FECHA: 18 de febrero de 2023 **No REP**: 230218

Dirigido a: Ing. Ingrid Solano Benítez

Dependencia: Oficina Asesora de informático (OAI)
Solicitado por:

Asunto: Estado actual del protocolo IPV6.

Respuesta:
El proceso de la adquisición del bloque de direcciones IPV6 a LACNIC por medio de TIGO-UNE, finalizó satisfactoriamente con la entrega del direccionamiento a la alcaldía de Cartagena.

El número IP asignado a su Organización el cual ya se encuentra publicado en el whois y listo para su uso.

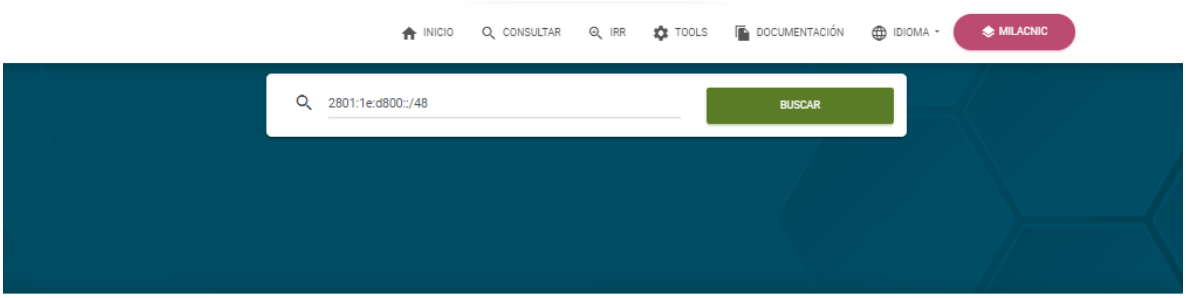
Bloque IPv6: 2801:1e:d800::/48
Organización: DISTRITO TURISTICO Y CULTURAL DE CARTAGENA DE INDIAS
OwnerID: CO-DCIN-LACNIC
Fecha de asignación: Wed Jan 11 15:37:17 UYT 2023.

El proceso de solicitud de ASN asignado a su Organización, el cual ya se encuentra publicado en el whois y disponible para su uso:

ASN: 272934
Organización: DISTRITO TURISTICO Y CULTURAL DE CARTAGENA DE INDIAS
OwnerID: CO-DCIN-LACNIC
Fecha de asignación: Wed Jan 11 15:37:34 UYT 2023.

Continuando con la implementación de e IPV6 en la alcaldía, se recomienda terminar con la migración a SD-WAN y una vez finalizada y probada se comenzara con el despliegue del direccionamiento en todos los equipos de borde, anexo el subneting para cada dependencia.

Ing. de soporte: LFB




```
% IP Client: 2800:e2:6a80:7a8:6022:ace3:9edd:815d

% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2023-02-18 14:34:30 (-03 -03:00)

inetnum:     2801:1e:d800::/48
status:      assigned
aut-num:     N/A
owner:       DISTRITO TURISTICO Y CULTURAL DE CARTAGENA DE INDIAS
ownerid:     CO-DCIN-LACNIC
responsible: Michael Cohen Arteaga
address:     Centro Plaza de La Aduana, cra 2,
address:     130001 - CARTAGENA -
country:     CO
phone:       +57  3015531494
owner-c:     MJA20
tech-c:      MJA20
abuse-c:     MJA20
created:     20230111
changed:     20230111

nic-hdl:     MJA20
person:      Michael Jack Cohen Arteaga
e-mail:      mcohena@cartagena.gov.co
address:     Centro Plaza de la Aduana, 32,
address:     130001 - Cartagena -
country:     CO
phone:       +57  3015531494
created:     20220804
changed:     20220805

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.
```

El servicio público es de todos | Función Pública

MEDICIÓN
DESEMPEÑO INSTITUCIONAL

SUBNETING CON EL POOL DE DIRECCIONES 2801:1E:D800::/48 SIMINISTRADAS POR LACNIC

CO-DCIN-LACNIC - - [RT-REGISTRO #208181]

Bloque IPv6: 2801:1e:d800::/48
Organización: DISTRITO TURISTICO Y CULTURAL DE CARTAGENA DE INDIAS
OwnerID: CO-DCIN-LACNIC
Fecha de asignación: Wed Jan 11 15:37:17 UYT 2023

dependencias | VLan servicios

			PREFIJO GOBAL			SUBRED				HOST INICIALES					HOST FINALES				
DEPENDENCIAS	IDENTIFICADOR	IPV4	16bits	32bits	48bits	64bits				80bits	96bits	112bits	128bits		80bits	96bits	112bits	128bits	
		SEGMENTACION	SEG1	SEG2	SEG3	SEG4				SEG5	SEG6	SEG7	SEG8		SEG5	SEG6	SEG7	SEG8	MASK
FATIMA-DADIS PRINCIPAL	ACP-3589577 - 101088383-IC001 ACCESO-31099	192.168.0.0	2801	001E	D800	0	0	0	0	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
SECRETARIA DE EDUCACION	ACCESO-31098	192.168.4.0	2801	001E	D800	0	1	0	4	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
BODEGA TORICES (ARCHIVO GENERAL)	ACCESO-31504	192.168.6.5	2801	001E	D800	0	2	0	6	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
SISBEN (SANTA RITA)	ACCESO-31419	192.168.13.0	2801	001E	D800	0	3	0	D	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
CASA DE JUSTICIA CHIQUINQUIRA	ACCESO-31392	192.168.20.0	2801	001E	D800	0	4	1	4	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
BIBLIOTECA JORGE ARTEL	ACCESO-31472	192.168.21.0	2801	001E	D800	0	5	1	5	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
CASA DE JUSTICIA COUNTRY	ACCESO-31393	192.168.22.0	2801	001E	D800	0	6	1	6	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
PARTICIPACION		192.168.23.0	2801	001E	D800	0	7	1	7	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
EDIFICIO INTELIGENTE		192.168.24.0	2801	001E	D800	0	8	1	8	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
SISBEN-ALCIBIA	ACCESO-31368	192.168.25.0	2801	001E	D800	0	9	1	9	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
BOMBEROS		192.168.29.0	2801	001E	D800	0	A	1	D	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
ADUANA 300MBPS	ACP-3436564 - 101173241-IC001	192.168.33.0	2801	001E	D800	0B		2	1	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
	ACP-3597898 - 213507669-IC001	192.168.4.66	2801	001E	D800			0	4	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
	ACP-3436549 - 101173233-IC001	192.168.3.0	2801	001E	D800			0	3	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.36.0	2801	001E	D800			2	4	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
EPM PRIMER PISO	ACCESO-31058	192.168.37.0	2801	001E	D800	0C		2	5	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
EPM MEZZANINE		192,168,40,1	2801	001E	D800			2	8	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
EPM SEGUNDO PISO		192,168,42,1	2801	001E	D800			2	A	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
EPM TERCER PISO		192,168,44,0	2801	001E	D800			2	C	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
EPM CUARTO PISO		192,168,46,0	2801	001E	D800			2	E	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
EPM QUINTO PISO		192,168,48,0	2801	001E	D800			3	0	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
EPM SEXTO PISO		192,168,50,0	2801	001E	D800			3	2	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
PORTUS (SE DEBE REUBICAR ESTE DIRECCIONAMIENTO)		192,168,52,0	2801	001E	D800	0	D	3	4	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.62.0	2801	001E	D800	0	E	3	E	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.71.0	2801	001E	D800	0	F	4	7	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.73.0	2801	001E	D800	1	0	1	9	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.74.0	2801	001E	D800	1	1	1	A	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.75.0	2801	001E	D800	1	2	1	B	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.76.0	2801	001E	D800	1	3	1	C	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.77.0	2801	001E	D800	1	4	1	D	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.78.0	2801	001E	D800	1	5	1	E	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
CASCADA	ACCESO-42505	192.168.79.0	2801	001E	D800	16		4	F	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.64.0	2801	001E	D800			4	0	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.65.0	2801	001E	D800			4	1	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.66.0	2801	001E	D800			4	2	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
PES MANGA - DADIS	ACCESO-43019	192.168.67.0	2801	001E	D800	17		4	3	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.68.0	2801	001E	D800			4	4	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.69.0	2801	001E	D800			4	5	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.70.0	2801	001E	D800			4	6	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64

GESTION DE RIESGO	ACCESO-49554	192.168.80.0	2801	001E	D800	18		5	0	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.81.0	2801	001E	D800			5	1	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		172.16.16.80.0	2801	001E	D800			5	2	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		10.0.80.0	2801	001E	D800			5	3	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		172.16.81.0	2801	001E	D800			5	4	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
BOMBEROS LIMBO	ACCESO-31415 ACCESO-31564 85	192.168.82.0	2801	001E	D800	1	9	5	5	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
BOMBEROS-BOSQUE		192.168.100.0	2801	001E	D800	1	A	6	4	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
BOMBEROS-SANTALUCIA		192.168.101.0	2801	001E	D800	1	B	6	5	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
ADMON DESPACHO	ACP-3436564 - 101173241-IC001	192.168.102.0	2801	001E	D800	1	C	6	6	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
LAN_DESPACHO	ACP-3597898 - 213507669-IC001	192.168.105.0	2801	001E	D800	1	D	6	9	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
DEVICE_DESPACHO	ACP-3436549 - 101173233-IC001	192.168.106.0	2801	001E	D800	1	E	6	A	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
VOIP_DESPACHO		192.168.109.0	2801	001E	D800	1	F	6	D	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
WIFI_DESPACHO1	110	10.0.106.0	2801	001E	D800	2	0	6	E	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
WIFI_DESPACHO2		192.168.107.0	2801	001E	D800	2	1	6	B	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
DATT MANGA	ACCESO-51290	192.168.108.0	2801	001E	D800	2	2	6	C	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
DATT RONDA REAL	ACCESO-51936	192.168.202.0	2801	001E	D800	2	3	C	A	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
DATT EL ESPINAL	ACCESO-31785	192.168.204.0	2801	001E	D800	24		C	C	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.218.0	2801	001E	D800			D	A	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
LOS ALPES	ACCESO-60826	192.168.219.0	2801	001E	D800	25		D	B	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.121.0	2801	001E	D800			7	9	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.122.0	2801	001E	D800			7	A	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.123.0	2801	001E	D800			7	B	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.124.0	2801	001E	D800			7	C	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.125.0	2801	001E	D800			7	D	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
SEDE TORRE 17	ACCESO-61067	10.0.127.0	2801	001E	D800	26		7	F	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		10.0.140.0	2801	001E	D800			8	C	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.135.0	2801	001E	D800			8	7	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.141.0	2801	001E	D800			8	D	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
TORRE 14 - PISO 1	ACCESO-61072	192.168.147.0	2801	001E	D800	27		9	3	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.130.0	2801	001E	D800			8	2	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
	136	10.0.135.0	2801	001E	D800			8	8	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
	137	192.168.136.0	2801	001E	D800			8	9	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
TORRE 14 - PISO 2	ACCESO-61071	192.168.142.0	2801	001E	D800	28		8	E	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.131.0	2801	001E	D800			8	3	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		10.0.135.0	2801	001E	D800			8	8	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.137.0	2801	001E	D800			8	9	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
TORRE 14 - PISO 3	ACCESO-61070	192.168.143.0	2801	001E	D800	29		8	F	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.132.0	2801	001E	D800			8	4	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
	136	10.0.135.0	2801	001E	D800			8	8	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.138.0	2801	001E	D800			8	A	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
TORRE 14 - PISO 4	ACCESO-61069	192.168.144.0	2801	001E	D800	2A		9	0	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.133.0	2801	001E	D800			8	5	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
	136	10.0.135.0	2801	001E	D800			8	8	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.139.0	2801	001E	D800			8	B	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
TORRE 14 - PISO 5	ACCESO-61068	192.168.145.0	2801	001E	D800	2B		9	1	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.134.0/25	2801	001E	D800			8	6	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
	136	10.0.135.0	2801	001E	D800			8	8	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.140.0	2801	001E	D800			8	0	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
		192.168.146.0	2801	001E	D800			9	2	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
CARCEL DE MUJERES	ACP-3653711 - 101093496-IC001		2801	001E	D800	2	C	5	8	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64
UNIDAD DE VICTIMAS	ACP-3450279 - 213300084-IC001		2801	001E	D800	2	D	5	9	0000	0000	0000	0000		FFFF	FFFF	FFFF	FFFF	/64

El futuro digital es de todos

MinTIC

FASE II
IMPLEMENTACIÓN IPV6

Transformación Digital para TODOS

GOBIERNO DIGITAL

#MásTIC ✓MejorPaís

FASE II
IMPLEMENTACION IPV6

Actividades de Fase II

Para efectuar la implementación se deben realizar las siguientes actividades y en el siguiente orden. Lo anterior basado en los resultados del Análisis de la información de activos de TI recopilada. La priorización para la implementación se define de acuerdo con los siguientes parámetros:

- Prioridad a los servicios con criticidad Alta, Media y Baja.
- Orden de implementación por Capa (0. Planeación, 1. Red, 2.SO, 3.BD, 4.APP)
- Solicitar el direccionamiento global al organismo regulador o proveedor de servicios de internet.

Revisión del Servidor DNS y Servidor DHCP IPv4

Para una apropiada adopción del protocolo IPv6, se debe hacer una revisión sobre el servidor de DNS, el cual consistente en:

1. Verificación de correspondencia de nombres con direcciones IPv4.
2. Eliminación de registros DNS duplicados y obsoletos.
3. Creación de objetos DNS que no estén registrados o que tengan problemas de registro DNS.

Así mismo, teniendo en cuenta que se tendrá una coexistencia entre dos protocolos, es necesario hacer la revisión del servidor de asignación automática de direcciones IPv4 (servidor DHCP), en los siguientes aspectos.

4. Verificación de los registros de direcciones IPv4 duplicados.
5. Verificación de registros de direcciones IPv4 obsoletos.
6. Eliminación de registros no coherentes.
7. Verificación de asignación correcta de los hosts en sus VLAN correspondientes.
8. Revisión de las asignaciones estáticas

Preparación de los dispositivos con conexión a internet.

La preparación de los dispositivos requiere tener presente varias de las consideraciones expuestas hasta ese momento, estas son:

- Haber adquirido un direccionamiento IP global.
- Contemplar el mecanismo de transición seleccionado.
- Haber definido el plan de direccionamiento IPv6.
- Contemplar que en este momento la mayoría de los sitios de internet en América Latina aún se comunican con direccionamiento IPv4, por lo tanto, es necesario mantener activo el protocolo IPv4.

Para la configuración de enrutadores, se debe tener en cuenta los siguientes aspectos:

Direccionamiento Global entregado por el RIR (Regional Internet Registry). En este se debe contemplar los siguientes aspectos:

- Solicitar al ISP realizar la configuración global asignada por el RIR(LACNIC).
- Realizar Backup de la configuración en el enrutador pasivo.
- Mantener el direccionamiento IPv4 actual, para evitar incidentes con los servicios publicados.
- Realizar pruebas de conectividad sobre IPv6.

Para la configuración del Firewall, se deben tener en cuenta los siguientes aspectos:

- Activar las características IPv6 para el dispositivo.
- De acuerdo con el plan de direccionamiento, asignar direcciones IPv6 estáticas a las interfaces de red del dispositivo.
- Verificar la gestión del dispositivo a través del direccionamiento IPV6 asignado. Se puede usar una interfaz de prueba para la administración y gestión del dispositivo, una vez las pruebas por esta interfaz sean satisfactorias, se puede realizar la configuración en la interfaz principal.
- Realizar la configuración para la comunicación con los enrutadores del ISP.

- Configurar ACL (Access Control List) de prueba para conectividad a Internet a través de IPv6.
- Realizar pruebas de conectividad IPV6 Firewall / enrutador y viceversa.
- Realizar Backup de la configuración del Firewall.

Nota: En este instante, aún no se hace publicación de los servicios sobre IPv6, por lo tanto, se deben mantener aseguradas las ACL tanto para IPv6 como para IPv4.

Preparación del servidor de direccionamiento DHCP IPv6.

Para la preparación del servidor de direccionamiento IPv6 (DHCP IPv6) se deben tener en cuenta las siguientes consideraciones:

- Haber adquirido un direccionamiento global (temporal o definitivo) emitido por su RIR https://www.lacnic.net/ (LACNIC).
- Tener pre-configurados los dispositivos de conexión a internet (Router, Firewall, entre otros).
- Haber definido un plan de direccionamiento IPv6 acorde con la topología de red de la entidad.
- Depurar previamente el DNS y el servidor DHCP IPv4.

Teniendo en cuenta que la Alcaldía Mayor de Cartagena, maneja el direccionamientos a través de los Router de Core locales, donde se alojan las configuraciones de las VLan de las entidades, integrado a un directorio activo en Windows server 2019 y el DNS.
La configuración del servidor debería ser integrado dentro de la misma solución y se debe tener en cuenta las siguientes consideraciones:

ACTIVIDAD	ESTADO
Activar las características IPv6 en el servidor.	

Asignar una dirección IPv6 estática, acorde con el plan de direccionamiento IPv6.	
Registrar la dirección IPv6 estática en el servidor de DNS (Esta dirección no es modificable ya que a través de esta los clientes de la red encontraran la dirección del servidor DNS IPv6).	
Revisar si la configuración del servidor DHCP de los Router de Core de las diferentes entidades, cuenta con ámbitos activos de IPv6.	
Cree un ámbito DHCP IPv6 de pruebas en todos los Router de Core de la topología de red.	
Crear un entorno de pruebas para validar la correcta asignación de direcciones IPv6. Si las pruebas son satisfactorias crear los ámbitos necesarios de acuerdo con su topología y el plan de direccionamiento.	
Establecer los dispositivos que son manejados por el DHCP IPv6 que requieran direccionamiento estático.	
De acuerdo con el plan de direccionamiento y la topología actual de red, se deben crear las VLAN IPv6 en cada uno de los Switch de Core para que permitan el tráfico a través de ellas y se verificara que los equipos puedan navegación hacia internet.	

Luego de las pruebas y/o correctivos, realizar Backup la configuración en los demás Switch Core en toda la red.	
Realizar una activación temporal del protocolo IPv6 en equipos de manera aleatorios de la red en una VLAN seleccionada, para la verificación de conectividad IPv6, esto requiere desactivación temporal de IPv4 en esos mismos equipos.	
Hacer un monitoreo del comportamiento de la conectividad en IPv6 durante un tiempo que se considere prudente.	

Para las soluciones Wireless:

ACTIVIDAD	ESTADO
Configurar la controladora Inalámbrica para su gestión a través de IPv6.	
Activar las características que permitan el uso del mecanismo de transición.	
Configurar una dirección IPv6 estática en la controladora.	
Realizar pruebas de conectividad IPv6 hacia el dispositivo.	
Mantener activa la configuración IPv4 del dispositivo.	
Configurar las VLAN correspondientes en IPv6 para los clientes inalámbricos.	

Configurar los puertos de la controladora para permitir el tráfico de las VLAN IPv6.	
Realizar pruebas de conectividad de los clientes inalámbricos y verificar la correcta asignación de direcciones IPv6 en dicho cliente.	

Preparación de servidores.

Siendo los servidores la columna vertebral de la infraestructura, donde se soportan las operaciones críticas de la entidad, es necesario tener consideraciones especiales para esta:

DESCRIPCIÓN	ESTADO
Verificar que los dispositivos de red de los servidores sean compatibles y se encuentran actualizados para su operación en IPv6	
Se necesita establecer un plan ordenado de asignación de direcciones para estos dispositivos.	
Validar la compatibilidad de los sistemas operativos de los servidores con IPv6.	
Verificar la correcta asignación de direcciones en los servidores de DNS y DHCP IPv4.	
Activar las características de IPv6 en cada uno de los sistemas operativos de los servidores	
Asignar una dirección IPv6 estática, de acuerdo con el plan de direccionamiento.	

Verificar la conectividad del servidor en IPv6.	
Verificar el correcto registro del servidor en el DNS con su correspondiente dirección en IPv6 y en el Servidor DHCP IPv6	

Nota: Siempre se deberá mantener activo el protocolo IPv4 durante las pruebas.

- Para los servidores virtuales las recomendaciones son similares, sin embargo, se debe considerar la activación de las características IPv6 en los servidores físicos que soportan las máquinas virtuales (Oracle VM).

  Otras consideraciones: gran parte de la infraestructura de servidores soporta las aplicaciones de la entidad, bases de datos, archivos e información crítica para la entidad, es por ello que la activación de las características IPv6 se realizará de manera gradual evitando impactos en la continuidad del negocio, por lo tanto, se deben abrir ventanas de mantenimiento específicas para estas configuraciones y pruebas.

Preparación de equipos de usuarios final y otros tipos de host.

DESCRIPCIÓN	ESTADO
Verificar que los dispositivos de red, de los equipos cliente, soportan, son compatibles y se encuentran actualizados para su operación en IPv6.	
Acorde al análisis de criticidad IPv6 (Bajo/Medio/Alto), es necesario establecer un plan ordenado de asignación de direcciones para estos dispositivos.	
Validar la compatibilidad de los sistemas operativos de los equipos cliente con IPv6.	

Verificar la correcta asignación de los equipos cliente en los servidores de DNS y DHCP IPv4.	
Activar las características de IPv6 en cada uno de los sistemas operativos de los equipos cliente.	
Asignar una dirección IPv6 automática, de acuerdo al plan de direccionamiento.	
Verificar la conectividad de los equipos cliente en IPv6.	
Verificar el correcto registro de los equipos cliente en el DNS con su correspondiente dirección en IPv6 y en el Servidor DHCP IPv6.	

Preparación de los Sistemas de Información y Bases de Datos

Para los sistemas de información

Iniciar el proceso de actualización de aplicaciones desarrolladas en lenguajes de programación NO compatibles con IPv6. Sin embargo, cada vez que se vaya a desarrollar una aplicación se deben tener en cuenta las mejores prácticas de desarrollo para incluir IPv6.

En los escenarios donde las aplicaciones no puedan trabajar IPv4 e IPv6 simultáneamente (Capa de Aplicación), se deben separar los entornos de la aplicación para que cada uno se comunique mediante su respectivo protocolo. Recordar: La actualización de la aplicación debe hacerse en ambos entornos.

Antes de poner en producción una aplicación modificada para IPv6, crear un ambiente de pruebas y cerciórese que arroja los resultados esperados.

Evitar alterar las aplicaciones en producción.

Crear copias de respaldo antes de cualquier modificación.

Para Bases de Datos

DESCRIPCIÓN	ESTADO
Crear una copia de seguridad de las bases de datos.	
Actualizar la tabla de Host, con las direcciones IPv6 correspondientes.	
Actualizar los Jobs, Procedimientos almacenados y toda configuración de base de datos que invoque a una aplicación, modificando acorde a la tabla de Host actualizada.	
Para las Bases de Datos, crear una copia de seguridad, realizar las configuraciones para IPv6 en un entorno de pruebas, modificando acorde a la tabla de Host actualizada.	
Validar los modelos de bases de datos con el fin de determinar si existen campos dentro de las tablas que deban modificarse, ya sea en su tamaño o en su tipo. Lo anterior para el almacenamiento de variables que tengan datos de dirección IPv6.	

Para las conexiones Cliente / Aplicación

De acuerdo con la manera en que se invoque a la aplicación, tener en cuenta:

- Para las Aplicaciones WEB, hacer el llamado a través del nombre del Host, ya que a través de la dirección IP puede generar inconvenientes. Es importante tener en cuenta

que si se desea acceder a una aplicación por su dirección IPv6 se debe usar la sintaxis adecuada de la dirección entre corchetes: [ ].

- Para las Aplicaciones Cliente/Servidor, actualizar orígenes de datos, documentos conexión o cualquier otro tipo de conector que la aplicación tenga, para que esta se realice a través de nombre de Host. En caso de que los clientes compilados ya tengan direcciones IP quemadas en el código, se recomienda recompilar la aplicación con el nombre del servidor en vez de la dirección IP.
- Para las unidades mapeadas, hacer el llamado de las unidades de red compartidas invocando directamente el nombre del Host donde se encuentra el recurso.

RECOMENDACIONES GENERALES

- Capacitar a todo el personal implicado en la gestión y manejo del protocolo IPv6.
- Socializar ante la organización el plan de implementación de IPv6.
- Todos los procesos de adquisición tecnología a futuro deben exigir la compatibilidad con IPv6.
- Aunque el porcentaje de compatibilidad de los equipos con IPv6 es importante, se deben tener en cuenta que todos los nuevos equipos deben adquirirse con compatibilidad en IPv6.

Dado que la entidad cuenta con infraestructura a la nube, se recomienda tener en cuenta los siguientes aspectos:

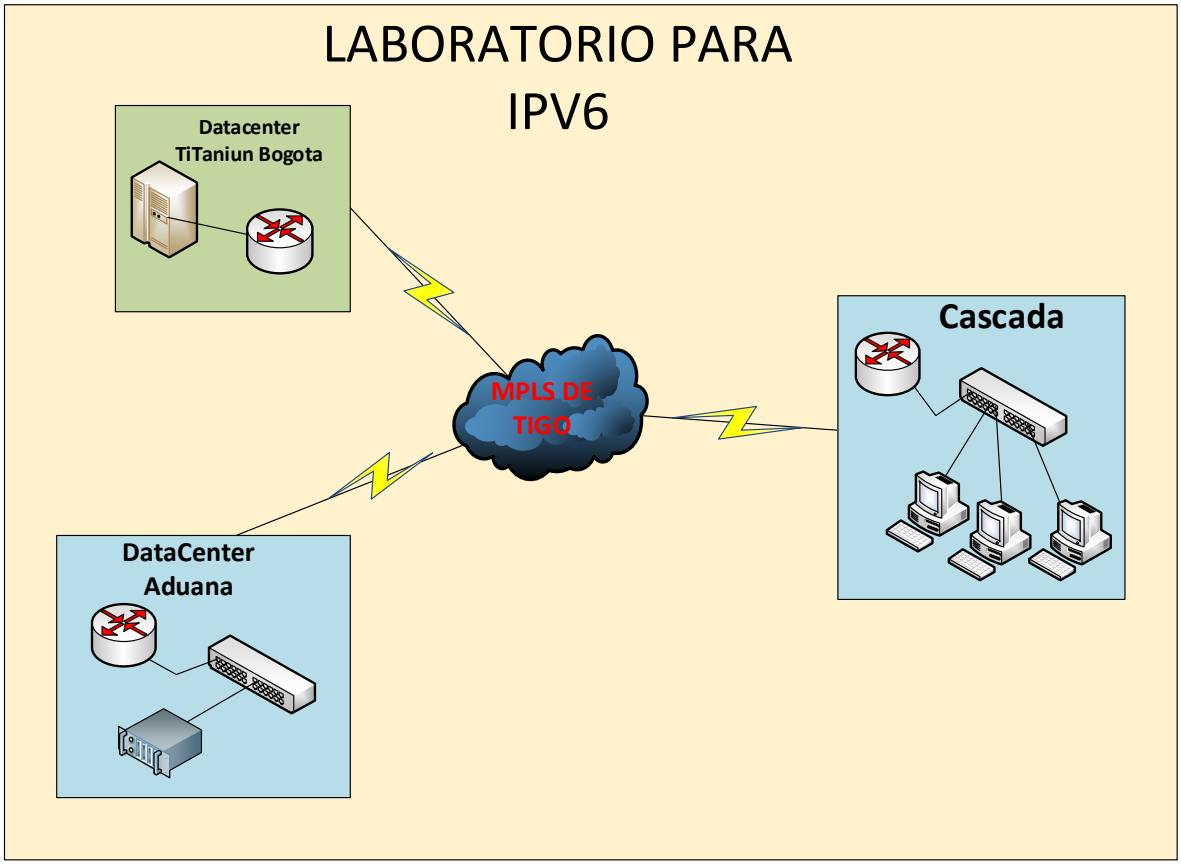
- Se debe contarse con el direccionamiento de la entidad propio para poderlo entregar al proveedor.
- Debe seleccionarse el segmento de red IPv6 que se asignará a las direcciones IP que se migrarán a la nube con el fin de que no se traslape con el direccionamiento interno. Estas direcciones serán anunciadas por el proveedor en su nube, por lo tanto, el rango debería ser único para los servicios que son públicos.
- Definir junto con el proveedor de servicios el mejor esquema de direccionamiento y segmentación de acuerdo con las condiciones adquiridas de la nube privada o pública.

RECOMENDACIONES DE ADQUISICIÓN

Como resultado del diagnóstico a continuación se presentan las recomendaciones de adquisición de infraestructura o software que permiten complementar el proceso de transición a IPv6.

- Adquirir una herramienta de control de IPv6. Esto permite gestionar el direccionamiento IPv6 de la entidad y administrarlo adecuadamente. Si bien inicialmente la asignación se realizará partiendo del plan de direccionamiento, es importante que a futuro se contemple la adquisición de dicha herramienta.
- Se recomienda que todos los contratos de adquisición de nuevas tecnologías, hardware y software incluyan la política de IPv6, la cual debe exigir que todos los equipos y software sean compatibles y desplegados en IPv6 cumpliendo con los requisitos técnicos mínimos que defina la Alcaldía de Mayor de Cartagena, así como los lineamientos de seguridad de IPv6 en general.

Diagrama Del laboratorio de prueba



Tareas para el laboratorio de Prueba.
Fase 1.

1. Adquisición del pull de direcciones o solicitar un pull de direcciones para realizar pruebas de comunicación
2. Informar a TIGO, la habilitación del protocolo IPV6 en todos los Router de borde donde se presta el servicio de comunicaciones.
3. Solicitar a seguridad la creación de varias VLans en IPV6 para habilitarlas en los sitios donde se van a realizar las pruebas.
4. Descripción del ejercicio: instalación de una Vlan en aduana y otra en cascada en el protocolo IPV6, y comenzar a hacer el despliegue del direccionamiento en cascada y en aduana.
5. Habilitar un servidor con el protocolo IPV6 para realizar pruebas de comunicación y ejecución de algunos programas en línea,

Fase 2

1. Configuración de los Firewall y tareas de seguridad.

Fase 3

1. Comenzar a realizar pruebas con base de datos.
2. Verificación el funcionamiento de los micrositios

Fase 4.

1. Despliegue del direccionamiento en toda la red, recordando que debe de trabajar simultáneamente los protocolos IPV4 y IPV6.