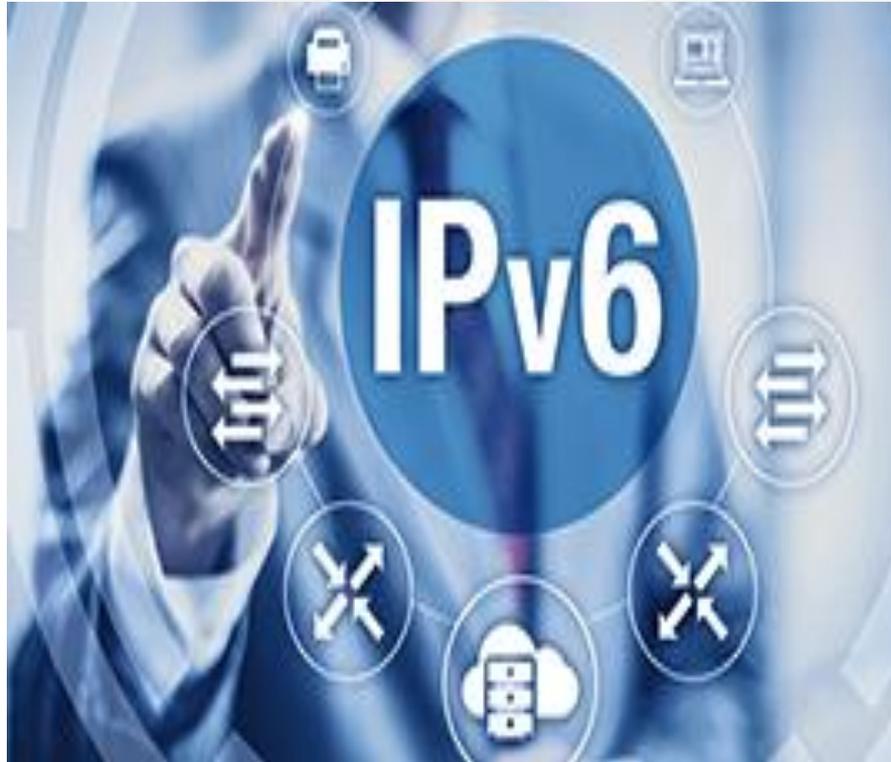


STRENGTHENING KENYA'S CYBERSECURITY POSTURE

Security Landscape in IPv4 and IPv6

Training Objectives



By the end of this session, you will:

- ✓ Identify critical **IPv4 vulnerabilities** (NAT, DHCP spoofing).
- ✓ Understand **IPv6-specific threats** (NDP spoofing, rogue RA).
- ✓ Apply mitigation strategies for hybrid (IPv4/IPv6) networks.

IPv4 Security Overview

- ❖ Widely deployed but originally not designed with security in mind
- ❖ Relies on NAT and stateful firewalls for basic protection
- ❖ Still vulnerable to multiple Layer 2 and Layer 3 threats



IPv4 Vulnerabilities

Legacy Risks Still Haunting Networks:

1. NAT Limitations:

NAT hides internal IPs but creates single points of failure

NAT also makes it difficult to find infected machines as they hide behind one IP address

Risk: State exhaustion attacks (results in DoS).

2. DHCP Spoofing:

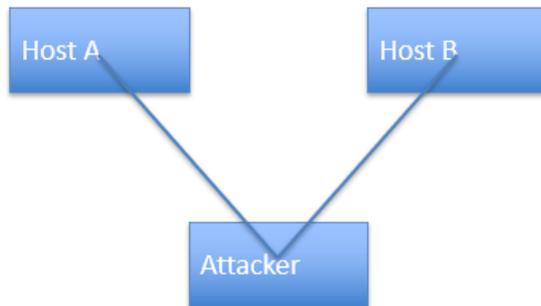
Attackers impersonate DHCP servers to redirect traffic.

Impact: Data interception (e.g., student login theft).

Demo – DHCP Spoofing in Action

Video:

<https://youtu.be/npscRIGCGLY?si=EQk4jD2Cag-X1zxB>



Steps:

- ❖ Attacker sends **fake DHCP offers**
- ❖ Devices connect to **rogue gateway**.
- ❖ Traffic redirected to malicious DNS

IPv6 Security Overview

- Built-in security features like IPSec (optional, not always implemented)
- Larger address space reduces scanning risk

IPv4-4.3B addresses: Low-effort, automated, wide-scale scanning quickly

IPv6 – 2^{128} addresses: Automated wide-scale scanning is futile.

- Stateless Address Autoconfiguration (SLAAC) introduces new risks (RA and NDP spoofing)

IPv6 Threats – New Challenges

IPv6 Solves Old Problems, Introduces New Ones

1. **NDP Spoofing:**

Fake Neighbor Advertisements poison caches.

Result: Man-in-the-middle (MITM) attacks.

2. **Rogue Router Advertisements (RA):**

- ✓ *Advertise fake default gateways*
- ✓ *Cause routing confusion or DoS*
- ✓ *Redirect traffic*

3. **Tunneling Attacks**

- ✓ *Attackers encapsulate IPv6 in IPv4 (e.g., 6to4,).*
- ✓ **Bypasses** firewalls.

Side-by-Side Comparison

Threat Type	IPv4	IPv6
Spoofing	DHCP Spoofing	NDP Spoofing
Gateway Attacks	ARP Poisoning	Rogue RA
Flood Attacks	SYN Floods	ICMPv6 Floods

Dual Stack Dangers

Top Attack surfaces:

- **IPv6-enabled by default** on modern OS → Unmonitored traffic
- **Asymmetric routing:** IPv4/6 paths differ → Bypasses controls
- **DNS inconsistencies:** A vs. AAAA record poisoning



Best Practices & Mitigation Strategies

IPv4

- ❖ Rate-limit NAT translations
- ❖ Isolate legacy IPv4-only devices
- ❖ Implement DHCP snooping
- ❖ Use Dynamic ARP Inspection

IPv6

- ❖ Disable unused transition mechanisms (6to4)
- ❖ Deploy RA Guard on switches
- ❖ Use NDP Monitoring

Dual – Stack

- ❖ Synchronize ACLs for both protocols
- ❖ Monitor IPv6 flow logs (often ignored!)
- ❖ General Network Segmentation
- ❖ Train administrators regularly

Q & A



Challenges in transitioning to or securing IPv6 ?

*Transforming education
through ICT*

Thank You

www.kenet.or.ke

Jomo Kenyatta Memorial
Library, University of Nairobi
P. O Box 30244-00100, Nairobi.
0732 150 500 / 0703 044 500