

“Yeni Nesil İnternet Protokolü , IPv6”



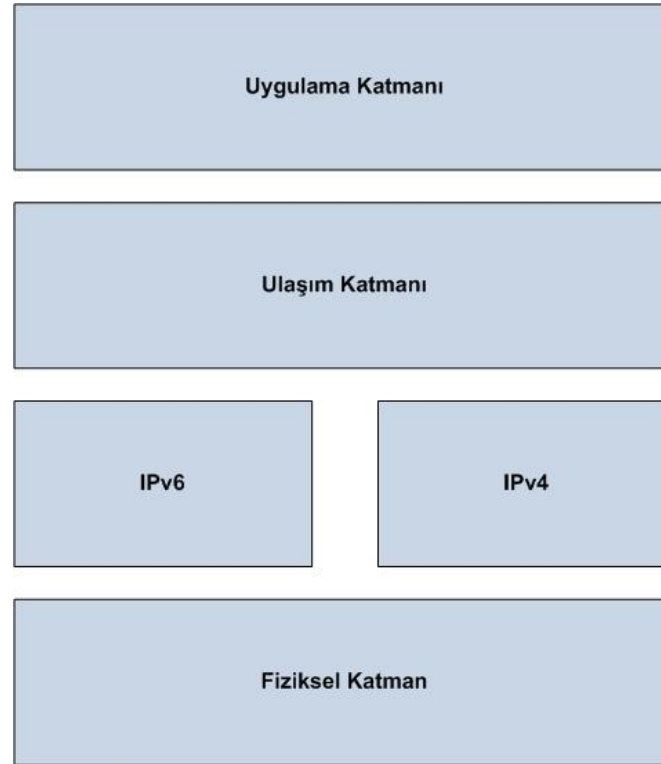
Beyhan ÇALIŞKAN (ULAKBİM)



- IPv6 geçiş yöntemleri
 - İkili yığın (dual stack)
 - Tünelleme
 - Çevirici (translator)
- Geçiş yöntemlerinde güvenlik
- Sorular



- İkili yığın



- İkili yığın -> güvenlik
 - İkili yığın mimarisi, diğer IPv6 geçiş yöntemlerinin de merkezinde !!
 - Modern işletim sistemlerinde (Microsoft Vista, Linux, Mac OS X, vb) IPv6 desteği varsayılan olarak açıktır.
 - IPv4 için alınan bütün güvenlik önlemleri IPv6 için de alınmalıdır.
 - IPv6 desteği bulunmayan ağlarda bile, ikili yığın düğümler IPv6 saldırılarına açık olabilir.



CORE-2007-0219:

OpenBSD's IPv6 mbufs remote kernel buffer overflow



IPv6 Geçiş Yöntemleri

CVE	Tarih	Uygulama / OS
2009-3641	10/28/2009	Snort
2009-3164	09/10/2009	Sun Solaris10, OpenSolaris
2009-2698	08/27/2009	Linux çekirdeği
2009-2208	06/25/2009	Freebsd 6.3, 6.4, 7.1, 7.2
2009-2187	06/25/2009	Sun Solaris10, OpenSolaris
2009-1906	06/03/2009	IBM DB2
2009-1360	04/22/2009	Linux çekirdeği
2009-0634	03/27/2009	Cisco IOS 12.3 - 12.4
2009-0633	02/04/2009	Cisco IOS 12.3 - 12.4
2009-0418	02/04/2009	HP -UX B.11.(11-23-31)
2009-0304	01/27/2009	Sun Solaris10, OpenSolaris
2008-3816	10/23/2008	Cisco ASA 5500, PIX 7.2.4.(9-10)
2008-4404	10/03/2008	IBM zSeries servers
2008-2476	10/03/2008	FreeBSD, OpenBSD, NetBSD, Force10 FTOS, Juniper JUNOS ve Wind River
2008-3530	09/05/2008	FreeBSD, NetBSD
2008-3686	08/14/2008	Linux çekirdeği
2008-1576	06/02/2008	Mac OS X
2008-2136	05/16/2008	Linux çekirdeği
2008-2085	05/12/2008	SIPp 3.1
2008-1153	03/27/2008	Cisco IOS 12.(1,2,3,4)
2008-1057	02/28/2008	OpenBSD 4.2
2008-0177	02/07/2008	KAME Project
2008-0630	02/06/2008	MPlayer
2008-0352	01/08/2008	Linux çekirdeği



- Tünelleme yöntemleri



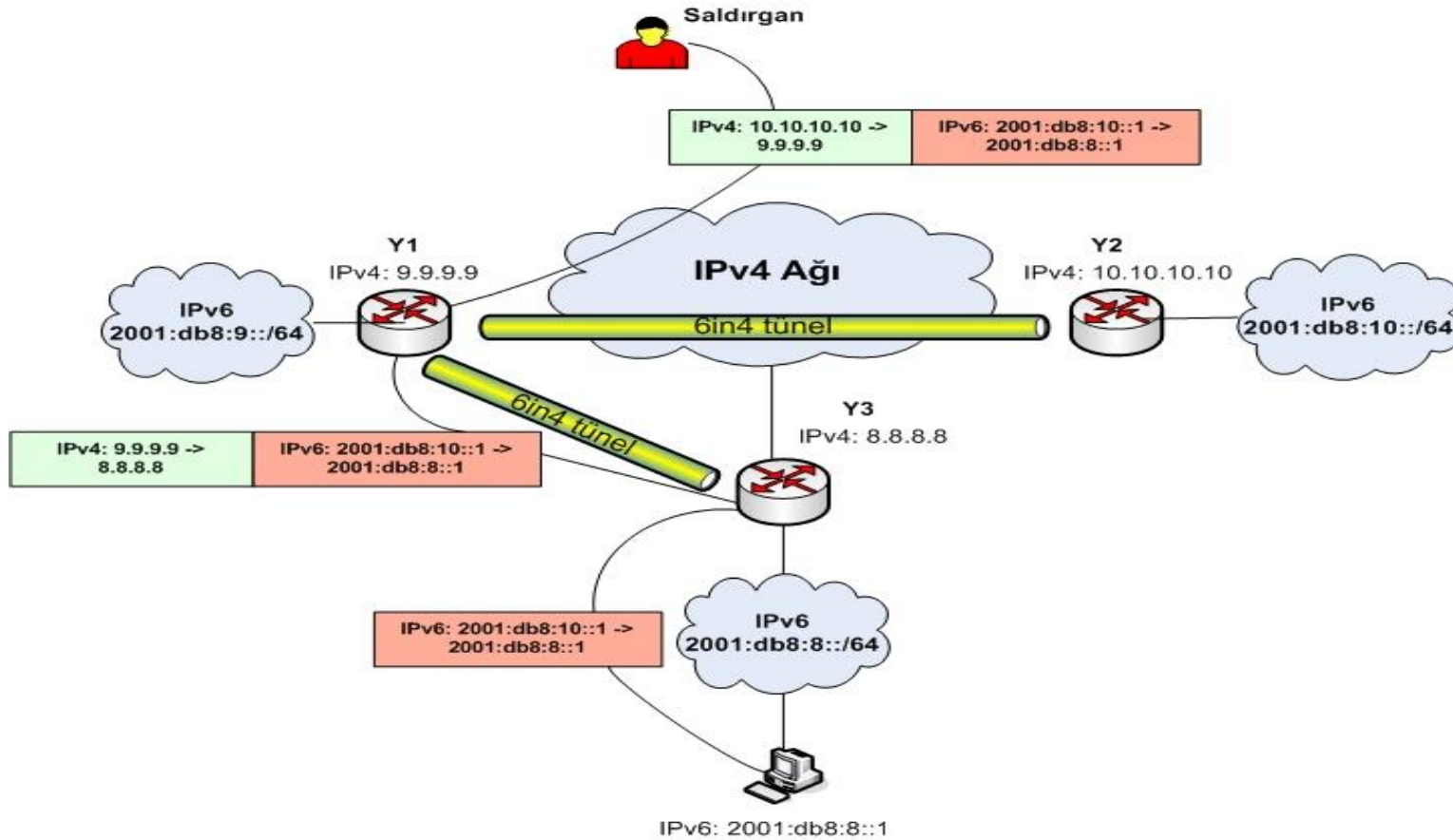
- Configured tunneling
- Automatic tunneling
- 6 to 4
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)
- Tunnel Broker
- Teredo
- DSTM
- Cisco 6PE
- 6 over 4



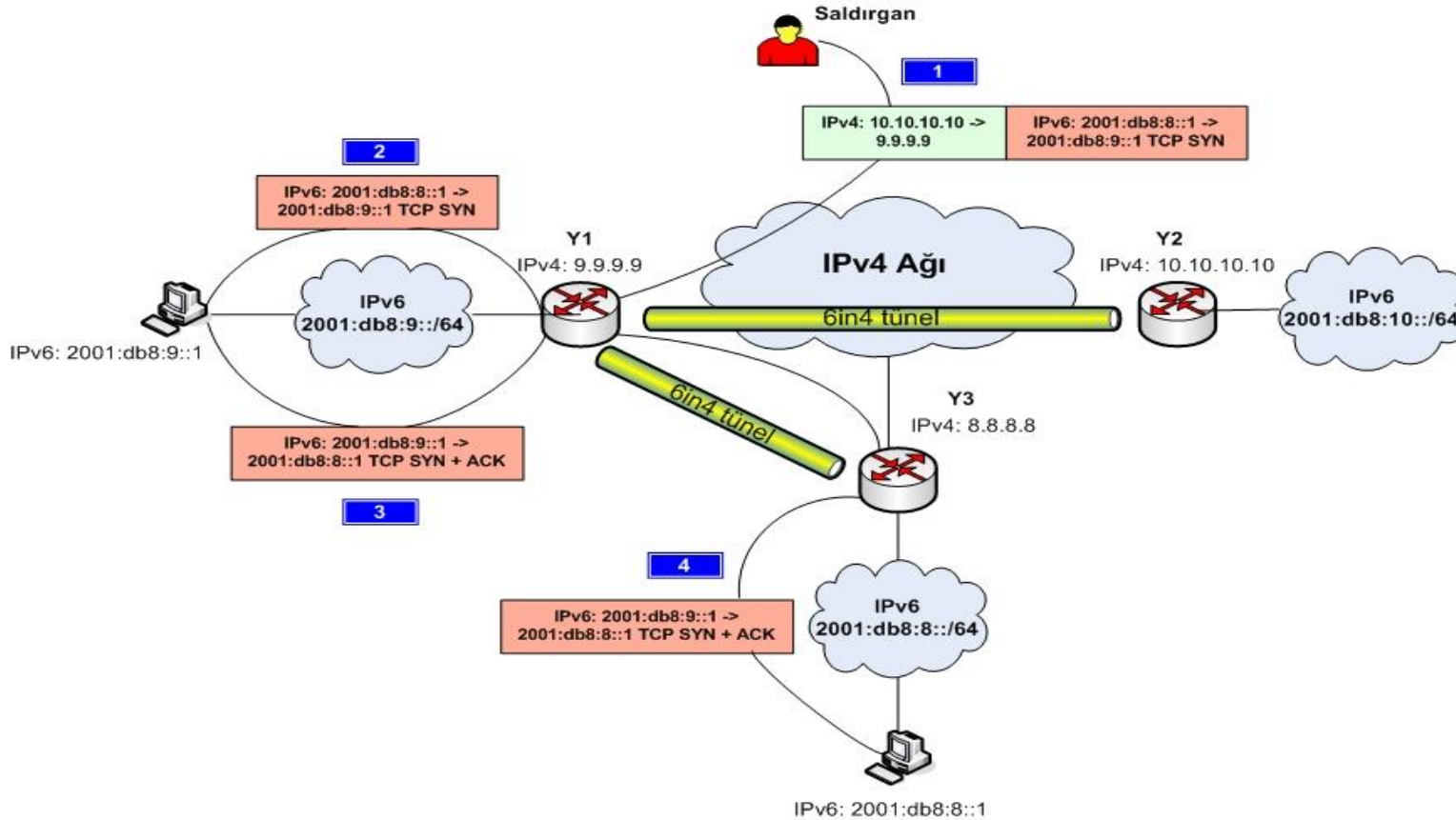
- **Tünelleme yöntemleri -> güvenlik**
 - Genel olarak tünelleme yöntemi kullanan tüm geçiş mekanizmaları ağda güvenlik sorunları oluşturmaktadır.
 - Tünelleme mekanizmalarının hiçbirinde kimlik doğrulama, bütünlük kontrolü ve gizlilik öğeleri yerleşik olarak bulunmaz.
 - Erişim kontrol listeleri ve ateş duvarı kurallarıyla korunan bir ağa, başlığı bu kurallara uyan bir paket tünel içerisinden gönderilirse, iç ağa erişim sağlanabilir.
 - Tünel enjeksiyon + dinleme ...



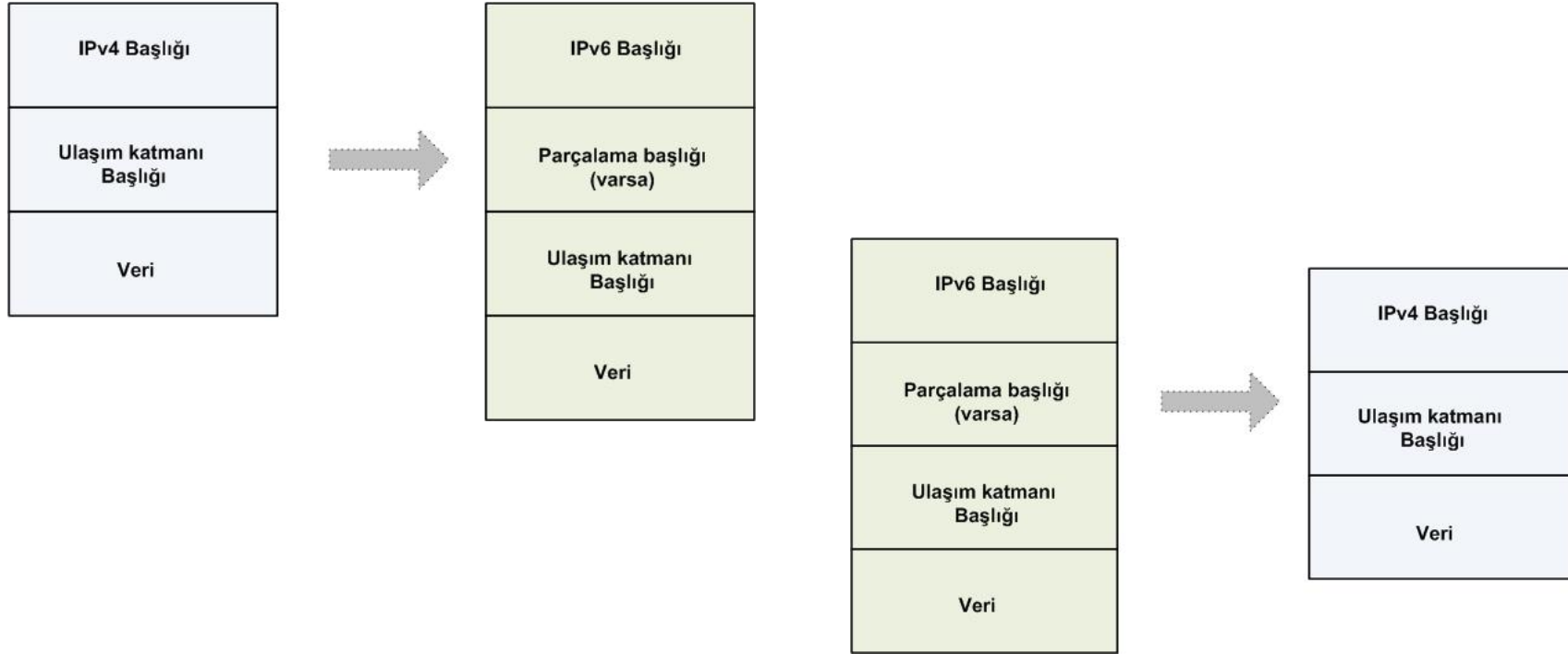
- Tünelleme yöntemleri -> güvenlik



- Tünelleme yöntemleri -> güvenlik



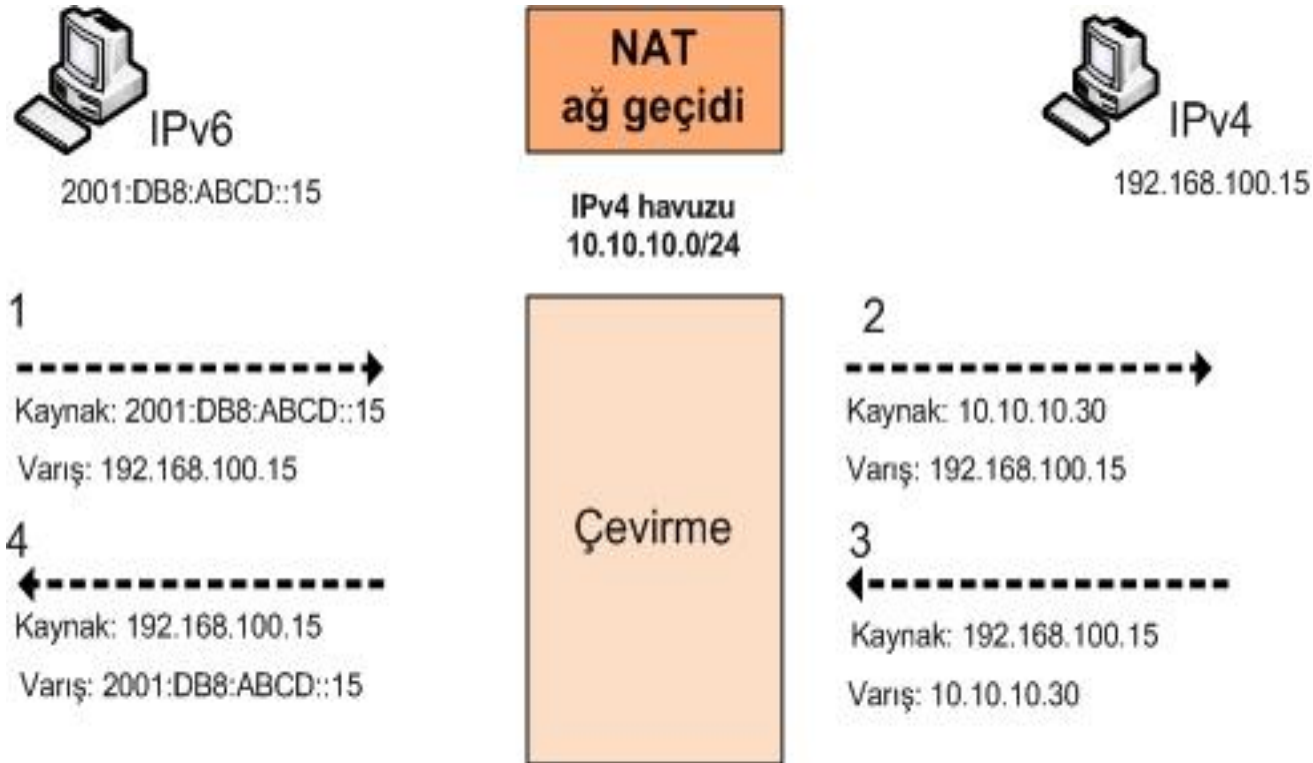
- Çevirici yöntemleri



- Çevirici yöntemleri
 - SIIT (Stateless IP/ICMP Translation)
 - NAT-PT (Network Address Translation-Protocol Translation)
 - Bump in the Stack (BIS)
 - Bump in the API (BIA)
 - Transport Relay Translator (TRT)
 - SOCKS



- Çevirici yöntemleri



- **Çevirici yöntemleri -> güvenlik**
 - Çevirici yöntemlerinin IPv6 geçiř çalışmalarının ilk zamanlarında geliştirildiđi ve ikili yığın çalışmayan eski cihaz ve işletim sistemleri için tasarlandıđı unutulmamalıdır.
 - Kullanılan çeviriciler DoS saldırılarının hedefi olabilir.
 - Uçtan uca güvenlik yok (IPsec)



Sorular



Beyhan ÇALIŞKAN

[beyhan @ ulakbim.gov.tr](mailto:beyhan@ulakbim.gov.tr)

312 298 93 76

