IPV6 AND SECURITY

Yi-Hsun Lai

Outline

- Why do we need IPv6
- Introduction to IPv6
- IPv6/IPv4 Transition
  - IPv4/IPv6 Dual Stack Schemes
  - IPv4/IPv6 Tunnel Mechanism
- IPv6 Tunnel Broker
  - Using Tunnel Broker

Why need IPv6

- 5 percent of the world's population uses 60 percent of the allocable IPv4 address space
- 20 percent of the world population wants to access to the Internet
- Huge address space
  - The IPv6 address space uses a 128-bit address
  - 340,282,366,920,938,463,463,374,607,431,768,211,456
  - 6.65 x 10^{23} addresses in every square meter on earth

Why need IPv6

- Header format simplification.
- IPv6 has been designed to be extensible by introducing a more flexible header structure
- survive a longer time in current complex networks than IPv4
- Both cellular and wireless networks have been further developed.

IPv6 improvement (1)

- Expanded Addressing Capabilities
  - IPv6 increases the IP address size from 32 bits to128 bits, to provide more levels of addressing hierarchy, a much greater number of addresses.
- Header Format Simplification
  - The simple IPv6 header makes the IPv6 packet faster at processing and more effective.

IPv6 improvement (2)

- Improved Support for Extensions and Options
  - More efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.
- Flow Labeling Capability
  - Some special traffic flows need special handling such as no-default quality of service or real-time service.

IPv6 improvement (3)

- Authentication and Privacy Capabilities
  - Extensions to support authentication, data integrity, and data confidentiality are specified for IPv6.
- Neighbor Discovery and Address Auto-configuration
  - Address Auto configuration: One of the most useful features of IPv6
  - Plug them into your network, and each of them will automatically be assigned a valid IPv6 address.
  - Find the information of the neighbor which is connecting with the device.

IPv6 Security features

- IPSec
  - Option in IPv4, require in IPv6
- SEND (SEcuring Neighbour Discovery)
  - Protection against Neighbor Discovery-based denial of service (DoS) attacks by nodes
- AAAv6
  - Provide Authentication, Authorization and Accounting

Attacks against IPv6

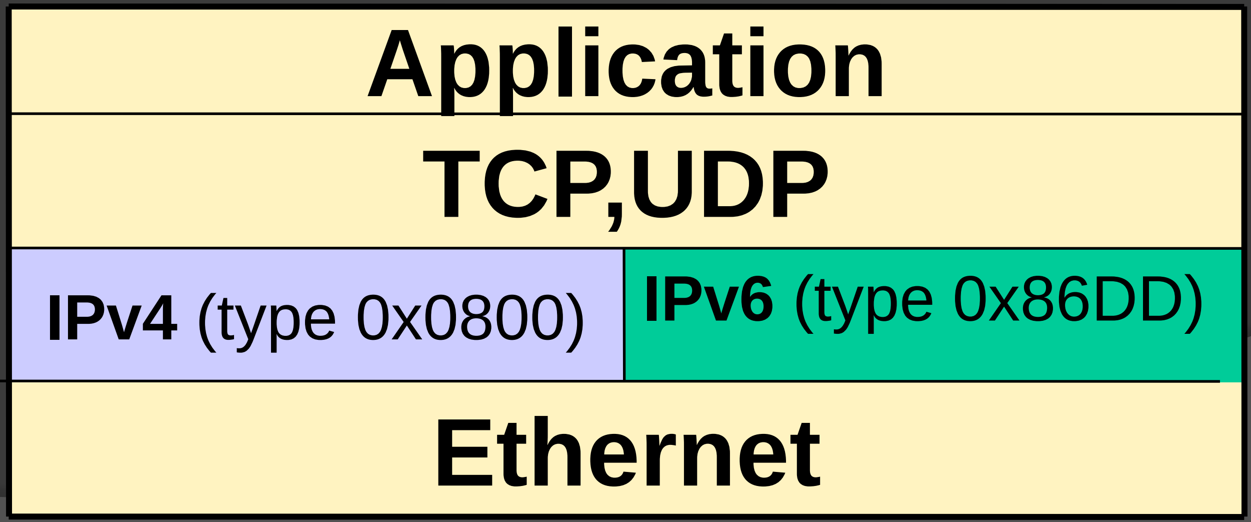
- DoS attacks
  - Attacker causes congestion on victim’s computer/network
- Hijack Attacks
  - Attacker gains unauthorized access to network.
- Impersonation
  - Packet forgery
- Man In the Middle
  - Snooping
  - Data Insertion/Deletion

IPv4-to-IPv6 Transition

- Today, most of the world has already been adopting IPv6
- Develop a well-planned transition mechanism to ensure IPv6 can coexist with IPv4.
  - IPv4/IPv6 Dual Stack Schemes
  - IPv4/IPv6 Tunnel Mechanism
  - Translate IPv4 headers to IPv6 headers and vice versa

IPv4/IPv6 Dual Stack Schemes

- Running IPv4 and IPv6 concurrently.
- End-hosts and network devices run both protocols.
- Dual-stack device will have to tackle the vulnerabilities of both protocols



Application

TCP,UDP

IPv4 (type 0x0800) | **IPv6** (type 0x86DD)

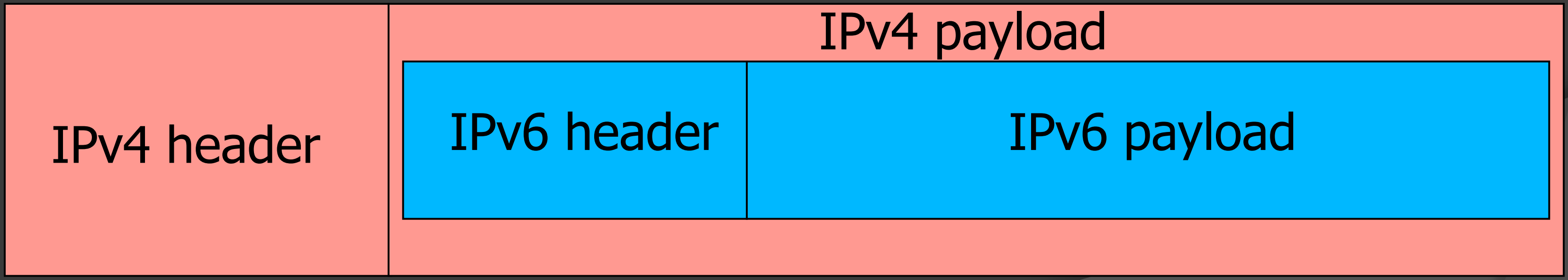
Ethernet

IPv4 / IPv6 Tunnel Mechanism

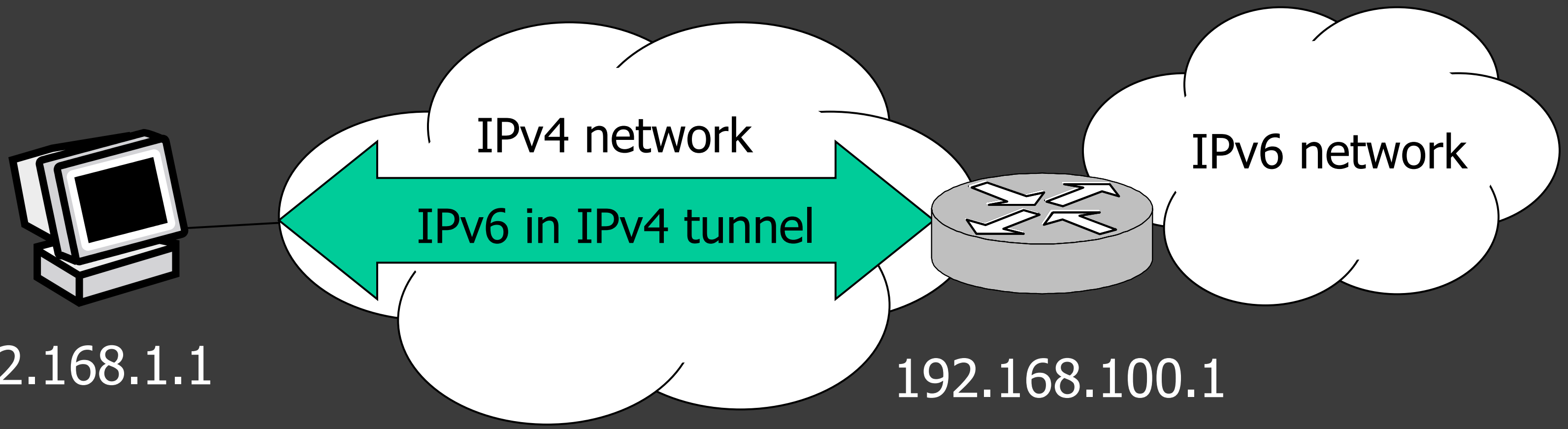
- Configured Tunnel (Manual)
- 6to4 Tunnel (Automatic)
- Tunnel broker
  - Defined in RFC3053
  - Client must support Dual-stack schemes

6to4 Tunneling (1)

- RFC3056 Connection of IPv6 domains via IPv4 clouds (6to4)
- 6to4 tunneling is a method we used when an end user wants to connect to IPv6 environment using their own IPv4 connection.
- It encapsulates IPv6 packets inside IPv4 packets for transmission over an IPv4 network



6to4 Tunneling(2)



IPv4 network

IPv6 in IPv4 tunnel

IPv6 network

192.168.1.1

192.168.100.1

6to4 prefix: 2002:c0a8:0101::/48

2002:c0a8:6401::/48

Security Issues (1)

- 6to4 routers do not check the data that is contained within the packets
- No trust mechanism exists between 6to4 routers and 6to4 relay routers.
- 6to4 architecture used to participate in DoS or reflected DoS, making another attack harder to trace

Security Issues (2)

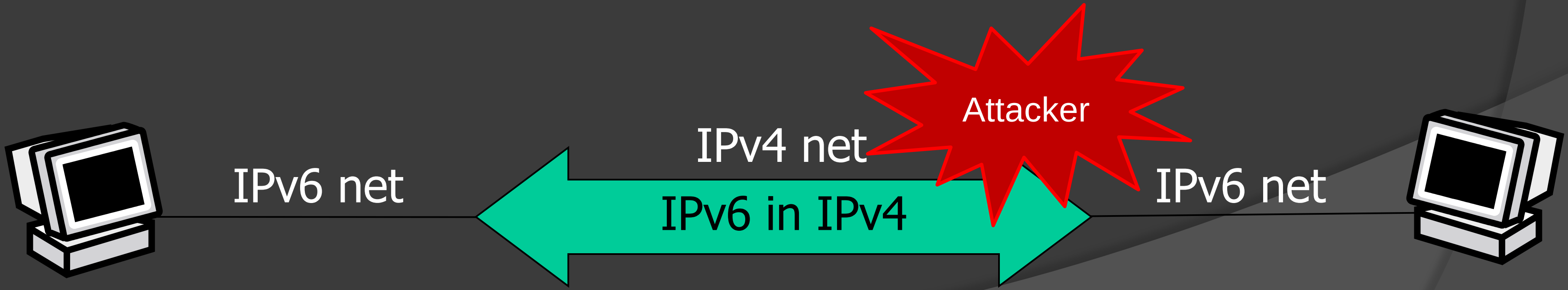
- Address spoofing
- For example, via 6to4 tunneling spoofed traffic can be injected from IPv4 into IPv6.

– IPv4 Src: Spoofed IPv4 Address

– IPv4 Dst: 6to4 Relay Anycast (192.88.99.1)

– IPv6 Src: 2002:: Spoofed Source

– IPv6 Dst: Valid Destination



Security Issues (3)

- Most IPv6 hosts will be 'dual stack'
- IPv4 systems will not have same security feature set as IPv6
- Double Handling of security policy (Mistakes easier).

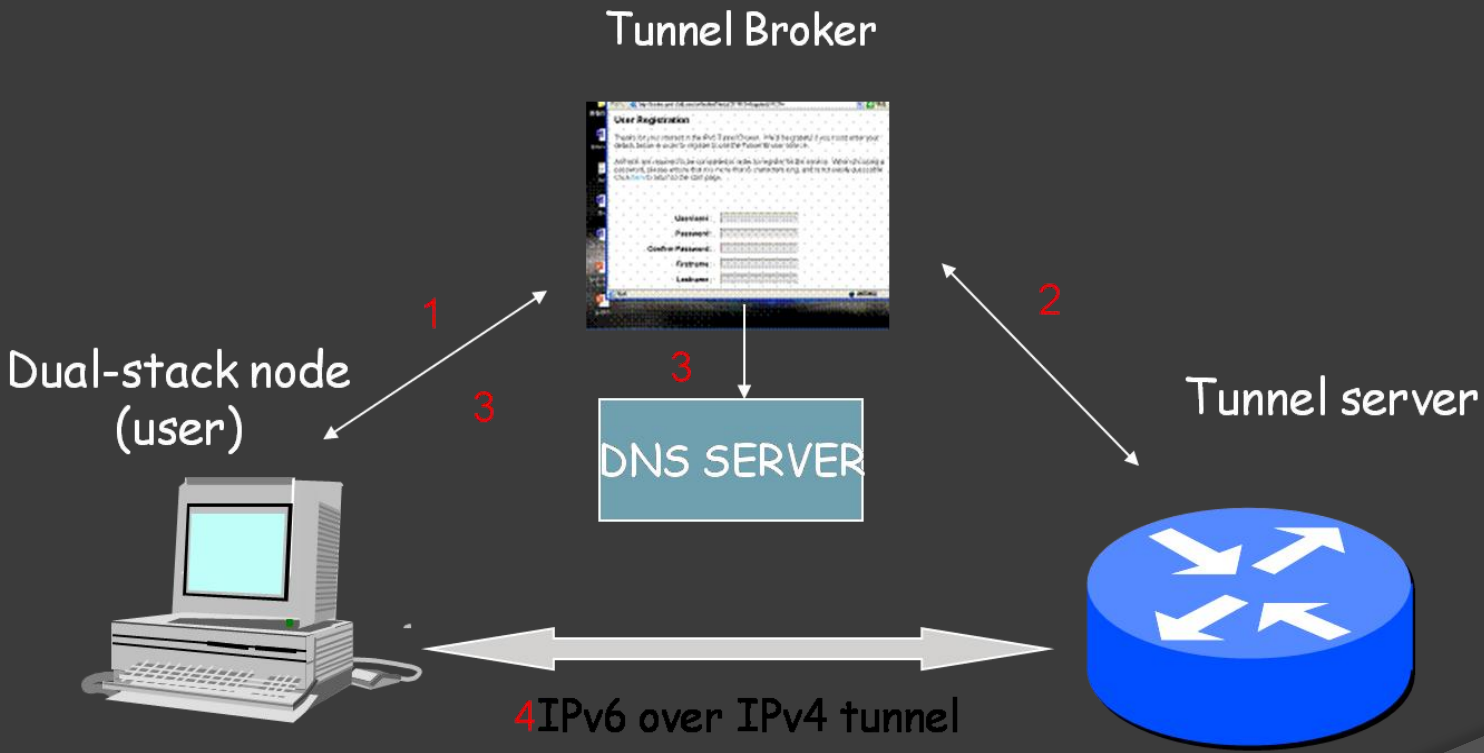
Tunnel Broker Motivation

- IPv6 tunneling over the internet requires heavy manual configuration
  - Network administrators are faced with overwhelming management load
  - Getting connected to the IPv6 world is not an easy task for IPv6 beginners
- The Tunnel Broker approach is an opportunity to solve the problem
  - The basic idea is to provide tunnel broker to automatically manage tunnel requests coming from the users

Tunnel Broker

- Main difference between 6to4 and Tunnel Broker:
  - They serve a different segment of the IPv6 community
- Tunnel Broker fits well for small isolated IPv6 sites
- 6to4: well suited for extranet and VPNs

Tunnel Broker



User Registration

[illegible]

[illegible]

Username:

Password:

Confirm Password:

Firstname:

Lastname:

How it works?

- User registers with the Tunnel Broker first.
- Tunnel Broker will search for a suitable Tunnel Server to allow the user to enter the IPv6 network.
- Tunnel Broker sends information regarding Tunnel Server and the assigned IPv6 address to the User
- User establishes the Tunnel and connects to the IPv6 network

Security Considerations Tunnel Broker (1)

- Interaction between the client and TB:
  - The usage of SSL to encrypt data
  - Rely on AAA facilities (RADIUS) to enforce access control
  - Transferring tunnel configuration parameters in a MIME type over https
- Interaction between the TB and TS
  - Use IPSec to secure SNMP messages

Security Considerations Tunnel Broker (2)

- What if a user disconnects the internet without tearing down the Tunnel?
  - Implementing keep-alive mechanism on every tunnel (assign a lifetime)
  - Allowing the TB to stop IPv6 traffic forwarding toward disconnect users
- Limiting the number of tunnels that a single user is allowed to set up at the same time to prevent DoS.

Conclusion

- IPv6 will slowly and gradually penetrate into our networks and develop on the Internet
- The transition from IPv4 to IPv6 presents even more challenges, we are still facing lots of challenges in the foreseeable future.

Thank you!

Questions???