Universidad Nacional Autónoma de México

DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

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

Indice

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.

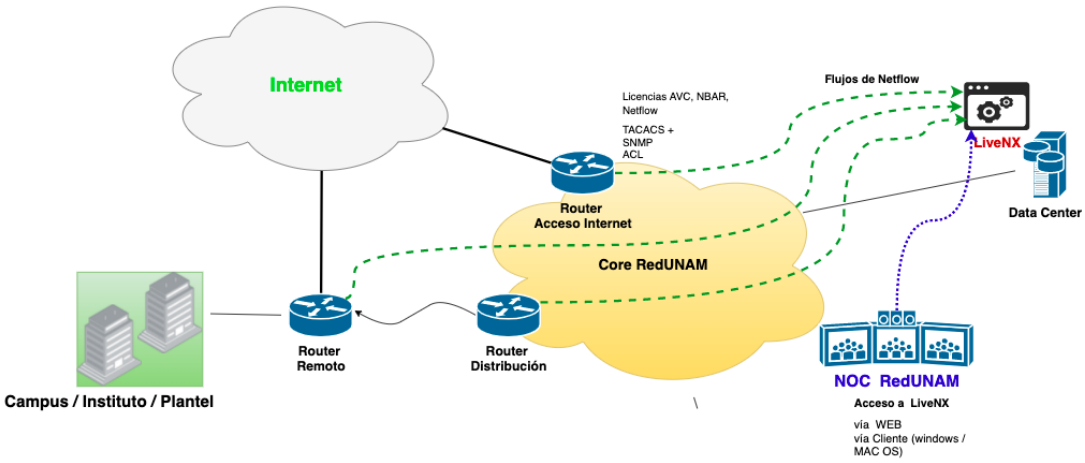
Con esta nueva herramienta podemos avanzar no solo en esta visualización, sino que podemos dar un salto en las capas del modelo OSI hasta la capa 7 de este modelo, ahora podremos visualizar que tipo de aplicaciones están siendo utilizadas, podremos indagar sobre lo que esta generando la utilización del 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. **Ruteadores:** 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. **SNMP (protocolo simple de gestión de red**). El cual permite que el ruteador envíe diversa información acerca de parámetros de uso de CPU, tipo de interfaces, temperatura, disponibilidad, etc.
c. **TACACS+:** 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. **ACL (Listas de Acceso)**: 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).
e. **Centro de Datos:** 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. **Aplicación LiveNX**: 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.

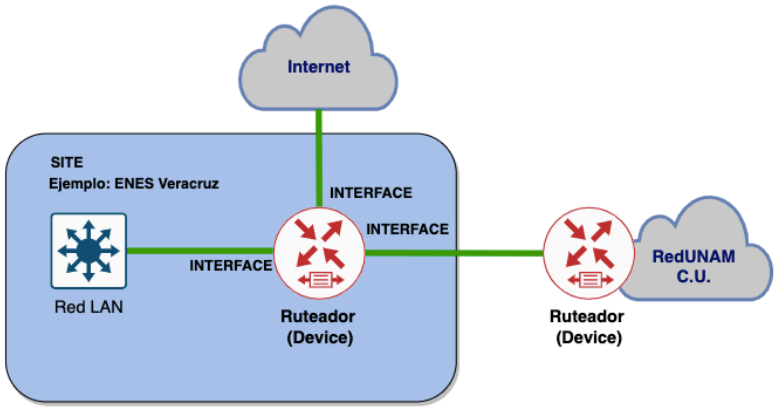
Restricciones.

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

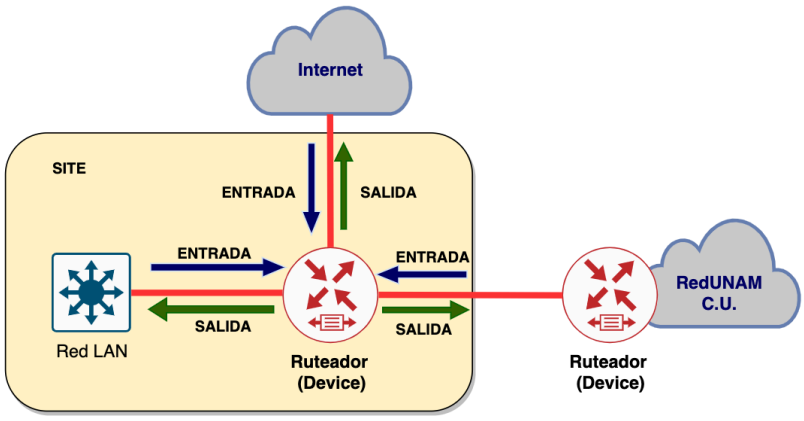
Cada una de nuestras entidades universitarias tendrán uno o hasta dos ruteadores (**DEVICES**) conectados entre sí para ofrecer los servicios de Acceso a Internet y/o Acceso a RedUNAM, habrá casos en que Ud. como Responsable de TIC pueda no ser solamente encargado de un solo sitio (**SITE**) sino de 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:

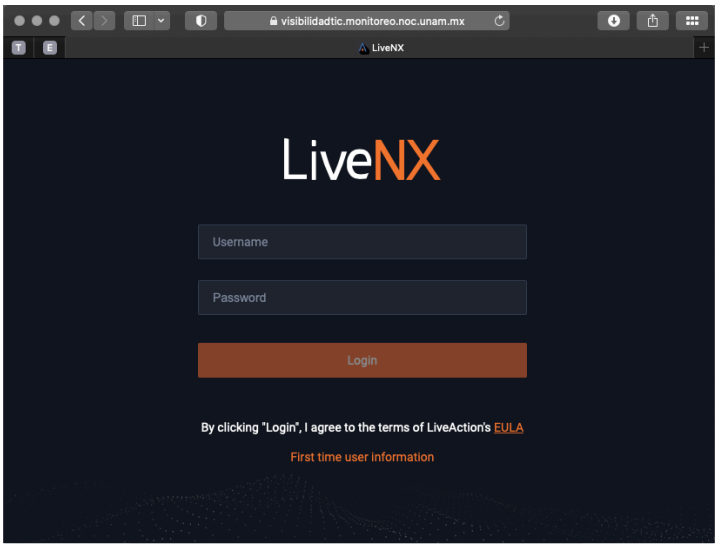


Por lo que habrá que tener en cuenta el sentido del tráfico al momento de consultar la gráfica y de igual manera al consultar el tipo de tráfico que pasa por la interfaz.

¿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:

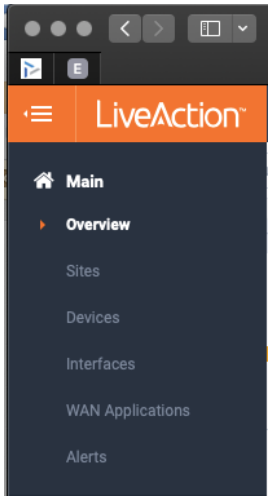
https://visibilidadtic.monitoreo.noc.unam.mx

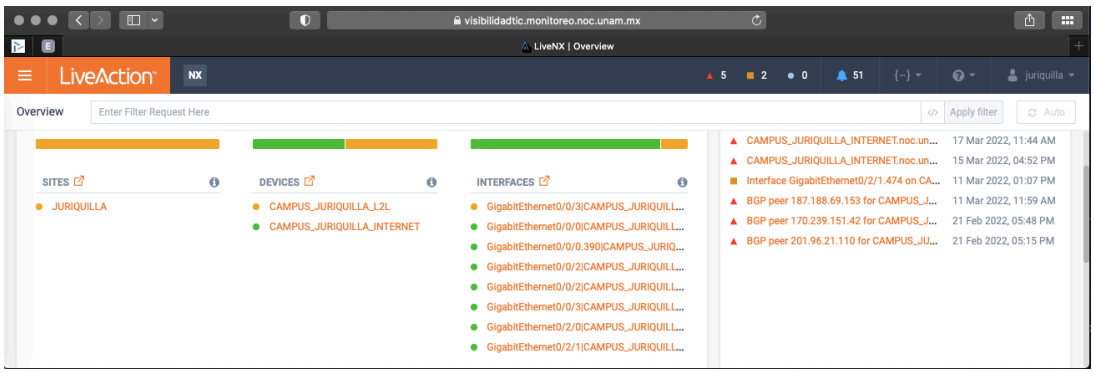
2. El usuario ingresará el usuario y contraseña (username y Password) que se le proporcionó vía correo electrónico.

Nota: en caso de no conocer las credenciales o haberlas olvidado favor de solicitar vía correo electrónico a noc.redunam@unam.mx 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**)

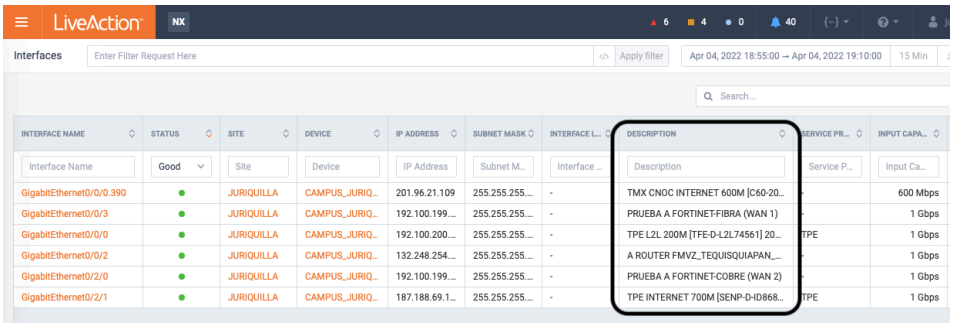




En esta pantalla de **OVERVIEW,** en la columna de **INTERFACES** seleccionar la interfaz que se quiere visualizar, una vez que se seleccione, dar clic y se abrirá en una nueva ventana:

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

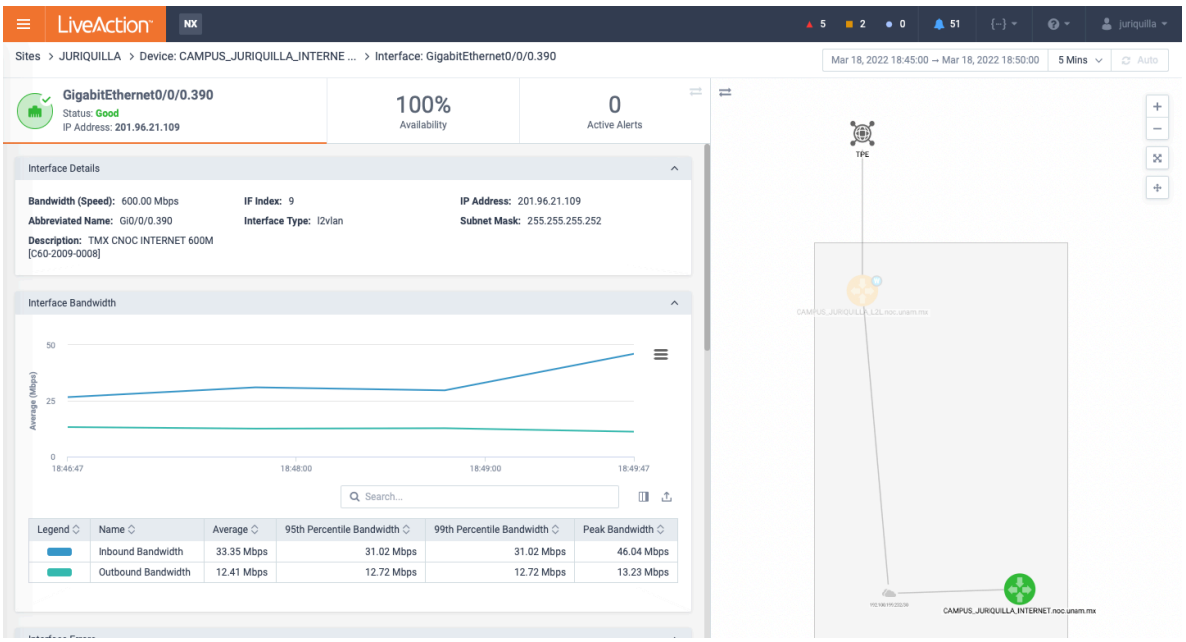
Se abrirá una nueva página con la información de las interfaces, entre ellas la descripción de las interfaces y su ancho de banda:



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.

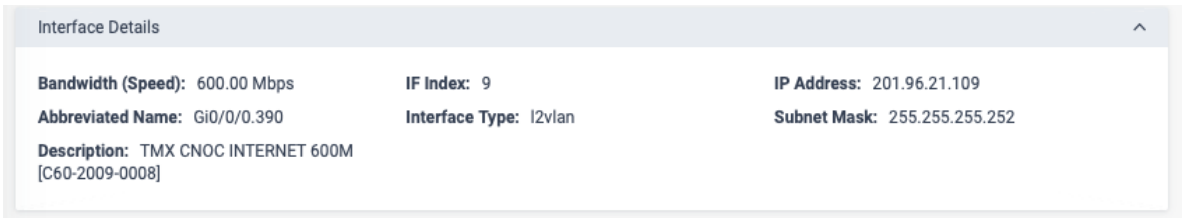


En esta pantalla pueden consultar:

Información de la Interfaz:

- **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):



- **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.

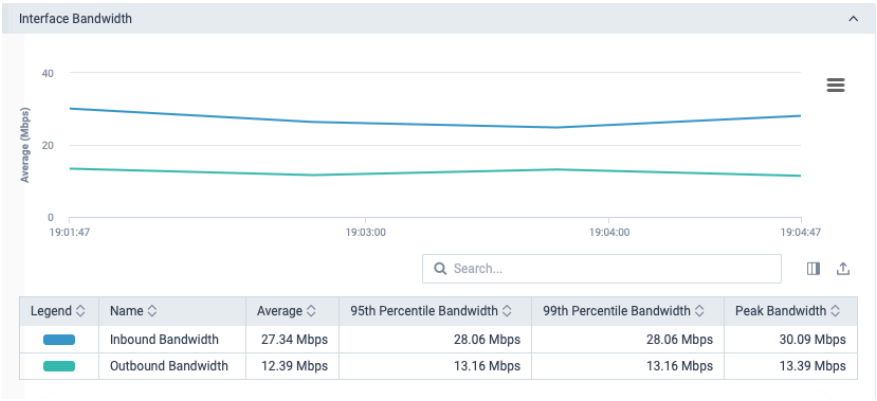
- **IF Index:** el índice de la interface dentro del dispositivo.
- **IP Address:** la dirección IPv4 configurada en la interfaz.
- **Subnet Mask:** la máscara de la IP signada a la interface.
- **Abbreviated Name:** el nombre de la interface monitoreada.
- **Interface Type:** El tipo de interface conectada.
- **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.

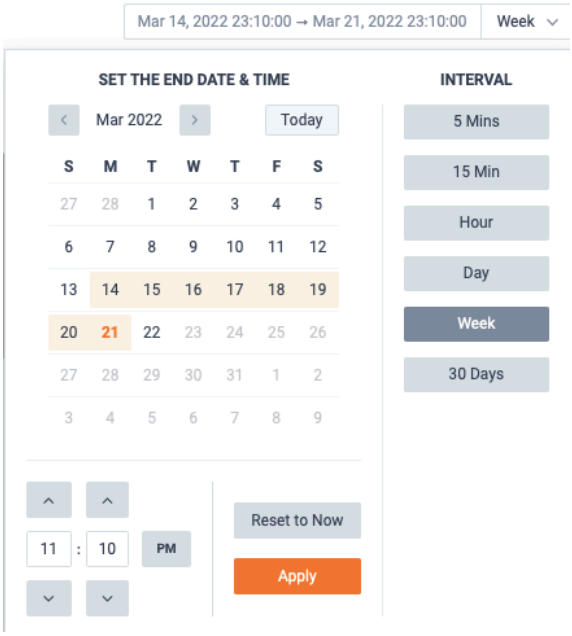
La gráfica maneja dos planos, en el eje de las X (horizontal) muestra el periodo de tiempo a consultar, y en el eje de las Y (vertical) nos muestra el ancho de banda en unidad de medida de Megabits por segundo (Mbps).



Legend	Name	Average	95th Percentile Bandwidth	99th Percentile Bandwidth	Peak Bandwidth
	Inbound Bandwidth	27.34 Mbps	28.06 Mbps	28.06 Mbps	30.09 Mbps
	Outbound Bandwidth	12.39 Mbps	13.16 Mbps	13.16 Mbps	13.39 Mbps

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.



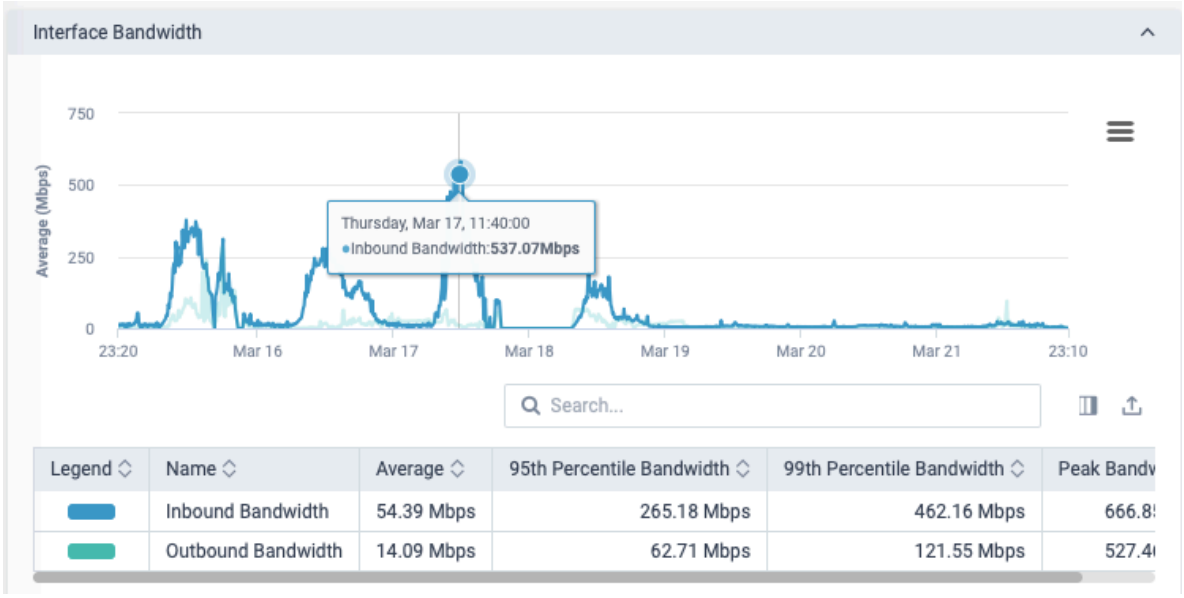
Aquí podemos seleccionar los intervalos de:

- 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	Name	Average	95th Percentile Bandwidth	99th Percentile Bandwidth	Peak Bandwidth
	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.

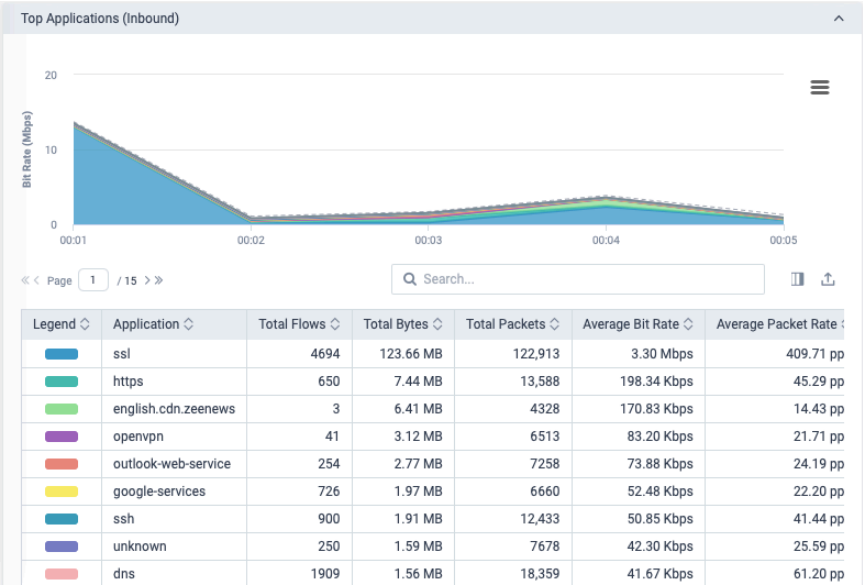
Top de aplicaciones mas usadas (Inbound / Outbound)

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).



Legend	Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate
	ssl	4694	123.66 MB	122,913	3.30 Mbps	409.71 pp
	https	650	7.44 MB	13,588	198.34 Kbps	45.29 pp
	english.cdn.zeenews	3	6.41 MB	4328	170.83 Kbps	14.43 pp
	openvpn	41	3.12 MB	6513	83.20 Kbps	21.71 pp
	outlook-web-service	254	2.77 MB	7258	73.88 Kbps	24.19 pp
	google-services	726	1.97 MB	6660	52.48 Kbps	22.20 pp
	ssh	900	1.91 MB	12,433	50.85 Kbps	41.44 pp
	unknown	250	1.59 MB	7678	42.30 Kbps	25.59 pp
	dns	1909	1.56 MB	18,359	41.67 Kbps	61.20 pp

La tabla contiene diversas columnas:

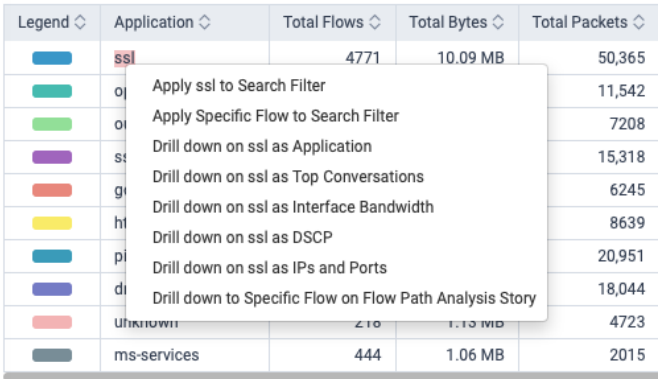
- **Legend.** El color a utilizer para cada una de las aplicaciones.
- **Application.** Nombre de las aplicaciones reconocidas por NBAR.
- **Total Flows.** Número total de flujos generados por la aplicación.
- **Total Bytes.** Número total de bytes generados por la aplicación.
- **Total Packets.** Número 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.

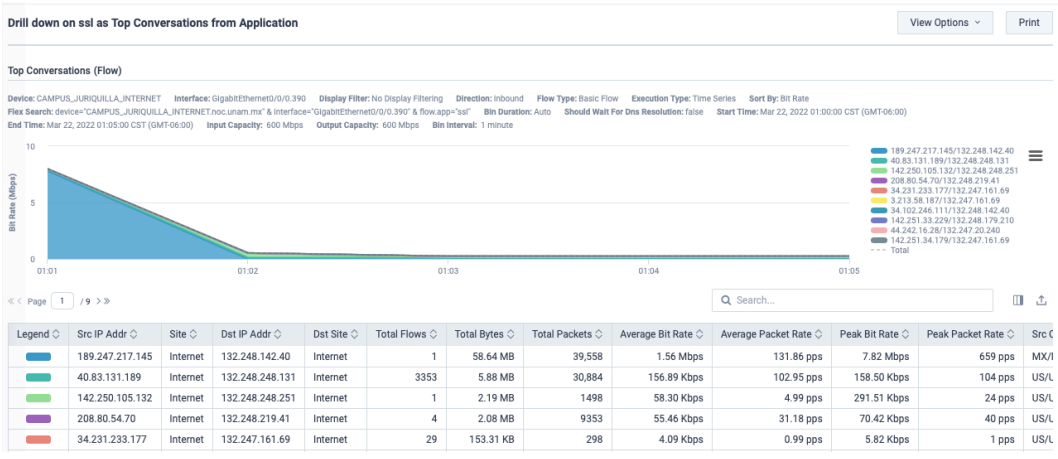
Navegar dentro de las Conversaciones.

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.



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.

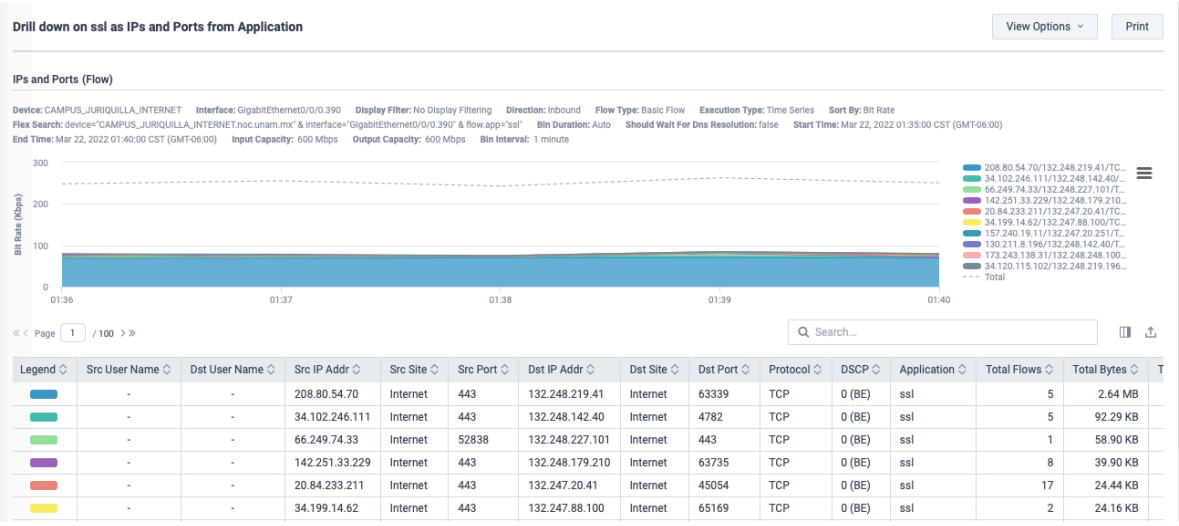


La descripción de los campos de la tabla es la siguiente:

- **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 *application* **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.



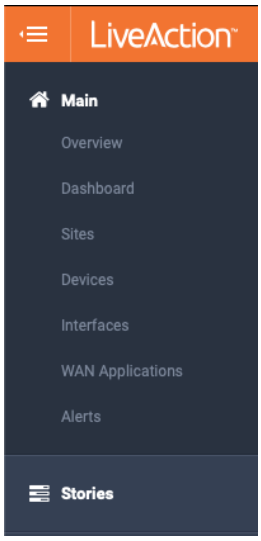
Legend	Src User Name	Dst User Name	Src IP Addr	Src Site	Src Port	Dst IP Addr	Dst Site	Dst Port	Protocol	DSCP	Application	Total Flows	Total Bytes
	-	-	208.80.54.70	Internet	443	132.248.219.41	Internet	63339	TCP	0 (BE)	ssl	5	2.64 MB
	-	-	34.102.246.111	Internet	443	132.248.142.40	Internet	4782	TCP	0 (BE)	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 KB

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.

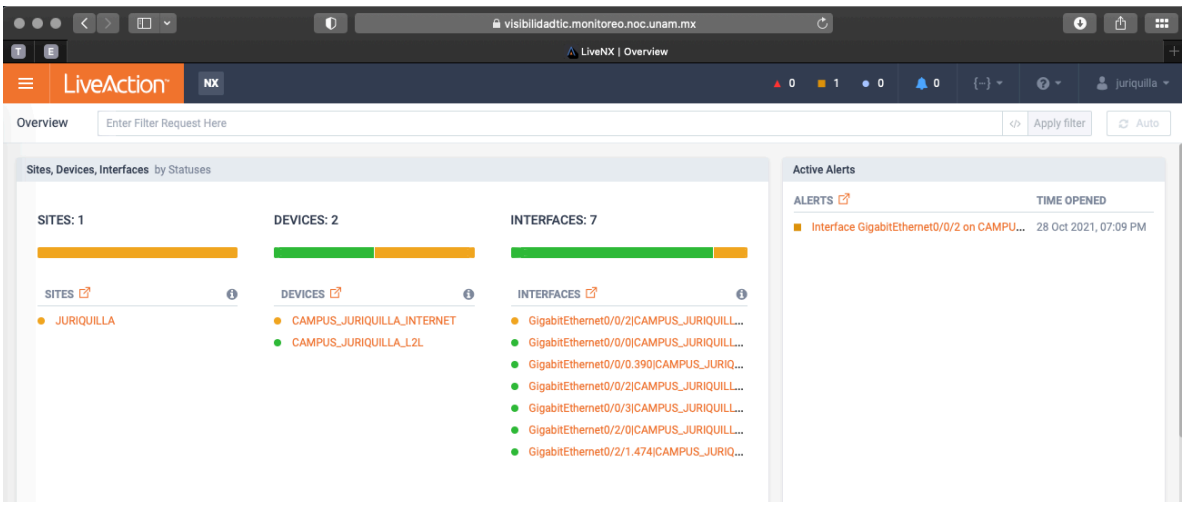
La mayoría de las tareas que realizará en LiveNX son accesibles desde la barra de navegación. La barra de navegación está disponible haciendo clic en el icono de menú en la parte superior izquierda de la barra de estado.

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.



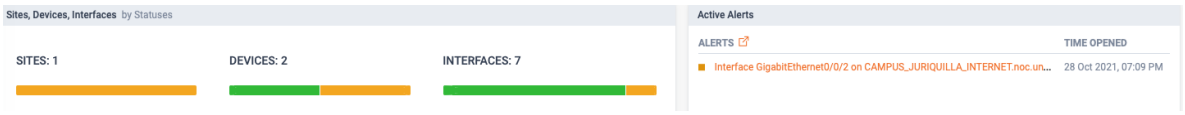
- **SITES.** Se refiere al nombre del sitio al que se esta ingresando, por lo regular es el nombre como se conoce a la entidad en la herramienta de monitoreo.

- **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.

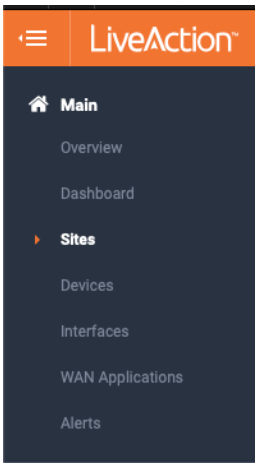
- **Barras de estado**, la herramienta nos presenta el estado del sitio que se esta monitoreando, en caso de existir una alarma, la barra de estado cambia de color, por ejemplo:



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.

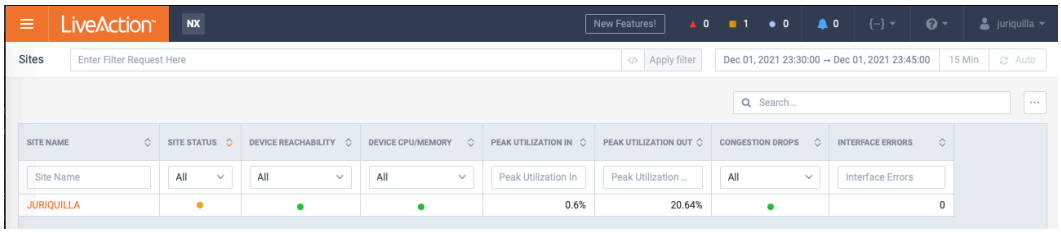
NOTA: En caso de que no haya alarmas el color de la barra de estado de cada una de las columnas SITE, DEVICES e INTERFACES deberá presentarse en verde, en caso contrario cambiará a color amarillo y nos ira mostrando de lo general (SITE) a lo particular (INTERFACES) en donde esta presentándose la alarma.

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.

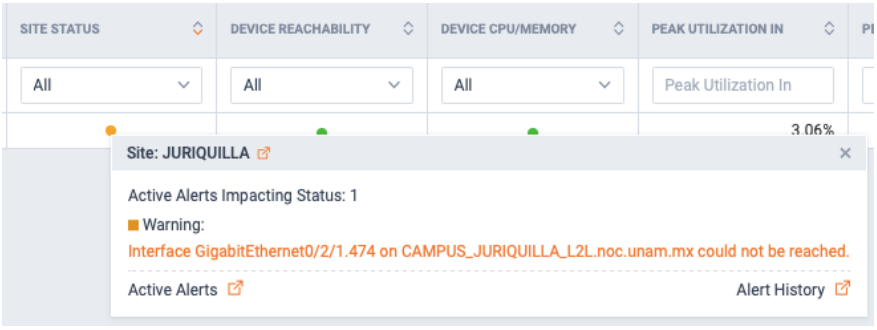
Al hacer clic en un sitio, se accederá a la página de detalles del sitio.



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

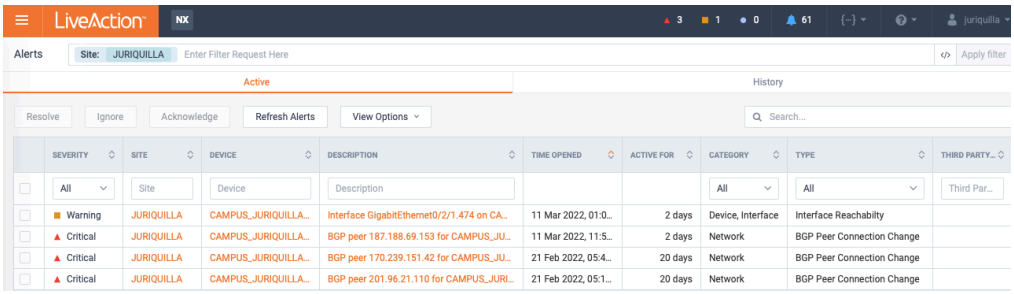
La información que se presenta en este apartado esta relacionada a la disponibilidad:

- **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.



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

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



En esta nueva pantalla podemos ver la categorización de las alertas por su severidad **(SEVERITY**), las cuales pueden ser **Critical, Warning** o **Informational (Infor),** las alertas criticas interrumpen servicios, en tanto que las warning pueden o no degradar servicios, en tanto que las informational 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.

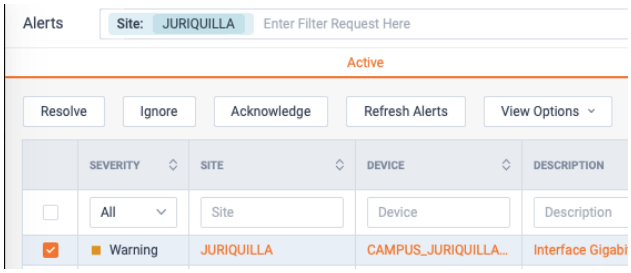
- **ACTIVE FOR.** En este campo podemos ver cuantos días ha estado activa dicha alerta. Aunque ya se haya atendido y haya sido resuelta si esta alerta no se borra del panel continuará contando el tiempo hasta que no haya sido retirada del panel.

- **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.

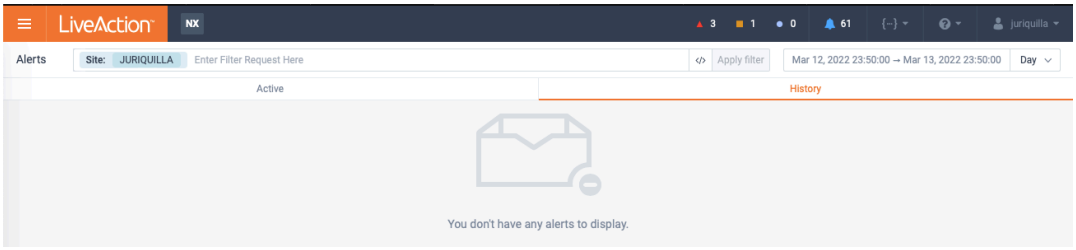
GESTIÓN DE ALERTAS: para llevar a cabo el borrado de las alertas una vez atendidas y resueltas se debe seleccionar la casilla referente a la alerta a borrar, esta casilla se encuentra en la primera columna de la tabla, la que esta más a la izquierda de la tabla, al seleccionarla se activaran las diferentes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



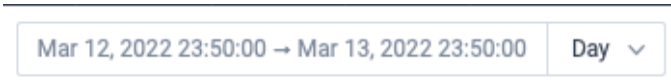
- **Resolve.** Se ha solucionado la alerta.
- **Ignore.** Se puede ignorar la alerta, no afecta a la operación del ninguno de los servicios o dispositivo.
- **Acknowledge.** Es una alerta conocida que por el momento no podemos solucionarla y no afecta a algún servicio.
- **Refresh Alerts.** Refrescar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

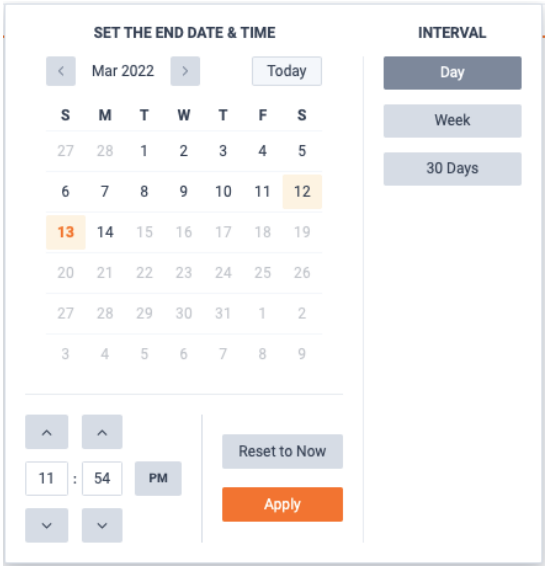
Al ingresar a este apartado puede que no vea ninguna alerta:



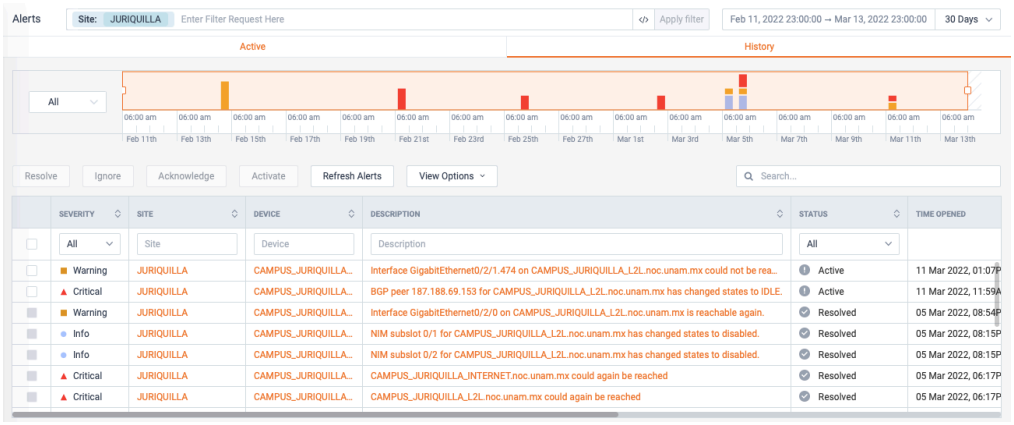
Para poder revisar en el pasado, tenemos la opción del lado superior derecho, la opción de las fechas que necesitamos revisar, esta opción aparecerá también en otros sitios de la herramienta para poder ver la utilización del ancho de banda en un tiempo especifico, por ejemplo:



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.



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



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).

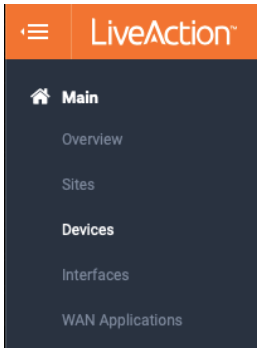
- **PEAK UTILIZATION IN**. Por default se tiene un lapso de 15 minutos de monitoreo , este campo nos muestra el pico de utilización en porcentaje del dispositivo de entrada.

- **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.

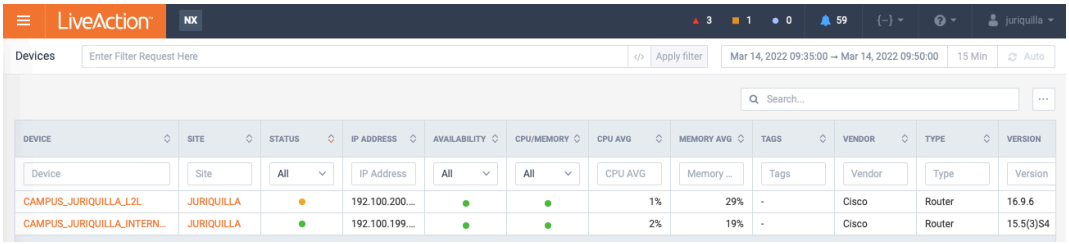
Objetivo: Acceder a **Devices**
Herramienta: haber ingresado a la herramienta y al Menú



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



- **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.

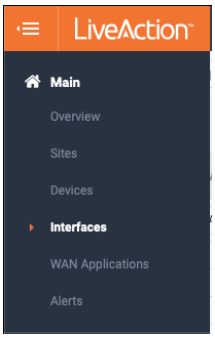
- **IP Addresses.** Direccionamiento IPv4 con el cual estamos monitoreando a cada uno de los dispositivos asignados a su perfil.

- **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

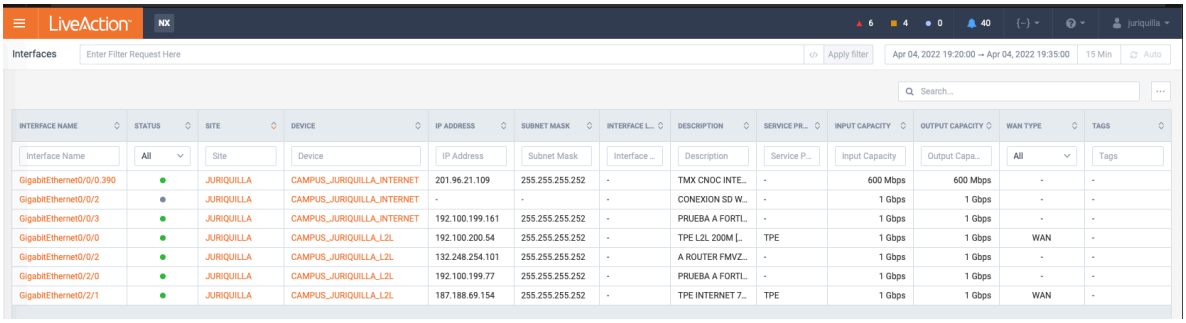


La opción de Interfaces nos dará la información relacionada a las interfaces contenidas en los **DEVICES** asignados al rol.

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



- **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 noc.redunam@unam.mx
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