Comparing IPv4 to IPv6 VPN encryption

eng. Nikolay Milovanov
CCIE SP# 20094
eng. Georgi Ribarski
CCIE Security #20584

Нов български университет

Agenda

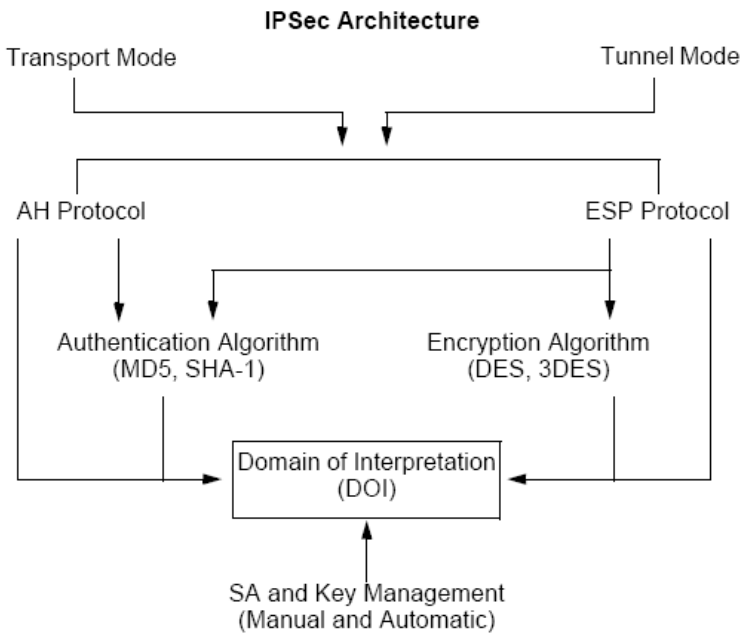
- IPSEC VPN encryption overview
- Changes that comes with IPv6
- Demo
- Tunnel transformation

IPSEC VPN encryption overview

IPSEC Concepts

- A virtual private network (VPN) provides a means for securely communicating between remote computers across a public wide area network (WAN), such as the Internet.
- A VPN connection can link two local area networks (LANs) or a remote dialup user and a LAN. The traffic that flows between these two points passes through shared resources such as routers, switches, and other network equipment that make up the public WAN. To secure VPN communication while passing through the WAN, the two participants create an IP Security (IPSec) tunnel1.
- An IPSec tunnel consists of a pair of unidirectional Security Associations (SAs)—one at each end of the tunnel—that specify the security parameter index (SPI), destination IP address, and security protocol (Authentication Header or Encapsulating Security Payload) employed.
- Through the SA, an IPSec tunnel can provide the following security functions:
  - Privacy (via encryption)
  - Content integrity (via data authentication)
  - Sender authentication and—if using certificates—nonrepudiation (via data origin authentication)

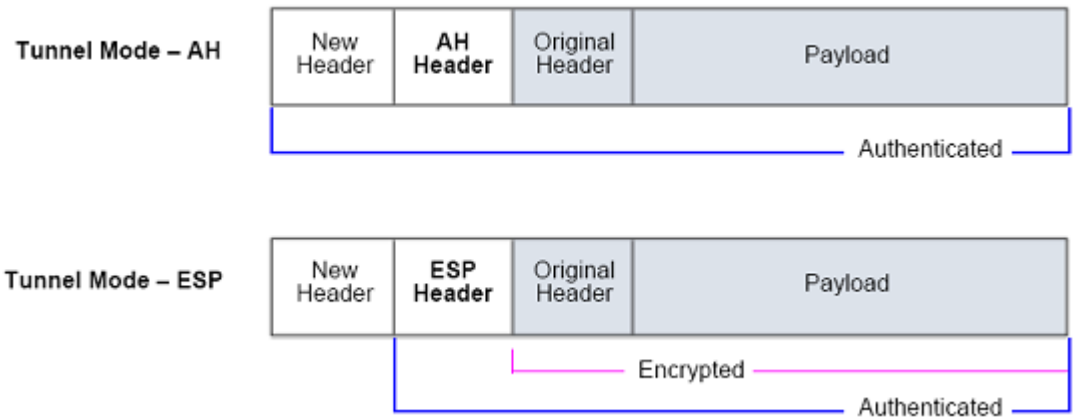
IPSEC Architecture



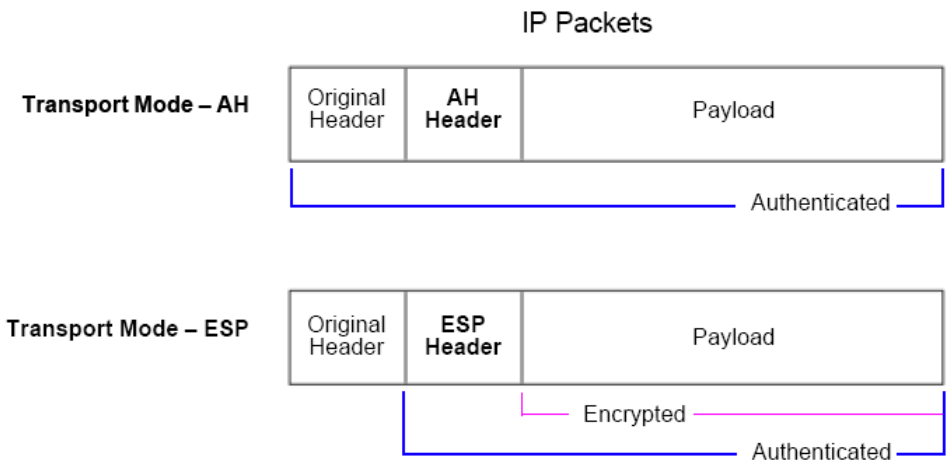
- Protocols
  - ESP
  - AH
- Modes
  - Tunnel
  - Transport

IPSEC modes

- Tunnel mode



- Transport mode



IPSEC protocols - AH

- Authentication Header (AH)
  - Provides a means to verify the authenticity/integrity of the content and origin of a packet. You can authenticate the packet by the checksum calculated via a hash-based message authentication code (HMAC) using a secret key and either MD5 or SHA-1 hash functions.
  - **Message Digest version 5 (MD5)**—An algorithm that produces a 128-bit hash (also called a digital signature or message digest) from a message of arbitrary length and a 16-byte key. The resulting hash is
  - used, like a fingerprint of the input, to verify content and source authenticity and integrity.
  - **Secure Hash Algorithm-1 (SHA-1)**—An algorithm that produces a 160-bit hash from a message of arbitrary length and a 20-byte key. It is generally regarded as more secure than MD5 because of the larger hashes it produces.

IPSEC protocols - ESP

- Encapsulating Security Payload (ESP) protocol
  - Provides a means to ensure **privacy (encryption),** and **source authentication** and **content integrity (authentication)**.
  - With ESP, you can encrypt and authenticate, encrypt only, or authenticate only. For encryption, you can choose either of the following encryption algorithms:
  - **Data Encryption Standard (DES)**—A cryptographic block algorithm with a 56-bit key.
  - **Triple DES (3DES)**—A more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key. DES provides a significant performance savings but is considered unacceptable for many classified or sensitive material transfers.
  - **Advanced Encryption Standard (AES)**—An emerging encryption standard which, when adopted by Internet infrastructures worldwide, will offer greater interoperability with other network security devices.

Key Management

- Manual Key
  - Administrators at both ends of a tunnel configure all the security parameters.
  - This is a viable technique for small, static networks where the distribution, maintenance, and tracking of keys are not difficult.
  - However, safely distributing Manual Key configurations across great distances poses security issues.

Key Management through – AutoKey IKE

- AutoKey IKE

  Supports the automated generation and negotiation of keys and security associations using the Internet Key Exchange (IKE) protocol..

  - *AutoKey IKE with Preshared Keys*
  - *AutoKey IKE with Certificates*

Security Association - SA

- SA is a unidirectional agreement between the VPN participants regarding the methods and parameters to use in securing a communication channel. Full bidirectional communication requires at least two SAs, one for each direction.
- An SA groups together the following components for securing communications:
  - Security algorithms and keys
  - Protocol mode (transport or tunnel)
  - Key management method (Manual Key or AutoKey IKE)
  - SA lifetime

Tunnel Negotiation – Phase 1

Phase 1 consists of the exchange of proposals for how to authenticate and secure the channel. The exchanges may be in one of these modes:

- **Main mode** - The initiator and recipient send three two-way exchanges (six messages total) to accomplish the following services:
  - First exchange, (messages 1 and 2): Propose and accept the encryption and authentication algorithms.
  - Second exchange, (messages 3 and 4): Execute a Diffie-Hellman exchange, and the initiator and recipient each provide a nonce (randomly generated number).
  - Third exchange, (messages 5 and 6): Send and verify their identities.
- **Aggressive mode** – The initiator and recipient accomplished the same but only in two exchanges:
  - First message: The initiator proposes the SA, initiates a Diffie-Hellman exchange, and sends a nonce and its IKE identity.
  - Second message: The recipient accepts the SA, authenticates the initiator, and sends a nonce, its IKE identity, and, if using certificates, the recipient's certificate.
  - Third message: The initiator authenticates the recipient, confirms the exchange, and, if using certificates, sends the initiator's certificate.
- NB!!! Because the participants' identities are exchanged in the clear (in the first two messages), **Aggressive mode** does not provide identity protection.

Tunnel Negotiation – Phase 1

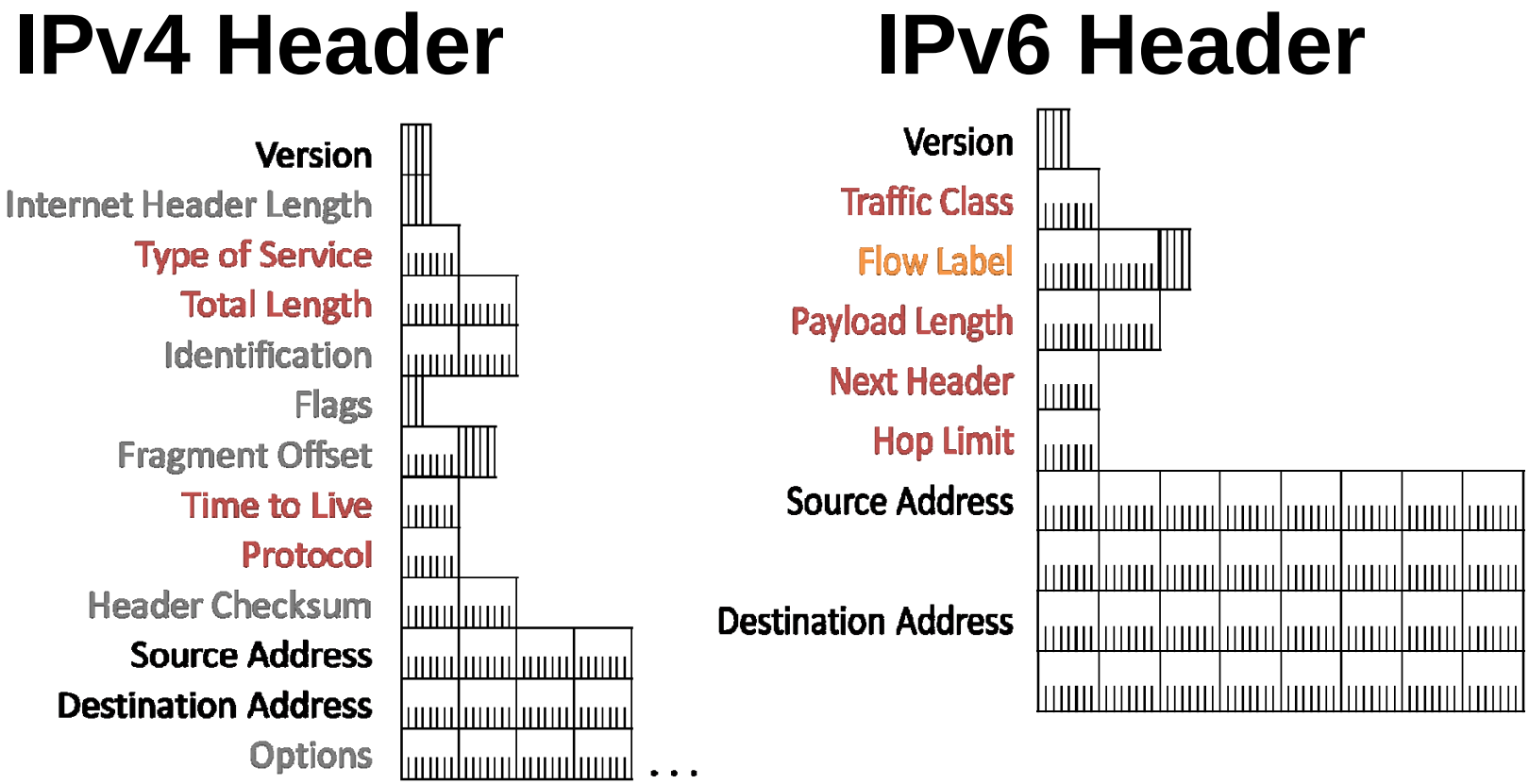
- Using either mode, the participants exchange proposals for acceptable security services such as:
  - Encryption algorithms (DES and 3DES) and authentication algorithms (MD5 and SHA-1).
  - A Diffie-Hellman Group (A Diffie-Hellman exchange allows the participants to produce a shared secret value.
  - Preshared Key or RSA/DSA certificates
- Typical Phase 1 proposals are:
  - **Standard:** pre-g2-aes128-sha and pre-g2-3des-sha
  - **Compatible:** pre-g2-3des-sha, pre-g2-3des-md5, pre-g2-des-sha, and pre-g2-des-md5
  - **Basic:** pre-g1-des-sha and pre-g1-des-md5

Tunnel Negotiation – Phase 2

- After the participants have established a secure and authenticated channel, they proceed through Phase 2, in which they negotiate the SAs to secure the data to be transmitted through the IPSec tunnel.
- Like the process for Phase 1, the participants exchange proposals to determine which security parameters to employ in the SA. A Phase 2 proposal specify:
  - Security protocol either Encapsulating Security Payload (ESP) or Authentication Header (AH)
  - Encryption and authentication algorithms.
  - If Perfect Forward Secrecy (PFS) is enabled shall also be specified a Diffie-Hellman group.
  - Replay Protection
- Typical Phase 2 proposals are:
  - Standard: g2-esp-3des-sha and g2-esp-aes128-sha
  - Compatible: nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, and nopfs-esp-des-md5
  - Basic: nopfs-esp-des-sha and nopfs-esp-des-md5

Changes in IPv6

IPv4 and IPv6 Headers



Implementing IPSEC in IPv6 (1)

- In IPv4, IPSEC is implemented as a supplement to the current IP standard. For the purpose 2 new protocols were developed:
  - AH protocol
  - ESP protocol
- In IPv6 we have pretty much the same but the protocols are integrated into the standard itself and instead of additional protocols we have extension headers:
  - AH authentication header
  - ESP extension header.

Implementing IPSEC in IPv6 (2)

- Everything else is unchanged e.g
  - Modes (tunnel and transport)
  - Key exchange mechanism
    - Autokey
    - Manual
  - Security Association
  - Phase 1 and 2 negotiations

Demo

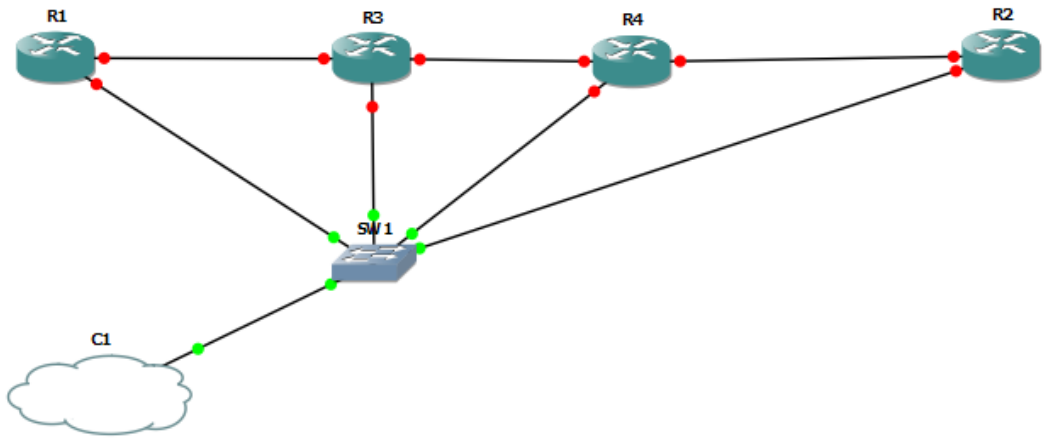
Demo setup

- HW (Laptop with 3G RAM)
- SW
  - Dynamips
  - Dynagen
  - GNS3 0.71
  - Wireshark 1.2.8 (SVN Rev 32676)

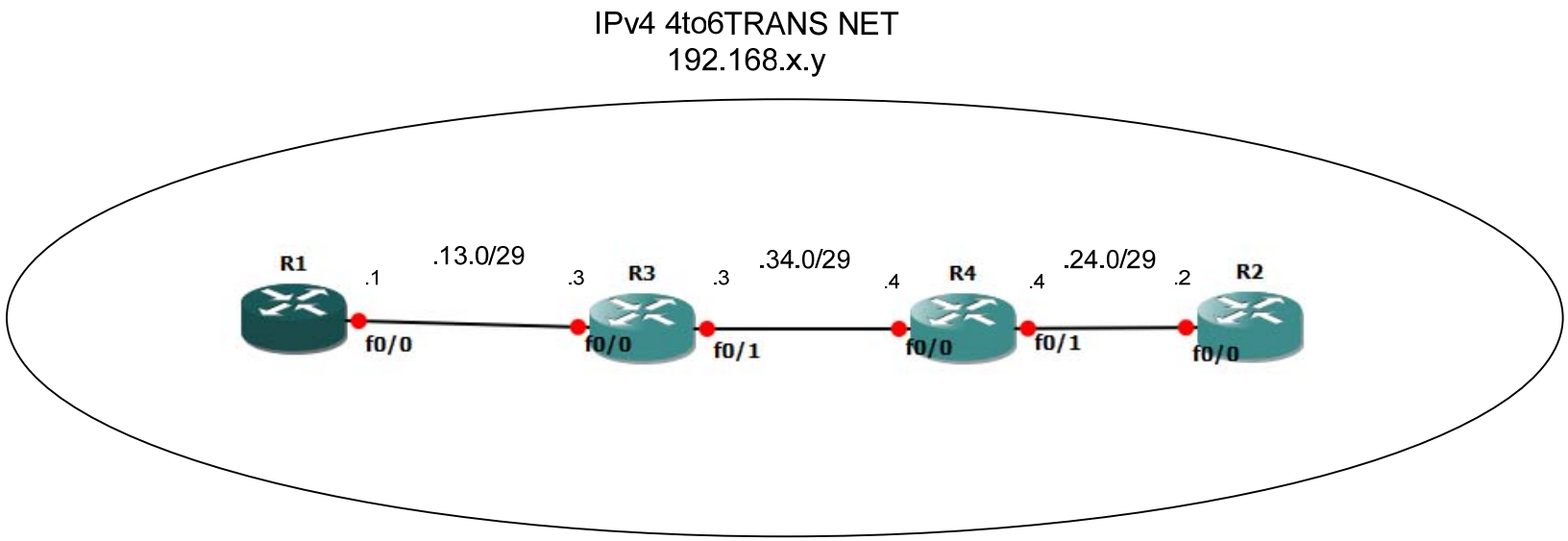
Physical topology

We have pretty straight setup:

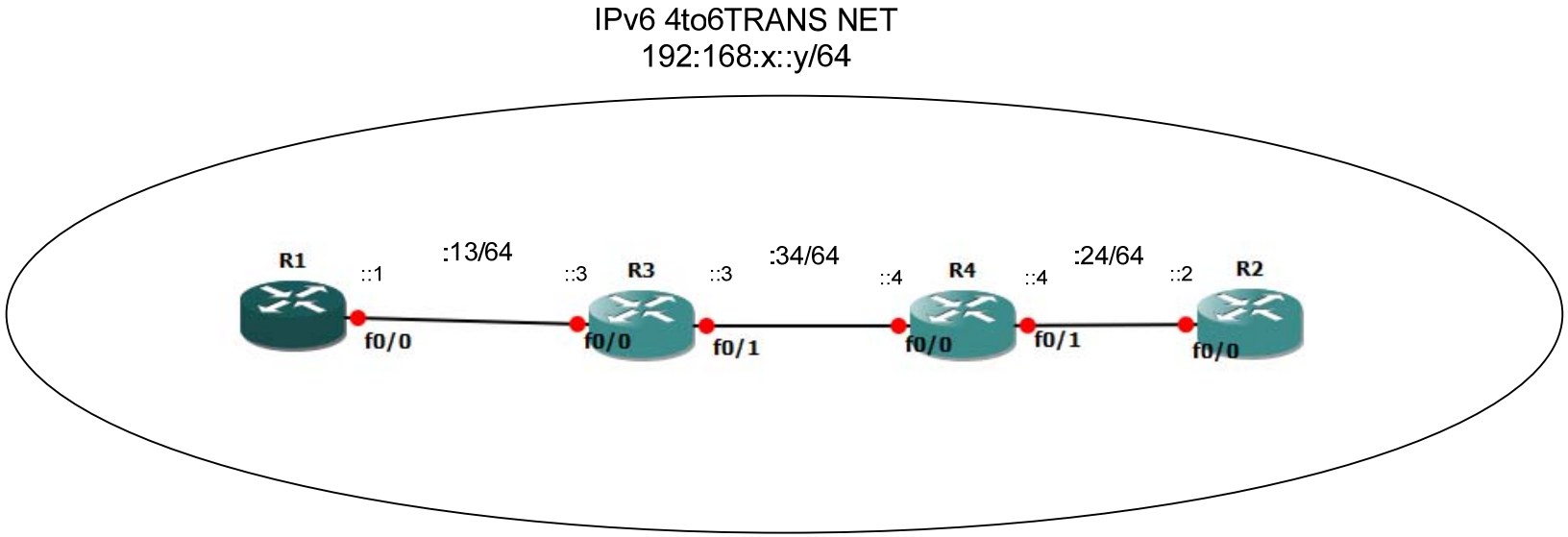
- 4 routers
- Only Fast Ethernet Interfaces
- Will may build tunnels between any two routers



IPv4 network



IPv6 network



Config – IPv4

```
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 43200
 crypto isakmp keepalive 10
!
crypto ipsec security-association idle-time 300
crypto ipsec df-bit clear
!
crypto ipsec transform-set 3DES_SHA esp-3des
       esp-sha-hmac
!
crypto ipsec profile tunnel100VPN
 set transform-set 3DES_SHA
!
crypto isakmp key 0 test321! address 192.168.13.1
```

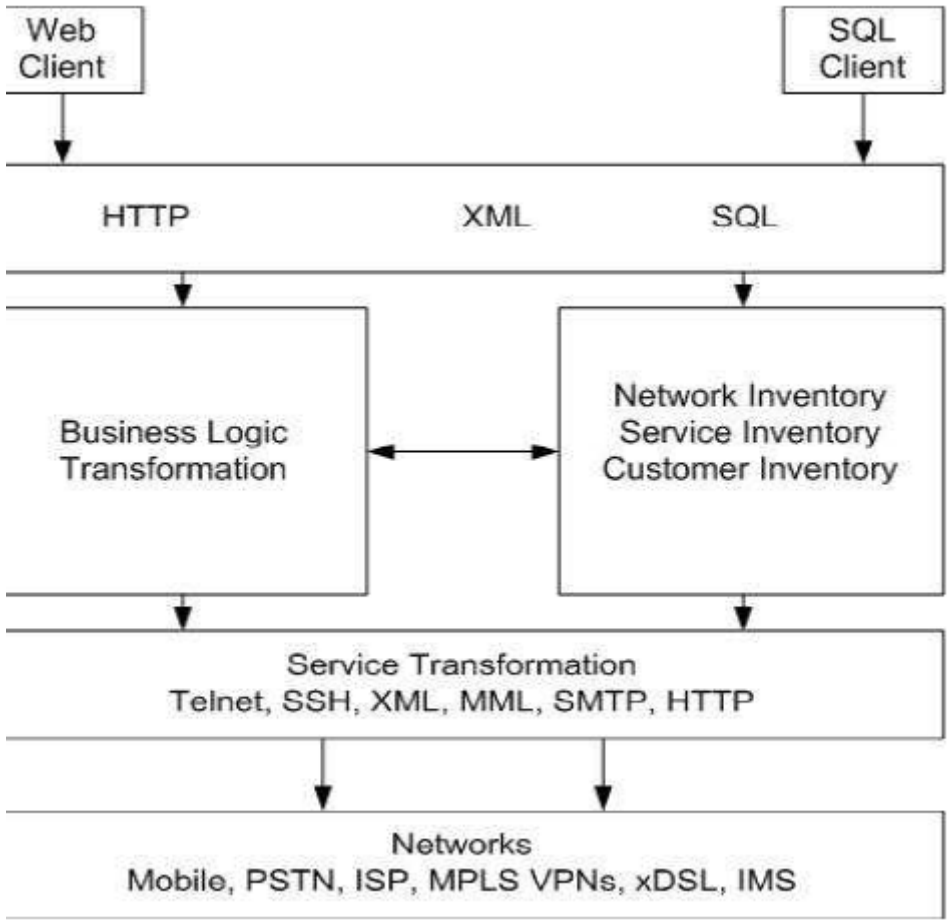
```
interface Tunnel200
 ip address 10.10.12.2 255.255.255.0
 tunnel source fa0/0
 tunnel destination 192.168.13.1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile tunnel100VPN
```

Config – IPv6

```
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 43200
 crypto isakmp keepalive 10
!
crypto ipsec security-association idle-time 300
crypto ipsec df-bit clear
!
crypto ipsec transform-set 3DES_SHA esp-3des
       esp-sha-hmac
!
crypto ipsec profile tunnel100VPN
 set transform-set 3DES_SHA
!
crypto isakmp key 0 test321! address ipv6
       192:168:24::2/64
```

```
interface Tunnel100
 no ip address
 ipv6 address 10:10:12::1/64
 tunnel source fa0/0
 tunnel destination 192:168:24::2
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile tunnel100VPN
```

Tunnel transformation



Comparing IPv4 to IPv6 VPN encryption

eng. Nikolay Milovanov
email: *nmil@niau.org*

eng. Georgi Ribarski
email: g.ribarski@gmail.com

Нов български университет