## Universidad Nacional Autónoma de México



# Manual de Usuario LiveNX

Herramienta de Visibilidad de la RedUNAM para los Responsables de TIC



Mtro. Hugo Rivera Martínez hugo.rivera@unam.mx

Ciudad Universitaria, 6 de abril de 2022

#### Alcance.

Este manual ha sido elaborado para uso y consulta de los responsables de TIC a quienes se les asigne una cuenta de acceso a la herramienta de visibilidad y uso del tráfico de la red en su dispositivo de Acceso a RedUNAM y/o Acceso a Internet.

#### Requisitos para utilizar la herramienta.

- 1. Contar con las credenciales de acceso (usuario y contraseña) a la aplicación.
- 2. Browser para poder acceder al url: <u>https://visibilidadtic.monitoreo.noc.unam.mx</u>



### Indice

Arquitectura de la solución       4         Capacidades de la Herramienta.       4         Restricciones.       5         Elementos a monitorear dentro de la herramienta LiveNX.       6         ¿Cómo revisar el uso de ancho de banda?       7         Gráfica de ancho de banda (Interface Bandwidth)       10         Modificar la línea de tiempo a consultar.       10         Top de aplicaciones mas usadas (Inbound / Outbound)       12         Navegar dentro de las Conversaciones.       14         Navegar dentro de las Aplicaciones, IP´s y Puertos.       15         Descripción de opciones del Menú.       17         Overview.       17         Sites       12         Alerts       20         Interfaces.       22         Interfaces.       24	Introducción	3
Capacidades de la Herramienta	Arquitectura de la solución	4
Restricciones.       5         Elementos a monitorear dentro de la herramienta LiveNX.       6         ¿Cómo revisar el uso de ancho de banda?       7         Gráfica de ancho de banda (Interface Bandwidth)       10         Modificar la línea de tiempo a consultar.       10         Top de aplicaciones mas usadas (Inbound / Outbound)       12         Navegar dentro de las Conversaciones.       14         Navegar dentro de las Aplicaciones, IP´s y Puertos.       15         Descripción de opciones del Menú.       17         Overview.       17         Sites       12         Alerts       20         Interfaces.       24	Capacidades de la Herramienta	4
Elementos a monitorear dentro de la herramienta LiveNX	Restricciones	5
¿Cómo revisar el uso de ancho de banda?7Gráfica de ancho de banda (Interface Bandwidth)10Modificar la línea de tiempo a consultar10Top de aplicaciones mas usadas (Inbound / Outbound)12Navegar dentro de las Conversaciones14Navegar dentro de las Aplicaciones, IP´s y Puertos15Descripción de opciones del Menú17Sites19Alerts20Devices23Interfaces24	Elementos a monitorear dentro de la herramienta LiveNX	6
Gráfica de ancho de banda (Interface Bandwidth)       10         Modificar la línea de tiempo a consultar.       10         Top de aplicaciones mas usadas (Inbound / Outbound)       12         Navegar dentro de las Conversaciones.       14         Navegar dentro de las Aplicaciones, IP´s y Puertos.       15         Descripción de opciones del Menú.       17         Sites       19         Alerts       20         Devices       23         Interfaces.       24	¿Cómo revisar el uso de ancho de banda?	7
Modificar la línea de tiempo a consultar	Gráfica de ancho de banda (Interface Bandwidth)	10
Top de aplicaciones mas usadas (Inbound / Outbound)       12         Navegar dentro de las Conversaciones.       14         Navegar dentro de las Aplicaciones, IP´s y Puertos.       15         Descripción de opciones del Menú.       17         Overview.       17         Sites       19         Alerts       20         Devices       23         Interfaces.       24	Modificar la línea de tiempo a consultar	10
Navegar dentro de las Conversaciones.       14         Navegar dentro de las Aplicaciones, IP's y Puertos.       15         Descripción de opciones del Menú.       17         Overview.       17         Sites       19         Alerts       20         Devices       23         Interfaces.       24	Top de aplicaciones mas usadas (Inbound / Outbound)	12
Navegar dentro de las Aplicaciones, IP´s y Puertos.       15         Descripción de opciones del Menú.       17         Overview.       17         Sites       19         Alerts       20         Devices       23         Interfaces.       24	Navegar dentro de las Conversaciones	14
Descripción de opciones del Menú.       17         Overview.       17         Sites       19         Alerts       20         Devices       23         Interfaces.       24	Navegar dentro de las Aplicaciones, IP´s y Puertos	15
Overview	Descripción de opciones del Menú	17
Sites       19         Alerts       20         Devices       23         Interfaces       24	Overview	17
Alerts       20         Devices       23         Interfaces       24	Sites	19
Devices	Alerts	20
Interfaces 24	Devices	23
	Interfaces	24



#### Introducción.

La DGTIC haciendo un esfuerzo tanto tecnológico, como financiero y de preparación de su personal académico, ha definido la distribución de accesos a una herramienta de monitoreo licenciado de la empresa LiveAction la cual busca mejorar la experiencia de los responsables de TIC en la visibilidad del tráfico de red y en sus capacidades para diagnosticar y analizar incidentes de su red que puedan afectar al desempeño de su red, aplicaciones y a su vez mejorar la experiencia de sus usuarios.

Actualmente el NOC RedUNAM proporciona el acceso a gráficas de utilización del ancho de banda a través del uso de la herramienta CACTI, la cual es una herramienta Open Source y con la cual solo podemos consultar la utilización del ancho de banda de cada uno de los enlaces que integran la RedUNAM. Esta herramienta permite a los responsables de TIC a consultar cuanto ancho de banda están utilizando ya sea lo que este saliendo de su red hacia RedUNAM o Internet o lo que este entrando de estos mismos orígenes hacia su LAN, pero es todo lo que se puede ver.

Con esta nueva herramienta podemos avanzar no solo en esta visualización, sino que podemos dar un salto en las capas del modelo OSI hasta la capa 7 de este modelo, ahora podremos visualizar que tipo de aplicaciones están siendo utilizadas, podremos indagar sobre lo que esta generando la utilización del ancho de banda, podemos pasar por la capa 3 y 4 de este modelo OSI para saber que direccionamiento IP esta originando una conversación y hacia que dirección IP destino se termina esta conversación, asimismo podemos ver que protocolo TCP/UDP y puerto están siendo utilizados en dicha conversación.

Esta nueva herramienta que se pone a su disposición es un paso de los muchos que se requieren para apoyarlos en sus tareas de transformación y sobre todo para apoyarlos en brindar un mejor servicio para la comunidad universitaria a quienes dan servicio en el día a día de esta Universidad.

Quedamos atentos a sus comentarios esperando que esta herramienta sea de utilidad.



#### Arquitectura de la solución

La integración de la herramienta con la infraestructura de ruteadores de RedUNAM se lleva a cabo a través de:



- a. **<u>Ruteadores</u>**: del fabricante Cisco tienen licencias de Visibilidad y Desempeño de Aplicaciones (AVC y AppX) así como el reconocimiento de aplicaciones (NBAR) y envío de flujos de aplicaciones (Netflow).
- b. <u>SNMP (protocolo simple de gestión de red</u>). El cual permite que el ruteador envíe diversa información acerca de parámetros de uso de CPU, tipo de interfaces, temperatura, disponibilidad, etc.
- c. <u>TACACS+:</u> acrónimo de Terminal Access Controller Access Control System, el cual permite autenticar a los usuarios que acceden a los ruteadores de RedUNAM, con estas credenciales LiveNX puede configurar las interfaces a monitorear con Netflow y SNMP.
- d. <u>ACL (Listas de Acceso)</u>: Los ruteadores tienen configurado permitir que solo ciertos servidores y host puedan ser los servidores de autenticación de acceso (TACACS+), servidores de monitoreo (Cacti, Nagios, LiveNX).
- <u>Centro de Datos</u>: nos proporciona los recursos de cómputo y almacenamiento para que la máquina virtual de LiveNX reciba la información de los ruteadores y dispositivos configurados para su monitoreo.
- f. <u>Aplicación LiveNX</u>: esta herramienta recibe los flujos y los interpreta para presentarlos vía web, con el monitoreamos la infraestructura WAN de RedUNAM, la configuración se puede llevar a cabo desde el cliente ya sea en sistema operativo windows o MAC OS.

#### Capacidades de la Herramienta

Dentro del perfil que se ha configurado para cada uno de los Responsables de TIC, se ha dispuesto que la herramienta proporcioné información de las interfaces que los dispositivos ruteadores que están instalados en la RedUNAM, proporcioné información relacionada a:

a. Utilización del ancho de banda en cada una de las interfaces (LAN/WAN).



- a. Utilización del ancho de banda de entrada y salida visualizada en unidades de Mbps.
- b. Porcentaje de utilización del enlace de acuerdo al ancho de banda contratado (0 100%).
- c. Consulta en periodos específicos de tiempo (15, 30, 60 mins. un día, una semana, un año)
- b. La utilización del ancho de banda de las aplicaciones.
  - a. Se puede visualizar el tipo de aplicaciones utilizadas en cada una de las interfaces configuradas del router.
  - b. Visualizar el tipo de protocolo y puerto que utilizan las aplicaciones, así como las direcciones IPs que intervienen en las conversaciones.
- c. Aviso de Alarmas que se presenten.
  - a. Alertas que se presenten en los cambios de estado de interfaces.
  - b. En los cambios de estados de protocolos de enrutamiento (OSPF/BGP en caso de estar configurado).
- d. Obtención de datos.
  - a. Los puntos A y B pueden ser bajados para consulta del responsable de TIC.

#### **Restricciones.**

- a. Al momento solo se pueden monitorear dispositivos de capa 3 con capacidad de enviar flujos de tráfico con el protocolo Netflow/IPFIX.
- b. El uso de la herramienta solo es para los Responsables de TIC.
- c. Los datos e información que se obtienen con la herramienta solo son para uso de la entidad que la consulta, no puede ser compartida a un tercero para fines que no sean de análisis de incidentes o comportamiento de la red, cualquier uso diferente a esto no es responsabilidad de la DGTIC y su personal Académico responsables de la operación y configuración de la RedUNAM y los componentes de la herramienta LiveNX.



#### Elementos a monitorear dentro de la herramienta LiveNX

Cada una de nuestras entidades universitarias tendrán uno o hasta dos ruteadores (**DEVICES**) conectados entre sí para ofrecer los servicios de Acceso a Internet y/o Acceso a RedUNAM, habrá casos en que Ud. como Responsable de TIC pueda no ser solamente encargado de un solo sitio (**SITE**) sino de más, por lo que podrá tener asignados más dispositivos, y por tanto mayor cantidad de interfaces (**INTERFACES**) para monitorear el estado de consumo de ancho de banda.

Estos elementos podemos verlos en el siguiente diagrama topológico:



La herramienta presentará graficas de consumo de ancho de banda con dos líneas de color azul para el tráfico de entrada (INBOUND) y de color verde para el tráfico de salida (OUTBOUND).

El siguiente diagrama muestra el sentido del tráfico en las interfaces de un dispositivo:



Por lo que habrá que tener en cuenta el sentido del tráfico al momento de consultar la gráfica y de igual manera al consultar el tipo de tráfico que pasa por la interfaz.



#### ¿Cómo revisar el uso de ancho de banda?

El primer paso es ingresar a la Herramienta LiveNX

#### Objetivo: Ingresar a la aplicación

Herramientas: url del sitio, así como usuario y contraseña para ingresar.



1. El usuario debe ingresar a:

https://visibilidadtic.monitoreo.noc.unam.mx

 El usuario ingresará el usuario y contraseña (username y Password) que se le proporcionó vía correo electrónico.

Nota: en caso de no conocer las credenciales o haberlas olvidado favor de solicitar vía correo electrónico a <u>noc.redunam@unam.mx</u> la reposición de este. La reposición se enviará en un lapso de máximo de 10 mins. una vez solicitada la reposición.

Posteriormente en el menú de la aplicación hay varias posibilidades, la primera es seleccionar la opción **Overview.** 

Una vez seleccionada la opción **Overview**, la pantalla presentará el resumen del o los sitios (**SITES**) asignados, los dispositivos (**DEVICES**) asociados al sitio, interfaces del o los dispositivos (**INTERFACES**)





		0		🔒 visibilidadtic.monitoreo.noc.ur	nam.mx		Ċ						
				🔥 LiveNX   Overvie	w								
≡ LiveAction <sup>∞</sup> ■	X						2	• 0	🌲 51				
Overview Enter Filter Request H	iere ()	DEVICES [2] CAMPUS_JURIQUILLA_LS CAMPUS_JURIQUILLA_IN	1 2L ITERNET	INTERFACES [2] GigabitEthernet0/0/3(CAM GigabitEthernet0/0/0)(CAM	<b>9</b> PUS_JURIQUILL PUS_JURIQUILL	4 4 8 4	CAMPU: CAMPU: Interface BGP pee	S_JURIQI S_JURIQI e Gigabiti er 187.18 er 170.23	UILLA_INTEI UILLA_INTEI Ethernet0/2 8.69.153 foi 9.151.42 foi	CAMPUS_J CAMPUS_J CAMPUS_J	Apply filte 17 Mar 2 15 Mar 2 11 Mar 2 11 Mar 2 21 Feb 2 21 Feb 2	r 2 Auto 022, 11:44 AM 022, 04:52 PM 022, 01:07 PM 022, 11:59 AM 022, 05:48 PM	
				<ul> <li>GigabitEthernet0/0/0.390(i</li> <li>GigabitEthernet0/0/2(2CAM</li> <li>GigabitEthernet0/0/2(2CAM</li> <li>GigabitEthernet0/0/3(3CAM</li> <li>GigabitEthernet0/2/0(CAM</li> <li>GigabitEthernet0/2/1(2CAM</li> </ul>	:ampus_juriq pus_juriquill pus_juriquill pus_juriquill pus_juriquill		bor pee	EI 201.90	21.110101	CAMP 03_90	211602	222, 00.13 P W	

En esta pantalla de **OVERVIEW**, en la columna de **INTERFACES** seleccionar la interfaz que se quiere visualizar, una vez que se seleccione, dar clic y se abrirá en una nueva ventana:

INTERFACES: 7		NOTA: para ver la descripción de cada una de las interfaces
	1	y conocer que esta conectado en cada interfaz del DEVICE
INTERFACES 🖸	0	hacer clic en la barra de color de la sección de INTERFACES.

Se abrirá una nueva página con la información de las interfaces, entre ellas la descripción de las interfaces y su ancho de banda:

■ LiveAction	NX						▲ 6 💻 4 🔹	0 🔔 40	{} -	0- <b>-</b>
terfaces Enter Filter	Request Here						Apply filter Apr 04, 20	22 18:55:00 → A	pr 04, 2022 19:10	:00 15 Min
							Q Se	arch		
INTERFACE NAME	STATUS	SITE	O DEVICE	IP ADDRESS 🗘	SUBNET MASK 🗘	INTERFACE L 🗘	DESCRIPTION	¢	SERVICE PR 🗘	INPUT CAPA
Interface Name	Good ~	Site	Device	IP Address	Subnet M	Interface	Description		Service P	Input Ca
GigabitEthernet0/0/0.390	•	JURIQUILLA	CAMPUS_JURIQ	201.96.21.109	255.255.255		TMX CNOC INTERNET 60	IOM [C60-20		600 Mbp
GigabitEthernet0/0/3	•	JURIQUILLA	CAMPUS_JURIQ	192.100.199	255.255.255		PRUEBA A FORTINET-FIB	RA (WAN 1)		1 Gbp
GigabitEthernet0/0/0	•	JURIQUILLA	CAMPUS_JURIQ	192.100.200	255.255.255		TPE L2L 200M [TFE-D-L2]	L74561] 20	TPE	1 Gbp
GigabitEthernet0/0/2	•	JURIQUILLA	CAMPUS_JURIQ	132.248.254	255.255.255		A ROUTER FMVZ_TEQUIS	QUIAPAN		1 Gbp
GigabitEthernet0/2/0	•	JURIQUILLA	CAMPUS_JURIQ	192.100.199	255.255.255		PRUEBA A FORTINET-COE	BRE (WAN 2)		1 Gbp
GloabitEthernet0/2/1	•	JURIOUILLA	CAMPUS JURIO	187.188.69.1	255.255.255		TPE INTERNET 700M [SE	NP-D-ID868	TPE	1 Gb

Aquí señalamos la descripción de cada una de las interfaces del o los dispositivos que se tienen configurados para el rol de nuestro acceso a la herramienta, con esta descripción ya sabremos hacia donde nos esta conectando esta interfaz.

#### Información de la Interfaz.

Una vez seleccionada la Interfaz, se podrán ver los detalles de esta interfaz, como son: información de la interfaz, gráficas de utilización de ancho de banda, aplicaciones más utilizadas, conversaciones, lo cual nos ayudará a visibilizar el comportamiento de nuestra red, sus aplicaciones y sus hosts.



> JURIQ	UILLA > Device: CAN	IPUS_JURIQUIL	LA_INTERNE > Interface:	GigabitEthernet0/0/0.390		M	lar 18 2022 18·45·00 → M	Apr 18 2022 18:50:00	5 Mine V C Auto
						IV	lai 10, 2022 10.45.00 → N	nai 10, 2022 10.30.00	STWINS V D Add
Status IP Add	bitEthernet0/0/0.3 s: Good dress: 201.96.21.109	90	10 Availa	0% ability	0 Active Alerts	1	۲		-
rface Detai	ails				^		TPE		•
dwidth (Sp	peed): 600.00 Mbps	IF Inde	: 9	IP Address: 201.96.21.1	09				Ŀ
reviated N	lame: Gi0/0/0.390	Interfac	e Type: I2vlan	Subnet Mask: 255.255.2	255.252				
cription: 1 0-2009-000	TMX CNOC INTERNET 60 08]	OM							
ríona Dand	d								
rface Band	dwidth				^		RQULLA L2L.noc.unem.mx		
rface Band	dwidth				^		RQUILL L2L noc.unem mx		
rface Band	dwidth				^ =		ROULLA L2L noc.unam mx		
rface Band	dwidth				^		ROULD LIZE noc.unem mr		
rface Band	dwidth				^ =		ROULL LEL nocurrent me		
rface Band	dwidth				^ =		ROULLA LZL nocurram me		
rface Band	dwidth				=		ROULLY LZL noc. yrwn me		
rface Band 50 25 0 18:46:47	dwidth		184500	18.4900	1849.47		ROULLI LZ noc unam me		
o 18:46:47	dwidth		18.48.00	18-9900	1849.47		ROULLA LZL noc onem me		
o 18:46:47	dwidth		18.45.00 Q. Search	18-990	18.49.47		NOULD L22 FRE share for		
rface Band 50 25 0 18:46:47 egend ≎	dwidth	Average 🗘	Q Search 95th Percentile Bandwidth ≎	18.4900 99th Percentile Bandwidth ≎	18.49.47				
rface Band 50 25 0 18:46:47 egend ≎	dwidth Name O Inbound Bandwidth	Average ≎ 33.35 Mbps	18.48:00 Q. Search 95th Percentile Bandwidth ≎ 31.02 Mbps	18-49:00 99th Percentile Bandwidth ≎ 31.02 Mbps	18.49.47		ROLL LEL NU UNI N		
rface Band 50 25 0 18:46:47 egend ≎	Name O Inbound Bandwidth Outbound Bandwidth	Average ◊ 33.35 Mbps 12.41 Mbps	18.45:00 Q. Search 95th Percentile Bandwidth ≎ 31.02 Mbps 12.72 Mbps	18-49:00 99th Percentile Bandwidth ≎ 31.02 Mbps 12.72 Mbps	18.49.47 () ± Peak Bandwidth 46.04 Mbps 13.23 Mbps		NOLLA LEL NEL GRAN AN		

En esta pantalla pueden consultar:

#### Información de la Interfaz:

GigabitEthernet0/0/0.390 Status: Good IP Address: 201.96.21.109	100% Availability	O Active Alerts
---	----------------------	--------------------

- Información de la Interfaz: GigabitEthernet0/0/0.390.
- Status: Good (que este operando con normalidad).
- IP Address: el direccionamiento IPv4 que se tiene configurada en esa interfaz.
- Availability: la disponibilidad de la interface en un periodo de tiempo en un tiempo definido (por default son 5 mins.).
- Active Alerts: las alertas que están presentes en la interfaz.

#### Detalles de la Interface (Interface Details):

Interface Details			^
Bandwidth (Speed): 600.00 Mbps	IF Index: 9	IP Address: 201.96.21.109	
Description: TMX CNOC INTERNET 600M [C60-2009-0008]	intenace type. izviai	Sublet mask. 200,200,200,202	

• **Bandwidth (Speed):** el ancho de banda contratado y conectado en esta interfaz. Este dato ayuda a calcular el porcentaje de utilización de dicha interfaz y para calcula a futuro un posible



crecimiento. De no tener este dato correctamente configurado en el dispositivo entonces la información presentada será incorrecta.

- **IF Index:** el índice de la interface dentro del dispositivo.
- IP Address: la dirección IPv4 configurada en la interfaz.
- Subnet Mask: la máscara de la IP signada a la interface.
- Abbreviated Name: el nombre de la interface monitoreada.
- Interface Type: El tipo de interface conectada.
- **Description:** La descripción configurada en la interfaz, esta información es tomada del dispositivo y es utilizada para identificar el enlace y saber a que proveedor hay que llamar para poder dar seguimiento a un incidente.

**NOTA:** estos datos son obtenidos por la herramienta LiveNX una vez que se esta haciendo el proceso de configuración dentro de la herramienta de este dispositivo utilizando el protocolo SNMP.

#### Gráfica de ancho de banda (Interface Bandwidth)

Esta es la gráfica de utilización del enlace que se esta consultando, como comentamos la línea azul en el ancho de banda de entrada y la verde el ancho de banda de salida.

La gráfica maneja dos planos, en el eje de las X (horizontal) muestra el periodo de tiempo a consultar, y en el eje de las Y (vertical) nos muestra el ancho de banda en unidad de medida de Megabits por segundo (Mbps).

Interfac	e Band	lwidth						^
40							=	=
Average (Mbps)								
0	:01:47			19:03:00		19:04:00	19:04:47	
					Q Search		11 1	<u>↑</u>
Leger	nd 🗘	Name 🗘	Average 🗘	95th Percent	tile Bandwidth 🗘	99th Percentile Bandwidth $\Diamond$	Peak Bandwidth 🗘	
		Inbound Bandwidth	27.34 Mbps		28.06 Mbps	28.06 Mbps	30.09 Mbps	s
-		Outbound Bandwidth	12.39 Mbps		13.16 Mbps	13.16 Mbps	13.39 Mbps	s

#### Modificar la línea de tiempo a consultar

La gráfica que se muestra por default es de una duración de 5 minutos. Para consultar un periodo más largo de tiempo se puede hacer a través de la selección del tiempo. En la parte superior derecha de la página del sitio, se muestra el icono desplegable, dando clic en él se despliega la siguiente ventana para la configuración del tiempo a consultar.



			Mar	14, 20	22 23:	10:00	→ Mar	21, 202	2 23:10:00	Week		
		SET	THE E	ND D/	INTER	RVAL						
	<	Mar 2	2022	>	Today				5 Mins			
	s	М	м т w		т	F	FS		15 M	Min		
	27	28	1	2	3	4	5		Но	ur		
	6	7	8	9	10	11	12		Da	ly		
	13	14	15	16	17	18	19					
	20	21	22	23	24	25	26		We	ek		
	27	28	29	30	31	1	2		30 D	ays		
	3	4	5	б	7	8	9					
/	~	^				Reset	to Nov	v				
1	1 :	10	PN	1								
`	/	~				Ар	ply					

Aquí podemos seleccionar los intervalos de:

- 5 minutos
- 15 minutos
- Una hora
- Un día
- Una semana o
- Hasta por 30 días.

a partir del día que se haga la consulta.

También podemos consultar en el tiempo si utilizamos las flechas en donde se encuentra la leyenda del mes , Jan 2022 en caso de querer consultar el ancho de banda utilizado en cierta fecha que ya haya sobrepasado los 30 días que nos da la herramienta, podemos retroceder por mes, seleccionando la flecha de la izquierda nos retrocede a meses anteriores al consultado y en la flecha a la derecha hacia meses posteriores, y poder llevar a cabo la consulta en los periodos de tiempo antes mencionados.

Como resultado podemos ver la gráfica de utilización extendida en el tiempo que hayamos configurado en la consulta.





Una facilidad de la gráfica es que con el puntero del mouse podemos seleccionar cualquier punto de las líneas del ancho de banda utilizado y nos mostrará una leyenda en donde nos de los datos específicos de la fecha y hora de consulta, así como el ancho de banda utilizado.

Debajo de la gráfica se presenta una tabla con varias columnas, a continuación, las describimos:

Legend $\Diamond$	Name 🗘	Average $\Diamond$	95th Percentile Bandwidth $\diamondsuit$	99th Percentile Bandwidth $\diamondsuit$	Peak Bandwidth $\diamondsuit$
	Inbound Bandwidth	1.70 Mbps	1.76 Mbps	1.76 Mbps	2.69 Mbps
	Outbound Bandwidth	1.31 Mbps	1.81 Mbps	1.81 Mbps	2.00 Mbps

- Legend. El color que se va a utilizar en la gráfica para cada uno de los anchos de banda a utiliza, de entrada, o salida.
- Name. El nombre que utilizará cada leyenda.
- Average. El promedio de utilización del ancho de banda en el periodo de tiempo consultado.
- **95th Percentile Bandwidth.** El 95 percentil indica que el 95 % del tiempo el ancho de banda utilizado esta por debajo del valor expuesto.
- **99th Percentile Bandwidth.** El 99 percentil indica que el 99 % del tiempo el ancho de banda utilizado esta por debajo del valor expuesto.
- Peak Bandwidth. Indica el pico de utilización de ancho de banda.

#### Top de aplicaciones mas usadas (Inbound / Outbound)

Estas gráficas nos mostrarán las aplicaciones más utilizadas en el periodo de tiempo consultado, al igual que en la gráfica de ancho de banda, se podrá modificar el periodo de tiempo a consultar.



Estas aplicaciones están categorizadas a partir de lo que el ruteador Cisco reconoce y clasifica a través del uso del protocolo de Reconocimiento de Aplicaciones Basado en Red (Network Based Application Recognition, NBAR), esta información es enviada al servidor LiveNX para que sea interpretada para ser presentada en estas gráficas.

Este reconocimiento de aplicaciones se actualiza cada 3 meses por parte del fabricante Cisco por lo que de manera constante estamos tratando de mantener actualizado el paquete de NBAR en cada uno de los ruteadores.

La gráfica mide la tasa de uso en Megabits por segundo (Mbps) (Eje Y), durante el transcurso del tiempo (Eje X).



La tabla contiene diversas columnas:

- Legend. El color a utilizer para cada una de las aplicaciones.
- Application. Nombre de las aplicaciones reconocidas por NBAR.
- Total Flows. Número total de flujos generados por la aplicación.
- Total Bytes. Número total de bytes generados por la aplicación.
- Total Packets. Número total de paquetes generados por la aplicación.
- Average Bit Rates. Tasa promedio de bits.
- Average Packet Rates. Tasa promedio de paquetes.
- Peak Bit Rates. Tasa de bits máxima.
- Peak Packet Rates. Tasa de paquetes máxima.

Esta gráfica de utilización nos permitirá visualizar que aplicaciones estan ocupando nuestro ancho de banda, nos permite adentrarnos (drill down) para saber que aplicaciones utilizan



más ancho de banda en cierto periodo de tiempo, así como que dirección IP es la que esta haciendo uso de esta aplicación con lo cual podemos detectar que aplición pueda saturar el enlace o si hay comunicaciones sospechosas hacia Internet o viceversa de Internet hacia nuestra red.

#### Navegar dentro de las Conversaciones.

Una funcionalidad adicional a esta tabla es que se puede navegar dentro de los datos de la aplicación, al dar click derecho o izquierdo, (dependiendo de la configuración del mouse) en el nombre de la apliación y se mostrará una ventana emergente con las opciones a consultar.

Legend $\Diamond$	Application $\Diamond$	Total Flows $\Diamond$	Total Bytes 🗘	Total Packets 🗘							
	ssl	4771	10.09 MB	50,365							
	oj Apply ssl to Sea	Apply ssl to Search Filter									
	oi Apply Specific F	Apply Specific Flow to Search Filter									
	St Drill down on ss	Drill down on ssl as Application									
	gi Drill down on ss	sl as Top Conversat	IONS	6245							
	h1 Drill down on ss	as interrace band	width	8639							
	pi Drill down on ss	as IPs and Ports		20,951							
	di Drill down to Sp	Drill down to Specific Flow on Flow Path Analysis Story									
	Uhknown	210	1.13 IVID	4723							
	ms-services	444	1.06 MB	2015							

**Drill down on application as Top Conversations**. Con está opción podemos revisar el top de conversaciones, al seleccionarla se abre una nueva ventana y nos muestra mas detalle de quienes estan utilizando esta aplicación (conversando).

En esta gráfica podemos ahondar sobre la aplicación que queremos consultar. Nos ayuda a visualizar que IP´s son las que están interviniendo en una conversación y que ancho de banda estan utilizando, con ello podriamos consultar con al usuario si es una comunicación válida o hay alguna incidencia a resolver.

Drill down o	n ssl as Top Conv	ersations	from Application							v	iew Options ~	Print			
Top Conversat	tions (Flow)														
Device: CAMPUS Flex Search: devi End Time: Mar 22	wides CAMPUS_URIQUILL_INTERNET Interface: GlgabitEthernet0/00.390 Display Filter: No Disp														
D Bit Rate (Mbps)	199 247 217 145/192 248,112 40 40 408,131,169/132,248,243,131 41 42 2010,132,137,244,242,843,131 41 42 2010,132,137,244,242,8431 42 42 2010,132,137,244,242,8431 42 42 2010,132,244,114,24 41 42 231,132,137,224,114,24 41 42 231,132,137,123,244,117,210 41 42 231,132,137,132,244,114,24 41 42 231,132,134,137,132,244,114,24 41 42 431,132,134,137,132,244,114,24 41 42 431,132,134,137,132,244,134,144,14 41 42 431,132,144,144,14 41 42 431,132,144,144,14 41 42 431,134,144,14 41 42 431,134,144,14 41 42 431,144,144,144,144,144,144,144,144,144,														
01:01			01:02		01	:03		01:04		01:05					
« < Page 1	)/9>»								Q Search		Π	1 1			
Legend 🗘	Src IP Addr 🛇	Site 🗘	Dst IP Addr 🛇	Dst Site 🗘	Total Flows 🗘	Total Bytes 🛇	Total Packets 🗘	Average Bit Rate 🗘	Average Packet Rate 🗘	Peak Bit Rate 🛇	Peak Packet Rate 🗘	Src C			
	189.247.217.145	Internet	132.248.142.40	Internet	1	58.64 MB	39,558	1.56 Mbps	131.86 pps	7.82 Mbps	659 pps	MX/I			
	40.83.131.189	Internet	132.248.248.131	Internet	3353	5.88 MB	30,884	156.89 Kbps	102.95 pps	158.50 Kbps	104 pps	US/L			
	142.250.105.132	Internet	132.248.248.251	Internet	1	2.19 MB	1498	58.30 Kbps	4.99 pps	291.51 Kbps	24 pps	US/L			
	208.80.54.70	Internet	132.248.219.41	Internet	4	2.08 MB	9353	55.46 Kbps	31.18 pps	70.42 Kbps	40 pps	US/L			
	34.231.233.177	Internet	132.247.161.69	Internet	29	153.31 KB	298	4.09 Kbps	0.99 pps	5.82 Kbps	1 pps	US/L			



La descripción de los campos de la tabla es la siguiente:

- Legend. Color a utilizar por cada conversación.
- Src IP Addr. Dirección IP origen.
- Site. Hacia donde se comunica.
- Dst IP Addr. Dirección IP destino.
- Dst Site. Sitio Destino
- Total Flows. Flujos totales generados en la conversación.
- Total Bytes. Bytes totales generados.
- Total Packets. Número total de paquetes.
- Average Bit Rate. Tasa promedio de bits.
- Average Packet Rates. Tasa promedio de paquetes.
- Peak Bit Rates. Tasa de bits máxima.
- Peak Packet Rates. Tasa de paquetes máxima.
- Src Country. País de origen de la conversación.
- **Dst Country.** País destino de la conversación.

#### Navegar dentro de las Aplicaciones, IP's y Puertos.

**Drill down on** <u>application</u> **as IPs and Ports**. Con esta opción podemos visualizar las conversaciones ahora también a través de las IP's (origen/destino) y los puertos que utilizan para tener más visibilidad para apoyar en el análisis y diagnóstico de posibles incidencias o comportamientos en el tráfico de la red.

Drill down a	on ssl as IPs and P		View Option	ns ~ Prir									
Ps and Ports	(Flow)												
Pevice: CAMPU: Flex Search: dev End Time: Mar 2	S_JURIQUILLA_INTERNET ice="CAMPUS_JURIQUIL 2, 2022 01:40:00 CST (GP	Interface: GigabitEthe LA_INTERNET.noc.unam.r VT-06:00) Input Capaci	ernet0/0/0.390 Displa mx" & interface="Gigabit ity: 600 Mbps Output	IY Filter: No Displ Ethernet0/0/0.39 I Capacity: 600 N	lay Filtering Dir 10° & flow.app="ss Abps Bin Interv	rection: Inbound Flow 7 I'' Bin Duration: Auto val: 1 minute	Type: Basic Flow Should Walt Fo	Execution Typ r Dns Resolution:	e: Time Series Start Tim	Sort By: Bit Ra e: Mar 22, 202	te 12 01:35:00 CST (GMT	-06:00)	
200 200 100 0												208.80.34, 70/132. 34, 102, 246, 111/13 66, 249, 74, 33/132, 2 142, 251, 33, 229/13 20, 84, 233, 211/132 34, 199, 14, 62/132, 2 157, 240, 19, 11/132 130, 211, 8, 196/132 130, 211, 8, 196/132 173, 243, 138, 31/13 34, 120, 115, 102/13 70tal	248.219.41/1C 2248.124.240/ 248.227.101/T 2.248.179.210 247.20.41/TC 247.20.41/TC 247.20.251/T 2.248.142.407 2.248.142.407 2.248.219.196
01:36		01:	37		01:38			01:39	0.00		01:40		
< Page 1	/100 > >>								Q Sea	rch			
Legend 🗘	Src User Name $\Diamond$	Dst User Name 🗘	Src IP Addr 🗘	Src Site 🗘	Src Port 🗘	Dst IP Addr 🗘	Dst Site 🗘	Dst Port 🗘	Protocol 🗘	DSCP 🗘	Application $\Diamond$	Total Flows 🗘	Total Bytes 🗘
-	-	-	208.80.54.70	Internet	443	132.248.219.41	Internet	63339	TCP	0 (BE)	ssl	5	2.64 MB
-	-	-	34.102.246.111	Internet	443	132.248.142.40	Internet	4782	TCP	0 (BE)	ssl	5	92.29 KB
-	-	-	66.249.74.33	Internet	52838	132.248.227.101	Internet	443	TCP	0 (BE)	ssl	1	58.90 KB
-	-	-	142.251.33.229	Internet	443	132.248.179.210	Internet	63735	TCP	0 (BE)	ssl	8	39.90 KB
	-	-	20.84.233.211	Internet	443	132.247.20.41	Internet	45054	TCP	0 (BE)	ssl	17	24.44 KB
			34.199.14.62	Internet	443	132.247.88.100	Internet	65169	TCP	0 (BE)	ssl	2	24.16 KE

La descripción de los campos de la tabla es la siguiente:



- Legend. Color a utilizar por cada conversación.
- Src User Name. Nombre del usuario origen, esta opción no presenta datos pues no se tienen los datos a mostrar.
- **Dst User Name**. Nombre del usuario destino, esta opción no presenta datos pues no se tienen los datos a mostrar.
- Src IP Addr. Dirección IP origen.
- Site. Hacia donde se comunica.
- Dst IP Addr. Dirección IP destino.
- Dst Site. Sitio Destino.
- Dst Port. Puerto destino.
- **Protocol.** Protocolo (TCP/UDP) utilizado.
- **DSCP.** Si se tuviera etiquetado con calidad de servicio diferente al default aquí se mostraría.
- Application. Protocolo de la aplicación o nombre de la aplicación reconocida por NBAR.
- Total Flows. Flujos totales generados en la conversación.
- Total Bytes. Bytes totales generados.
- Total Packets. Número total de paquetes.
- Average Bit Rate. Tasa promedio de bits.
- Average Packet Rates. Tasa promedio de paquetes.
- Peak Bit Rates. Tasa de bits máxima.
- Peak Packet Rates. Tasa de paquetes máxima.



#### Descripción de opciones del Menú.

**Objetivo:** Barra de navegación **Herramientas**: haber ingresado a la herramienta



El icono de menú de la barra de estado en la parte superior izquierda de la página expande la barra de navegación que muestra las opciones que estan disponibles para consulta.en su perfil de usuario.

La mayoría de las tareas que realizará en LiveNX son accesibles desde la barra de navegación. La barra de navegación está disponible haciendo clic en el icono de menú en la parte superior izquierda de la barra de estado.

Se mostraran las diferentes opciones de acciones que tiene disponible en su perfil.

**Objetivo:** Pantalla Overview **Herramientas**: haber ingresado a la herramienta

#### Pantalla Overview.

La página de Overview (descripción general) muestra el estado de los sitios, los dispositivos y las interfaces. También muestra alertas activas y alertas históricas que se hallan presentado en el o los dispositivos configurados para su perfil.

Para cada uno de los SITES, DEVICES e INTERFACES habrá links y en cada uno de los links el usuario puede profundizar utilizando estos enlaces para explorar más.



		0	í	visibilidadtic.monitoreo.noc.	unam.mx		Ċ				C		:::
				🛕 LiveNX   Overv	iew								+
≡ LiveAction <sup>™</sup>	чх						<mark>=</mark> 1	• 0	🌲 0				
Overview Enter Filter Request H	lere									<>	Apply filte	r 📿 Au	to
Sites, Devices, Interfaces by Statuses	S					Ad	tive Alerts	s					
						A	LERTS 🗹				TIME OP	ENED	
SITES: 1		DEVICES: 2		INTERFACES: 7		11	Interface	e GigabitE	thernet0/0/	2 on CAMPU	. 28 Oct 20	21, 07:09 PM	
SITES 🗹	0	DEVICES 🗹	0	INTERFACES 🗹	0								
JURIQUILLA		CAMPUS_JURIQUILLA	INTERNET	<ul> <li>GigabitEthernet0/0/2 CAI</li> </ul>	VPUS_JURIQUILL								
		CAMPUS_JURIQUILLA	_L2L	<ul> <li>GigabitEthernet0/0/0 CAI</li> <li>GigabitEthernet0/0/0.390</li> </ul>	VPUS_JURIQUILL								
				<ul> <li>GigabitEthernet0/0/2 CAI</li> </ul>	MPUS_JURIQUILL								
				<ul> <li>GigabitEthernet0/0/3 CAI</li> </ul>	VIPUS_JURIQUILL								
				<ul> <li>GigabitEthernet0/2/0 CAI</li> <li>GigabitEthernet0/2/1 474</li> </ul>	VPUS_JURIQUILL								
				<ul> <li>Organizationicity 2/ 1.474</li> </ul>	10/mii 00_00NiQ								

- **SITES.** Se refiere al nombre del sitio al que se esta ingresando, por lo regular es el nombre como se conoce a la entidad en la herramienta de monitoreo.
- **DEVICES:** Se refiere a los dispositivos asociados al SITE, son los quipos ruteadores que están instalados en la entidad universitaria y que proporcionan los servicios de Acceso a RedUNAM y Acceso a Internet a través de los enlaces WAN contratados con un proveedor de servicios (ISP).
- **INTERFACES.** En esta columna se enlistan cada una de las interfaces que integran los **DEVICES** y que están siendo monitoreados con la herramienta. Para saber a que **DEVICE** esta relacionado se pude colocar encima de ella y aparecerá el nombre completo de la interfaz.
- Active Alerts. En este apartado se pueden visualizar las alertas que se han presentado en las INTERFACES Y DEVICES, en caso de presentarse una alarma, podrá darle clic en alguna de ellas y aparecerá una nueva ventana que nos proporciona mas detalles de esta, más adelante detallaremos esta pantalla.



• **Barras de estado**, la herramienta nos presenta el estado del sitio que se esta monitoreando, en caso de existir una alarma, la barra de estado cambia de color, por ejemplo:

Sites, Devices, Interfaces by Statuses		Active Alerts					
			ALERTS 🗹	TIME OPENED			
SITES: 1	DEVICES: 2 INTERFACES: 7		Interface GigabitEthernet0/0/2 on CAMPUS_JURIQUILLA_INTERNET.noc.un	28 Oct 2021, 07:09 PM			

Verde: que esta todo funcionando correctamente.

Amarillo: se presenta una alarma en alguno de los componentes referidos a la columna.

Rojo: se presenta una alarma que interrumpe la operación de alguno de los componentes de la columna.



**NOTA**: En caso de que no haya alarmas el color de la barra de estado de cada una de las columnas SITE, DEVICES e INTERFACES deberá presentarse en verde, en caso contrario cambiará a color amarillo y nos ira mostrando de lo general (SITE) a lo particular (INTERFACES) en donde esta presentándose la alarma.

#### **Objetivo:** Acceder a **Sites Herramienta:** haber ingresado a la herramienta y al Menú



La página de navegación de Sitios presenta una lista de todos los sitios en LiveNX y destaca un resumen de sus estados de rendimiento.

Al hacer clic en un sitio, se accederá a la página de detalles del sitio.

≡ LiveAction <sup>®</sup>	NX				New Features! 🔒 0	<b>1</b> • 0	0 {-} ~					
Sites         Enter Filter Request Here         Ø         Apply filter         Dec 01, 2021 23:30:00 -> Dec 01, 2021 23:45:00         15 Min         Ø         Auto												
						Q Search						
SITE NAME	SITE STATUS 🗘	DEVICE REACHABILITY 🗘	DEVICE CPU/MEMORY	PEAK UTILIZATION IN	PEAK UTILIZATION OUT $\diamondsuit$	CONGESTION DROPS	INTERFACE ERRORS	\$				
Site Name	All ~	All ~	All ~	Peak Utilization In	Peak Utilization	All ~	Interface Errors					
JURIQUILLA	•	•	•	0.6%	20.64%	•		0				

El **SITE NAME** por lo regular tendrá el nombre de la entidad a monitorear.

La información que se presenta en este apartado esta relacionada a la disponibilidad:

• **SITE STATUS**: nos puede mostrar las alertas que están activas en el dispositivo al momento de consultar, de un clic en el círculo, en caso de estar en un color diferente al amarillo aparecerá una ventana emergente con el resumen de la alerta que esta presente.



SITE STATUS	<b>\$</b>	DEVICE REACHABILITY	٥	DEVICE CPU/MEMOR	Y O	PEAK UTILIZATION IN	$\diamond$	PI
All	~	All	~	All	~	Peak Utilization In		
•		•		-		3	06%	
	Site: JURIQU	IILLA 🗹					×	¢
	Active Alerts Warning: Interface Gig	Impacting Status: 1	on CAI	MPUS_JURIQUILLA_I	L2L.noc.u	inam.mx could not be re	ached	
	Active Alerts	: <b>1</b> 7				Alert Hist	ory 🗹	i

Al abrir la ventana emergente aparecen dos opciones <u>Active Alerts</u> y <u>Alert</u> History las cuales nos dan diferentes visiones de las alertas que se han presentado en el dispositivo <u>(DEVICE)</u>.

Active Alerts. Nos muestran las alertas que están activas en el dispositivo:

≡	LiveActi					▲ 3	<b>1</b> •	0	4 61	{} <b>- 0 -</b>	👗 juriquilla 👻		
Alerts	Site: JL	IRIQUILLA Ente	er Filter Request Here								Apply filter		
			Active		History								
Res	olve Ignore	Acknowle	edge Refresh Alerts	View Options v				Q Sea	irch				
	SEVERITY \$	SITE \$	DEVICE \$		TIME OPENED	ACTIVE FOR 🗘	CATEGORY	0	TYPE	٥	THIRD PARTY 🗘		
	All ~	Site	Device	Description			All	~	All	~	Third Par		
	Warning	JURIQUILLA	CAMPUS_JURIQUILLA	Interface GigabitEthernet0/2/1.474 on CA	11 Mar 2022, 01:0	2 days	Device, Int	terface	Interfac	ce Reachabilty			
	Critical	JURIQUILLA	CAMPUS_JURIQUILLA	BGP peer 187.188.69.153 for CAMPUS_JU	11 Mar 2022, 11:5	2 days	Network		BGP Pe	er Connection Change			
	Critical	JURIQUILLA	CAMPUS_JURIQUILLA	BGP peer 170.239.151.42 for CAMPUS_JU	21 Feb 2022, 05:4	20 days	Network		BGP Pe	er Connection Change			
	Critical	JURIQUILLA	CAMPUS_JURIQUILLA	BGP peer 201.96.21.110 for CAMPUS_JURI	21 Feb 2022, 05:1	20 days	Network		BGP Pe	er Connection Change			

En esta nueva pantalla podemos ver la categorización de las alertas por su severidad <u>(SEVERITY</u>), las cuales pueden ser <u>Critical, Warning</u> o <u>Informational (Infor)</u>, las alertas criticas interrumpen servicios, en tanto que las <u>warning</u> pueden o no degradar servicios, en tanto que las <u>informational</u> no interrumpen o degradas los servicios, sólo es información que puede ser de interés para la operación del dispositivo.

Hay otros campos referentes al **SITE** y **DEVICE**, los cuales son los asignados a su cuenta de usuario, en device puede que se presenten mas de un dispositivo, dependiendo de la cantidad de dispositivos configurados en su entidad universitaria.

- **DESCRIPTION**. En este campo se presenta una descripción de la alerta que se esta presentando, no es personalizable ni editable, es la alerta que la propia herramienta interpreta sobre los eventos que transcurren en el dispositivo.
- **TIME OPENED.** Este campo se refiere a la fecha y hora en que se presenta la alerta. Pueden existir alertas previas a la fecha en que se consulte debido a que se resolvieron, pero no se borraron del panel, o que aún este presente la alerta y no se ha resuelto.
- ACTIVE FOR. En este campo podemos ver cuantos días ha estado activa dicha alerta. Aunque ya se haya atendido y haya sido resuelta si esta alerta no se borra del panel continuará contando el tiempo hasta que no haya sido retirada del panel.
- CATEGORY. Esta columna nos informa sobre el tipo de alerta que se esta presentando, si se refiere a un tema de DISPOSITIVO, INTERFACES, RED, APLICACIÓN o SISTEMA.
- **TYPE.** Este campo esta relacionado a la categoría de la alerta que se esta presentando, puede ser una categoría de RED y el TYPE del cambio de estado de un protocolo, por ejemplo. Estos



dos últimos campos nos ayudan a hacer un primer diagnóstico de la alerta para iniciar un segundo proceso de diagnóstico con el objetivo de resolver lo que esta sucediendo en el dispositivo o servicio involucrado.

**GESTIÓN DE ALERTAS:** para llevar a cabo el borrado de las alertas una vez atendidas y resueltas se debe seleccionar la casilla referente a la alerta a borrar, esta casilla se encuentra en la primera columna de la tabla, la que esta más a la izquierda de la tabla, al seleccionarla se activaran las diferentes acciones que puede aplicar a la alerta seleccionada.

Active												
Resol	Ignore	Acknowledg	e	Refresh Alerts	Vie	w Options 🗸						
	SEVERITY 🗘	SITE		DEVICE	٥	DESCRIPTION						
	All ~	Site		Device		Descriptio						

- **Resolve.** Se ha solucionado la alerta.
- **Ignore.** Se puede ignorar la alerta, no afecta a la operación del ninguno de los servicios o dispositivo.
- Acknowledge. Es una alerta conocida que por el momento no podemos solucionarla y no afecta a algún servicio.
- Refresh Alerts. Refrescar la tabla de alertas para revisar si se presenta alguna alerta nueva.

**HISTORY ALERTS**. Es la otra opción que existe, la cual nos presenta un histórico de las alertas que se han presentado en el dispositivo.

Al ingresar a este apartado puede que no vea ninguna alerta:

≡ LiveAction <sup>™</sup> NX	🔺 3 📁 1 🔹 0 🌲 61 {-} 🖓 🚱 🍰 juriquilla
Alerts Site: JURIQUILLA Enter Filter Request Here	Apply filter         Mar 12, 2022 23:50:00 → Mar 13, 2022 23:50:00         Day
Active	History
É	
You don't have an	iy alerts to display.

Para poder revisar en el pasado, tenemos la opción del lado superior derecho, la opción de las fechas que necesitamos revisar, esta opción aparecerá también en otros sitios de la herramienta para poder ver la utilización del ancho de banda en un tiempo especifico, por ejemplo:



Se tienen diferentes opciones, las cuales podrán seleccionar de acuerdo con sus necesidades, sólo habrá que considerar que cuanto más tiempo atrás se quiera consultar el procesamiento de la herramienta puede llevar más tiempo pues es una herramienta que es utilizada por casi 100 usuarios.



		SET	THE E	ND D/	ATE &	TIME	
	<	Mar	2022	>		Тс	day
	s	м	т	w	т	F	s
	27	28	1	2	3	4	5
	6	7	8	9	10	11	12
	13	14	15	16	17	18	19
	20	21	22	23	24	25	26
	27	28	29	30	31	1	2
	3	4	5	б	7	8	9
	^	^				Reset	to Now
1	1 :	54	PN	4		10001	tonton
,	~	~				Ар	ply

Como ejemplo, al seleccionar 30 días se presentan las siguientes alertas de manera históricas:

Site: JUR	Enter Filter Req	uest Here		\$	Apply filter Feb 11, 202	2 23:00:00 → Mar 13, 2022 2	3:00:00 30 Days 🗸
	1	Active			History		
All	06:00 am 06:00 am 06: Feb 11th Feb 13th Fe	00 am 06:00 am 06:00 b 15th Feb 17th Feb 1	am 06:00 am 06:00 am 9th Feb 21st Feb 23rd	06:00 am 06:00 am 06:00 am 1 Feb 25th Feb 27th Mar 1st	06:00 am Mar 3rd Mar 5th	06:00 am 06:00 am 06 Mar 7th Mar 9th M	x00 am 06:00 am lar 11th Mar 13th
ve Ignore	Acknowledge	Activate Refresh A	lerts View Options ~		Q Sea	rch	
SEVERITY 🗘	SITE \$	DEVICE	DESCRIPTION			≎ status	TIME OPENED
All ~	Site	Device	Description			All ~	
Warning	JURIQUILLA	CAMPUS_JURIQUILLA	Interface GigabitEthernet0/2/1.4	74 on CAMPUS_JURIQUILLA_L2L.n	oc.unam.mx could not be rea.	Active	11 Mar 2022, 01:07P
Critical	JURIQUILLA	CAMPUS_JURIQUILLA	BGP peer 187.188.69.153 for CA	MPUS_JURIQUILLA_L2L.noc.unam	mx has changed states to IDL	E. I Active	11 Mar 2022, 11:59A
Warning	JURIQUILLA	CAMPUS_JURIQUILLA	Interface GigabitEthernet0/2/0 o	n CAMPUS_JURIQUILLA_L2L.noc.u	nam.mx is reachable again.	Resolved	05 Mar 2022, 08:54P
<ul> <li>Info</li> </ul>	JURIQUILLA	CAMPUS_JURIQUILLA	NIM subslot 0/1 for CAMPUS_JU	JRIQUILLA_L2L.noc.unam.mx has c	hanged states to disabled.	Resolved	05 Mar 2022, 08:15P
<ul> <li>Info</li> </ul>	JURIQUILLA	CAMPUS_JURIQUILLA	NIM subslot 0/2 for CAMPUS_JU	JRIQUILLA_L2L.noc.unam.mx has c	hanged states to disabled.	Resolved	05 Mar 2022, 08:15P
Critical	JURIQUILLA	CAMPUS_JURIQUILLA	CAMPUS_JURIQUILLA_INTERNE	T.noc.unam.mx could again be read	hed	Resolved	05 Mar 2022, 06:17P
Critical	JURIQUILLA	CAMPUS_JURIQUILLA	CAMPUS_JURIQUILLA_L2L.noc.u	unam.mx could again be reached		Resolved	05 Mar 2022, 06:17P
	Site: JUR	Site: JURQUILLA Enter Filter Rec All	Site: JURIQUILA Enter Filter Request Here  Ative  All   Geb0 am 06:00 am 00:00 am 00	Site:         JURIQUILLA         Enter Filter Request Here           All         ✓         06:00 am         06:00 am <t< td=""><td>Site:     JURIQUILLA     Enter Filter Request Here        <ul> <li>Active</li> <li>Active</li> <li>Active</li> <li>Occo am</li> <li>O</li></ul></td><td>Site:       JURIQUILLA       Enter Filter Request Here       Image: Constraint of the second of th</td><td>Site:       JURIQUILLA       Enter Filter Request Here       chive       History         Active       History         All          <ul> <li>Mar 2bit</li> <li>Mar 2bit</li></ul></td></t<>	Site:     JURIQUILLA     Enter Filter Request Here <ul> <li>Active</li> <li>Active</li> <li>Active</li> <li>Occo am</li> <li>O</li></ul>	Site:       JURIQUILLA       Enter Filter Request Here       Image: Constraint of the second of th	Site:       JURIQUILLA       Enter Filter Request Here       chive       History         Active       History         All <ul> <li>Mar 2bit</li> <li>Mar 2bit</li></ul>

Los Campos restantes de Device se refiere a la disponibilidad y estatus del dispositivo:

- **DEVICE REACHABILITY.** Nos proporciona la información de si el dispositivo puede ser alcanzable desde el servidor de LiveNX ubicado en Ciudad Universitaria.
- DEVICE CPU/MEMORY. Nos alerta si el estado del CPU o Memoria se encuentra dentro de los parámetros funcionales (menor a 80% de utilización).
- **PEAK UTILIZATION IN**. Por default se tiene un lapso de 15 minutos de monitoreo, este campo nos muestra el pico de utilización en porcentaje del dispositivo de entrada.
- **PEAK UTILIZATION OUT**. este campo nos muestra el pico de utilización en porcentaje del dispositivo de salida.



- **CONGESTION DROPS.** En caso de congestion del dispositivo mostrara si el estado es optimo o tiene alguna degradación.
- INTERFACE ERRORS. Esta última columna muestra la cantidad de errores del dispositivo en esta ventana de 15 minutos de monitoreo.

#### **Objetivo:** Acceder a **Devices Herramienta:** haber ingresado a la herramienta y al Menú



La página de navegación de **Devices** presenta una lista de todos los dispositivos de capa 3, gestionados por el NOC RedUNAM, asociados al perfil de usuario y configurados en LiveNX.

Al hacer clic en un sitio, se accederá a la página de detalles de los dispositivos.

#### Objetivo: Características de Devices

Herramienta: haber ingresado a la herramienta y al Menú

≡ LiveAction <sup>™</sup>	NX							1 • 0 🌲	59 {-} ~	0- <b>2</b>		
Devices Enter Filter Request F	Devices         Enter Filter Request Here $\phi$ Apply filter          Mar 14,2022 093500 - Mar 14,2022 095000          15 Min $Q$ Auto											
Q. Search												
DEVICE	SITE 🗘	STATUS 🗘	IP ADDRESS	AVAILABILITY 🗘	CPU/MEMORY 🗘	CPU AVG	MEMORY AVG	TAGS 🗘	VENDOR 🗘	туре 🗘	VERSION	
Device	Site	All ~	IP Address	All ~	All ~	CPU AVG	Memory	Tags	Vendor	Туре	Version	
CAMPUS_JURIQUILLA_L2L	JURIQUILLA	•	192.100.200	•	•	1%	29%	-	Cisco	Router	16.9.6	
CAMPUS_JURIQUILLA_INTERN	JURIQUILLA	•	192.100.199	•	•	2%	19%	-	Cisco	Router	15.5(3)S4	

- **Device.** En este campo se muestran los nombres de los dispositivos que están siendo monitoreados y que están asociados a su perfil de usuarios, cabe hacer notar que habrá perfiles que tienen mas de un dispositivo ya que hay perfiles que son responsables de TIC de uno o mas entidades universitarias, por lo que también asociamos a su perfil estos dispositivos.
- Site. A que sitio esta relacionado este dispositivo.
- **Status**. Se presentará, al igual que en los campos de Devices, un icono de color que determina el estado del dispositivo.



- IP Addresses. Direccionamiento IPv4 con el cual estamos monitoreando a cada uno de los dispositivos asignados a su perfil.
- Availability. Se presenta un semáforo de color, el cuál en caso de presentarse algún incidente cambiará el color de verde a amarillo (precaución) o rojo (incidente). En el caso de cambiar de color puede dar clic en el semáforo y les dará una ventana con información a detalle.
- CPU/Avg | Memory/Avg. Al igual que a disponibilidad, se muestra un semáforo de color, en caso de que el CPU o Memoria tengan una utilización mayor al 80% cambiará el color del semáforo y habrá que tomar acciones para solucionar el incidente, por ejemplo, reportarlo a la mesa de servicio.
- Vendor. Nos da la información que fabricante es el equipo, en este caso es Cisco.

#### Objetivo: Acceder a Interfaces

Herramienta: haber ingresado a la herramienta y al Menú



La opción de Interfaces nos dará la información relacionada a las interfaces contenidas en los **DEVICES** asignados al rol.

Estas interfaces podrán ser los enlaces L2L (dedicados hacia C.U.), VPN (red de MPLS con QoS) y hacia Internet, dependerá de la cantidad de enlaces que tiene cada uno de los **DEVICES** de la entidad.

Al hacer clic en un sitio, se accederá a la página de detalles de los dispositivos.

#### **Objetivo:** Características de **Interfaces Herramienta:** haber ingresado a la herramienta y al Menú

≡ LiveAction <sup>™</sup> ■								<b>▲</b> 6 <b>■</b> 4	• 0 🐥 40			
Interfaces Enter Filter Request Here								Apply filter Apr 0	4, 2022 19:20:00 → Ap	04, 2022 19:35:00	15 Min 🧷 Auto	
	Q. Search											
INTERFACE NAME 🗘 STATUS 🗘	SITE 🗘	DEVICE $\Diamond$	IP ADDRESS	SUBNET MASK	INTERFACE L 0	DESCRIPTION	SERVICE PR 0	INPUT CAPACITY	OUTPUT CAPACITY 🗘	WAN TYPE	TAGS O	
Interface Name All ~	Site	Device	IP Address	Subnet Mask	Interface	Description	Service P	Input Capacity	Output Capa	All ~	Tags	
GigabitEthernet0/0/0.390	JURIQUILLA	CAMPUS_JURIQUILLA_INTERNET	201.96.21.109	255.255.255.252		TMX CNOC INTE		600 Mbps	600 Mbps			
GigabitEthernet0/0/2	JURIQUILLA	CAMPUS_JURIQUILLA_INTERNET				CONEXION SD W		1 Gbps	1 Gbps			
GigabitEthernet0/0/3	JURIQUILLA	CAMPUS_JURIQUILLA_INTERNET	192.100.199.161	255.255.255.252		PRUEBA A FORTL.		1 Gbps	1 Gbps			
GigabitEthernet0/0/0	JURIQUILLA	CAMPUS_JURIQUILLA_L2L	192.100.200.54	255.255.255.252		TPE L2L 200M [	TPE	1 Gbps	1 Gbps	WAN		
GigabitEthernet0/0/2	JURIQUILLA	CAMPUS_JURIQUILLA_L2L	132.248.254.101	255.255.255.252		A ROUTER FMVZ		1 Gbps	1 Gbps			
GigabitEthernet0/2/0	JURIQUILLA	CAMPUS_JURIQUILLA_L2L	192.100.199.77	255.255.255.252		PRUEBA A FORTL.		1 Gbps	1 Gbps		•	
GigabitEthernet0/2/1	JURIQUILLA	CAMPUS_JURIQUILLA_L2L	187.188.69.154	255.255.255.252		TPE INTERNET 7	TPE	1 Gbps	1 Gbps	WAN	•	

• Interface Name. Describe la interfaz a consultar.



- **Status**. Se presentará, al igual que en los campos de **Devices**, un icono de color que determina el estado del dispositivo.
- Site. A que sitio esta relacionada la interfaz.
- **Device.** En este campo se muestran los nombres de los dispositivos que están siendo monitoreados y que están asociados a su perfil de usuarios, cabe hacer notar que habrá perfiles que tienen mas de un dispositivo ya que hay perfiles que son responsables de TIC de uno o mas entidades universitarias, por lo que también asociamos a su perfil estos dispositivos.
- IP Addresses. Direccionamiento IPv4 asignada a cada una de las interfaces.
- Mask. Máscara de red asociada al direccionamiento IPv4 de cada interfaz.
- **Description.** Descripción configurada a cada interfaz, en esta descripción esta el identificador del enlace, en caso de ser un enlace WAN y las siglas del proveedor TPE en caso de ser Total Play o TMX CNOC en caso de ser de TELMEX.
- Service Provider. El proveedor de servicio que proporciona el enlace WAN.
- Input Capacity. Ancho de banda de entrada configurado en cada interfaz, físicamente se tienen interfaces de 1 Gbps, pero el ancho de banda contratado puede ser diferente a este Gbps, por lo que se configura manualmente en cada una de las interfaces, de este dato la herramienta toma la información que presenta en este campo.
- **Output Capacity.** Ancho de banda de salida configurado en cada interfaz, funciona igual que el input capacity.

Para cualquier duda o apoyo pueden enviar correo a <u>noc.redunam@unam.mx</u> en donde podemos apoyarlos a utilizar la herramienta.





Mtro. Hugo Rivera Martínez NOC RedUNAM Supervisión del proyecto Elaboración del documento

**Colaboraciones:** 

Ing. Carlos Vicente Altamirano NOC RedUNAM Revisión del Documento

Ing. Lourdes Jiménez Ramírez NOC RedUNAM Revisión del Documento

Ing. Marcial Martínez Quinto NOC RedUNAM Revisión del Documento

