IPV6 NETWORK PLANNING AND IMPLEMENTATION

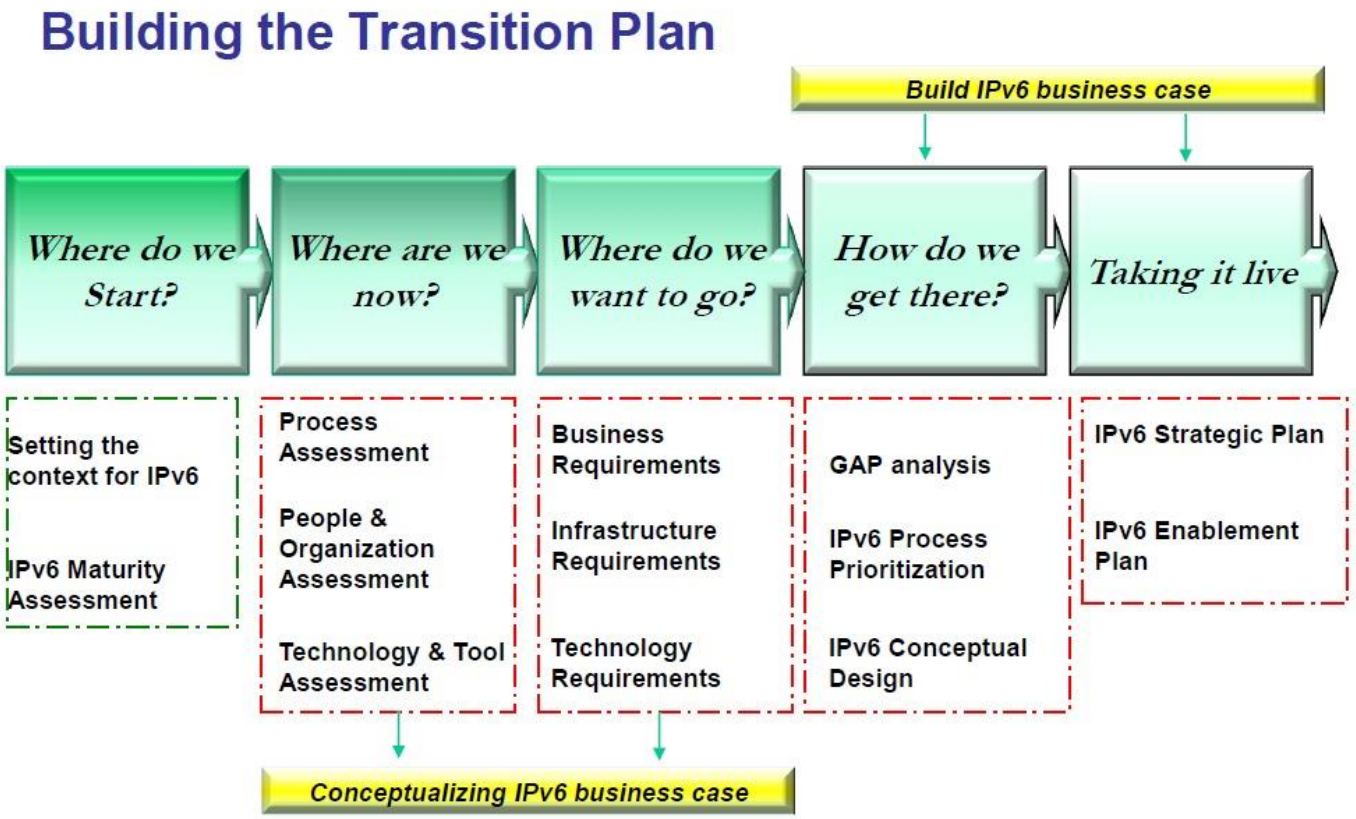
IPV4 TO IPV6 TRANSITIONS

- Implementing any new technology brings with it a new set of problems.
- Being aware of their strengths and weakness are vital.
- IPv6 also introduces its own sets of problems.

COMMON MISUNDERSTANDING

- IPv6 has less issues than IPv4.
- IPv6 offers security by default.
- IPv6 makes it harder to perform reconnaissance.
- Services in IPv6 are more secure.
- Moving to IPv6 will solve all the problems.
- Monitoring IPv6 and IPv4 simultaneously is difficult.

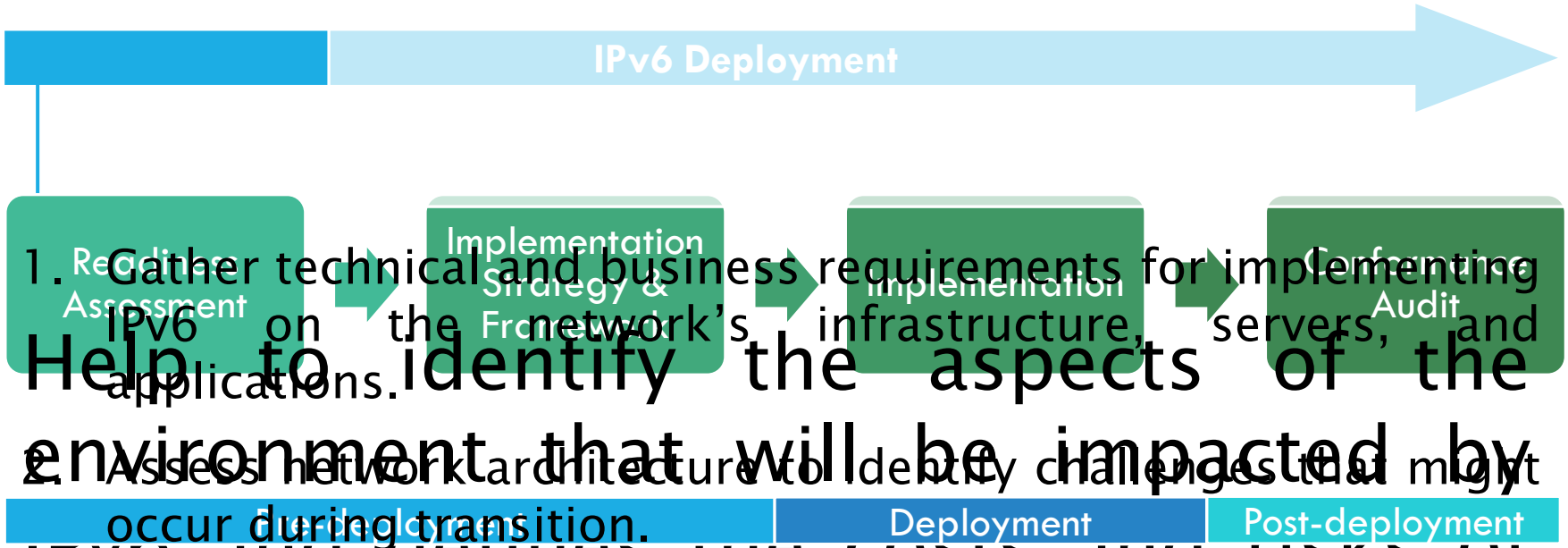
TRANSITION PLAN



IPV6 BUSINESS PLANNING

IPv6 For Business

1. Business Planning
    1. Identify business Drivers
    2. Identify Benefits, Costs , Risks & Resources
    3. Develop a Business Case
    4. Establish an IPv6 Transition Group
2. Technical Planning
3. IPv6 Address Plan
4. IPv6 Routing
5. IPv6 Network Transition Mechanism & Strategies
6. Network Services
7. Security
8. Applications
9. Training & Awareness Planning
10. Web Facing Servers
    1. HTTP Servers
    2. eMail Servers



Help to identify the aspects of the environment that will be impacted by IPv6 and defines the costs and risks of IPv6 adoption.

1. Gather technical and business requirements for implementing IPv6 on the network's infrastructure, servers, and applications.
2. Assess network architecture to identify challenges that might occur during transition.
3. Assess security implications that may occur during and after deployment.
4. Perform an automated network discovery to validate all devices and software.
5. Assess IPv6 readiness on all vendor devices.
6. Assess IPv6 knowledge of network engineers.

Provide customers with an architectural framework for integration of IPv6 in phases within the current IPv4 environment and a strategy for deploying IPv6 within the enterprise.

1. Recommend changes and upgrades
2. Design a high level network that maps the customer's business objectives and technical requirements to a proposed network architecture.
3. Develop logical network topology diagrams, detailed IPv6 address plan, device configuration templates, software release recommendations, acceptance test plan and operational support plans. Also include secure deployment strategies.
4. Design deployment timeline to ensure minimal impact to business operations

Implement the solution. Transition to IPv6 without disruption or causing vulnerability. The actual IPv6 implementation may involve an initial POC (Prove of Concept) deployment followed by progression to broader infrastructure.

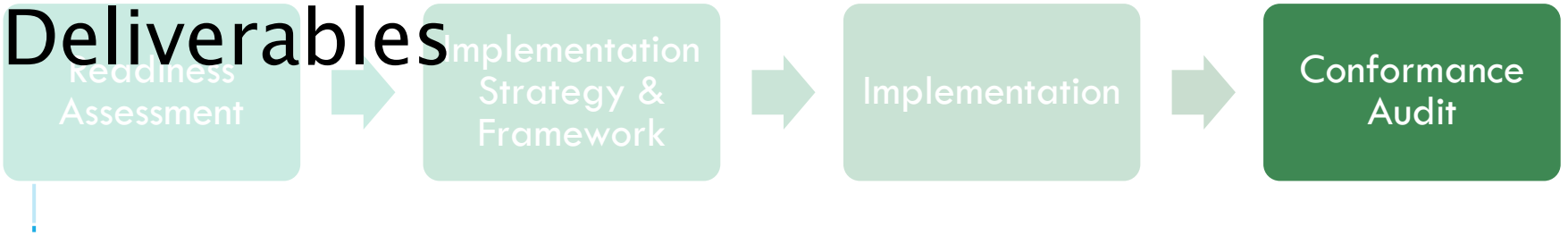
This will typically be carried by System Integrator (SI) with consultation of the expert.

Readiness Assessment → Implementation Strategy & Framework → Implementation → Conformance Audit

Carry out conformance and interoperability IPv6 implementation. The purpose is to measure the level of the network's IPv6 conformance in respect to the networks **infrastructure & device capability, applications and services and security** and ensure it conforms to NAv6's test specification which also incorporates ***IPv6 Ready Logo Program***.

1. IPv6 conformance and interoperability
   a) Validate inter IPv6 network accessibility by internal users (Level 1 Conformance)
   b) Validate inter IPv6 network accessibility by internal users (Level 2 Conformance)
   c) Validate Internet accessibility over IPv6 by internal users (IPv6 contents such as Google, Youtube, Facebook, etc.) (Level 3 Conformance)
2. End-to-end network scalability and performance
3. Dual-stack router/network performance and device and firmware interoperability
4. Application performance and security impact.

Deliverables



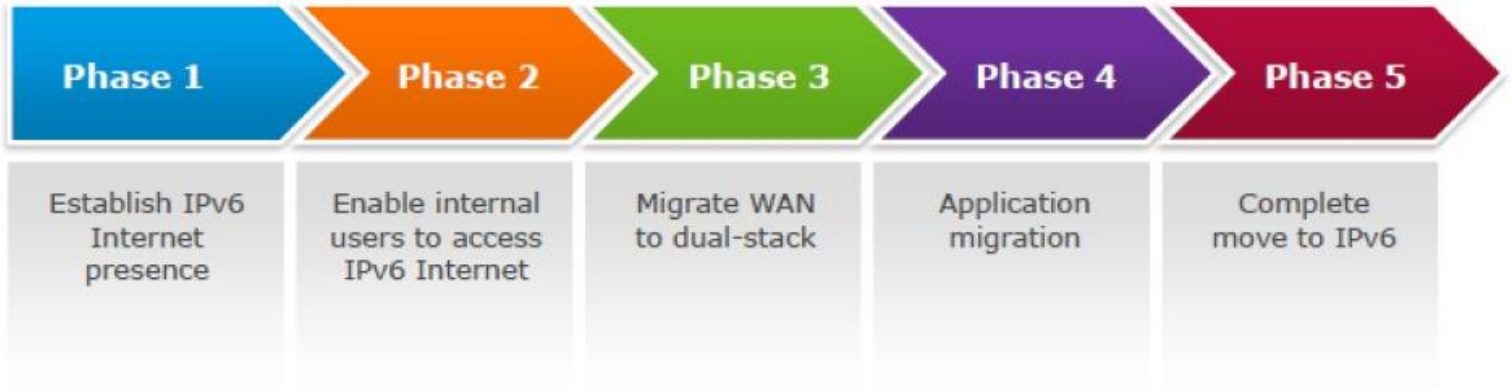
A comprehensive **IPv6 Assessment Report** which includes details on IPv6 readiness of infrastructure, devices, applications/services and security.

A comprehensive **IPv6 Deployment Recommendation Document** that provides recommendation and framework on phased approach to deploy IPv6 specific to the organization.

A comprehensive **IPv6 Conformance Audit Report** that details the level of conformance and identifies issues that needs to be addressed. It will also include interoperability test results for the various components of the network.

IPV6 TRANSITION

IPv6 Transition Technologies



VARIOUS TRANSITION APPROACHES

IPv4 will be used for years after IPv6 deployment

Dual Stack

- Servers/clients speaking both protocols
- Application/service can select either protocol to use

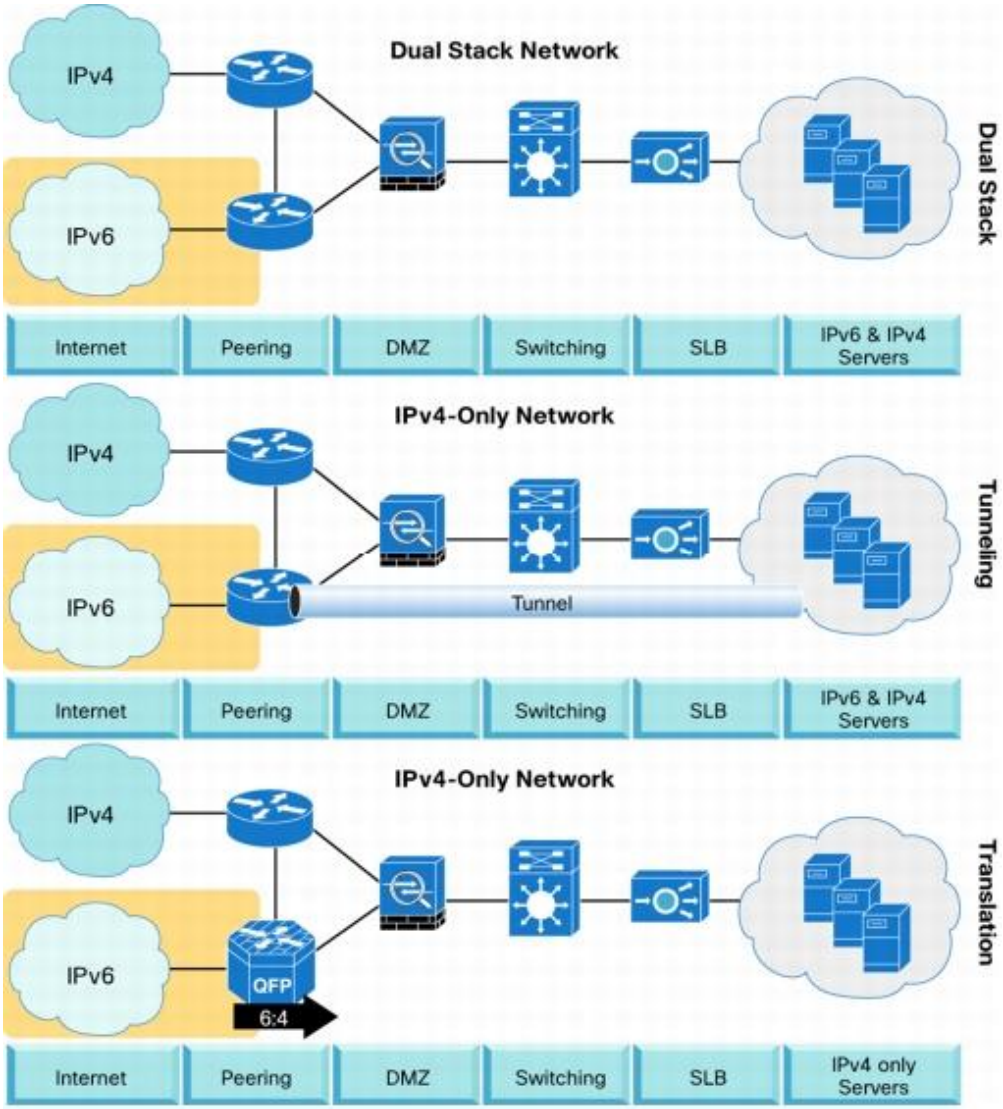
Tunneling (“connecting IPv6 clouds”)

- IPv6 packet is data payload of IPv4 packet/or MPLS frames

Translation methods (“IPv4<->IPv6 services”)

- Layer 3: Rewriting IP header information (NAT-PT)
- Layer 4: Rewriting TCP headers
- Layer 7: Application layer gateways (ALGs)

IPV6 TRANSITION TECHNIQUE



IPV4 TO IPV6 TRANSITION TECHNOLOGIES USED TO PROVIDE IPV6 CONNECTIVITY

(1) Dual-Stack

(2) Configured tunnels (6in4)

(3) Generic Routing Encapsulation (GRE)

(4) IPv6 Rapid Deployment (6rd)

(5) Native IPv6 behind NAT44 CPEs (6a44)

(6) Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

(7) Connection of IPv6 Domains via IPv4 Clouds (6to4)

(8) Tunneling IPv6 over UDP through NATs (Teredo) – No longer supported by Microsoft

(9) IPv6 over IPv4 without Explicit Tunnels (6over4)

(10) Anything In Anything (AYIYA)

(11) IPv6 Tunnel Broker with the Tunnel Setup Protocol

THE IPV4 TO IPV6 TRANSITION TECHNOLOGIES USED FOR PROVIDING IPV4 CONNECTIVITY

(1) Stateless IP/ICMP Translation Algorithm (SIIT)

(2) Stateful NAT64

(3) Combination of Stateful and Stateless Translation (464XLAT)

(4) Dual-Stack Lite (DS-Lite)

(5) Mapping of Address and Port – Encapsulation (MAP-E)

(6) Mapping of Address and Port – Translation (MAP-T)

BENEFITS OF DUAL-STACK DEPLOYMENT

By deploying dual-stack, you can test IPv6-only devices/services without disrupting IPv4 connectivity

Dual stack IPv6 + IPv4 NAT: legacy IPv4 applications (email, www) can be used next to new IPv6 applications (p2p, home networking, ...)

- IPv6 offers the next generation of applications

DEPLOYMENT PLAN

Obtain Global IPv6 address space from your ISP

- customers will get a /48 prefix from ISP

Obtain external connectivity

- You can do dual-stack connectivity
- Also can use tunnel to to get IPv6 service

DEPLOYMENT PLAN….

Internal deployment

- Determine an IPv6 firewall/security policy
- Develop an IPv6 address plan for your site
- Determine address management policy (RA/DHCPv6?)
- Migrate to dual-stack infrastructure on the wire
  - Network links become IPv6 enabled
- Enable IPv6 services and applications
  - Starting with DNS
- Enable IPv6 on host systems (Linux, WinXP, ...)
- Enable management and monitoring tools

IPV6 HOST/ROUTER CONFIGURATION

- In IPv6, IPV6 address are assigned using ICMPv6 messages
- There are five address assignment option are available in IPv6
  - Manual
  - Random
  - Stateless Address Autoconfigurations (SLAAC)
  - Dynamic Host Configurations Protocols Version 6 (DHCPv6)
  - Cryptographically Generated Address (CGA)

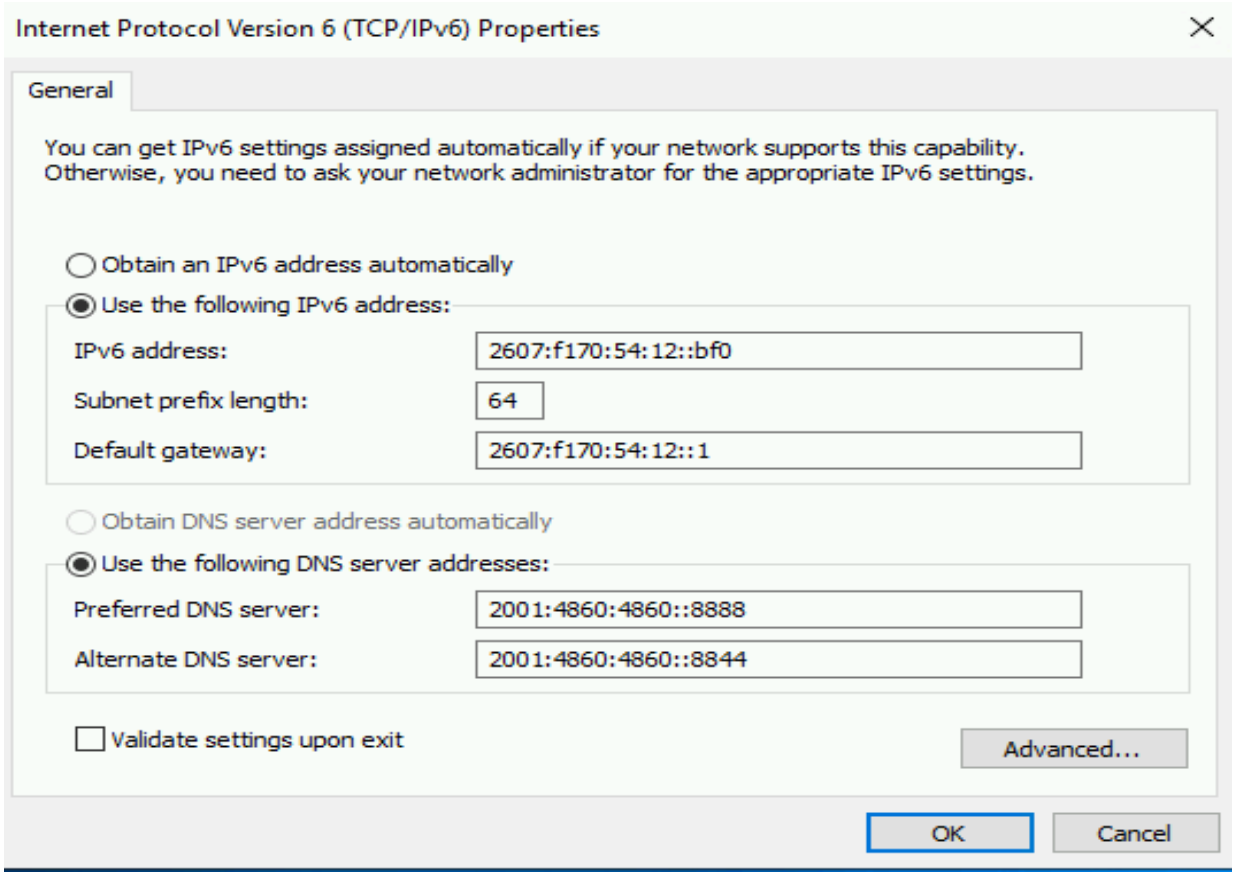
MANUAL CONFIGURATION

Configuration Manual IPv6 in Windows 10

- Start > Network > Network and Sharing Center > Change Adapter Setting, right-click on the Ethernet connection IPv6 and choose Properties, right-click "Internet Protocol Version 6 (TCP/IPv6)" and click on Properties, then set "Use the following IPv6 address".

Note : Other OSes using difference approach

MANUAL CONFIGURATION

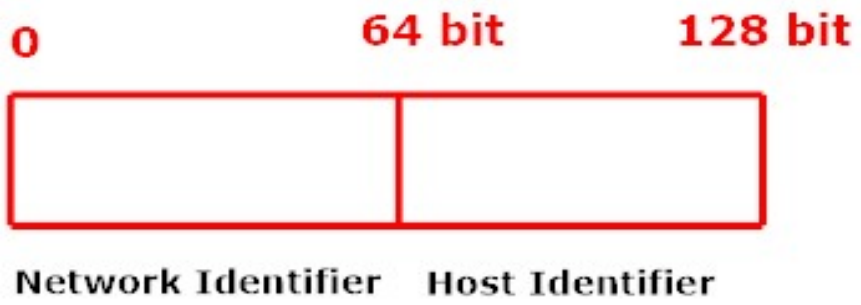


RANDOM CONFIGURATION

Autogenerate a random address as defined in RFC 3041.

This assignment mechanism was developed mainly to limit the exposure of a globally reachable address and to increase privacy.

SLAAC CONFIGURATION



- In SLAAC, the IPv6 address are assigned using ICMPv6 Neighbour Discovery Protocol (NDP) messages i.e Router Solicitation, Router Advertisement, Neighbour Solicitation, Neighbour Advertisement and Router Redirect.
- In the above figure the lowest 64 bit address which is the Network Identifier assigned using Router Discovery process using Router Solicitation (RS) and Router Advertisement (RA).

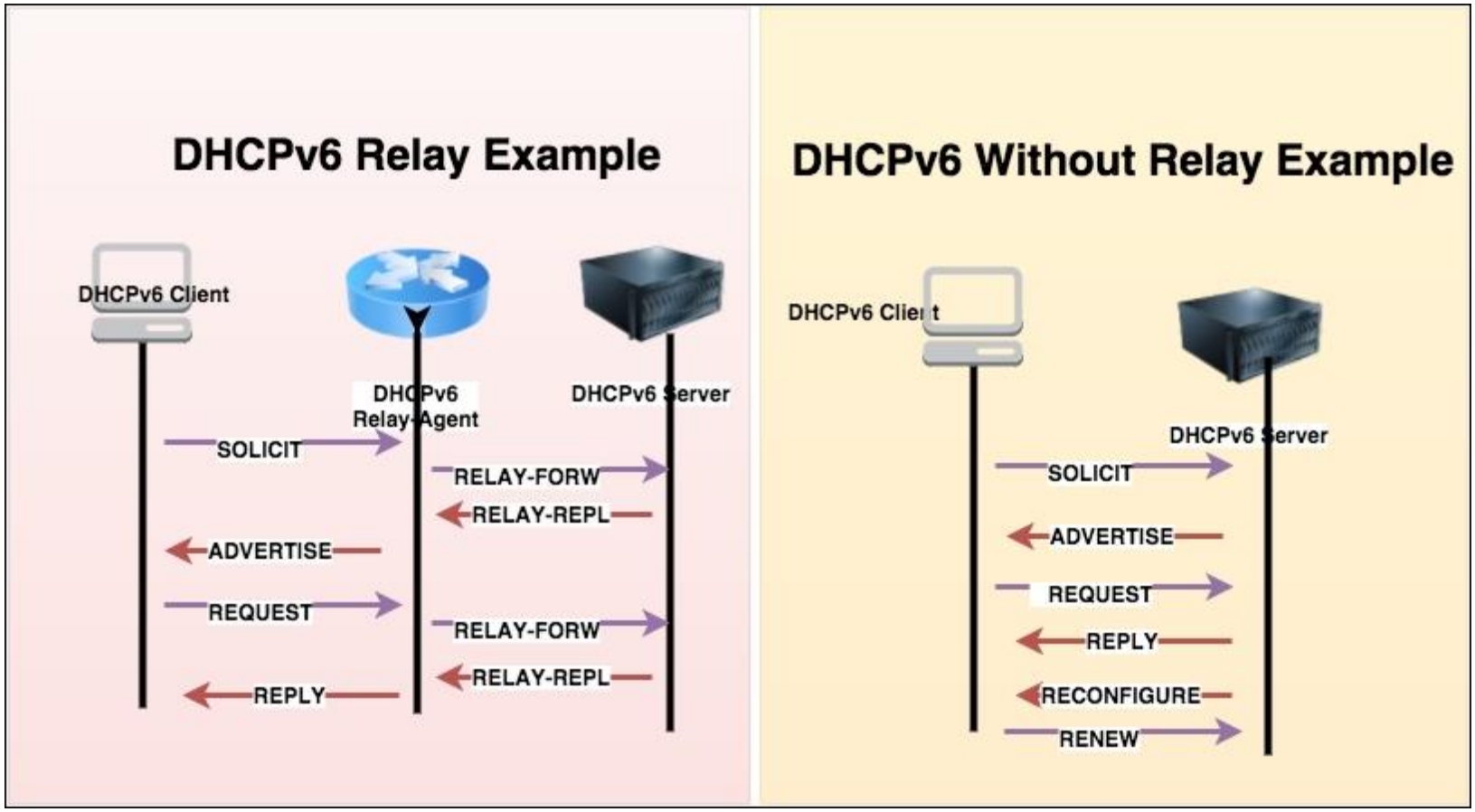
SLAAC CONFIGURATION

- The highest 64 bit assigned using Neighbour Discovery process which involves Neighbour Solicitation (NS) and Neighbour Advertisement (NA) and EUI-64.

DHPV6 CONFIGURATION

- The Dynamic Host Configuration Protocol version 6 (DHCPv6) is a network protocol for configuring Internet Protocol version 6 (IPv6) hosts with IP addresses, IP prefixes and other configuration data required to operate in an IPv6 network.
- It is the IPv6 equivalent of the Dynamic Host Configuration Protocol for IPv4.

DHPV6 CONFIGURATION……



https://subscription.packtpub.com/book/networking_and_servers/9781785887819/5/ch05lvl1sec32/dhcpv6

CGA CONFIGURATION

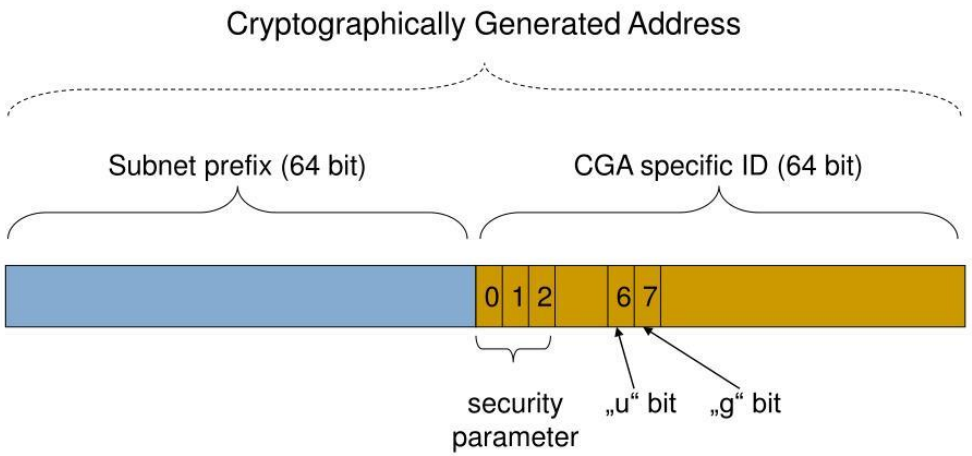
A Cryptographically Generated Address (CGA) is an Internet Protocol Version 6 (IPv6) address that has a host identifier computed from a cryptographic hash function.

This procedure is a method for binding a public signature key to an IPv6 address in the Secure Neighbor Discovery Protocol (SEND).

CGA CONFIGURATION…

CGA - structure

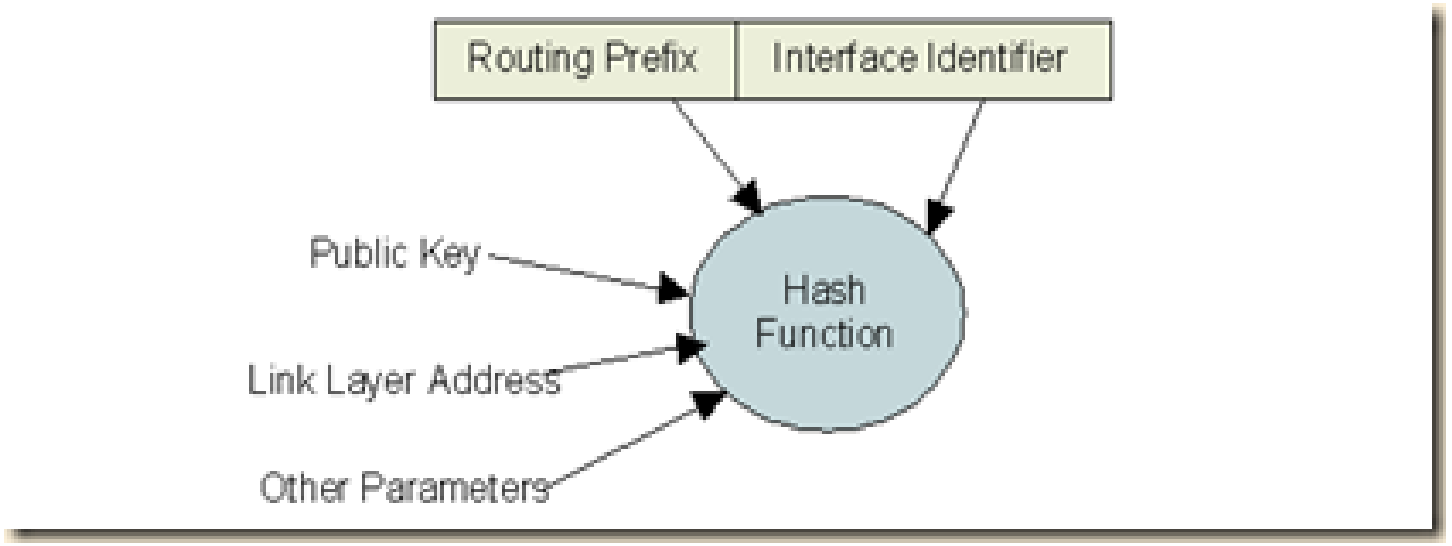
IPv6 Deployment and Support



IPv6 Security 43

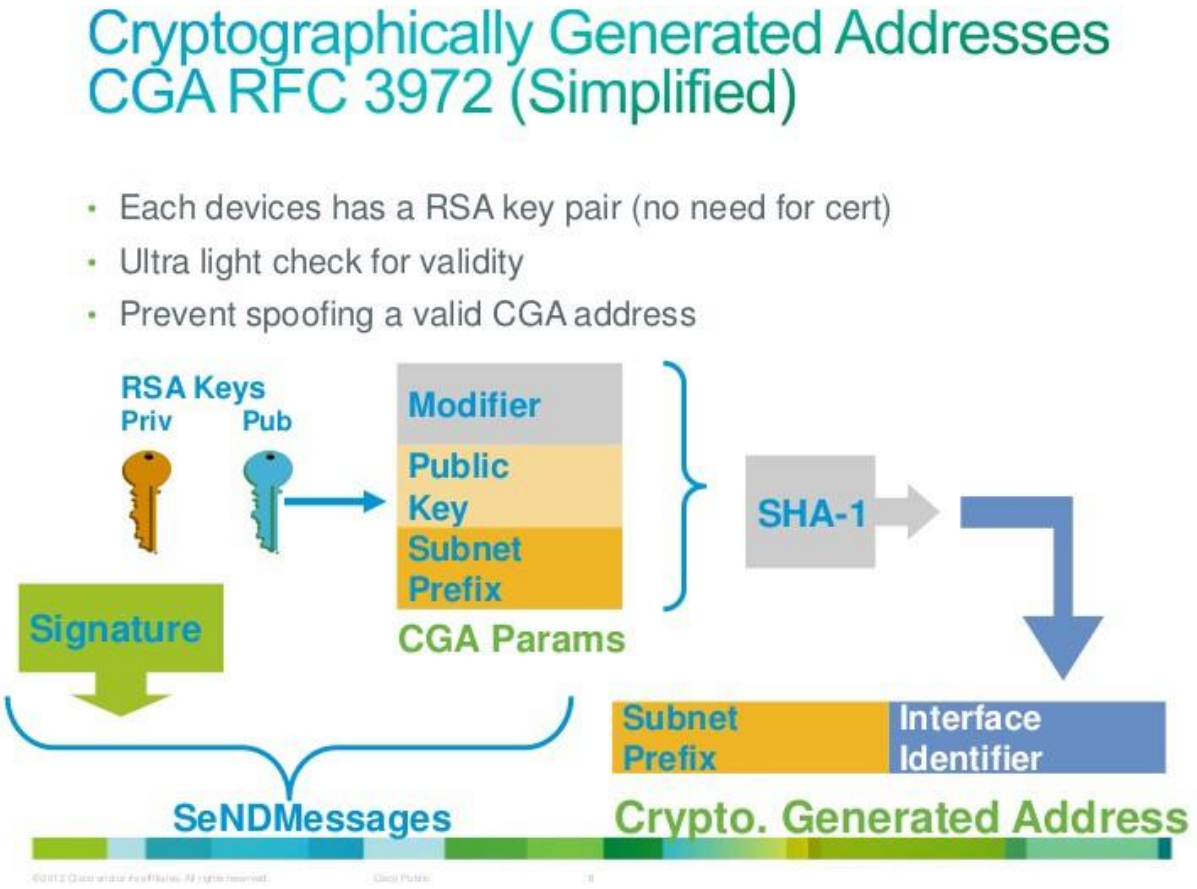
https://www.slideserve.com/thyra/ipv6-security-powerpoint-ppt-presentation

CGA CONFIGURATION…



https://medium.com/@craig_10243/ipv6-with-cga-and-bitcoin-a761d0185d5d

CGA CONFIGURATION…



https://medium.com/@craig_10243/ipv6-with-cga-and-bitcoin-a761d0185d5d

ADDRESS

Most sites will receive /48 assignments:

16 bits left for subnetting - what to do with them?

NEW THINGS TO THINK ABOUT

Every /64 subnet has far more than enough addresses to contain all of the computers on the planet, and with a /48 you have 65536 of those subnets - use this power wisely!

With so many subnets your ISP may end up carrying thousands of routes - consider internal topology and aggregation to avoid future problems.

NEW THINGS TO THINK ABOUT

Renumbering will likely be a fact of life. Although v6 does make it easier, it still isn't pretty

- Avoid using numeric addresses at all costs
- Avoid hard-configured addresses on hosts except for servers (this is very important for DNS servers
- use the feature that you can assign more than one IPv6 address to an interface (IPv6 alias address for servers)
- Anticipate that changing ISPs will mean renumbering

IPV6 DEPLOYMENT OPTIONS

The simplest - deploy dual stack network environment

If the hosts/services are not dual stack enabled - does not break anything - this tend to be a false assumption (Windows Vista, Mac OS X shipped with IPv6 enabled)

If the L3 devices cannot cope with IPv6 or administrators are not favor of upgrading the router

- Add additional IPv6 capable L3 device

IPV6 SERVICES

Server clusters

- Open source solution: *BSD pf
- Commercial platforms: Veritas Cluster Server, Big Iron F5, Windows Server 2008 - Network Load Balancer

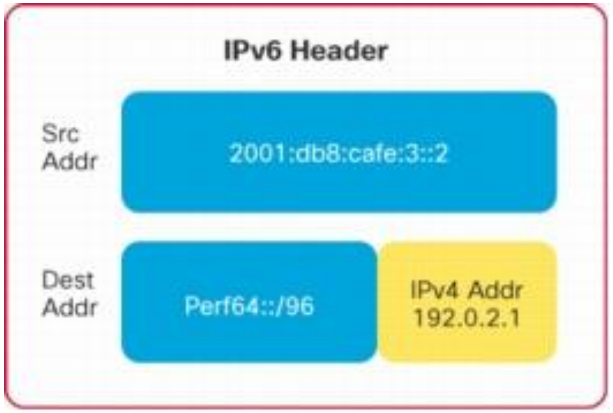
First-Hop Redundancy:

- HSRPv6 (Cisco only)
- VRRPv6 - standardization at IETF

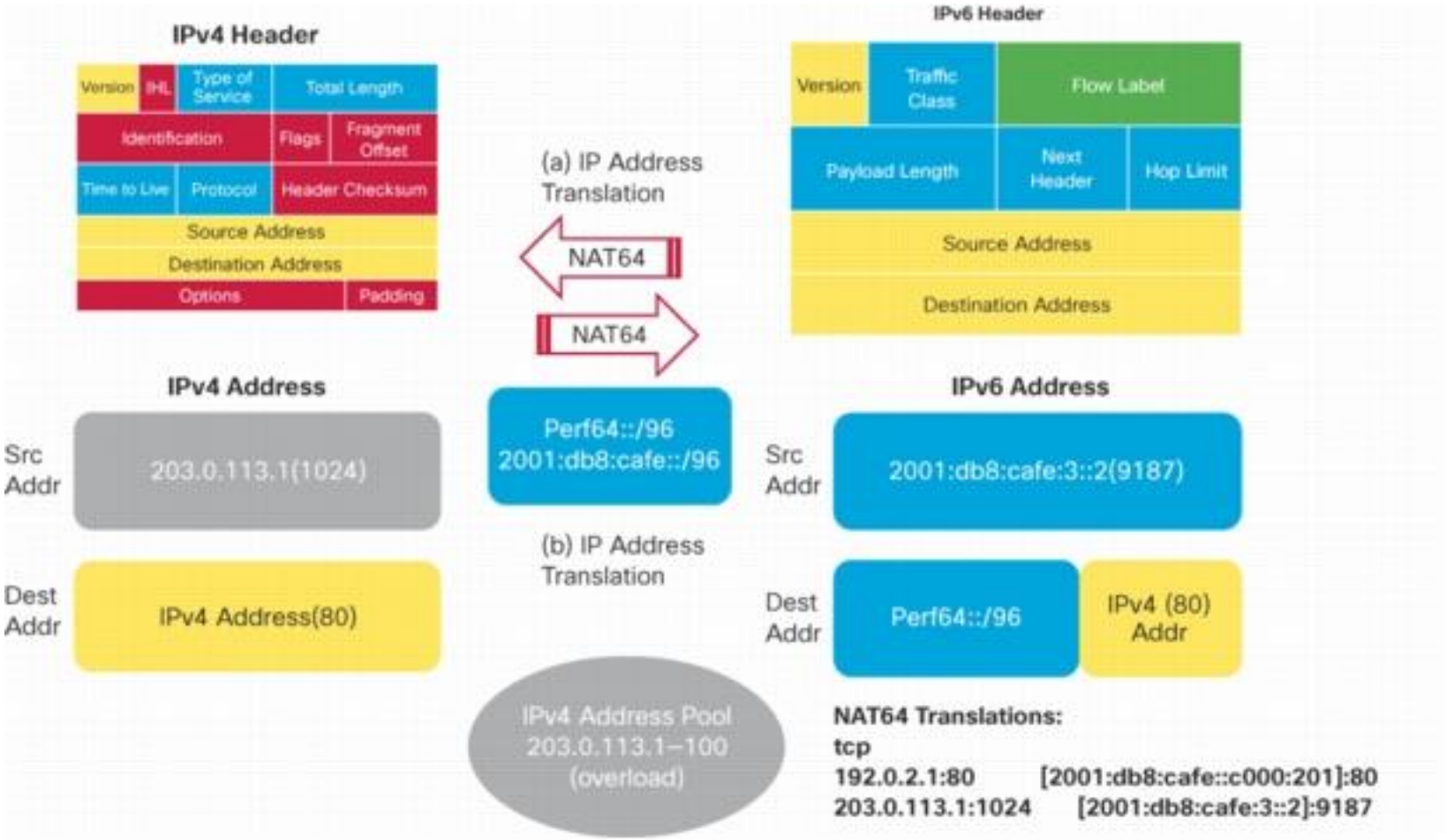
Traffic load balancing

- Multilink PPP - supported if multilink PPP supported
- Equal-Cost Multi-Path routing - if IPv6 routing supported...
- Ethernet Link Aggregations - L2 solution

DNS64 SYNTHESIZING AN A RECORD INTO AN AAAA RECORD

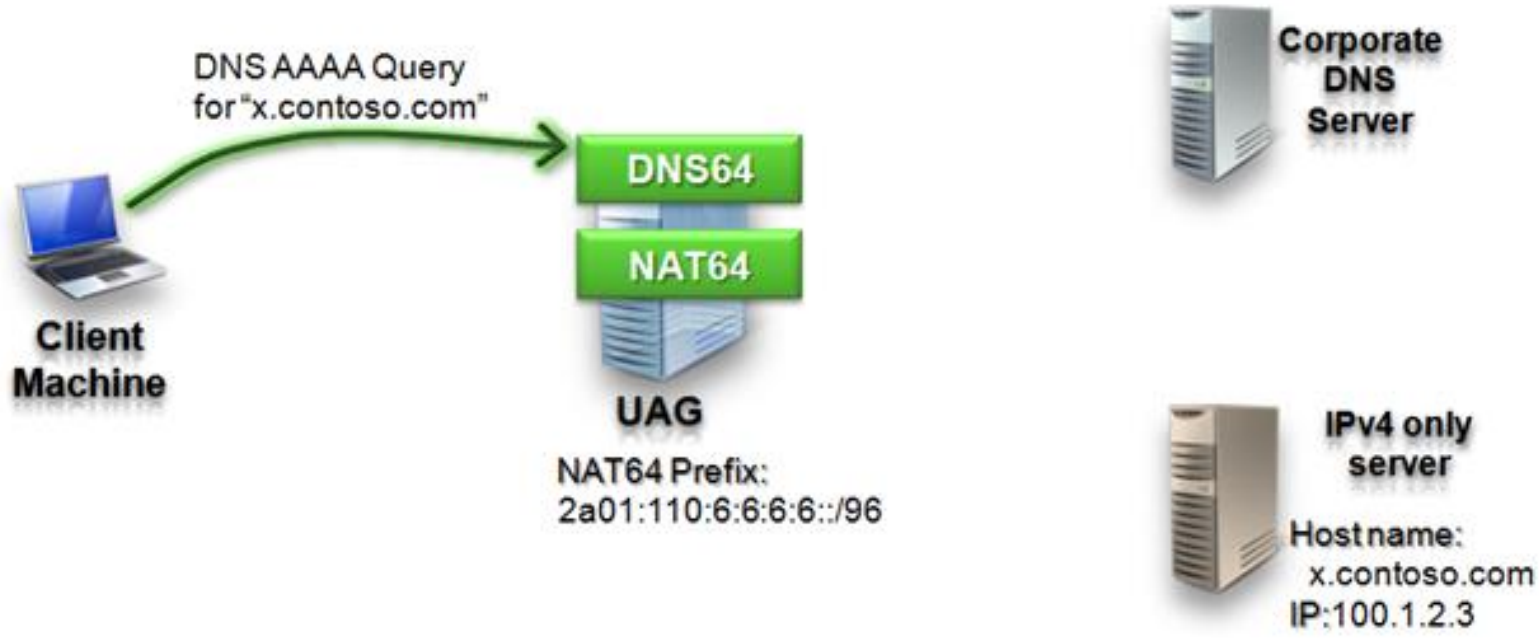


NAT64 TRANSLATION



NAT64 AND DNS64 IN ACTION

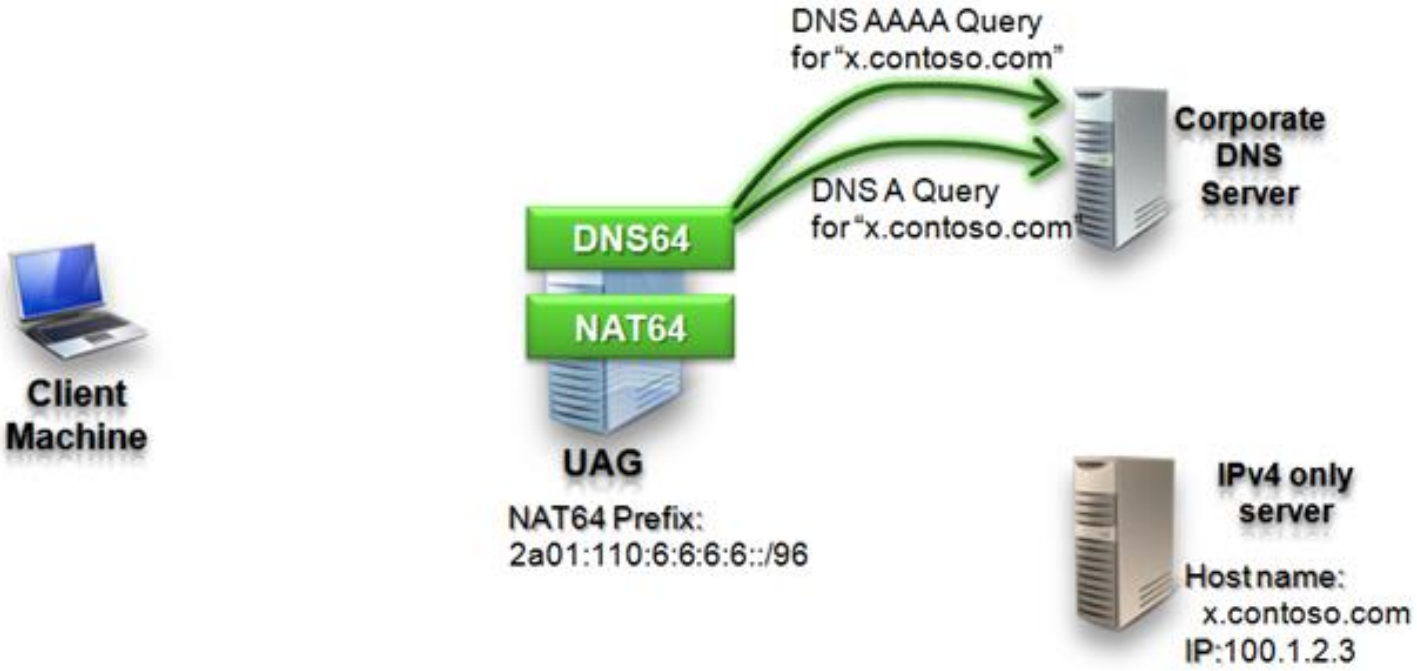
In the first step of the example, the client tries to find the IP address of a server called **x.contoso.com**:



NAT64 AND DNS64 IN ACTION

Step 2: DNS64 query

After it getting the query from the client the DNS64 sends two DNS queries: both IPv4 query (A query) & IPv6 query (AAAA query) to the DNS server.



NAT64 AND DNS64 IN ACTION

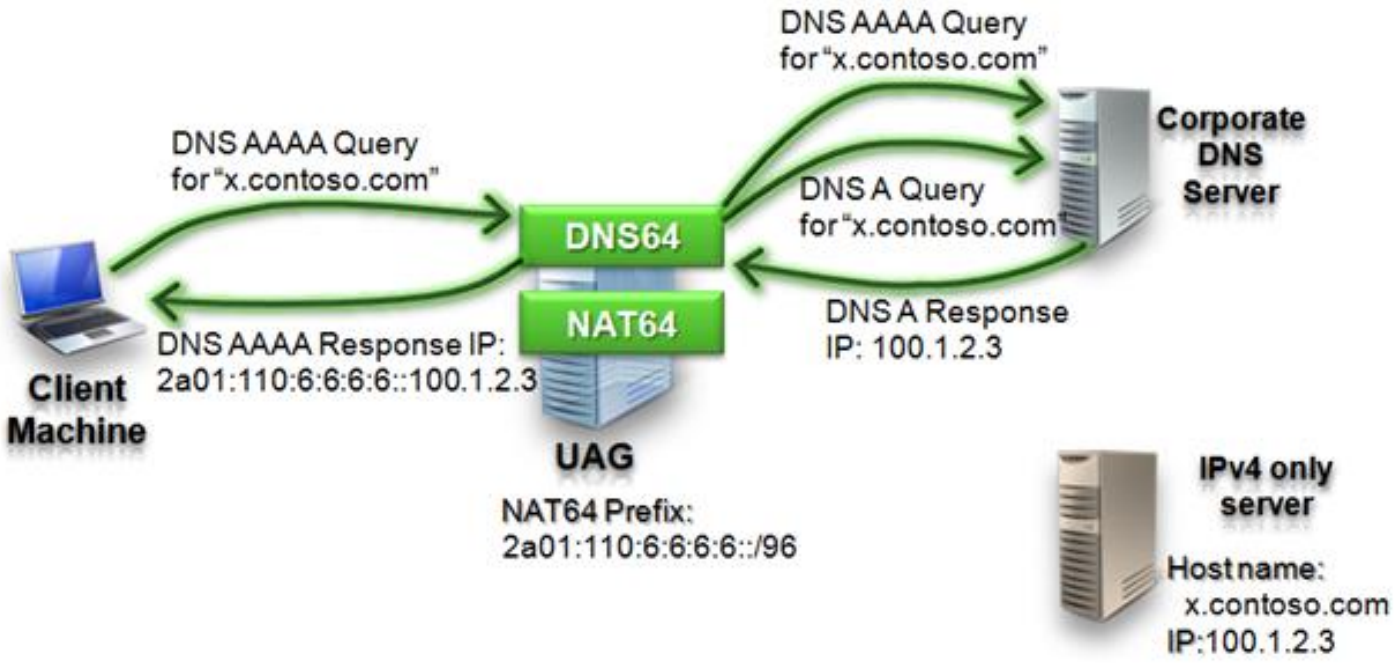
Step 3: DNS Response

- After DNS64 gets the responses from the corporate DNS server it decides which address to return to the client:
  - If DNS64 got in the response an IPv6 address (AAAA Response) then the application server has IPv6 connectivity so DNS64 returns this address to the client.
  - If the DNS64 gets both IPv4 and IPv6 address, it will return the IPv6 address.
- If DNS64 got in response only an IPv4 address it is assumed that there is only IPv4 connectivity to this server and therefore NAT64 will have to bridge all traffic.
- Since the client needs an IPv6 address DNS64 generates an IPv6 address from the IPv4 address based on the NAT64 prefix configured.

NAT64 AND DNS64 IN ACTION

Step 3: DNS Response

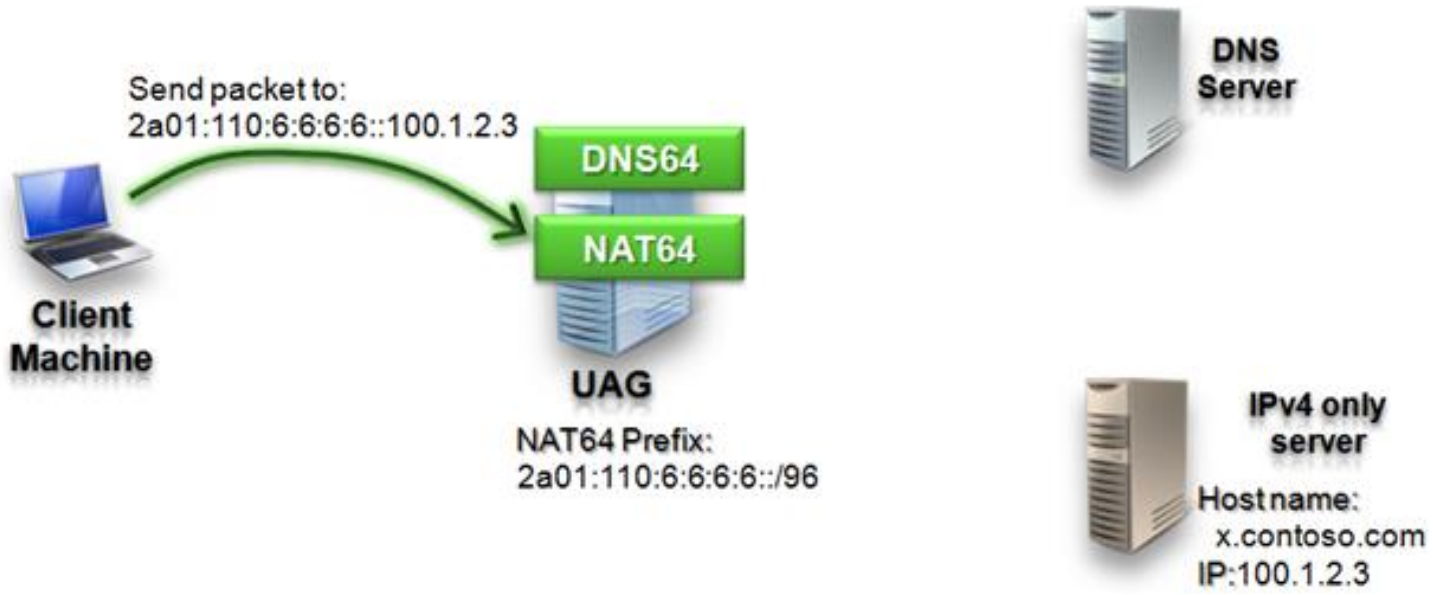
In this example, **x.contoso.com** is an IPv4 only server that needs NAT64 to bridge all traffic:



NAT64 AND DNS64 IN ACTION

Step 4: Client sends packets to server

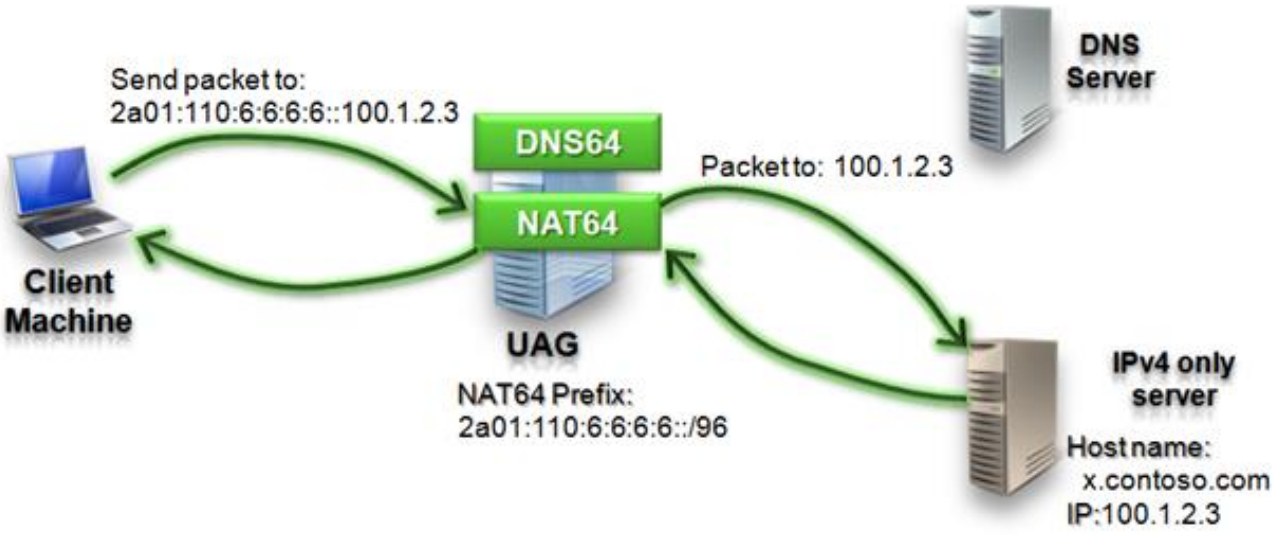
The packets are sent to the NAT64 since all IPv6 addresses that are included in the NAT64 prefix are routed to it:



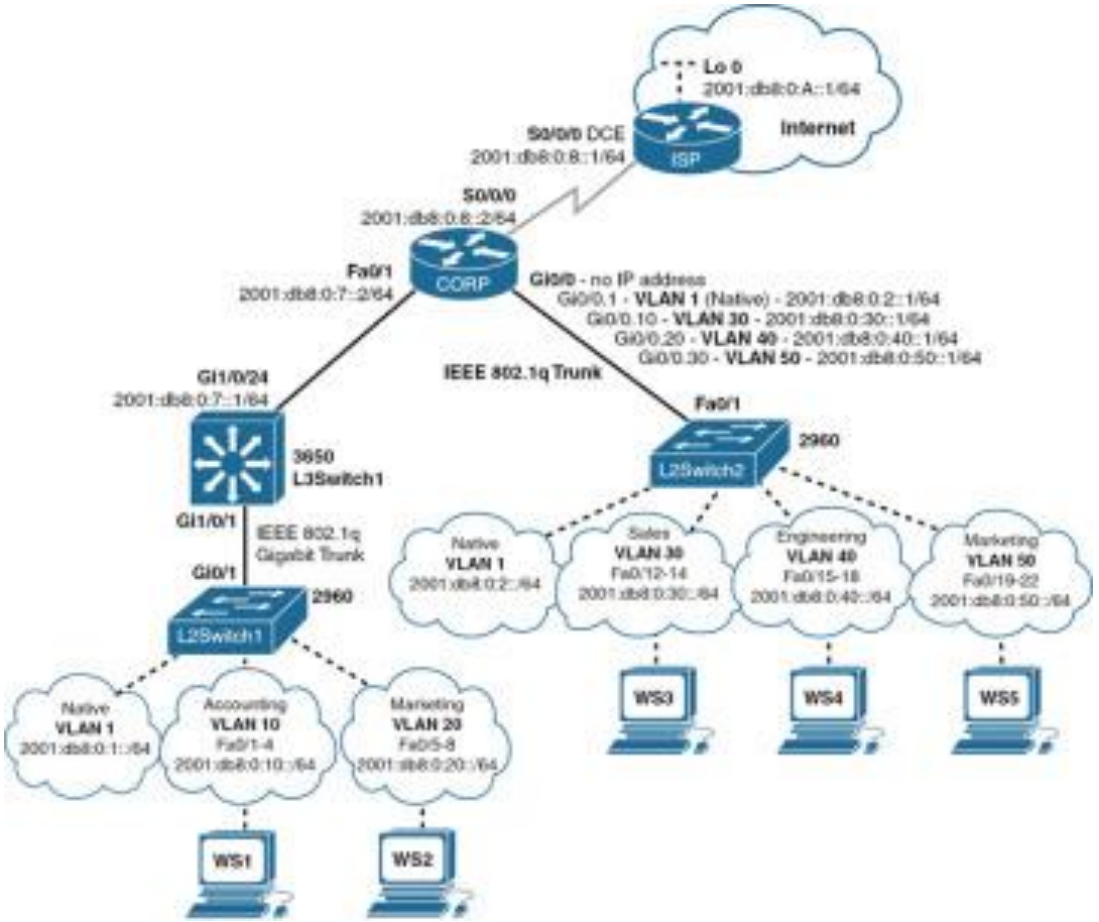
NAT64 AND DNS64 IN ACTION

Step 5: NAT64 forwards the packet using IPv4

- NAT64 receives the data package and tries to determine the IPv4 address that is associated with the destination IPv6 address.
- Then it creates a new IPv4 packet that has the same payload and sends it to the application server.



IPV6 NETWORK LAYOUT



https://www.ciscopress.com/articles/article.asp?p=3004580&seqNum=5

MANAGEMENT AND MONITORING

Device configuration and monitoring –SNMP

Statistical monitoring e.g. Cricket/MRTG

Service monitoring – Nagios

Intrusion detection (IDS)

Etc..

THANK YOU