“IPv6 Güvenliği ”

IPv6 HAZIR
Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi

Emre YÜCE - TÜBİTAK ULAKBİM

2 Haziran 2010

Sunum İçeriği

- Kısaca IPv6
- IPv6 Saldırı
  - IPv4 ile benzerlik gösteren saldırılar
  - IPv6'ya özgü saldırılar
    - Ağ tarama ve Keşif (Reconnaissance) yöntemleri
    - Yerel ağ saldırıları
    - Gezgin IPv6 (mobile IPv6) saldırıları
    - Geçiş yöntemi temelli saldırılar

Kısaca IPv6

- Internet Protocol Version 6 (IPv6) 1998 yılında yayımlanan RFC 2460 ile tanımlanmıştır.
- Avantajları
  - 128 bitlik adres yapısı ile geniş adres uzayı
  - Otomatik adres dağıtma özelliği ile kolay yönetilebilirlik
  - Basitleştirilmiş paket başlığı yapısı ile hızlı yönlendirme
  - Zorunlu IPsec desteği
  - Genişleme başlıkları ile Servis Kalitesi (Quality of Service, QoS), gezgin IPv6 (mobile IPv6), IPsec desteğinin kolay sağlanabilmesi
  - Geliştirilmiş çoklu gönderim (multicast) desteği

Kısaca IPv6

- IPv6 Saldırıları
  - IPv4 ile benzerlik gösteren saldırılar
    - SQL injection, taşırma saldırıları
    - DOS saldırıları
  - IPv6'ya özgü saldırılar
    - Ağ tarama ve Keşif (Reconnaissance) yöntemleri
    - Yerel ağ saldırıları
    - Gezgin IPv6 (mobile IPv6) saldırıları
    - Geçiş yöntemi temelli saldırılar

Ağ Tarama ve Keşif Yöntemleri

- Saldırının ilk adımı
- Ağ hakkında bilgi edinme
  - Potansiyel kurbanların tespit edilmesi
  - Servisler ve olası güvenlik zafiyetlerinin belirlenmesi

Ağ Tarama ve Keşif Yöntemleri

- IPv6 ağlarında ağ tarama yöntemlerinin durumu:
  - IPv6 adres aralığı büyüklüğü nedeni ile adres uzayının tamamının taranması mümkün değildir.
  - Taranacak adres uzayını daraltacak sebepler
    - Sıradan (::1, ::2 vb.) veya
    - Hatırlanması kolay kelime şeklinde (::baba,::dede, ::face) IPv6 adresleri kullanılması
  - DNS kullanımı artacak, DNS sunucuları geçerli adres bulmak için önemli kaynaklar olacak.
  - Geçiş yöntemlerinde kullanılan standart adresler ağın taranmasını ve keşfini kolaylaştıracak.

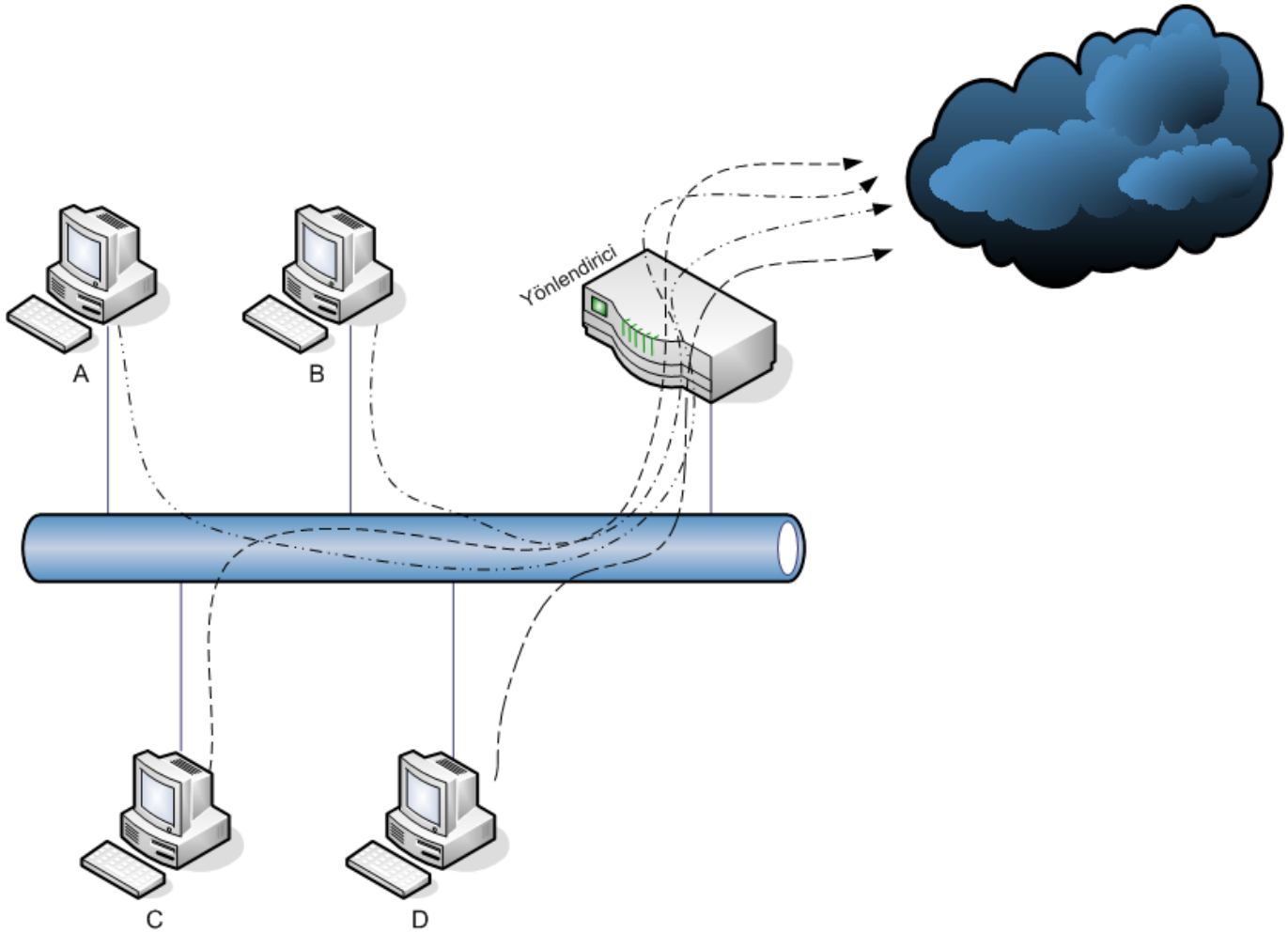
Ağ Tarama ve Keşif Yöntemleri

- IPv6 ağlarında ağ keşfi yöntemlerinin durumu:
  - Komşu keşfi (neighborhood discovery), Durum denetimsiz adres yapılandırması (stateless address configuration) mesajları
    - Fiziksel güvenliği sağlanmış bağlantılar üzerinden iletileceği düşünülmüştür.
    - Yerel ağa dâhil olmayı başaran bir cihaz tüm ağ güvenliğini tehdit edebilir. (Gezgin IPv6, kablosuz ağlar vb.)
  - Çoklu gönderim ve herhangi birine gönderim adreslerinin ağ keşfi amacıyla kullanılması mümkündür.

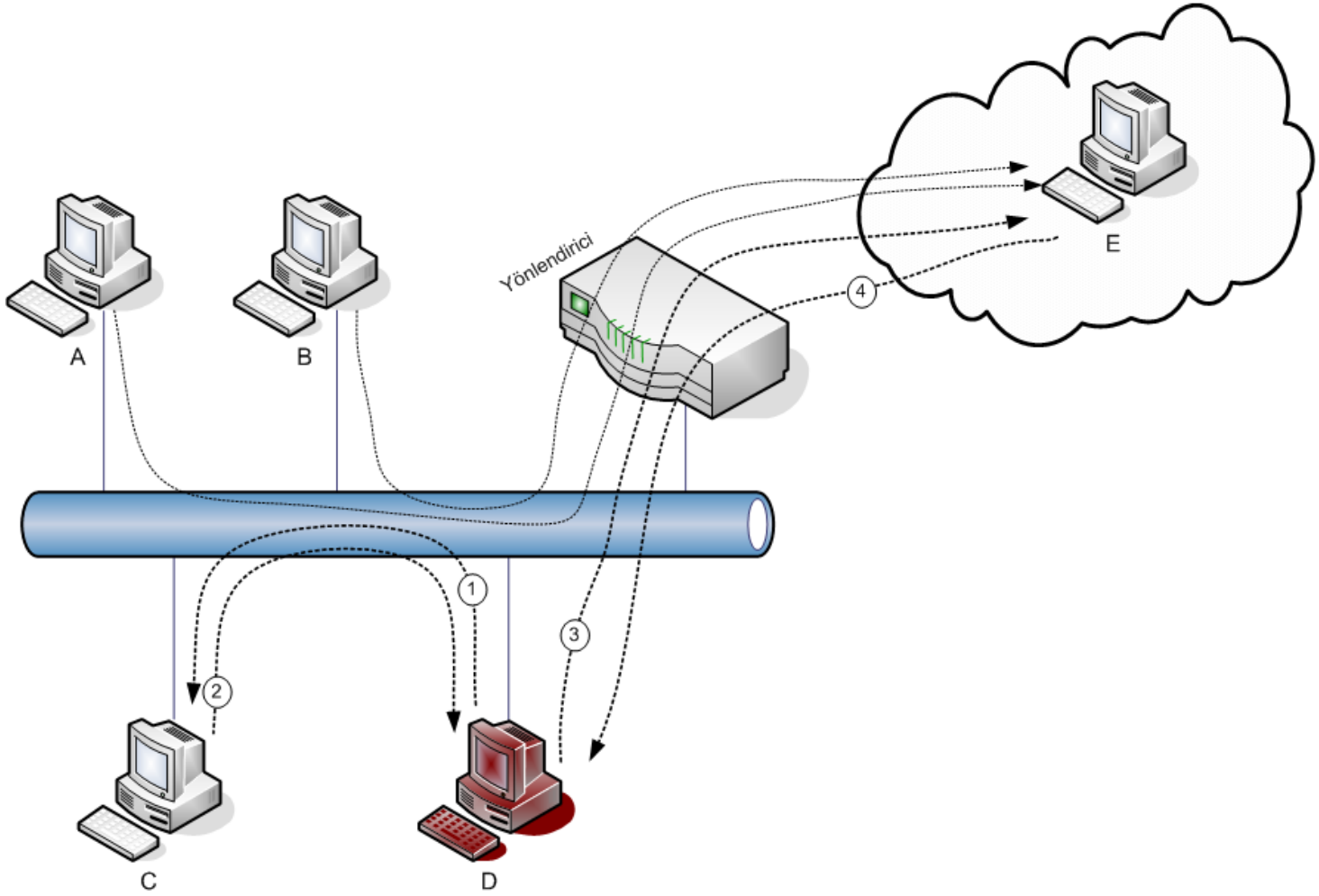
Yerel Ağ Saldırıları

- Yerel ağ saldırıları
  - ICMPv6 mesajları ağ yapılandırılmasında kullanıldığı için tamamen engellenemiyor.
  - NDP (Neighborhood Discovery Protocol) mesajları
  - Sahte yönlendirici ilanı (router advertisement) mesajları
    - Ortadaki adam saldırısı
    - Servisi dışı bırakma saldırısı

Sahte Yönlendirici



Sahte Yönlendirici



Yerel Ağ Saldırıları

- Yerel ağ saldırıları
  - Duplicate Address Detection (DAD)
    - İstemcinin IPv6 adresi alması engellenebilir.

Yerel Ağ Saldırıları

- Nasıl engellenebilir?
  - Yerel ağdaki bir paketin kaynak ve hedef adresi yerel bağlantılı adres (link-local address) olmalı.
  - Paketin hop limit değeri maksimum değer olan 255 olmalı.
    - Başka bir deyişle paketin herhangi bir yönlendiriciden geçmemiş olduğu onaylanmalı.

Yerel Ağ Saldırıları

- Nasıl engellenebilir?
  - SEcure Neighbor Discovery (SEND)
    - RFC 3971
  - The Cryptographically Generated Addresses (CGA)
    - RFC 3972

Yerel Ağ Saldırıları

- Sahte Yönlendirici ilanı mesajları nasıl engellenebilir?
  - Saldırı tespit sistemine tanıtılan geçerli yönlendirici ilanı mesajları tespit edilebilir.
    - Çok fazla manuel ayarlama gerektiriyor.

Yerel Ağ Saldırıları

- Yerel ağ saldırıları nasıl engellenebilir?
  - NDPMon (Neighbor Discovery Protocol Monitor)
    - IPv6 için ARPWatch uygulaması.
    - Yerel ağdaki komşu keşfi mesajlarını izler, geçersiz veya sahte komşu keşfi mesajlarını tespit eder.
    - Yönlendirici ilanı mesajlarında yer alan MAC adresi, bağlantılı yerel adres ve önek değerlerinin geçerli olup olmadığını kontrol eder.
    - Komşu ilanı (NA) ve komşu talebi (NS) mesajlarını bellekte tutar ve değişiklikleri bildirir.

NDPMon Örnek XML dosyası

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<?xml-stylesheet type="text/xsl" href="config.xsl" ?>
<!DOCTYPE config_ndpmon SYSTEM "/usr/local/etc/ndpmon/config_ndpmon.dtd">
<config_ndpmon>
        <ignor_autoconf>1</ignor_autoconf>
        <syslog_facility>LOG_LOCAL1</syslog_facility>
        <admin_mail>evyncke@cisco.com</admin_mail>
        <actions_low_pri>
                <sendmail>1</sendmail>
                <syslog>1</syslog>
        </actions_low_pri>
        <actions_high_pri>
                <sendmail>1</sendmail>
                <syslog>1</syslog>
        </actions_high_pri>
        <use_reverse_hostlookups>1</use_reverse_hostlookups>
```

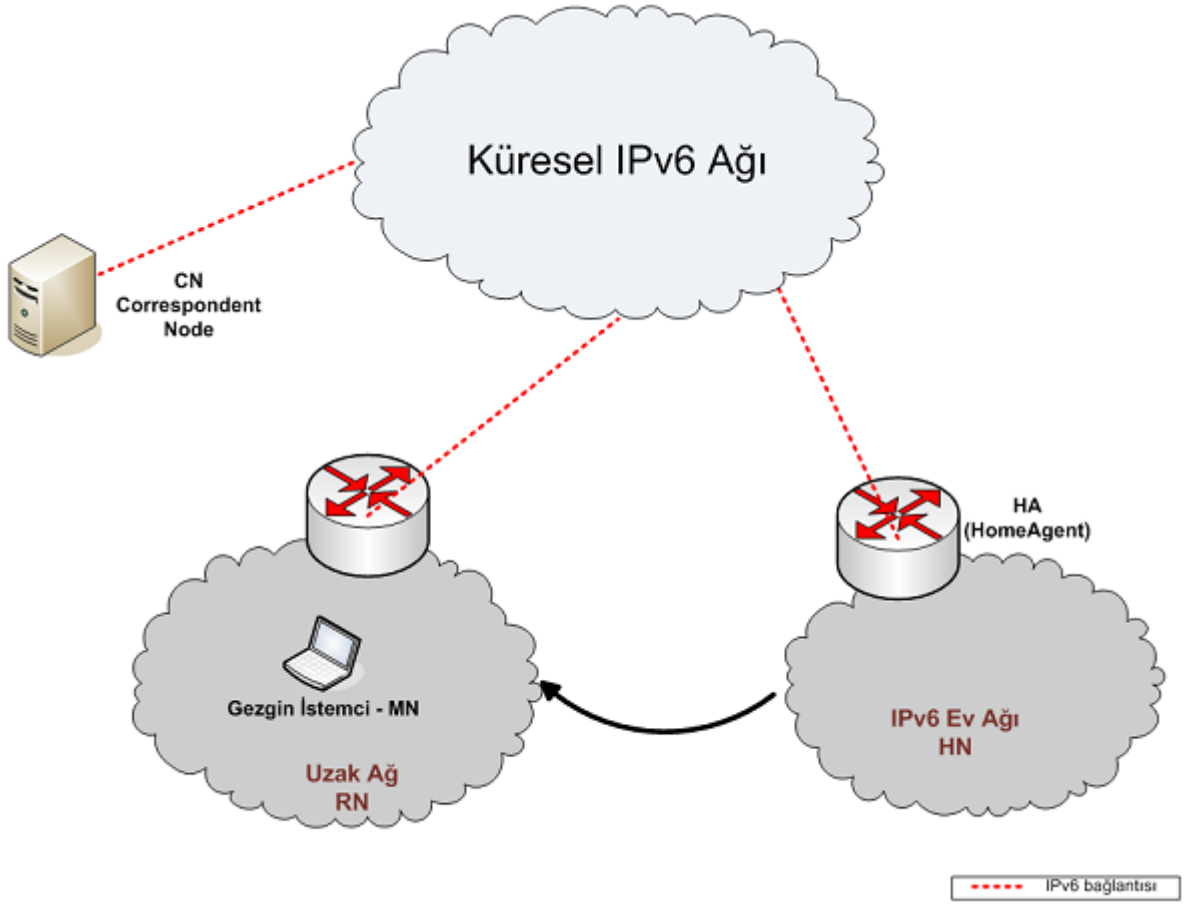
NDPMon Örnek XML dosyası

```
<routers>
        <router>
            <mac>00:04:27:fd:52:40</mac>
            <lla>fe80:0:0:0:204:27ff:fefd:5240</lla>
            <prefixes>
                <prefix
mask="64">2001:db8:0:10:0:0:0:0</prefix>
            </prefixes>
            <addresses/>
        </router>
    </routers>
</config_ndpmon>
```

Gezgin IPv6

- Bileşenler
  - Home Agent
  - Mobile Node
  - Correspondent Node
- Care Of Address (CoA)
- Binding Update (BU) ve Binding Acknowledgement (BA) mesajları
- Route Optimization
- Mobile Node - Home Agent arası tünel

Gezgin IPv6


Küresel IPv6 Ağı
CN
Correspondent
Node
HA
(HomeAgent)
Gezgin İstemci - MN
Uzak Ağ
RN
IPv6 Ev Ağı
HN
IPv6 bağlantısı

Gezgin IPv6

- Sahte MN
  - HA ve CoA IPv6 adresleri bilinen bir bağlantıda saldırgan sahte BU mesajları ile oturum ele geçirebilir.
  - HA ve MN arasında doğrulama ile çözülebilir.
- MN – CN BU saldırısı
  - MN ve CN arasındaki oturumun ele geçirilmesi

Gezgin IPv6

- Servis Dışı Bırakma saldırıları
  - HA ‘ya gönderilen BU mesajları ile servis dışı bırakılması
  - MN ‘ye sahte mobil önek gönderilmesi ile iletişiminin kesilmesi

Gezgin IPv6

- Saldırıların önlenmesi
  - HA – MN arası iletişimde IPsec kullanılmalı
    - Mesajlar şifrelenmeli ve doğrulanmalı
    - Dolaşılabilirlik ve IPsec desteği zayıf
      - Cisco cihazlarda yok.
      - BSD ve Linux ‘larda ayrı ayrı ele alınmalı.
  - MN – CN arasındaki iletişimde IPsec kullanılamaması.

IPv6 Geçiş Yöntemleri

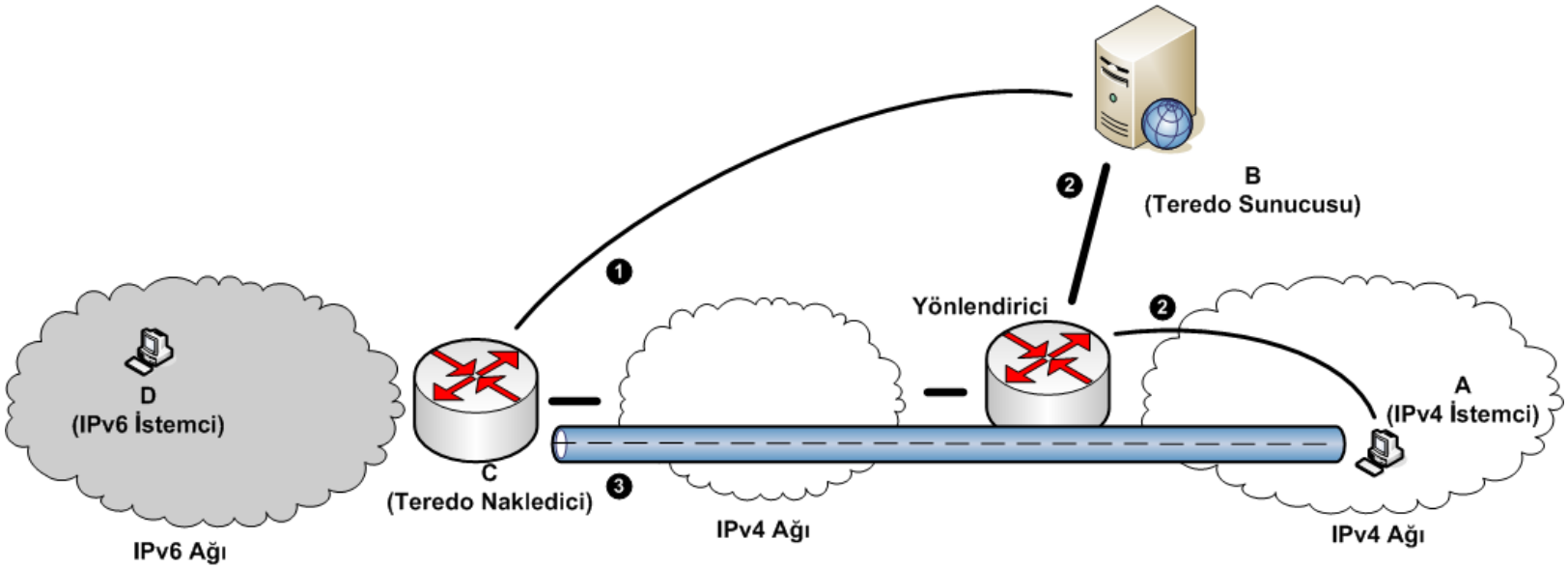
- Önerilen Geçiş Yöntemleri
  - Yalın IPv6
  - İkili Yığın
  - Tünelleme
    - Elle ayarlanmış tünelleme
    - 6to4
    - Teredo
  - Çeviri
    - Transport Relay Translation (TRT)

IPv6 Geçiş Yöntemleri

- İkili Yığın
  - Cihazlar hem IPv4 hem de IPv6 adresine sahiptir.
  - Her iki protokolden gelecek olan saldırılara karşı önlem alınmalı.
  - IPv4 ve IPv6 ağ yapılarının farklı olması problem oluşturmaktadır.
  - Cihazların her iki protokolü de desteklemesi performans açısından dezavantaj.
    - Yönlendiriciler hem IPv4 hem de IPv6 yönlendirme tablolarını tutmaktadır.

IPv6 Geçiş Yöntemleri

- Teredo
  - NAT arkasındaki istemcilerin IPv6 bağlantı sağlaması.



IPv6 Geçiş Yöntemleri

- Tünelleme
  - Elle ayarlanmış statik tüneller, dinamik tünellere göre daha güvenli.
  - IPv4 içinde IPv6 paketleri, paket sarmalaması açıldıktan sonra kontrol edilmeli
    - Tünel içinde bağlantılı yerel adrese, multicast adreslerine paket gönderilebilir = keşif saldırıları.
  - Dinamik tünelleme bileşenlerine servis dışı bırakma saldırıları
    - 6to4 Nakledici yönlendirici
    - Teredo sunucu
    - Teredo Nakledici Yönlendirici
  - Teredo NAT yapısında delik açma

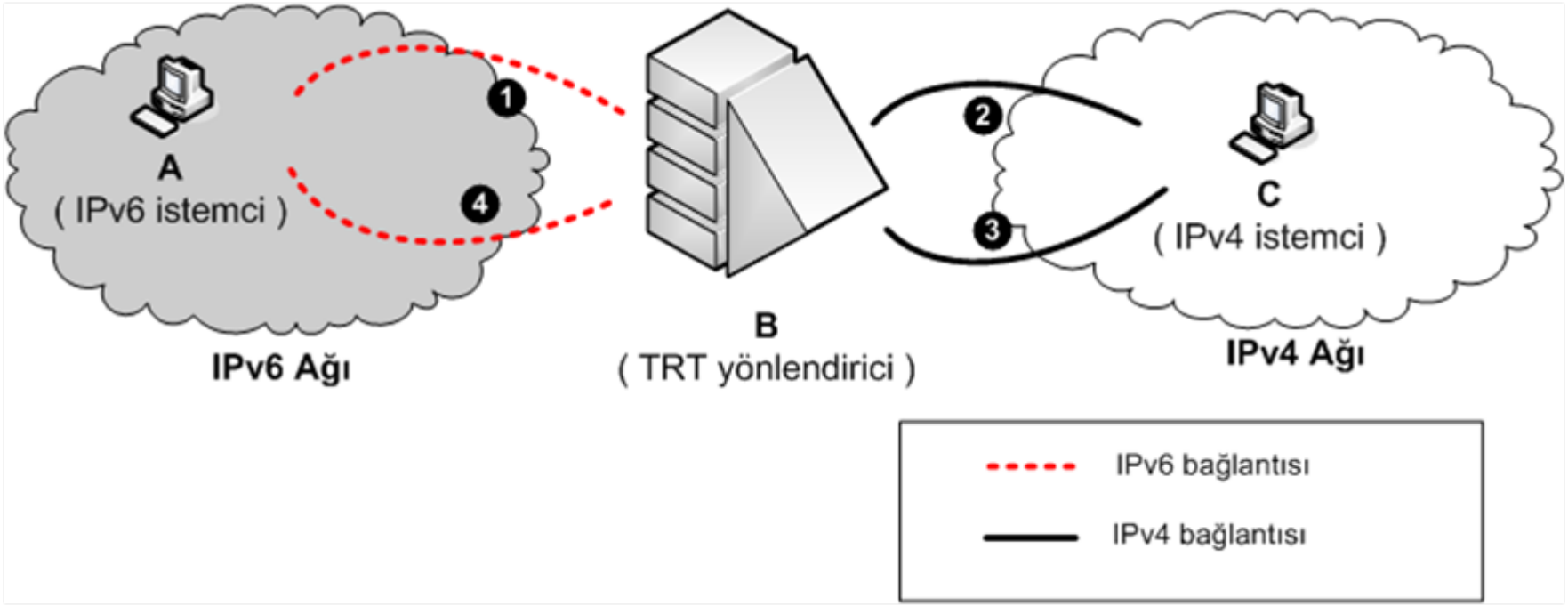
IPv6 Geçiş Yöntemleri

- Tünelleme
  - Ağda protokol 41 kontrol edilmeli.
  - Windows Vista ve Windows 7 otomatik IPv6 desteğine sahip. İstemci
    - Gerçek IPv4 adresine sahip ise 6to4 ile
    - Sanal IPv4 adresine sahip ise Teredo ile

    IPv6 ağına bağlanıyor.

IPv6 Geçiş Yöntemleri

- Çeviri
  - Transport Relay Translator (TRT)



IPv6 Geçiş Yöntemleri

- Çeviri
  - Servis Dışı bırakma saldırısı
    - TRT yönlendiricisi durum bilgisi tutuyor (stateful).
  - Çeviri yötemleri uçtan uca yapıyı bozduğu için IPsec desteklemiyor.

Sonuç ve Değerlendirme

- Güvenlik duvarı kuralları ve erişim kontrol listeleri IPv6 ‘ya göre düzenlenmeli.
- IPv6 desteği verilmemiş bir ağ, IPv6 protokolünü kullanan saldırı araçlarına karşı güvenlidir önermesi yanlıştır.
  - Otomatik IPv6 desteği veren işletim sistemleri ve tünelleme yöntemleri.
- Ağdaki cihazların IPv6 desteği olup olmadığı, varsa hangi seviyede IPv6 desteği verdiği incelenmelidir.
- Kullanılan geçiş yöntemlerine yönelik güvenlik önlemleri alınmalı.

Son Söz

- IPv6 geçiş sürecinde en kritik nokta
  - IPv6 güvenlik konularının ve
  - ağdaki IPv6 kullanımının

  farkında olmaktır!

Teşekkürler

TÜBİTAK ULAKBİM

IPv6 HAZIR
Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi

BTK BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

TÜBİTAK ULAKBİM

1982 Gazi Üniversitesi

Çanakkale Onsekiz Mart Üniversitesi 1992