IPV6 TÜNELLEME TEKNİKLERİ

Gökhan AKIN
gokhan.akin@itu.edu.tr

Asım GÜNEŞ
asim.gunes@itu.edu.tr

İstanbul Teknik Üniversitesi
Bilgi İşlem Daire Başkanlığı

9 Kasim 2007
INET-TR Ankara

IPV6 Tünelleme

AMAÇ:

IPV6 desteklemeyen altyapılardan IPV6 haberleşmesi ve hizmetlerini devam ettirmek.

IPV4 ağ alt yapısından IPV6 ağ alt yapısına geçişi kolaylaştırmak.

Tünelleme Teknikleri

1. **Sabit Teknikler**
2. **Otomatik Teknikler**

- ISATAP : Kurumiçi Unicast Trafik için

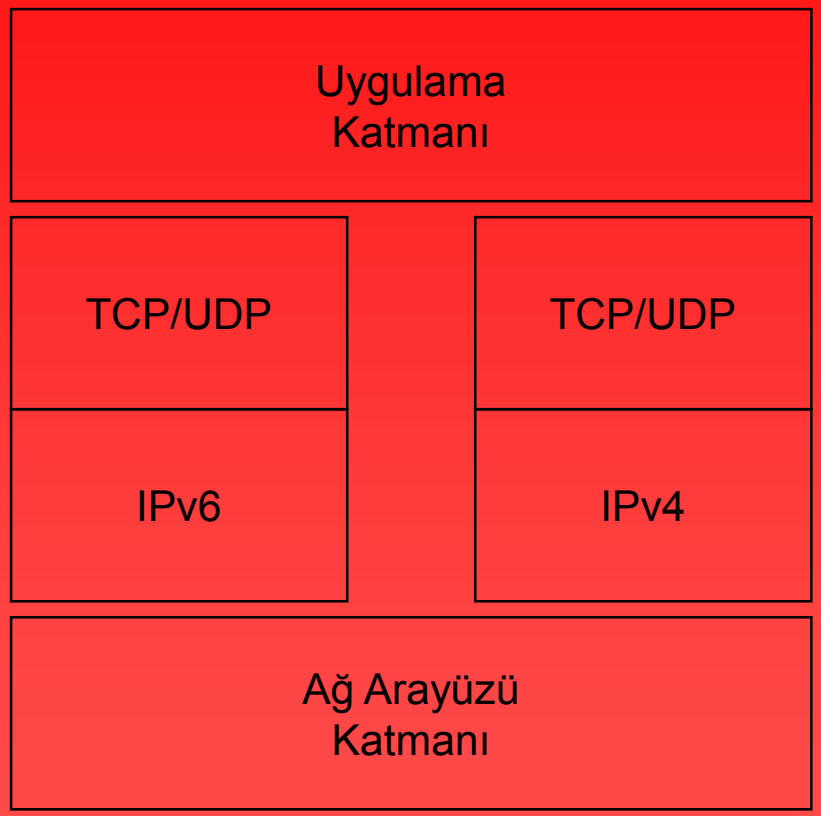
- 6to4 : İnternet'te Unicast Trafik için

- Teredo : NAT sistemler arasında kullanmak için

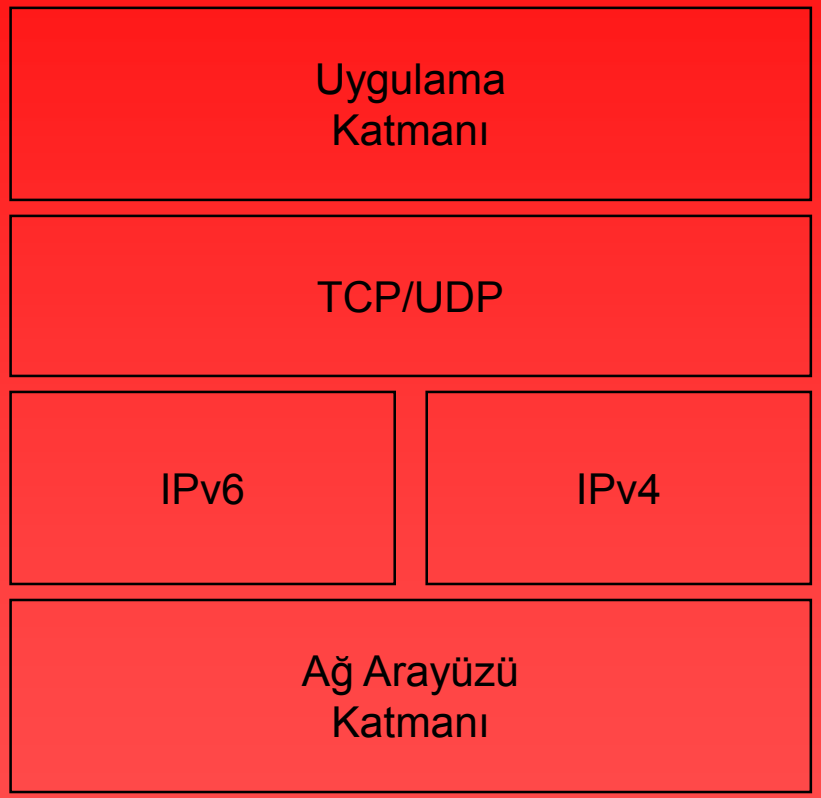
- Otomatik IPV6 Tünelleme : Yerini ISATAP'e bırakmıştır.

- 6over4 : IPV6 multicast desteği vardır.

İşletim Sistemi Mimarileri



Dual stack mimarisi

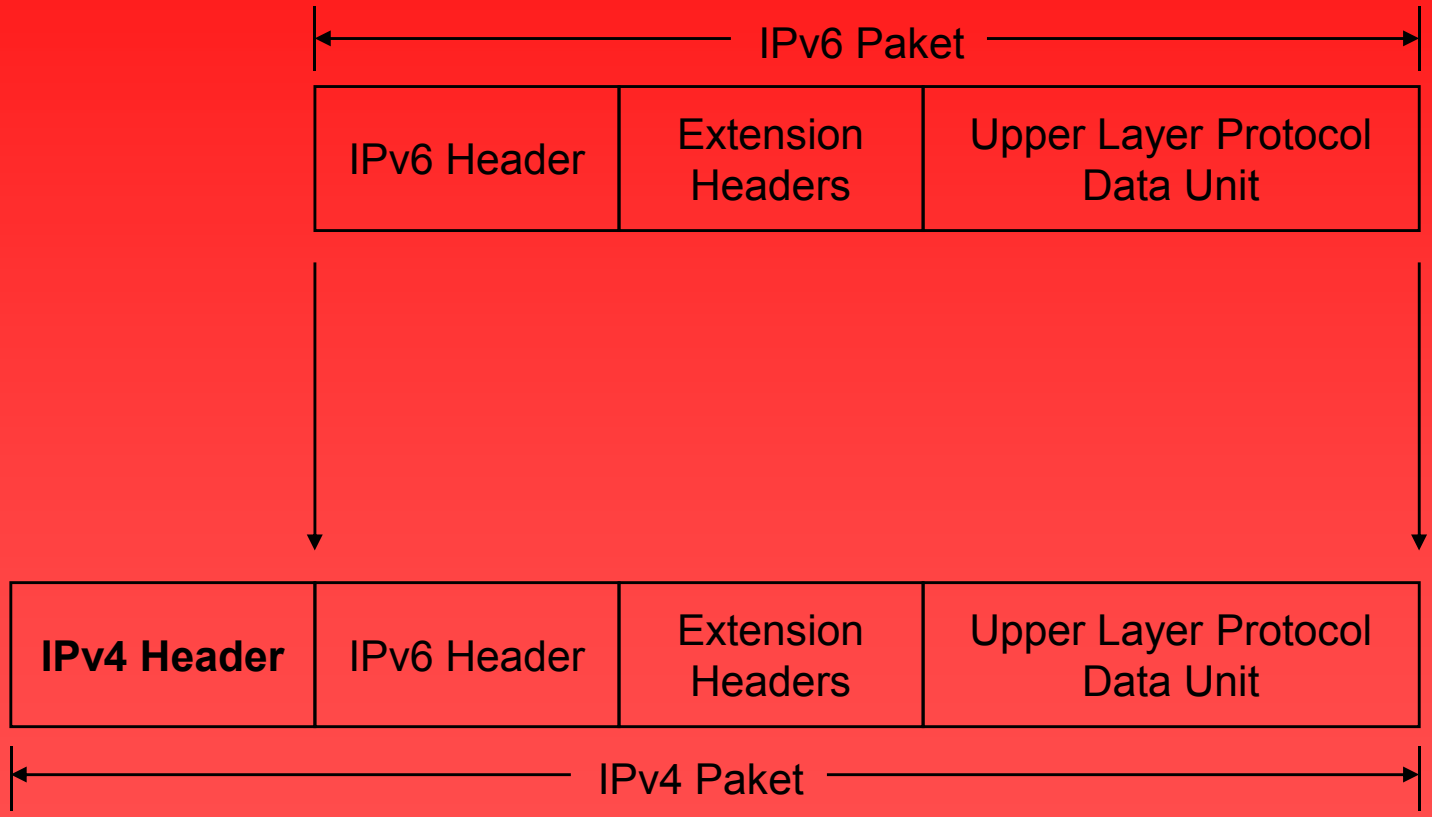


Dual IP layer mimarisi

DNS Mimarisi

- Çift adres kayıdı
  - IPv4 uçlar için A kaydı
  - IPv6 uçlar için AAAA kaydı
- Gerekli ise Çift Pointer (PTR) kayıdı

IPv6'nın IPv4 ile Tünellemesi



IPv4 başlığındaki protokol kısmı 41 olarak ayarlanır.

ISATAP (RFC 4214)

(Intra-Site Automatic Tunnel Addressing Protocol)

Aynı kurum içersinde dual stack mimarisine sahip istemcilerin otomatik olarak ipv4 ağ altyapısı üzerinden ipv6 istemcilere ulaşmasını sağlayan protokoldur. IPV4 başlığında protokol no olarak 41 gözükür.

ISATAP Adreslemesi

[*64-bit ön adres*]**:0:5EFE:***a.b.c.d*

Ön adres: Global IPV6 adresi
veya
Site-Local adres olabilir.

a.b.c.d : Ondalik şekilde IPV4 adresi

Örnekler:

- fe80::5EFE:160.75.8.128
- 2001:a98:8000:1::160.75.8.128

Temel ISATAP Mekanizması


```
Tunnel adapter Automatic Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . : harici.itu.edu.tr
        IP Address. . . . . . . . . . . . : fe80::5efe:160.75.126.38%2
        Default Gateway . . . . . . . . . :
```

ISATAP Paket Yapısı

No.	Time	Source	Destination	Protocol	Info
1	0.000000	fe80::5efe:a04b:580	fe80::5efe:a04b:49be	ICMPv6	Echo request
2	0.001134	fe80::5efe:a04b:49be	fe80::5efe:a04b:580	ICMPv6	Echo reply
3	0.999804	fe80::5efe:a04b:580	fe80::5efe:a04b:49be	ICMPv6	Echo request
4	1.002956	fe80::5efe:a04b:49be	fe80::5efe:a04b:580	ICMPv6	Echo reply
5	1.999739	fe80::5efe:a04b:580	fe80::5efe:a04b:49be	ICMPv6	Echo request
6	2.000975	fe80::5efe:a04b:49be	fe80::5efe:a04b:580	ICMPv6	Echo reply
7	2.999679	fe80::5efe:a04b:580	fe80::5efe:a04b:49be	ICMPv6	Echo request
8	3.000933	fe80::5efe:a04b:49be	fe80::5efe:a04b:580	ICMPv6	Echo reply

```
⊞ Frame 1 (114 bytes on wire, 114 bytes captured)
⊞ Ethernet II, Src: HewlettP_4f:e0:90 (00:15:60:4f:e0:90), Dst: Cisco_75:0b:4a (00:0f:35:75:0b:4a)
⊟ Internet Protocol, Src: 160.75.5.128 (160.75.5.128), Dst: 160.75.73.190 (160.75.73.190)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 100
    Identification: 0x6cf6 (27894)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: IPv6 (0x29)
  ⊞ Header checksum: 0x3da6 [correct]
    Source: 160.75.5.128 (160.75.5.128)
    Destination: 160.75.73.190 (160.75.73.190)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 40
    Next header: ICMPv6 (0x3a)
    Hop limit: 128
    Source address: fe80::5efe:a04b:580
    Destination address: fe80::5efe:a04b:49be
⊟ Internet Control Message Protocol v6
    Type: 128 (Echo request)
    Code: 0
    Checksum: 0x8a10 [correct]
    ID: 0x0000
    Sequence: 0x0015
    Data (32 bytes)
```

ISATAP Yönlendiricinin Belirlenmesi

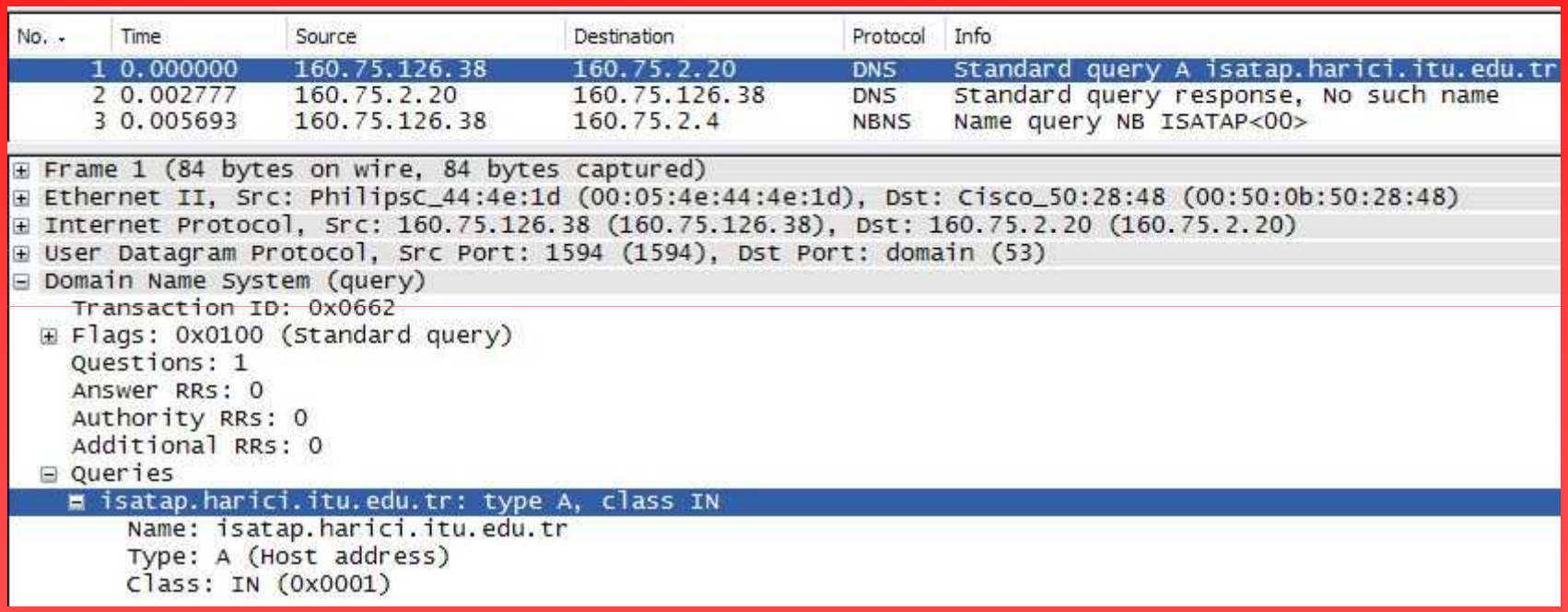
Aynı firma içindeki Native IPV6 istemciler ile haberleşme olabilmesi için ISATAP Yönledirici gerekir.

ISATAP Yönlendiricinin Belirlenmesi için:

- isatap.domainadi olarak DNS Sunucusundan sorgulanır.
- host dosyasına bakılır.
- Windows istemciler “ISATAP” NETBIOS adi ile sorgularlar.
- ISATAP yönledirici elle manuel olarak cihaza belirtilebilir.

  (Windows için örnek: netsh interface ipv6 isatap set router)

ISATAP Yönlendirici Sogusu

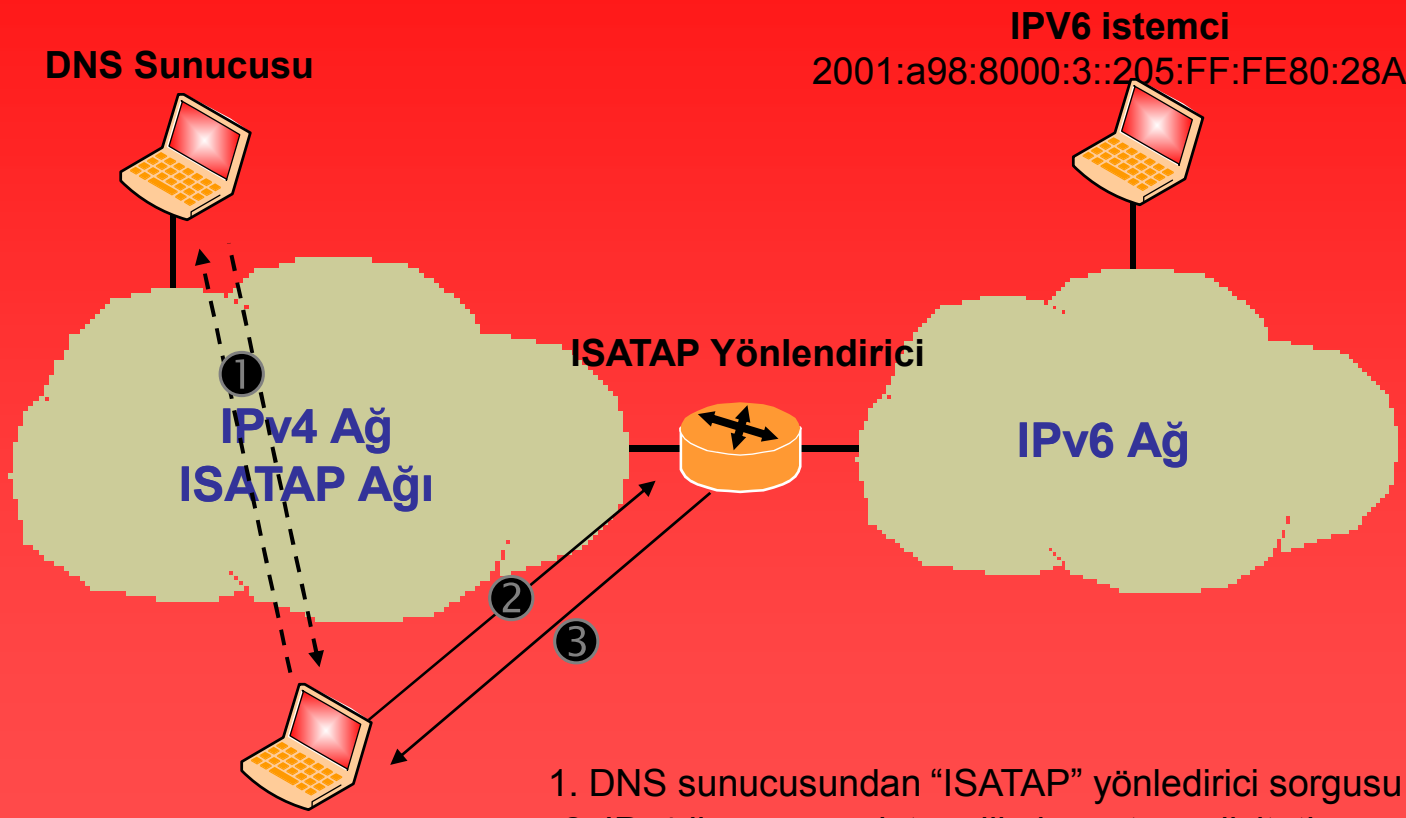


No.	Time	Source	Destination	Protocol	Info
1	0.000000	160.75.126.38	160.75.2.20	DNS	Standard query A isatap.harici.itu.edu.tr
2	0.002777	160.75.2.20	160.75.126.38	DNS	Standard query response, No such name
3	0.005693	160.75.126.38	160.75.2.4	NBNS	Name query NB ISATAP<00>

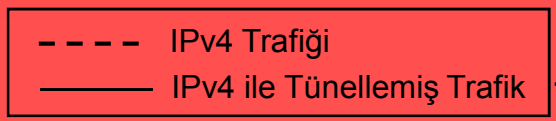
```
⊞ Frame 1 (84 bytes on wire, 84 bytes captured)
⊞ Ethernet II, Src: PhilipsC_44:4e:1d (00:05:4e:44:4e:1d), Dst: Cisco_50:28:48 (00:50:0b:50:28:48)
⊞ Internet Protocol, Src: 160.75.126.38 (160.75.126.38), Dst: 160.75.2.20 (160.75.2.20)
⊞ User Datagram Protocol, Src Port: 1594 (1594), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0x0662
  ⊞ Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ isatap.harici.itu.edu.tr: type A, class IN
        Name: isatap.harici.itu.edu.tr
        Type: A (Host address)
        Class: IN (0x0001)
```

ISATAP Prefix Atanması

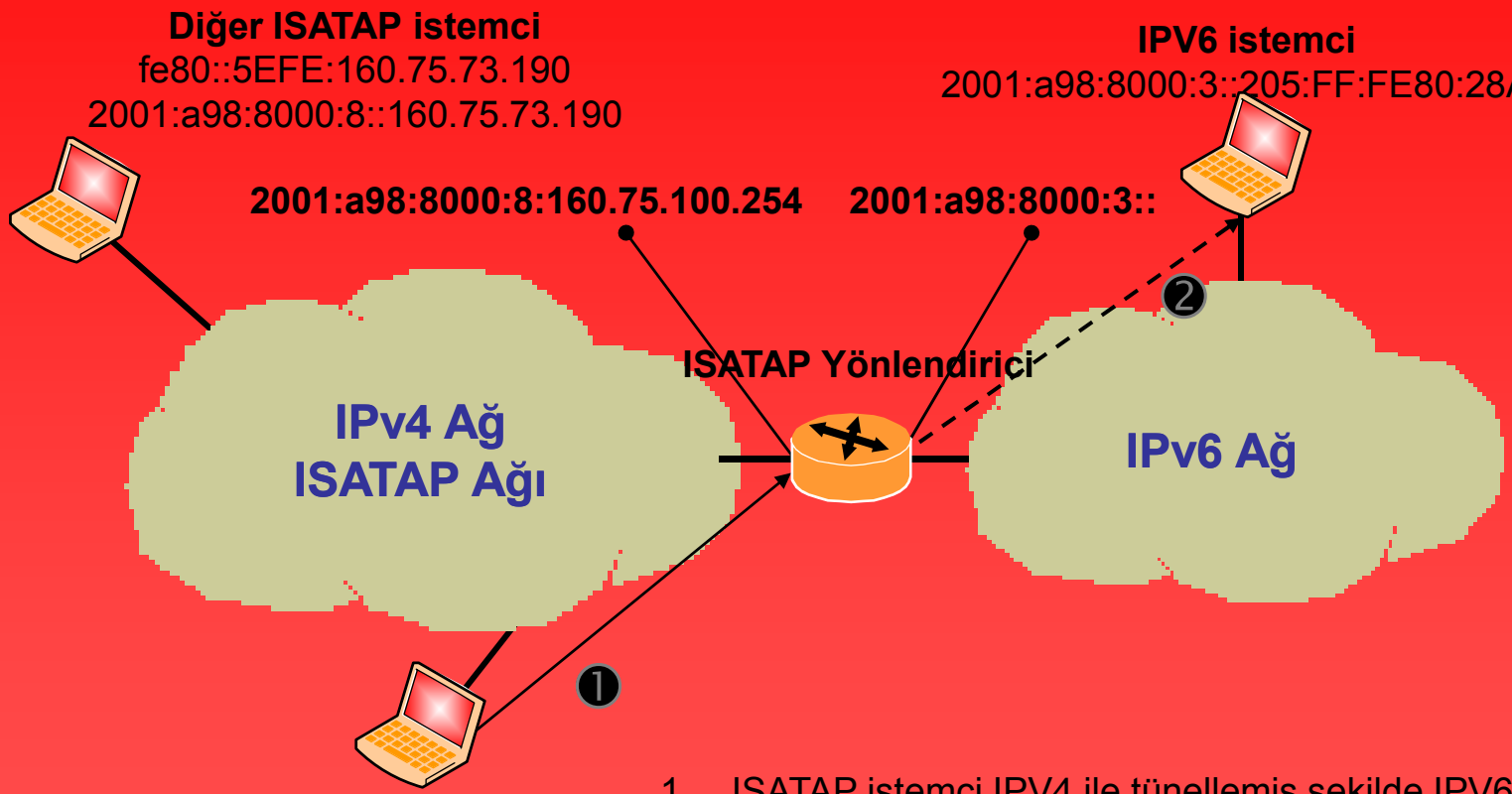
Atanacak Prefix:2001:a98:8000:8::/64



1. DNS sunucusundan “ISATAP” yönledirici sorgusu
2. IPv4 ile encapsulate edilmiş router solicitation mesajı
3. IPv4 ile encapsulate edilmiş router advertisement mesajı



ISATAP Yönlendirmesi



1. ISATAP istemci IPV4 ile tünellemiş şekilde IPV6 trafiği ISATAP yönlendiriciye yollar.
2. Yönlendirici paketi Native IPv6 paket olarak hedefe ulaştırır.

IPv6 Trafiği
IPv4 ile Tünellemiş Trafik

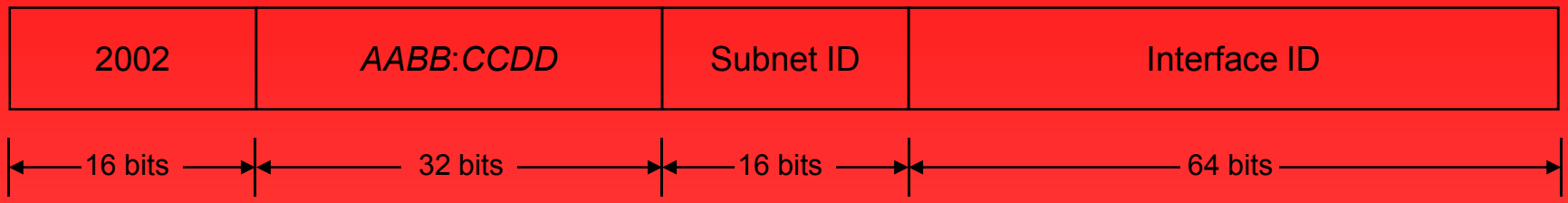
6to4 (RFC 3056)

(Connection of IPv6 Domains via IPv4 Clouds)

Dual stack mimarisine sahip istemcilerin otomatik olarak IPV4 ağ altyapısı üzerinden IPV6 istemcilere ulaşmasını sağlayan protokolüdür.

IPV4 başlığında protokol numarası olarak 41 gözükür.

6to4 Adreslemesi



Bütün 2002::/16 6to4 adreslemesi için rezerve edilmiştir.

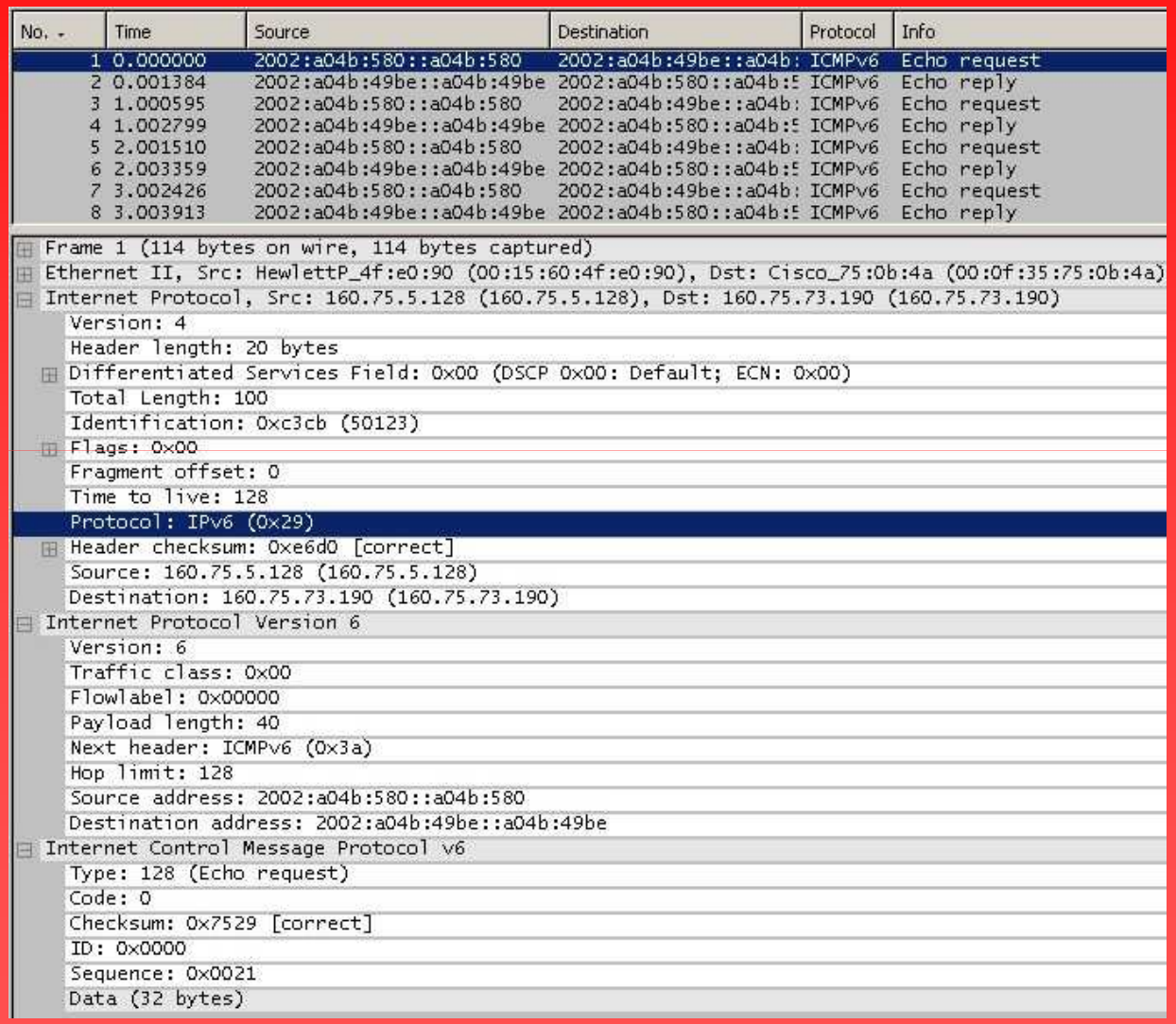
AABB:CCDD :IPV4 adresinin onaltılık olarak gösterilmiş halidir.

Temel 6to4 Mekanizması


```
Tunnel adapter 6to4 Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . : harici.itu.edu.tr
        IP Address. . . . . . . . . . . . : 2002:a04b:7e26::a04b:7e26
        Default Gateway . . . . . . . . . : 2002:c058:6301::c058:6301
```

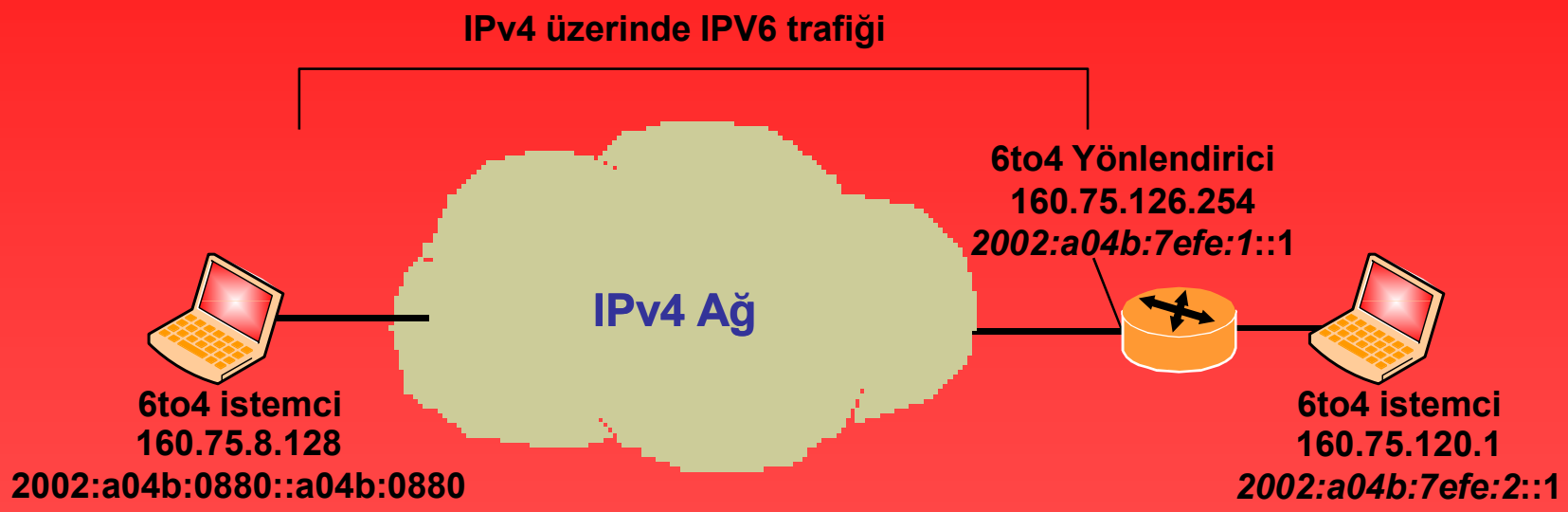
6to4 Paket Yapısı



No.	Time	Source	Destination	Protocol	Info
1	0.000000	2002:a04b:580::a04b:580	2002:a04b:49be::a04b:	ICMPv6	Echo request
2	0.001384	2002:a04b:49be::a04b:49be	2002:a04b:580::a04b:5	ICMPv6	Echo reply
3	1.000595	2002:a04b:580::a04b:580	2002:a04b:49be::a04b:	ICMPv6	Echo request
4	1.002799	2002:a04b:49be::a04b:49be	2002:a04b:580::a04b:5	ICMPv6	Echo reply
5	2.001510	2002:a04b:580::a04b:580	2002:a04b:49be::a04b:	ICMPv6	Echo request
6	2.003359	2002:a04b:49be::a04b:49be	2002:a04b:580::a04b:5	ICMPv6	Echo reply
7	3.002426	2002:a04b:580::a04b:580	2002:a04b:49be::a04b:	ICMPv6	Echo request
8	3.003913	2002:a04b:49be::a04b:49be	2002:a04b:580::a04b:5	ICMPv6	Echo reply

```
⊞ Frame 1 (114 bytes on wire, 114 bytes captured)
⊞ Ethernet II, Src: HewlettP_4f:e0:90 (00:15:60:4f:e0:90), Dst: Cisco_75:0b:4a (00:0f:35:75:0b:4a)
⊟ Internet Protocol, Src: 160.75.5.128 (160.75.5.128), Dst: 160.75.73.190 (160.75.73.190)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 100
    Identification: 0xc3cb (50123)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: IPv6 (0x29)
  ⊞ Header checksum: 0xe6d0 [correct]
    Source: 160.75.5.128 (160.75.5.128)
    Destination: 160.75.73.190 (160.75.73.190)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 40
    Next header: ICMPv6 (0x3a)
    Hop limit: 128
    Source address: 2002:a04b:580::a04b:580
    Destination address: 2002:a04b:49be::a04b:49be
⊟ Internet Control Message Protocol v6
    Type: 128 (Echo request)
    Code: 0
    Checksum: 0x7529 [correct]
    ID: 0x0000
    Sequence: 0x0021
    Data (32 bytes)
```

6to4 Yönlendirici



6to4 Relay'in Belirlenmesi

Global Native IPV6 istemciler ile haberleşme olabilmesi için 6to4 Relay gerekir.

6to4 Relay'inBelirlenmesi için:

- DNS Sunucusundan sorgulanır.
- RFC 3068
- 6to4 relay elle manuel olarak cihaza belirtilebilir.

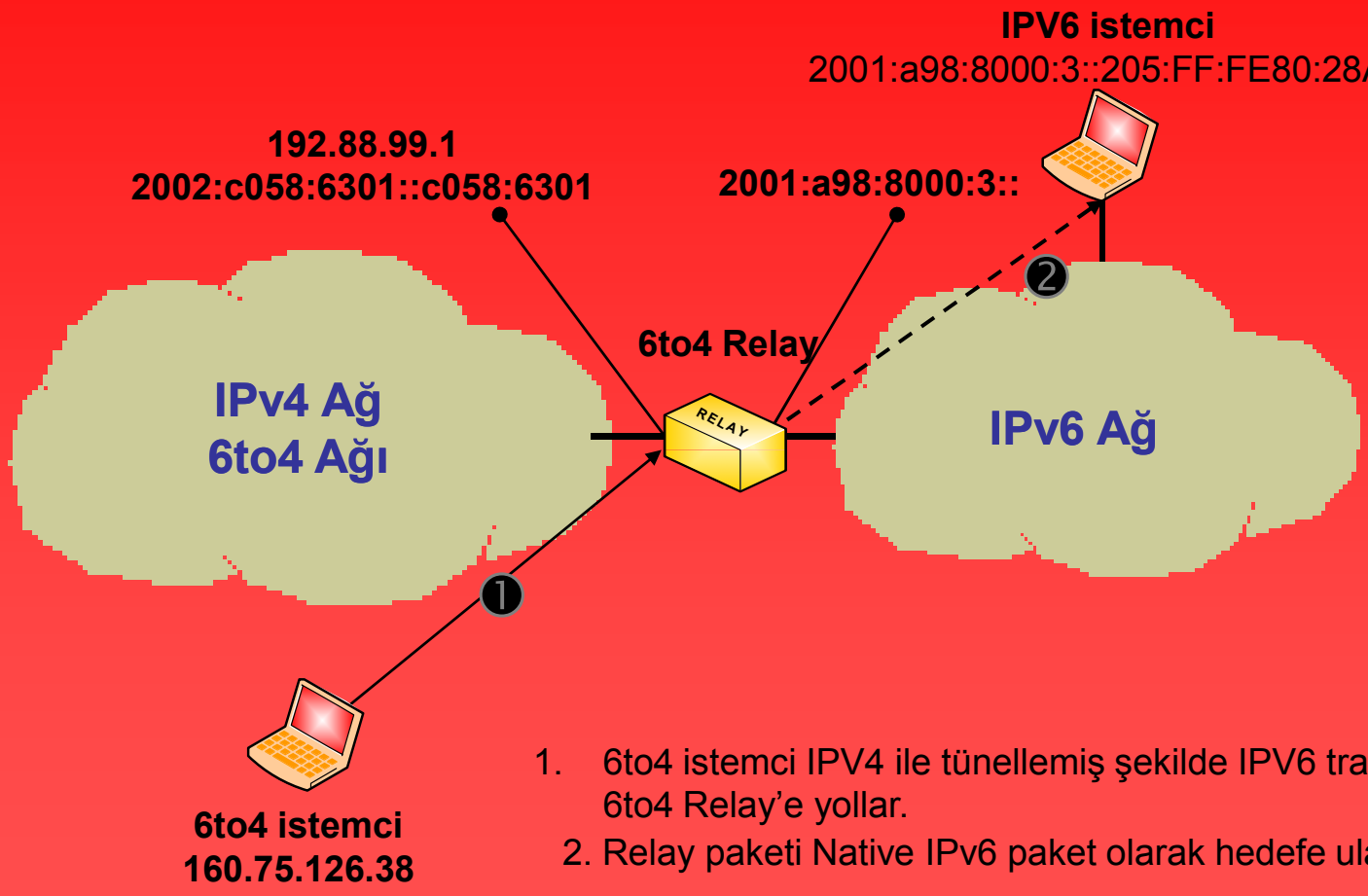
(Örnek: netsh interface ipv6 6to4 set relay)

6to4 Relay Sorgusu

No.	Time	Source	Destination	Protocol	Info
1	0.000000	160.75.126.38	160.75.2.20	DNS	Standard query A 6to4.ipv6.microsoft.com
2	0.002736	160.75.2.20	160.75.126.38	DNS	Standard query response A 192.88.99.1

```
⊞ Internet Protocol, Src: 160.75.2.20 (160.75.2.20), Dst: 160.75.126.38 (160.75.126.38)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 1594 (1594)
⊟ Domain Name System (response)
    Transaction ID: 0xea63
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⊞ Queries
  ⊟ Answers
    ⊟ 6to4.ipv6.microsoft.com: type A, class IN, addr 192.88.99.1
        Name: 6to4.ipv6.microsoft.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 43 minutes, 4 seconds
        Data length: 4
```

6to4 Relay Kullanımı



1. 6to4 istemci IPV4 ile tünellemiş şekilde IPV6 trafigi 6to4 Relay'e yollar.
2. Relay paketi Native IPv6 paket olarak hedefe ulaştırı.

```
Tunnel adapter 6to4 Tunneling Pseudo-Interface:

        Connection-specific DNS Suffix  . : harici.itu.edu.tr
        IP Address. . . . . . . . . . . . : 2002:a04b:7e26::a04b:7e26
        Default Gateway . . . . . . . . . : 2002:c058:6301::c058:6301
```

---- IPv6 Trafiği

——— IPv4 ile Tünellemiş Trafik

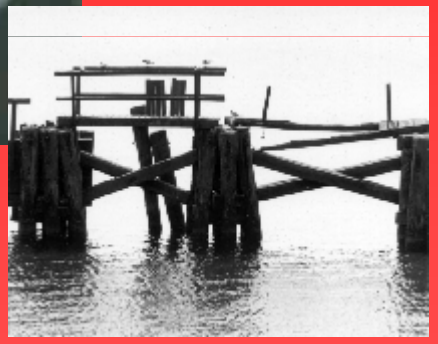
6to4 Relay Adresleri

If you wish to add, correct or remove entries from this list, please send me mail.

Global				
Name	**Location**	**Bandwidth**	**Contact**	**Notes**
2002:c058:6301::	Global	n/a	n/a	See RFC-3068. This is an anycast address for the closest relay router
North America				
Name	**Location**	**Bandwidth**	**Contact**	**Notes**
6to4.ipv6.microsoft.com	Redmond, WA? / -	?	Microsoft	Open
ipv6-lab-gw.cisco.com	San Jose / Sprint?	100 mbps	Cisco	By request, please. See also Cisco's IPv6 Page
Asia / Pacific Oceana				
Name	**Location**	**Bandwidth**	**Contact**	**Notes**
6to4.ipv6.aarnet.net.au	Sydney, Australia	100 mbps	AARNET NOC	Open, Australia (or vicinity) only
kddilab.6to4.jp	Tokyo, Japan / ?	100 mbps	kddilab	Open
6to4.ipv6.ascc.net	Taipei, Taiwan / ?	100 mbps	Academia Sinica Computing Center	Open / Experimental
Africa				
6to4.ipng.unix.za.net	Cape Town, South Africa / ?	48 mbps	Univ. of Cape Town	Open
Europe				
Name	**Location**	**Bandwidth**	**Contact**	**Notes**
6to4.ipv6.bt.com	Adastral Park, UK / ?	10 mbps	Stuart Prevost	Open
skbys-00-00.6to4.xs26.net	Banska Bystrica, Slovakia	34 mbps	Access to Six	Open
6to4.ipv6.uni-leipzig.de	Leipzig, Germany	100 mbps	Uwe	Open / Experimental
6to4.ipv6.fh-regensburg.de	Regensburg, Germany	34 mbps	Hubert Feyrer	Open / Experimental

Teredo (RFC 4380) - 1

(Tunneling IPv6 over UDP through NATs)



Protokol, diğer adı shipworm olarakta geçen canlıdan ismini almıştır.

Teredo (RFC 4380) - 2

(Tunneling IPv6 over UDP through NATs)

6to4 tekniği ile NAT arkasındaki cihazlara:
NAT tercüme tablosunda kayıt olmadığı için
veya
NAT cihazının sadece TCP ve UDP protokollerini gecirebilmesi protokol 41 geçirememesinden dolayı erişim sorunu yaşanır.

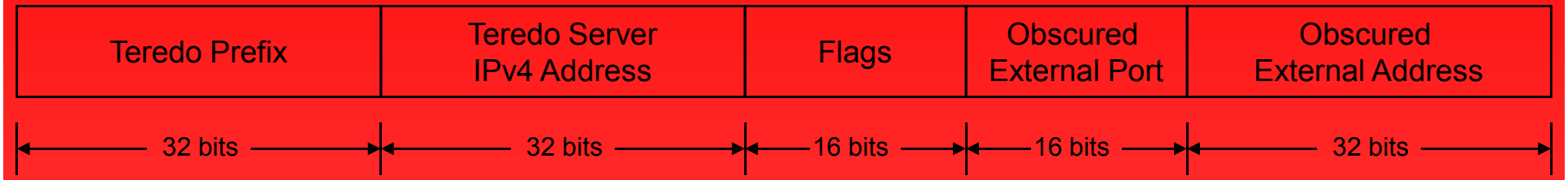
Teredo (RFC 4380) - 3

(Tunneling IPv6 over UDP through NATs)

NAT arkasındaki istemcilerinde IPV6 ile haberleşmelerinin sağlanması için geliştirilmiştir.

Teredo son çare (last resort) çözümüdür. Native IPV6, ISATAP veya 6to4 ile haberleşilemesse kullanılır.

Teredo Adreslemesi - 1



Teredo Prefix : 2001:0000::/32

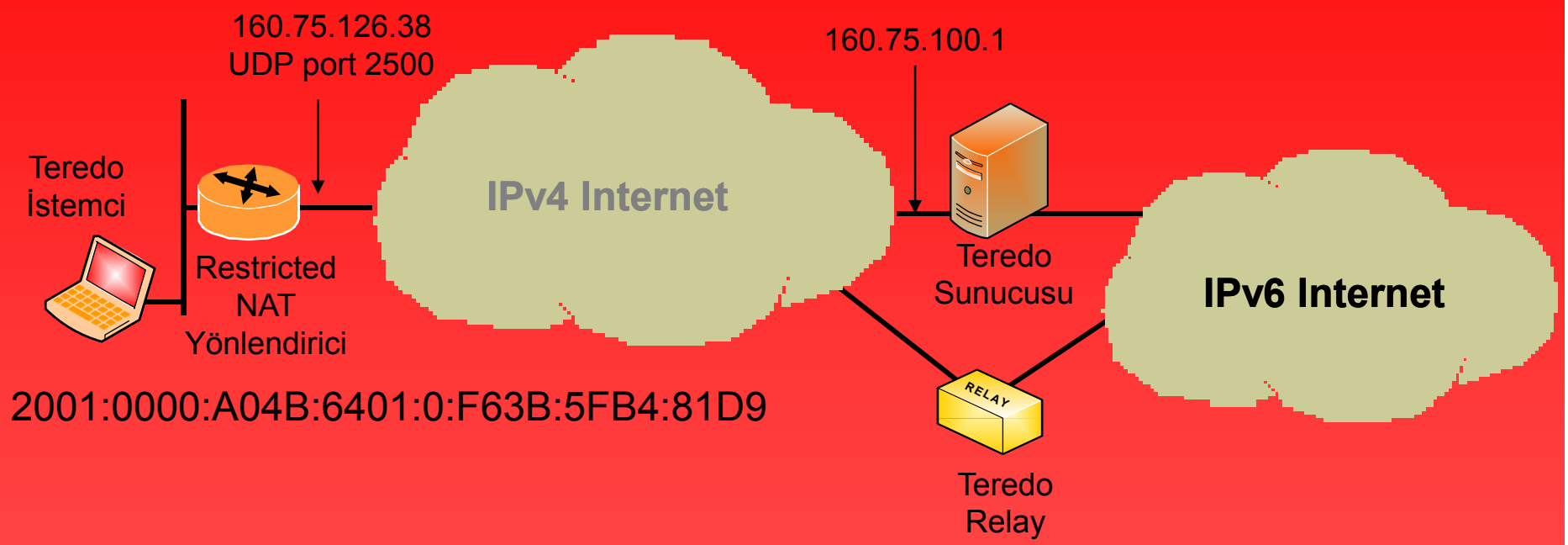
Teredo Server IPV4 Address: Teredo sunucu IPV4 adresi

Flags: İlk biti cone NAT arkasında ise 1 yoksa sıfır ayarlanan değer (Not: Microsoft rezerve olan kısımları raslansal olarak atayarak IPV6 Address scan ataklarınına karsı koruma getirmiştir)

Obscured External Port: kullanılan UDP port numarasını onaltılık şeklinde 0xFFFF ile XOR'lanmış şekli

Obscured External Address: IPV4 adresinin onaltılık şekilde 0xFFFFFFFF ile XOR'lanmış şekli

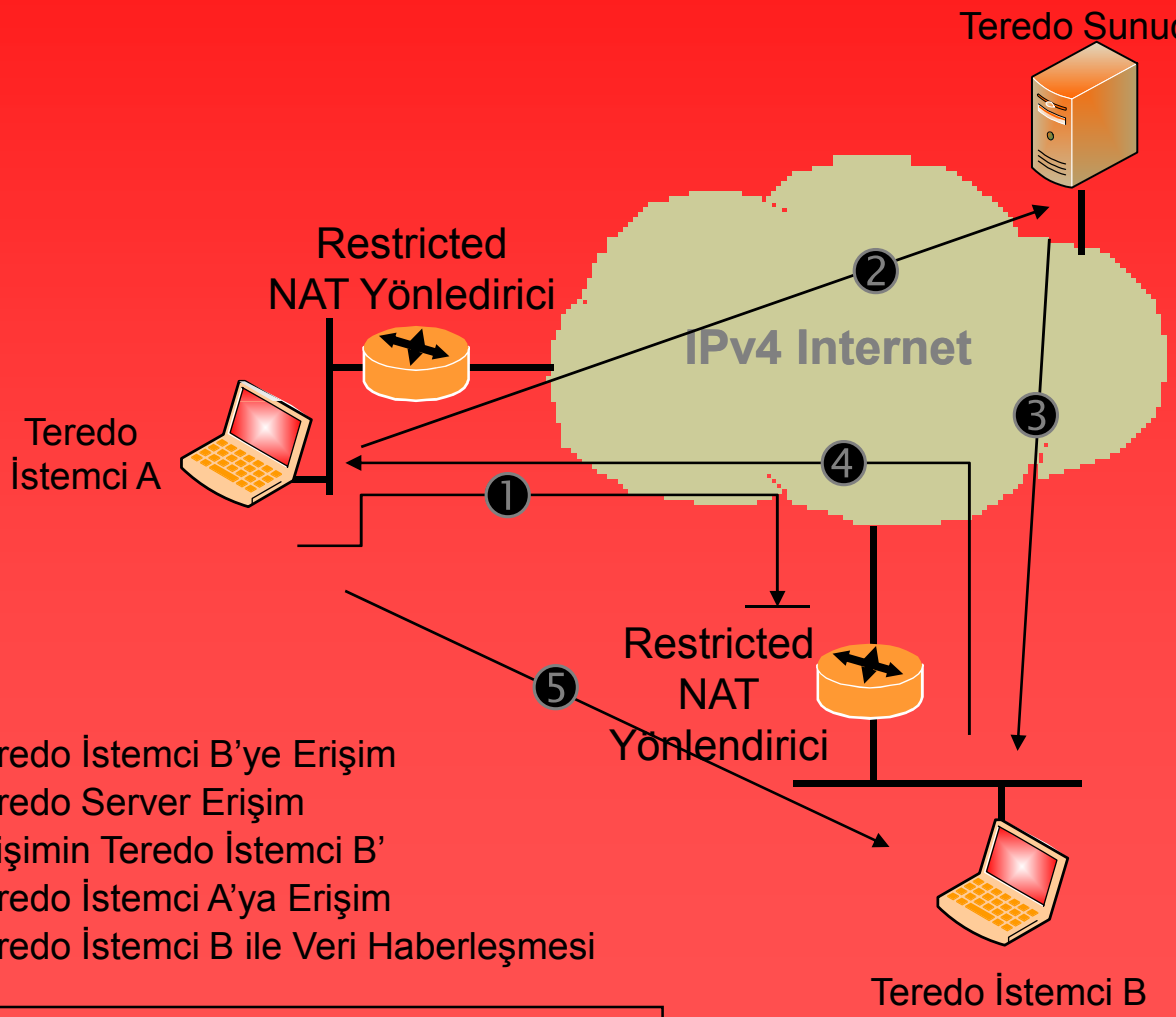
Teredo Adreslemesi - 2



2001:0000:A04B:6401:0:F63B:5FB4:81D9

HESAP ADIMLARI:
Teredo Sunucusu : 160.75.100.1 = A04B:6401:0:
UDP Port No: 2500 = 09C4 **XoR** FFFF = F63B
160.75.126.38 = a04b:7e26 **XoR** = 5FB4 81D9

Farklı NAT kümeleri Arkasındaki İstemcilerin Teredo ile Haberleşmesi



1. Teredo İstemci B'ye Erişim
2. Teredo Server Erişim
3. Erişimin Teredo İstemci B'
4. Teredo İstemci A'ya Erişim
5. Teredo İstemci B ile Veri Haberleşmesi

IPv4 UDP ile IPV6 Tünelleme Paketi

Teredo ve Güvenlik

Teşekkürler

www2.itu.edu.tr/~akingok

Kaynaklar:

www.microsoft.com/ipv6

www.cisco.com/go/ipv6

www.symantec.com/avcenter/ reference/Teredo_Security.pdf, Symantec Corp

Karlsson B. ‘Implementing IPv6 Networks’ Cisco Press

RFC 4214, 3056, 4380