Internet de las Cosas en educación

Asunto: Mejore las experiencias de aprendizajey enseñanza mediante Internet de las Cosas (Internet of Things, IoT) sobre una base segura

Resumen de la solución
IoT en educación

Alcatel·Lucent
Enterprise

IoT cambia fundamentalmente la ecuación de la educación

Internet de las Cosas (Internet of Things, IoT) tiene potencial para transformar la educación ya que altera profundamente la forma de recoger datos en escuelas, institutos y universidades, conectarse con los usuarios y automatizar procesos. IoT recurre a redes de objetos físicos mediante el uso de sensores embebidos, actuadores y otros dispositivos que pueden captar y transmitir información sobre las actividades en tiempo real. Cuando IoT se combina con tecnologías como movilidad del usuario y análisis de datos, proporciona un nuevo paradigma educativo. IoT permite a las instituciones:

- Crear nuevas vías de aprendizaje para los estudiantes promoviendoexperiencias más personalizadas y dinámicas de aprendizaje como libros de texto digitales inmersivos y aprendizaje basado en juegos.
- Cambiar la forma de impartir las lecciones y pruebas de conocimientos con equipos audiovisuales avanzados, grabadores digitales de vídeo de las lecciones y exámenes en línea.
- Simplificar la operativa para que los administradores del centro gestionen proactivamente la infraestructura principal y puedan crear procesos más eficientes y económicos para gestión de climatización, iluminación y paisaje.
- Proporcionar un entorno más seguro a estudiantes y profesores con cámaras digitales de vigilancia, cerraduras de puertas inteligentes y autobuses escolares conectados.

Posibilidades de IoT en educación

Las soluciones IoT prometen lograr que escuelas y universidades sean más inteligentes y más exitosas. IoT cuenta con el potencial para redefinir la interacción entre estudiantes, profesores y administradores y su conexión a la tecnología y los dispositivos en las clases, lo cual contribuye a mejorar las experiencias de aprendizaje y los resultados educativos, así como a reducir los costes. Estos son algunos ejemplos de soluciones IoT para educación:

- **Pizarras inteligentes y otros soportes digitales interactivos** que pueden recoger y analizar datos para que profesores y estudiantes los utilicen en clase –o en cualquier otro lugar y en cualquier momento– optimizando así las instrucciones y mejorando los resultados del aprendizaje.
- **Soluciones como sensores inteligentes de temperatura y equipos inteligentes de calefacción, ventilación y aire acondicionado que** reducen el consumo de energía y automatizan la gestión operativa.
- **Tarjetas inteligentes de identificación de los estudiantes, dispositivos para control de asistencia, sistemas de seguimiento del autobús escolar** que supervisan el paradero de los estudiantes.
- **Cerraduras inalámbricas de puertas, cámaras de vigilancia conectadas y sistemas** de reconocimiento facial que ofrecen seguridad a profesores, studiantes y al personal.
- **Programas avanzados** de investigación con sistemas más avanzados y automatizados en las principales áreas de estudio, como medicina, agricultura e ingeniería.

Retos de la implantación de IoT

Resumen de la solución IoT en educación
IoT aporta un flujo de datos sin precedentes, lo cual genera desafíos en cuanto a prestaciones, operativos y de gestión a la infraestructura de la red, así como mayores riesgos de seguridad desde todos los puntos. Para solucionar estas cuestiones, los administradores de red en las instituciones educativas necesitan adaptar los diseños de la red tradicional para ofrecer nuevos niveles de inteligencia, automatización y seguridad a la red.

Escuelas y universidades necesitan una infraestructura de red económica que maneje de forma segura enormes flujos de datos, pero que también sea sencilla de gestionar y manejar. La infraestructura debe:

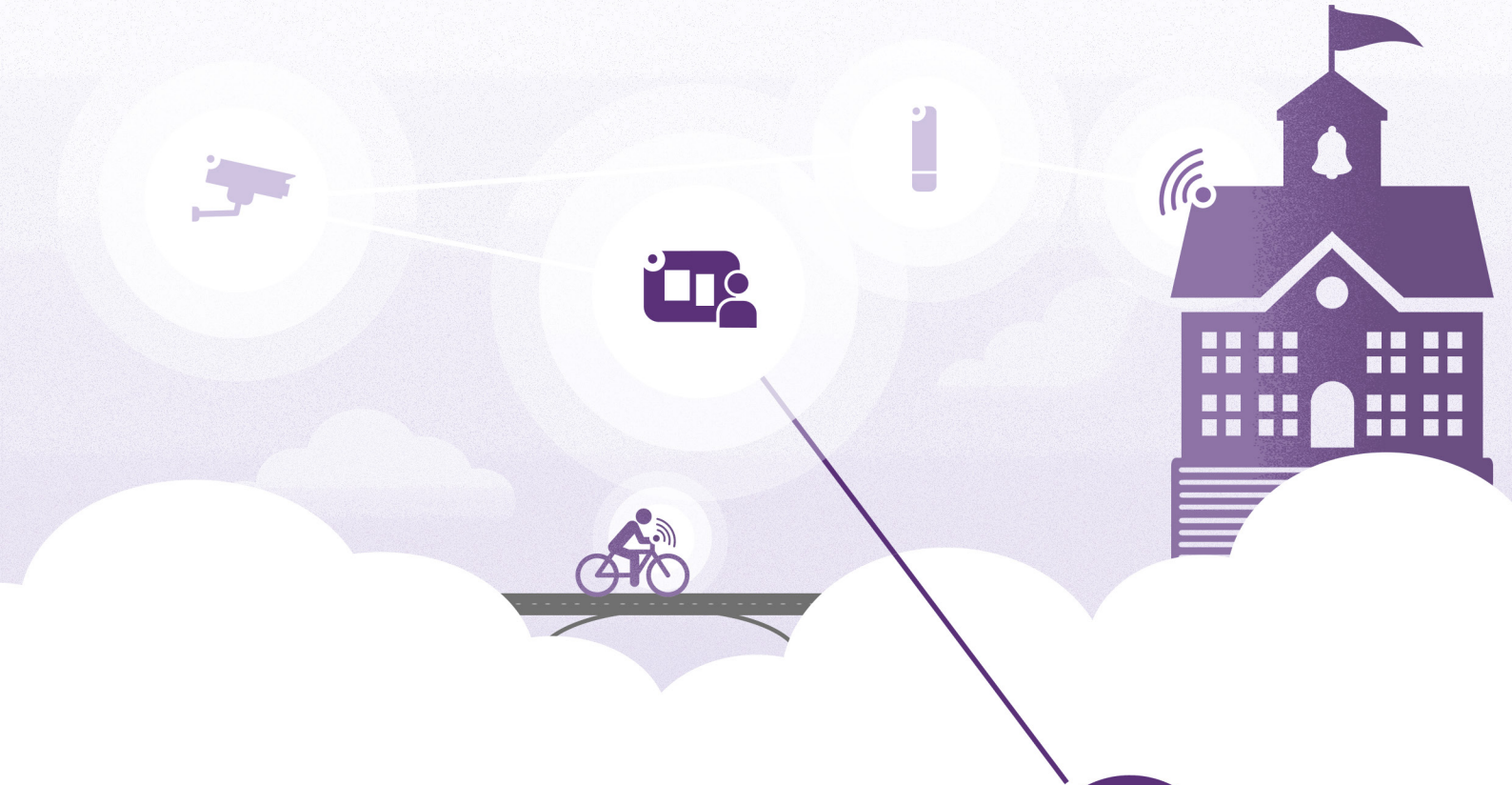
- **Ofrecer un proceso sencillo y automatizado para la incorporación de dispositivos IoT.** Los grandes sistemas IoT pueden contener miles de dispositivos o sensores, y el suministro y la gestión manual de todos estos puntos aumenta la complejidad y la posibilidad de errores. La incorporación automatizada permite que la infraestructura de la red reconozca los dispositivos dinámicamente, así como asignarlos a la red segura más apropiada.
- **Suministrar los recursos correctos a la red para que el sistema IoT funcione de manera adecuada y eficiente.** Muchos dispositivos en el sistema IoT aportan información crítica que exige un determinado nivel de calidad del servicio. Por ejemplo, algunas aplicaciones educativas requieren reservar el ancho de banda adecuado en una infraestructura de red de altas prestaciones para garantizar la prestación y fiabilidad del servicio.
- **Proporcionar un entorno seguro frente a ciberataques y pérdida de datos.** Debido que los numerosos dispositivos y sensores de la red IoT conllevan un gran número de vectores de ataque potencial, la seguridad es fundamental para aminorar los riesgos de cibercrimen. La seguridad es necesaria a múltiples niveles, incluyendo el confinamiento de las propias redes IoT.

Los profesionales de TI tienen previsto potenciar IoT

Los profesionales de TI en diversos sectores ya tienen previsto potenciar el uso de soluciones IoT en el próximo futuro. De acuerdo co el estudio de 451 Research sobre tendencias en Internet de las Cosas, un 67% de los profesionales de TI que respondieron al cuestionario dijeron que sus compañías ya han implementado una solución IoT o tenían un sistema IoT en fase de pruebas. Un 21% de los encuestados dijeron que sus compañías prevén implementar soluciones IoT en los próximos 12 meses, y un 11% afirma que sus compañías planean implementar IoT en un plazo superior a un año.

IoT acrecienta la exposición de escuelas y universidades a ciberdelitos

El crecimiento de IoT en educación también conlleva una explosión de las amenazas de ciberseguridad ya que la proliferación de sensores y dispositivos conectados aumenta enormemente la exposición de la red a ataques. IoT es especialmente susceptible ya que muchos dispositivos IoT se fabrican sin tener en cuenta la seguridad, o bien son construidos por compañías que no comprenden los actuales requisitos de seguridad. En consecuencia, los sistemas IoT se han ido convirtiendo en el eslabón débil para la seguridad de la red en las instituciones educativas.



- La red de una universidad, cuyo nombre no ha sido desvelado, fue atacada por su propio sistema de 5.000 dispositivos IoT, incluyendo máquinas de venta automática y bombillas inteligentes, según el 2017 Data Breach Digest de Verizon. Los dispositivos pirateados generaron miles de búsquedas de nombres de dominios (Domain Name Service, DNS) cada 15 minutos, lo cual provocó que la red de la universidad fucionara con enorme lentitud o incluso que fuera inaccesible.[1]
- Supremacistas blancos piratearon en 2017 las impresoras y faxes conectados a la red en varias universidades, como la Universidad de California en Berkeley, para que las máquinas imprimieran propaganda racista.[2]
- La botnet Mirai, que paralizó en servicio de Internet en la costa este de EE.UU. y gran parte de Europa Occidental mediante el control remoto de millones de dispositivos IoT, realizó un ataque en 2016 a la red informática en la Universidad Rutgers. El software Mirai se diseñó para piratear enrutadores con una baja seguridad, cámaras de seguridad y monitores para bebés.[3]

Un estudiante de un instituto de Michigan fue detenido en 2015 cuando efectuaba un ataque de denegación de servicio distribuido (distributed denial of service attack, DDoS) diseñado para cortar intermitente la red informática de la escuela. La botnet que provocó el ciberataque se dirigía a ispositivos conectados a la red IoT como cámaras de vigilancia y enrutadores.[4]

Construcción de una infraestructura segura de la red IoT

La protección del tráfico y los dispositivos de IoT en las redes de escuelas y universidades es un desafío que no se puede superar con una sola tecnología de seguridad. Exige un enfoque estratégico que aproveche diversas protecciones de seguridad.

Para ayudar a las instituciones educativas a aprovechar las ventajas y a mitigar los riesgos de la implantación de IoT, Alcatel-Lucent Enterprise (ALE) proporciona una estrategia de seguridad multinivel. La estrategia de ALE ofrece protección en cada capa de la infraestructura, desde cada usuario y cada dispositivo hasta la propia capa de la red. También proporciona una estrategia de confinamiento de IoT para simplificar y proteger la incorporación de dispositivos y suministrar los recursos adecuados a la red para el funcionamiento correcto y eficiente del sistema, todo ello en un entorno seguro que proteja a las organizaciones frente a ciberataques.

Confinamiento de IoT

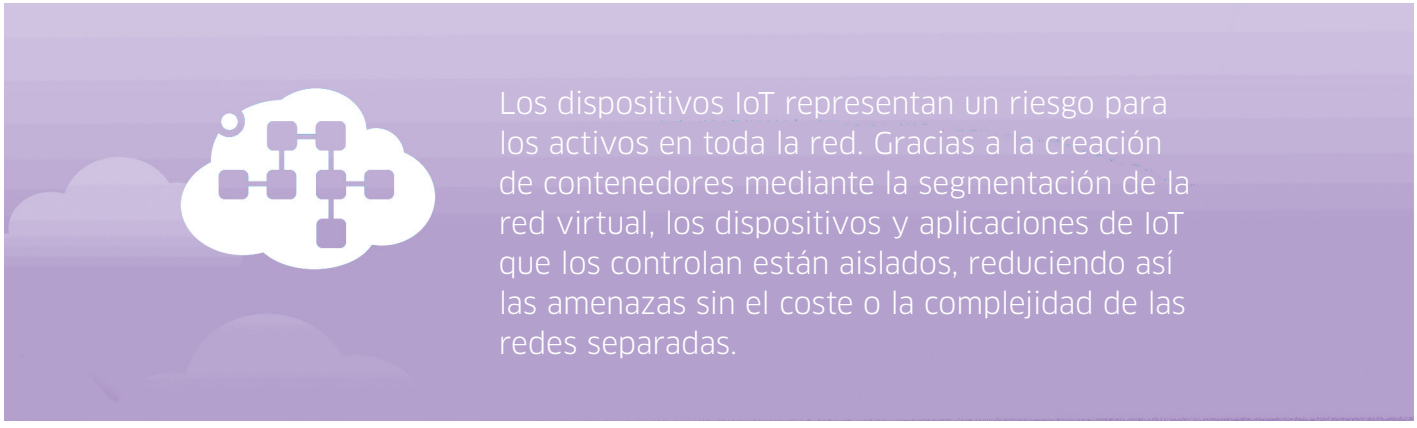
Para permitir el confinamiento de IoT, todos los usuarios, dispositivos y aplicaciones de la red de ALE son perfiles asignados. Estos perfiles, que definen funciones, autorizaciones de acceso, niveles de calidad de servicio y otro tipo de información relacionada, se transmite a todos los conmutadores y puntos de acceso de la red.

- Los dispositivos se encuentran en “contenedores virtuales”, que aplican técnicas de virtualización de la red de manera que diversos dispositivos y redes pueden utilizar la misma infraestructura física mientras permanecen aislados del resto de la red.
- En estos contenedores virtuales se aplican normas de calidad de servicio y seguridad.
- Al dividir la red mediante contenedores virtuales, si se produce una brecha en una parte de la red virtual ello no afecta a otros dispositivos o aplicaciones en otras redes virtuales.
- Cuando se conecta un nuevo dispositivo IoT, la red reconoce automáticamente su perfil y asigna al dispositivo al entorno virtual apropiado.
- La comunicación se limita a los dispositivos de este entorno virtual y a la aplicación en el centro de datos que controla estos dispositivos.
- Debido a que todos los usuarios también tienen perfiles dentro de la red de ALE, el acceso a los contenedores virtuales de IoT se pueden limitar a las personas y grupos autorizados.

Máxima seguridad

In addition to IoT containment, ALE networking technologies provide layered security across multiple levels of the network.

- Al nivel del usuario, los perfiles aseguran que los usuarios obtengan la autenticación y autorización con los derechos de acceso apropiados.
- Al nivel del dispositivo, la red asegura que los dispositivos tengan autenticación y cumplan las normas de seguridad establecidas.
- Al nivel de la aplicación, la red puede establecer normas relativas a cada aplicación o grupo de aplicaciones, como bloqueo, máximo ancho de banda y control de quien accede a cada aplicación.
- Al nivel de la red, los conmutadores de ALE utilizan código seguro diversificado. Éste protege las redes frente a vulnerabilidades intrínsecas, código oculto, malware embebido y potenciales puertas traseras que puedan afectar a conmutadores, enrutadores y otro hardware de misión crítica.
- El análisis inteligente de ALE utiliza inspección avanzada de paquetes y otras tecnologías para detectar el tipo de datos y aplicaciones que se mueven por la red, posibilitando así la identificación de patrones inusuales de tráfico en la red y actividad no autorizada.



Gestión operativa y de la red de extremo a extremo

Las soluciones de ALE para redes en educación también ofrecen ventajas significativas de tipo operativo y para su gestión.

- **ALE permite el funcionamiento de varias redes virtuales separadas como una sola infraestructura,** lo cual supone un ahorro de gasto de capital en varias redes físicas.
- **La solución ALE Unified Access permite el funcionamiento conjunto de redes cableadas e inalámbricas** como una sola red robusta, con un conjunto común de servicios de red, un marco normativo común, una técnica común de autenticación y una sola base de datos de autenticación.
- **Las soluciones de ALE para redes también tienen un solo sistema de gestión para todos los elementos de la infraestructura,** incluyendo la gestión unificada de redes LAN y WLAN. El paquete de gestión Alcatel-Lucent OmniVista® 2500 proporciona un solo panel para gestionar entornos virtuales, conmutadores, puntos de acceso y otros componentes de la red.

Gama para redes de altas prestaciones

Los conmutadores, puntos de acceso y controladores de ALE ofrecen capacidades de elevado ancho de banda y baja latencia de última generación y pueden gestionar un gran número de dispositivos en entornos de alta densidad. Los productos y soluciones para redes de ALE pueden cubrir la necesidades de las redes en instituciones educativas de cualquier tamaño. ALE también suministra una selección de conmutadores, puntos de acceso y enrutadores robustos para el despliegue de redes en el exterior o en entornos adversos.

Ya están aquí las redes y las estrategias basadas en IoT para educación

Los productos y soluciones de ALE constituyen la base de una red segura para ayudar a escuelas y universidades a implementar sistemas IoT que pueden crear nuevos métodos de aprendizaje para los estudiantes, mejorar la forma que tienen los profesores de impartir las clases y de aumentar el rendimiento escolar. Las soluciones IoT seguras también ayudan a simplificar las operaciones a los administradores del centro y a proporcionar un entorno más seguro a estudiantes y profesores. El confinamiento de IoT de ALE y las estrategias de seguridad por capas reducen los riesgos y simplifican la configuración de las redes IoT al facilitar la incorporación de dispositivos, proporcionando así un funcionamiento más eficiente y una enorme mejora de la seguridad. ALE ayuda a las organizaciones a aprovechar al máximo las ventajas de IoT a través de mayores niveles de inteligencia, automatización y seguridad de la red.

¿Desea más información?

Para más información sobre las soluciones IoT de ALE, visite Seguridad de IoT de ALE.

Educación conectada

Donde la Educación se conecta a la tecnología que funciona. Para su escuela, instituto o universidad. Con una cobertura global y un enfoque local, suministramos redes y comunicaciones a medida para el entorno educativo que facilitan una colaboración segura y fiable entre el centro el los estudiantes.

1 University attacked by its own vending machines, smart light bulbs & 5,000 IoT devices
2 More Anti-Semitic Fliers Printed at Universities
3 Ex-Rutgers student pleads to cyberattacks, creating IoT botnet that brought down Internet
4 Michigan High School Student Facing Charges After launching DDoS attack on School Network