A Internet das Coisas (IoT) na Educação

Melhore as experiências de ensino e aprendizado, aproveitando a IoT em uma base segura

Resumo da Solução
IoT na Educação

Alcatel·Lucent
Enterprise

A IoT muda fundamentalmente a equação da educação

A Internet das Coisas (IoT) tem o potencial de transformar a educação, alterando profundamente a forma como as escolas e as universidades coletam dados, interagem com os usuários e automatizam os processos. A IoT refere-se à rede de objetos físicos interligados por meio de sensores integrados, atuadores e outros dispositivos que podem coletar e transmitir informações sobre a atividade do campus em tempo real. Quando a IoT é combinada com tecnologias como mobilidade do usuário e análise de dados, traz um novo paradigma na educação. A IoT permite que as instituições:

- Criem novas formas de aprendizado para os estudantes oferecendo experiências mais personalizadas e dinâmicas, como livros didáticos digitais imersivos e aprendizado baseado em jogos.
- Mudem a forma como os professores ministram as aulas e testam o aprendizado, utilizando equipamento audiovisual inteligente, gravadores de vídeo digital para registro das aulas e testes on-line.
- Simplifiquem as operações para os administradores das escolas, monitorando proativamente a infraestrutura crítica e criando processos mais eficientes e econômicos para gerenciamento de climatização, iluminação e estrutura.
- Ofereçam um ambiente mais seguro para estudantes e professores, com câmeras de vigilância digital, travas de portas inteligentes e transportes escolares conectados.

Cenários da IoT na Educação

As soluções de IoT prometem tornar as escolas e universidades mais inteligentes, e mais bem-sucedidas. A IoT tem o potencial de redefinir como os estudantes, professores e administradores interagem e se conectam com a tecnologia e os dispositivos nos ambientes de sala de aula, ajudando a aprimorar as experiências de aprendizado, melhorar os resultados educacionais e reduzir custos. Exemplos de soluções de IoT para a área da educação incluem:

- Lousas inteligentes e outras mídias digitais interativas, que podem coletar e analisar dados para professores e estudantes usarem nas salas de aula ou em qualquer outro lugar, a qualquer momento, otimizando o ensino e melhorando os resultados do aprendizado.
- Soluções como sensores de temperatura inteligentes e equipamentos de climatização inteligentes, que reduzem o consumo de energia e automatizam o gerenciamento das operações.
- Cartões inteligentes de identificação dos estudantes, dispositivos de acompanhamento de presença, sistemas de rastreamento de transporte escolar e sensores de estacionamento que monitoram a localização física dos estudantes.
- Travas de portas sem fio, câmeras de vigilância conectadas e sistemas de reconhecimento facial que fornecem segurança para professores, estudantes e funcionários.
- Programas de pesquisa aprimorados, com sistemas automatizados e mais avançados nas principais áreas de estudo, como medicina, agricultura e engenharia.

Desafios na implantação da IoT

A IoT traz fluxos de dados sem precedentes, apresentando desafios de desempenho, operacionais e de gerenciamento para a infraestrutura da rede, junto com maiores riscos de segurança em todos os terminais. Para solucionar esses problemas, os administradores das instituições de ensino precisam adaptar seus projetos de rede tradicionais para fornecer novos níveis de inteligência, automação e segurança.

Escolas e Universidades precisam de uma infraestrutura de rede com o melhor custo-benefício, que possa tratar com segurança o grande fluxo de dados, mas que também seja simples de gerenciar e operar. A infraestrutura deve:

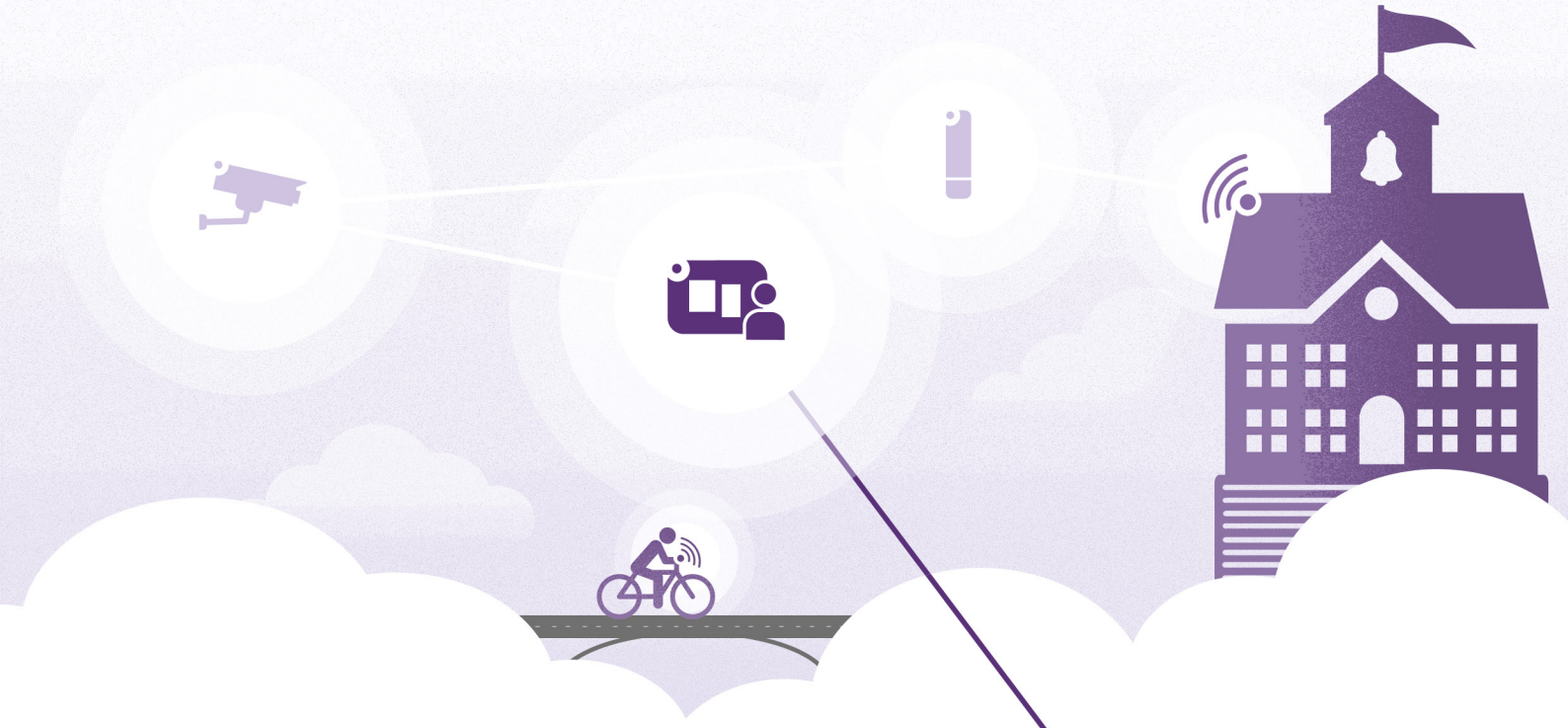
- **Utilizar um processo simples e automatizado para a integração de dispositivos IoT.** Grandes sistemas IoT podem conter milhares de dispositivos e sensores, portanto adicionar e gerenciar manualmente todos esses terminais é complexo e propenso a erros. A integração automatizada permite que a infraestrutura de rede reconheça dinamicamente os dispositivos e os atribua para a rede de segurança correta.
- **Fornecer os recursos de rede apropriados para que o sistema de IoT funcione de forma adequada e eficiente.** Muitos dispositivos no sistema de IoT utilizam informações essenciais, que exigem um nível específico de QoS. Por exemplo, alguns aplicativos utilizados na Educação exigem uma determinada largura de banda, em uma infraestrutura de rede de alto desempenho, para garantir a confiabilidade e o fornecimento do serviço.
- **Fornecer um ambiente seguro contra ataques cibernéticos e perda de dados.** Os inúmeros dispositivos e sensores conectados na rede IoT levam a uma abundância de possíveis vetores de ataque, e por isso a segurança é fundamental para reduzir os riscos de crimes cibernéticos. A segurança é necessária em vários níveis, incluindo a contenção das próprias redes IoT.

Os profissionais de TI estão fazendo planos para mais IoT

Profissionais de TI de vários setores já estão planejando o aumento no uso de soluções de IoT, em um futuro próximo. De acordo com a pesquisa da 451 Research de 2017, Tendências na Internet das Coisas, 67% dos profissionais de TI pesquisados disseram que suas empresas já implantaram uma solução de IoT ou tinham um sistema IoT em piloto. 21% dos entrevistados disseram que suas empresas planejavam implantar soluções de IoT dentro de 12 meses, e 11% dizem que suas empresas planejam implementar IoT em mais de um ano.

A IoT contribui para a exposição de Escolas e Universidades aos crimes cibernéticos

O crescimento da IoT na área da educação também traz uma explosão de ameaças à segurança cibernética, pois a proliferação de sensores e dispositivos conectados expande muito a superfície de ataque da rede. A IoT para a Educação é especialmente sensível, porque muitos dispositivos IoT são fabricados sem ter a segurança em mente, ou são criados por empresas que não entendem os requisitos de segurança atuais. Consequentemente, cada vez mais, os sistemas de IoT representam o elo mais fraco na segurança da rede de instituições de ensino.



- A rede de uma universidade anônima foi atacada pelo seu próprio sistema de 5.000 dispositivos IoT, incluindo máquinas de venda automática e luzes inteligentes, de acordo com o 2017 Data Breach Digest da Verizon. Os dispositivos invadidos realizaram centenas de pesquisas de DNS (Domain Name Service) a cada 15 minutos, fazendo com que a conectividade da rede se tornasse insuportavelmente lenta ou até mesmo inacessível.[1]
- Em 2017, supremacistas brancos invadiram impressoras e máquinas de fax na rede, em várias universidades, incluindo a Universidade da Califórnia, Berkeley, fazendo com que as máquinas imprimissem propaganda racista.[2]
- O botnet Mirai, que prejudicou o serviço de Internet em toda costa leste dos EUA e uma grande parte da Europa Ocidental escravizando remotamente milhões de dispositivos IoT, começou em 2016 como um ataque à rede de computadores da Universidade Rutgers. O software Mirai foi criado para sequestrar roteadores, câmeras de segurança e monitores de bebês com baixa segurança.[3]

Um estudante do ensino médio de Michigan foi pego em 2015 conduzindo um ataque DDoS (Distributed Denial of Service) concebido para derrubar intermitentemente a rede de computadores da escola. O botnet que causou o ataque cibernético foi direcionado para dispositivos IoT na rede, como câmeras de vigilância e roteadores.[4]

Criando uma infraestrutura de rede IoT segura para a Educação

Proteger o tráfego e os dispositivos IoT nas escolas e universidades é um desafio que não pode ser resolvido por qualquer tecnologia de segurança. Exige uma abordagem estratégica que tira proveito de várias medidas de segurança.

Para ajudar as instituições de ensino a aproveitarem os benefícios e reduzirem os riscos da implantação de IoT, a Alcatel-Lucent Enterprise (ALE) oferece uma estratégia de segurança em vários níveis. A estratégia da ALE fornece proteção em cada camada da infraestrutura, a partir de cada usuário e dispositivo individual até a própria infraestrutura da rede. Ela também fornece uma estratégia de contenção de IoT para simplificar e proteger a integração de dispositivos, e oferece os recursos de rede apropriados para que o sistema funcione de forma correta e eficiente, tudo em um ambiente seguro para garantir a proteção das instituições contra ataques cibernéticos.

IoT Containment

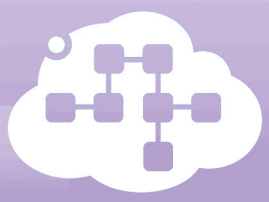
Para habilitar o IoT Containment, todos os usuários, dispositivos e aplicativos dentro da rede da ALE são associados a perfis. Esses perfis, que definem funções, autorizações de acesso, níveis de QoS e outras informações sobre políticas, são transmitidos a todos os switches e pontos de acesso na rede.

- Os dispositivos são atribuídos a "recipientes (containers) virtuais" usando técnicas de virtualização de rede, permitindo que vários dispositivos e redes usem a mesma infraestrutura física, enquanto permanecem isolados do resto da rede.
- Nesses "recipientes virtuais", as regras de QoS e segurança são aplicadas.
- Com a divisão da rede em "containers" virtuais, caso ocorra alguma violação em uma parte da rede virtual, isso não afetará outros dispositivos ou aplicativos em outras redes virtuais.
- Quando um novo dispositivo IoT estiver conectado, a rede reconhecerá automaticamente seu perfil e atribuirá o dispositivo ao ambiente virtual adequado.
- A comunicação é limitada aos dispositivos dentro desse ambiente virtual, e aos aplicativos do datacenter que controlam esses dispositivos.
- Como todos os usuários têm perfis dentro da rede da ALE, o acesso aos "containers" virtuais de IoT pode ser limitado a indivíduos e grupos autorizados.

Segurança aprofundada

Além do IoT Containment, as tecnologias de rede da ALE fornecem a segurança por camada, nos vários níveis da rede.

- No nível do usuário, os perfis garantem que os usuários sejam autenticados e autorizados com os direitos de acesso adequados.
- No nível do dispositivo, a rede assegura que os dispositivos sejam autenticados e estejam de acordo com as regras de segurança estabelecidas.
- No nível do aplicativo, a rede pode estabelecer regras sobre cada aplicativo ou grupo de aplicativos, incluindo bloqueio, limitação de largura de banda e controle de quem pode acessar quais aplicativos.
- No nível da rede, os switches da ALE utilizam o secure diversified code. Ele protege redes contra vulnerabilidades intrínsecas, quebras de código, malwares infiltrados e possíveis backdoors que poderiam comprometer os switches, roteadores e outros hardwares essenciais.
- A função "smart analytics" da ALE usa inspeção profunda de pacotes e outras tecnologias para detectar os tipos de dados e aplicativos se movimentando pela rede, tornando possível identificar padrões incomuns de tráfego e atividades não autorizadas.



Os dispositivos IoT representam riscos para os equipamentos de toda a rede. Ao definir os "containers" através da segmentação da rede virtual, os dispositivos e aplicativos IoT que os controlam são isolados, reduzindo as ameaças sem o custo ou a complexidade de redes separadas.

Gerenciamento e operação da rede, de ponta a ponta

As soluções de rede da ALE também oferecem à área da Educação vantagens significativas na sua operação e gerenciamento.

- A ALE permite que várias redes distintas operem em uma única infraestrutura comum, eliminando a necessidade de mais investimento CAPEX em múltiplas redes físicas.
- A estrutura de Acesso Unificado da ALE permite que as tecnologias com fio e sem fio trabalhem juntas, como uma rede única e robusta, com serviços de rede, regras de políticas, um esquema de autenticação em comum, e uma única base de dados de autenticação.
- As soluções de rede da ALE também têm um único sistema de gerenciamento para todos os elementos da infraestrutura, incluindo gerenciamento unificado das redes LAN com fio e sem fio. O gerenciamento Alcatel-Lucent OmniVista® 2500 oferece um painel de controle unificado para gerenciar ambientes virtuais, switches, Access Points e todos os outros componentes da rede.

Um portfólio de rede de alto desempenho

Os switches, Access Points e controladoras da ALE suportam a última geração de recursos de alta largura de banda e baixa latência, e podem gerenciar um grande número de dispositivos em ambientes de alta densidade. Os produtos e soluções de rede da ALE atendem às necessidades de rede das instituições de ensino, de todos os tamanhos. A ALE também oferece uma seleção de switches robustos, Access Points e roteadores para implantações externas ou em condições adversas.

Redes e estratégias IoT seguras para a área da Educação. Aqui, e agora.

Os produtos e soluções da ALE criam a base para uma rede segura, que ajuda as escolas e universidades a implantarem sistemas de IoT que podem criar novas formas de aprendizado para os estudantes e melhorar a forma como os professores ensinam e testam os conhecimentos. As soluções IoT seguras também ajudam a simplificar as operações para os administradores das escolas, ao mesmo tempo em que fornecem um ambiente mais seguro para estudantes e professores. As estratégias de IoT Containment e segurança por camada, da ALE, reduzem os riscos e simplificam a configuração das redes de IoT ao facilitar a integração dos dispositivos, com operações mais eficientes e mais segurança. A ALE ajuda as instituições a utilizarem todos os possíveis benefícios da IoT, com melhores níveis de inteligência, automação e segurança da rede.

Quer saber mais?

Para obter mais informações sobre as soluções de IoT da ALE, vá para ALE IoT Security.

Connected Education

Onde a Educação se conecta com a tecnologia que funciona. Para sua escola ou universidade. Com foco local e alcance global, oferecemos comunicações e redes especialmente projetadas para o ambiente educacional que permitem colaboração segura e confiável entre sua instituição de ensino e os estudantes.

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