)

- ND specifies 5 types of ICMP packets :
  - – **Router Advertisement** (RA) :
    - periodic advertisement (of the availability of a router) which contains:
      - » list of prefixes used on the link (autoconf)
      - » a possible value for Max Hop Limit (TTL of IPv4)
      - » value of MTU
  - – **Router Solicitation** (RS) :
    - the host needs RA immediately (at boot time)



Neighbor Discovery (5)

- – **Neighbor Solicitation** (NS):
  - – to determine the link-layer @ of a neighbor
  - – or to check its impeachability
  - – also used to detect duplicate addresses (DAD)
- – **Neighbor Advertisement** (NA):
  - – answer to a NS packet
  - – to advertise the change of physical address
- – **Redirect** :
  - – Used by a router to inform a host of a better route to a given destination

Address Resolution

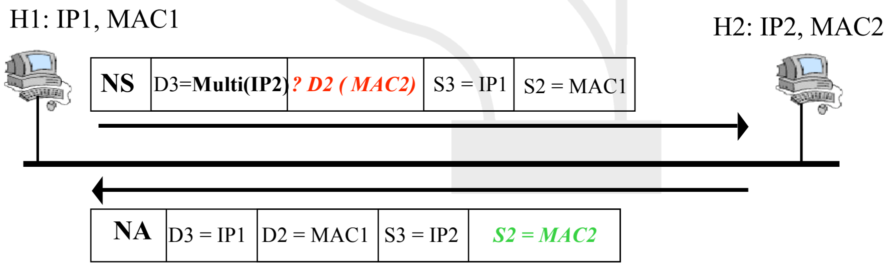
- Find the mapping: Dst IP @ ➔ Link-Layer (MAC) @

- Recalling IPv4 & ARP
  - ARP Request is broadcasted
    - e.g. ethernet @: FF-FF-FF-FF-FF-FF
    - Btw, it contains the Src's LL @
  - ARP Reply is sent in unicast to the Src
    - It contains the Dst's LL @

Address Resolution (2)
IPv6 with Neighbor Discovery

At boot time, every IPv6 node has to join 2 special multicast groups for each network interface:

- All-nodes multicast group: **ff02::1**
- Solicited-node multicast group: **ff02:1:ffxx:xxxx** (derived from the lower 24 bits of the node's address)

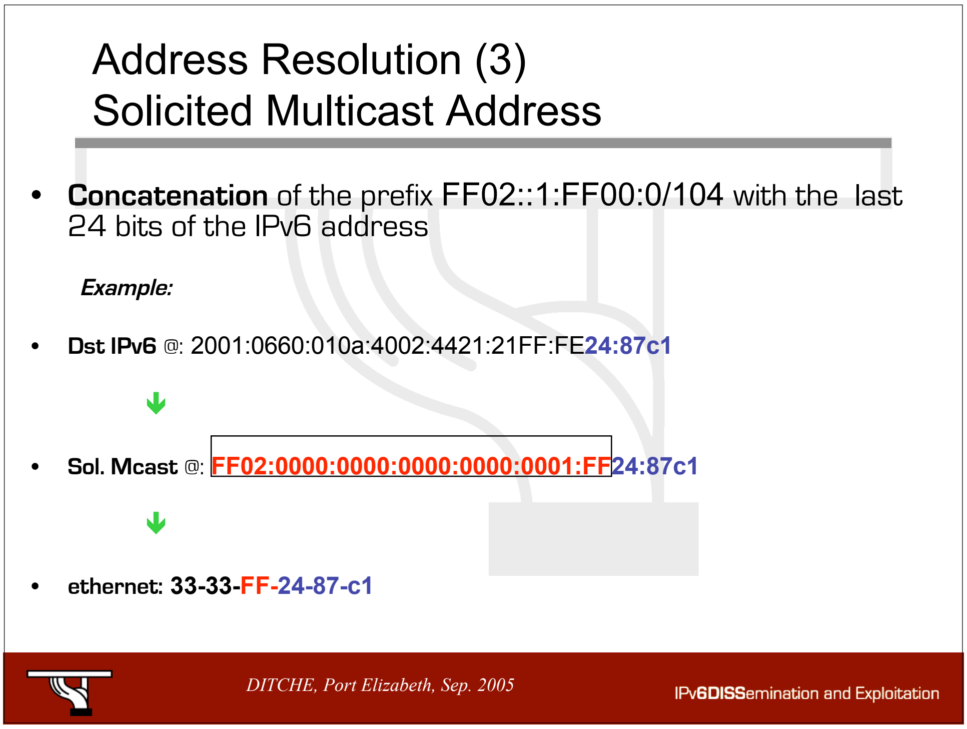


H1: IP1, MAC1

H2: IP2, MAC2

NS	D3=**Multi(IP2)**	*? D2 (MAC2)*	S3 = IP1	S2 = MAC1

NA	D3 = IP1	D2 = MAC1	S3 = IP2	*S2 = MAC2*



Address Resolution (3)
Solicited Multicast Address

- **Concatenation** of the prefix FF02::1:FF00:0/104 with the last 24 bits of the IPv6 address

Example:

- **Dst IPv6** @: 2001:0660:010a:4002:4421:21FF:FE**24:87c1**

↓

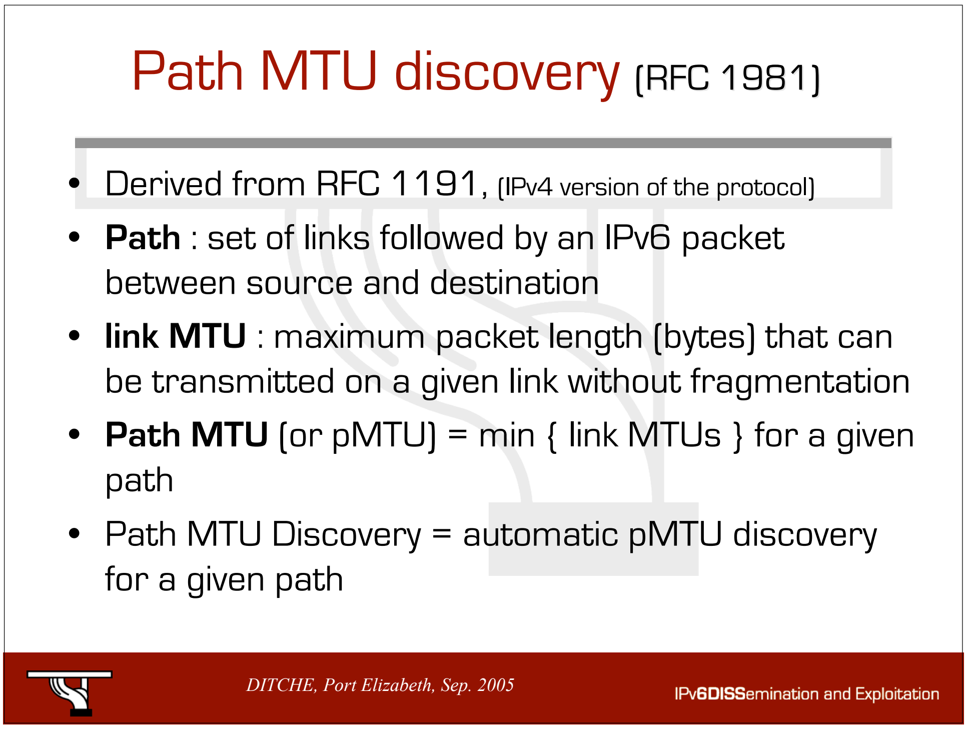
- **Sol. Mcast** @: **FF02:0000:0000:0000:0000:0001:FF24:87c1**

↓

- **ethernet: 33-33-FF-24-87-c1**

DITCHE, Port Elizabeth, Sep. 2005

IPv6**DISS**emination and Exploitation



Path MTU discovery (RFC 1981)

- Derived from RFC 1191, (IPv4 version of the protocol)
- **Path** : set of links followed by an IPv6 packet between source and destination
- **link MTU** : maximum packet length (bytes) that can be transmitted on a given link without fragmentation
- **Path MTU** (or pMTU) = min { link MTUs } for a given path
- Path MTU Discovery = automatic pMTU discovery for a given path

DITCHE, Port Elizabeth, Sep. 2005

IPv6**DISS**emination and Exploitation

Path MTU discovery (2)

- Protocol operation
  - makes assumption that pMTU = link MTU to reach a neighbor (first hop)
  - if there is an intermediate router such that link MTU < pMTU ➔ it sends an ICMPv6 message: "Packet size Too Large"
  - source reduces pMTU by using information found in the ICMPv6 message

  => Intermediate network element aren't allowed to perform packet fragmentation