

Centro de Pesquisas do Instituto Mauá de Tecnologia  
Divisão de Eletrônica e Telecomunicações

**IMT – ACESSO AO *NETWORK SERVER***

São Caetano do Sul

2018



## RESUMO

O *Network Server* é um servidor voltado para Internet das coisas (*IoT – Internet of Things*) e caracteriza-se por gerenciar os dados enviados por um *node* (dispositivo embarcado com transmissor de rádio frequência referente ao protocolo *LoRaWAN*) disponibilizando-os ao usuário final de uma aplicação que se utiliza deste servidor. Este serviço encontra-se em uma plataforma de nuvem hospedada em um *datacenter* localizado no Instituto Mauá de Tecnologia (IMT), *campus* São Caetano do Sul. A esta documentação propõe-se permitir que o usuário realize o acesso ao servidor para cadastrar e ativar os *nodes* referentes à respectiva aplicação. De maneira objetiva sugerir métodos para que os dados armazenados no banco de dados possam ser recuperados e até mesmo transmitidos à aplicação no momento imediato do envio de um pacote de informação pelo *node* da aplicação através desse servidor.

**Palavras chave:** servidor, *IoT*, *LoRaWAN*, *node*, acesso, envio, pacote.

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b>	<b>5</b>
<b>2</b>	<b>ACESSO AO NETWORK SERVER</b>	<b>6</b>
<b>2.1</b>	<b>SIGN IN</b>	<b>6</b>
<b>2.2</b>	<b>CONFIGURAÇÃO DA APLICAÇÃO</b>	<b>8</b>
2.2.1	DETALHES DA APLICAÇÃO	9
2.2.2	CONFIGURAÇÕES DE REDE	10
<b>2.3</b>	<b>USUÁRIOS DA APLICAÇÃO</b>	<b>11</b>
<b>2.4</b>	<b>CADASTRO DE NODES</b>	<b>11</b>
2.4.1	CRIAÇÃO DE NODES	11
2.4.2	ATIVAÇÃO DE NODES	14
2.4.3	REGISTRO DE ATIVIDADES DO NODE	16
<b>3</b>	<b>RECUPERAÇÃO DE DADOS DO NODE PARA APLICAÇÃO</b>	<b>17</b>

## 1 INTRODUÇÃO

Com o intuito de habilitar uma conexão segura ao servidor e receber o dado referente a cada sensor na aplicação em campo, o Centro de Pesquisas do Instituto Mauá de Tecnologia disponibilizou um acesso ao *Network Server*. O *Network Server* trata-se de um servidor para *Internet das Coisas (IoT – Internet of Things)*, com o propósito de habilitar o usuário final a receber o dado enviado pelo *node* assim que este é enviado ao servidor. Bem como permitir a recuperação de dados de histórico de cada *node* dentro de um determinado período de tempo.

O servidor, ao receber os dados duplamente criptografados, armazena os valores em um banco de dados também de maneira criptografada com uma chave da aplicação denominada *appSKey (application Session key)*. A outra chave de criptografia se dá pela chave do servidor, denominada *nwkSkey (network Session key)*. Enquanto a primeira é utilizada pela aplicação para descriptografar os dados do banco de dados no momento da recuperação destes, a segunda chave também funciona como uma segurança da integridade do pacote de dados enviado (*MIC - Message Integrity Code*). A estes recursos de descriptografia não serão abordados no escopo deste documento. Para saber mais consulte documentação disponível em [LoRa Alliance](#).

## 2 ACESSO AO NETWORK SERVER

### 2.1 SIGN IN

O cadastro de usuários e aplicações não é realizada através do usuário final da aplicação. É necessário que um e-mail seja enviado para [fernando.martins@maua.br](mailto:fernando.martins@maua.br), identificando o motivo da aplicação. A partir daí, será efetuado, pelo Centro de Pesquisas, o cadastro do usuário e a criação da aplicação, delegando-se a cada usuário o acesso à aplicação correspondente.

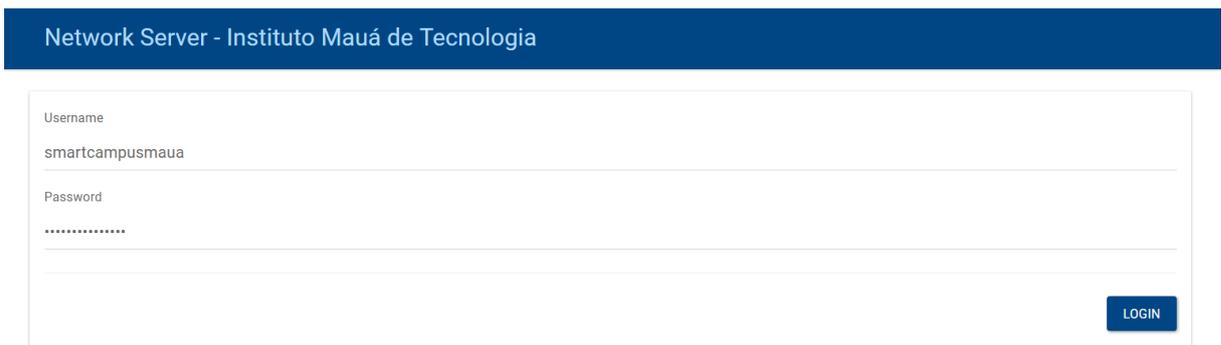
Após obtida a resposta por email, o usuário poderá administrar a própria aplicação. Para isso, deve-se acessar o *website* que hospeda a interface referente ao [Network Server](https://networkserver.maua.br) (<https://networkserver.maua.br>). Acessando-o de qualquer dispositivo com conexão à Internet, uma interface gráfica deve ser mostrada conforme a Figura 1 abaixo:

The image shows a web browser window with a dark blue header bar containing the text "Network Server - Instituto Mauá de Tecnologia". Below the header is a white login form. The form has two input fields: "Username" with the placeholder text "username" and "Password" with the placeholder text "password". A blue "LOGIN" button is located at the bottom right of the form.

Figura 1 - Interface gráfica *Network Server* . Página de *login* para usuários já cadastrados.

Pede-se que sejam inseridos as variáveis referentes ao nome de usuário (*Username*) e senha (*Password*). Após preenchidas estas informações, ao ser pressionado a tecla *ENTER* ou clicando-se sobre o botão *LOGIN*, será permitido ao usuário acessar as informações referentes somente à respectiva aplicação ou aplicações delegadas.

No exemplo a seguir, Figura 2, foram inseridos *Username/Password* como *smartcampusmaua/smartcampusmaua*.



The screenshot shows a login form titled "Network Server - Instituto Mauá de Tecnologia". It contains two input fields: "Username" with the value "smartcampusmaua" and "Password" with a masked value "\*\*\*\*\*". A blue "LOGIN" button is located at the bottom right of the form.

Figura 2 - Dados referentes ao *login* inseridos nos campos determinados.

Após ter sido realizado o *LOGIN*, será mostrado o ambiente da aplicação referente ao usuário conforme a Figura 3 a seguir:



The screenshot shows the application environment interface. The header includes "Network Server - Instituto Mauá de Tecnologia" and "Organizations smartcampusmaua". The "Applications" section is active, displaying a table with the following data:

ID	Name	Description
3	Hidrometros	Medidores de vazão de água no Smart Campus

Figura 3 - Interface de ambiente de uma aplicação. Neste caso, a aplicação denominada Hidrometros.

Nota-se que ao entrar na Área de Acesso ao Usuário, há um campo referente ao *ID* da aplicação, *Name* (Nome), e *Description* (Descrição). No exemplo deste tutorial será abordado uma Aplicação denominada Hidrometros, referente ao ID igual a 3 que caracteriza-se por monitorar a vazão de água no *Smart Campus*. Essas configurações serão criadas pelo Centro de Pesquisas, conforme a solicitação e descrição da aplicação enviada anteriormente pelo usuário através do *e-mail*.

## 2.2 CONFIGURAÇÃO DA APLICAÇÃO

Clicando-se em Hidrometros, é possível, segundo as abas superiores *Application Configuration* e *Application Users*, configurar os parâmetros, e.g., mostrados a seguir conforme a Figura 4:

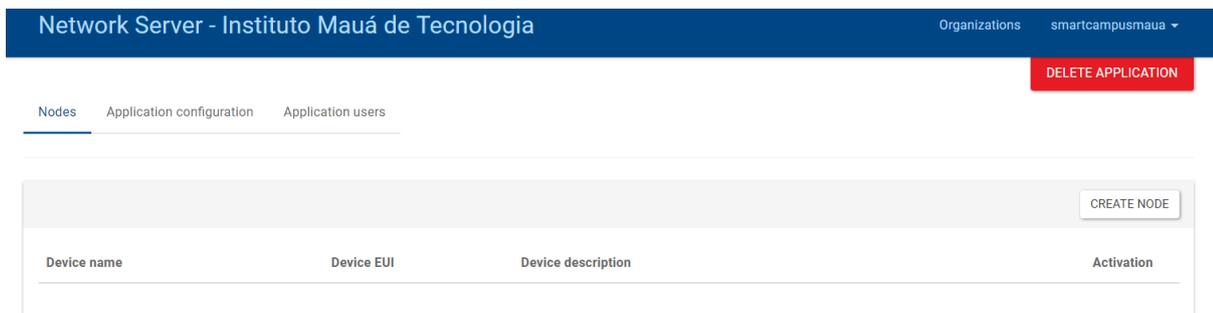


Figura 4 - Guia para a criação de *nodes* dentro da aplicação Hidrometros.

### 2.2.1 DETALHES DA APLICAÇÃO

Para configurar os parâmetros relativos ao protocolo *LoRaWAN*, deve-se clicar na guia *Application Configuration*. É imprescindível que se configure estes parâmetros antes de se adicionar qualquer *node*, pois estas configurações serão utilizadas por todos eles. A partir deste momento será aberta a seguinte tela conforme mostrada na Figura 5, a seguir:



Figura 5 - Configuração de nome e descrição de aplicação na guia Application Details.

Em *Application Details* é possível editar o nome da aplicação e também a descrição da aplicação. As configurações do protocolo *LoRaWAN* estão na aba *Network Settings*, conforme a Figura 6 a seguir:

## 2.2.2 CONFIGURAÇÕES DE REDE

Network Server - Instituto Mauá de Tecnologia Organizations smartcampusmaua ▾

[Nodes](#) [Application configuration](#) [Application users](#) DELETE APPLICATION

Application details Network settings

**Class-C nodes**

Class-C nodes

When checked, it means that the nodes for this application are operating in Class-C mode (always listening) and that data will be sent directly to the node. In any other case, the data will be sent as soon as a receive window occurs.

**ABP (activation by personalisation)**

ABP activation

When checked, it means that the nodes for this application will be manually activated and that over-the-air activation (OTAA) will be disabled.

**Receive window**

RX1

RX2 (one second after RX1)

**Relax frame-counter**

Enable relax frame-counter

Note that relax frame-counter mode will compromise security as it enables people to perform replay-attacks.

**Receive window delay**

0

The delay in seconds (0-15) between the end of the TX uplink and the opening of the first reception slot (0=1 sec, 1=1 sec, 2=2 sec, 3=3 sec, ... 15=15 sec).

**RX1 data-rate offset**

0

Sets the offset between the uplink data rate and the downlink data-rate used to communicate with the end-device on the first reception slot (RX1). Please refer to the LoRaWAN specs for the values that are valid in your region.

**RX2 data-rate**

0

The data-rate to use when RX2 is used as receive window. Please refer to the LoRaWAN specs for the values that are valid in your region.

**ADR interval**

0

The interval (of frames) after which the network-server will ask the nodes for this application to change data-rate and / or TX power if it can change to a better data-rate or lower TX power. Setting this to 0 will disable ADR.

**Installation margin (dB)**

0

The installation margin which is taken into account when calculating the ideal data-rate and TX power. A higher margin will lower the data-rate, a lower margin will increase the data-rate and possibly packet loss. 5dB is the default recommended value.

GO BACK SUBMIT

Figura 6 - Configurações de rede referentes ao protocolo LoRaWAN entre node e Network Server.

À princípio, as configurações a serem setadas devem ser apenas checar o tipo de ativação por ativação por personalização *ABP* (*Activation By Personalization*) e a janela de recepção (*Receive Window*) como *RX1*. Após estas configurações, deve-se clicar em *SUBMIT* para salvar as alterações realizadas.

## 2.3 USUÁRIOS DA APLICAÇÃO

Na aba *Application Users* é possível criar outros usuários para a mesma aplicação, porém isto não será abordado visto que os usuários devem ser **criados apenas pelo Centro de Pesquisas**. Essa guia delega o direito do usuário *smartcampusmaua* na aplicação Hidrometros, por exemplo, conforme a Figura 7 a seguir:



ID	Username	Admin
4	smartcampusmaua	<input checked="" type="checkbox"/>

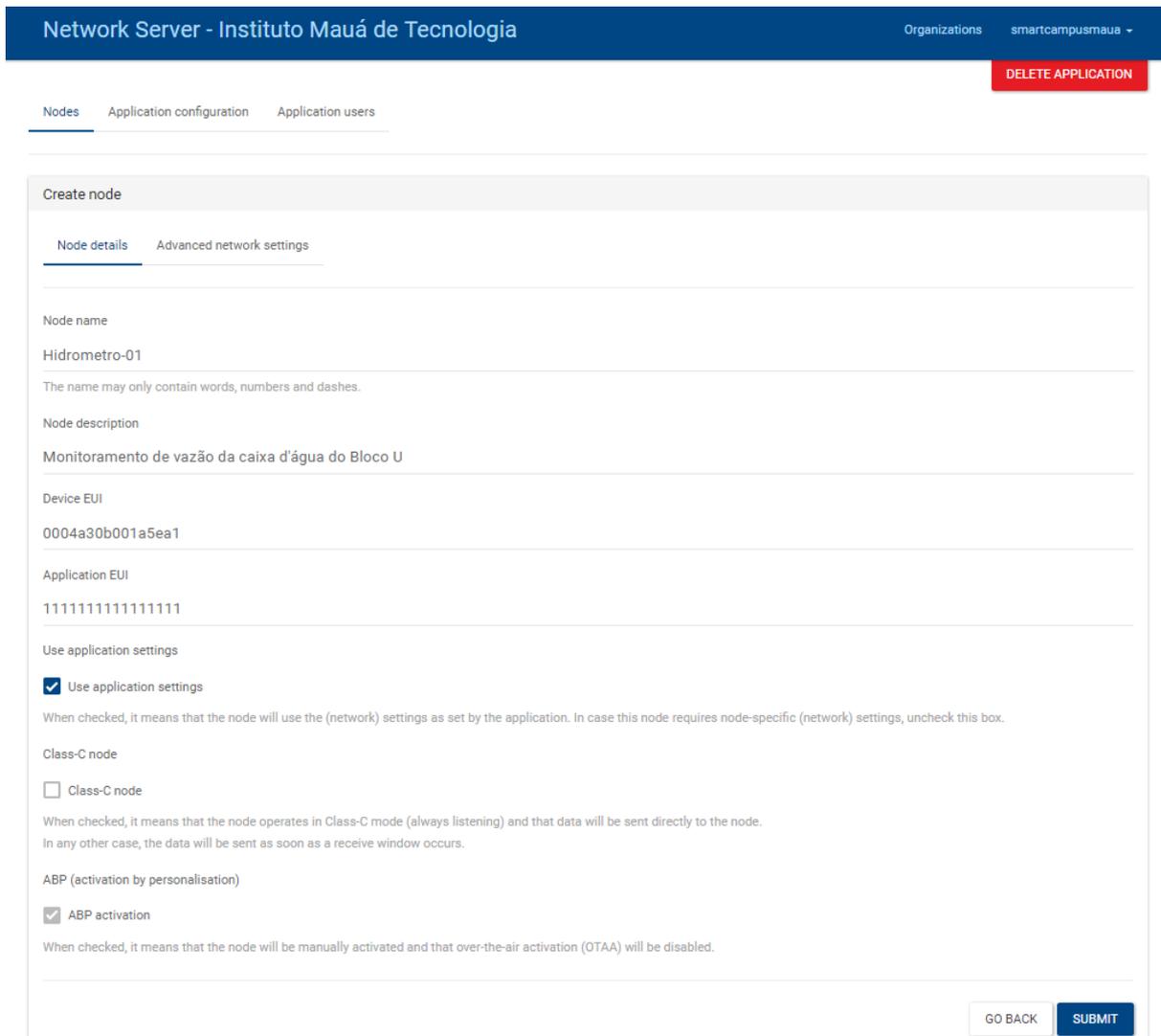
Figura 7 - Guia *application users* que delega permissões do usuário em uma aplicação.

## 2.4 CADASTRO DE NODES

### 2.4.1 CRIAÇÃO DE NODES

Após configurados os parâmetros referentes ao protocolo *LoRaWAN* através das guias anteriores, deve-se voltar à guia *Nodes* para o cadastro de cada *node* da aplicação correspondente bem como a ativação referente a cada cadastro efetuado.

A Figura 4 mostra a guia *Nodes*. Ao observá-la, nota-se um ícone *create node* ao lado direito da lista a ser cadastrada. Ao ser clicado, deve-se registrar nos campos determinados os dados relativos a cada um. A Figura 8 mostra exatamente os campos a serem preenchidos.



The screenshot shows the 'Create node' form in the Network Server interface. The form is titled 'Create node' and has two tabs: 'Node details' (selected) and 'Advanced network settings'. The form contains the following fields and options:

- Node name:** Hidrometro-01. Below the field, it says: "The name may only contain words, numbers and dashes."
- Node description:** Monitoramento de vazão da caixa d'água do Bloco U
- Device EUI:** 0004a30b001a5ea1
- Application EUI:** 1111111111111111
- Use application settings:** A checkbox labeled 'Use application settings' is checked. Below it, it says: "When checked, it means that the node will use the (network) settings as set by the application. In case this node requires node-specific (network) settings, uncheck this box."
- Class-C node:** A checkbox labeled 'Class-C node' is unchecked. Below it, it says: "When checked, it means that the node operates in Class-C mode (always listening) and that data will be sent directly to the node. In any other case, the data will be sent as soon as a receive window occurs."
- ABP (activation by personalisation):** A checkbox labeled 'ABP activation' is checked. Below it, it says: "When checked, it means that the node will be manually activated and that over-the-air activation (OTAA) will be disabled."

At the bottom right of the form, there are two buttons: 'GO BACK' and 'SUBMIT'.

Figura 8 - Campos a serem preenchidos para o cadastro de cada *node*.

Como *node-name*, podem ser utilizados somente os caracteres de letras, números e símbolos. Não serão aceitos caracteres como “espaço”. Sugere-se que haja uma padronização do tipo {Nome-da-aplicação}-{número-do-node}. Por exemplo para aplicação hidrômetro, o primeiro *node* cadastrado devera ser “Hidrometro-01”.

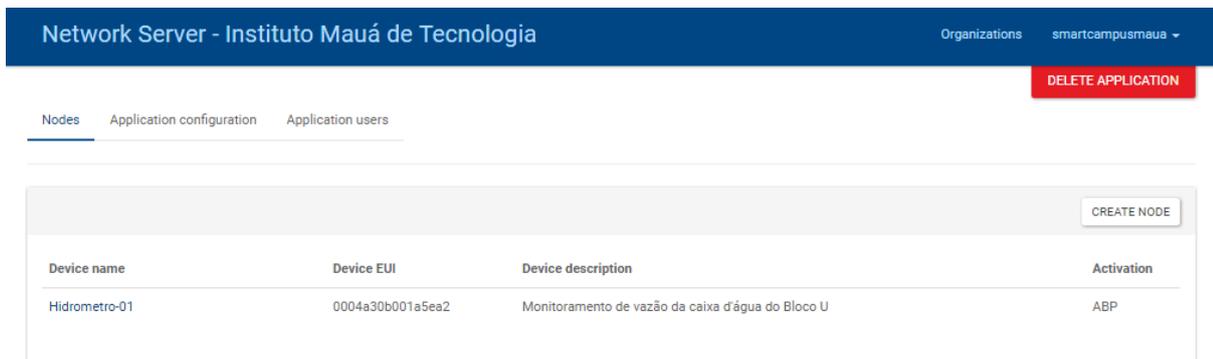
O campo *Description* deverá conter informações relevantes e sucintas sobre o dispositivo bem como interessante descrever onde esatará localizado. O node denominado Hidrometro-01 está localizado no Bloco U, portanto, uma sugestão para a descrição é “Monitoramento de vazão da caixa d'água do Bloco U”. Abordando-se o propósito e a localização de maneira simples e objetiva.

O campo *Device-EUI* (*EUI – End Device Unique Identifier*) refere-se ao único identificador de 16 *bytes* de cada *node* (o *node* também é denominado de *end-device*). Este deve ser recuperado através de um comando serial junto ao circuito integrado *RN2903* de rádio frequência LoRa. Cada dispositivo possui um *dev-EUI* diferente proveniente da fábrica. É possível ainda alterá-lo para o valor desejado, porém é fortemente não recomendado. Para informações sobre como obter o *dev-EUI* de um dispositivo, por favor, deve-se consultar a documentação de RECUPERAÇÃO DO PARÂMETRO DEV\_EUI. Para este exemplo foi recuperado do node um *dev-EUI* igual a “0004a30b001a5ea2” (uma *string* hexadecimal contendo 16 *bytes*)

O campo *application-EUI* refere-se também a um único identificador da aplicação. Por padrão, deve-se manter a *string hexadecimal* “1111111111111111”, contendo 16 bytes.

Para se utilizar das configurações de rede inseridas anteriormente em *Application Settings*, deve-se checar o item *User application Settins*. Isso significa que todos os *nodes* desta aplicação utilizarão o métodos abordado em *Network Setting*.

Clicando-se em *SUBMIT*, após as configurações realizadas será mostrada a guia referente a todos os nodes cadastrados de uma aplicação. A figura 9, a seguir, demonstra apenas a listagem de cadastro de um único *node*. Conforme aumentando-se o número de *nodes*, estes estarão em ordem alfabética de acordo com o campo *Device-name* (referente ao campo anterior *Node-name*).



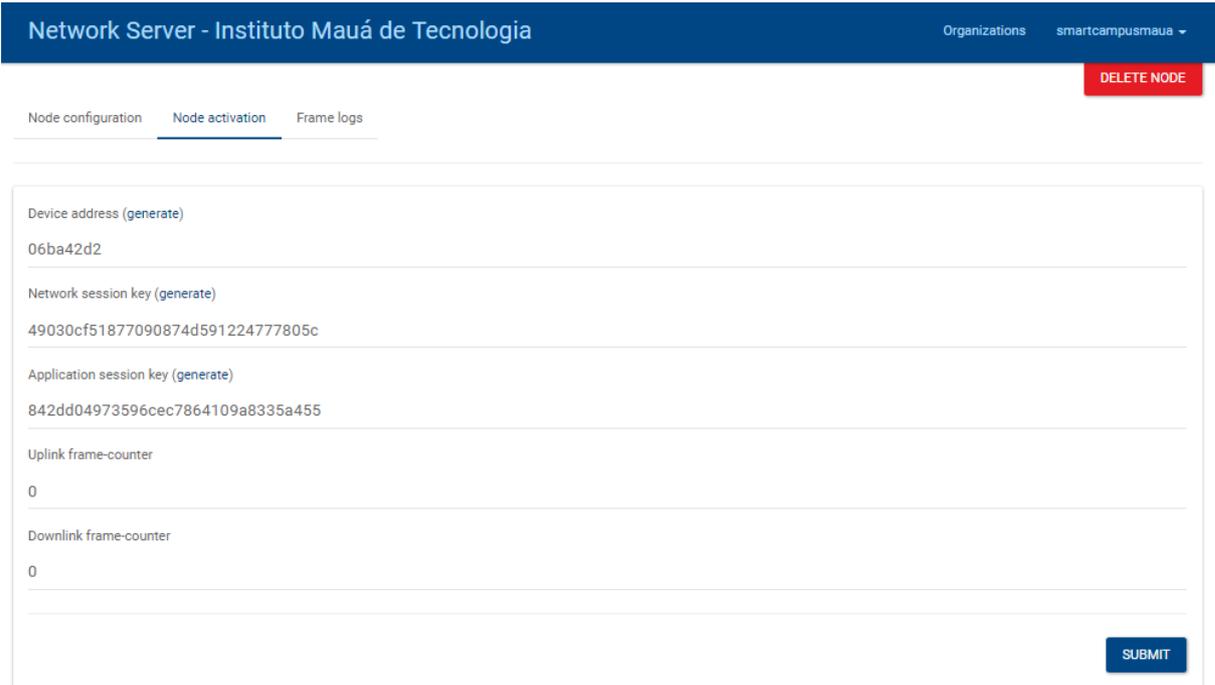
The screenshot shows the 'Network Server - Instituto Mauá de Tecnologia' interface. It features a navigation bar with 'Nodes', 'Application configuration', and 'Application users' tabs. A 'CREATE NODE' button is visible in the top right. Below the navigation, a table lists the nodes:

Device name	Device EUI	Device description	Activation
Hidrometro-01	0004a30b001a5ea2	Monitoramento de vazão da caixa d'água do Bloco U	ABP

Figura 9 - Listagem de *nodes* cadastrados em uma aplicação .

## 2.4.2 ATIVAÇÃO DE NODES

Após o cadastro de *nodes*, detalhado acima, ainda é necessário ativá-los. De acordo com o tipo de ativação selecionada, o *Network Server* começará a receber e a gerenciar os dados dos *nodes* conectados a ele. O modelo de ativação escolhido foi o modelo *ABP*. Este modelo consiste em ao ser recebida a informação de um node, o *Network Server* compara com os dados imputados na guia *Node Activation*. Caso correspondam os dados relativos a *devAdd*, *nwkSkey* e *appSkey*, então uma conexão será estabelecida entre *node-server-node*. Para gerar os parâmetros necessários, é preciso ir até a aba mencionada *Node-Activation*, clicando-se no *node* em que se deseja ativar. A Figura 10, a seguir, demonstra um exemplo de como registrar estes parâmetros na guia *Node-Activation*.



The screenshot shows the 'Node activation' tab in the Network Server interface. It contains several input fields with generated values:

- Device address (generate): 06ba42d2
- Network session key (generate): 49030cf51877090874d591224777805c
- Application session key (generate): 842dd04973596cec7864109a8335a455
- Uplink frame-counter: 0
- Downlink frame-counter: 0

A 'SUBMIT' button is located at the bottom right of the form area. In the top right corner of the interface, there is a 'DELETED NODE' button and a dropdown menu for 'Organizations' set to 'smartcampusmaua'.

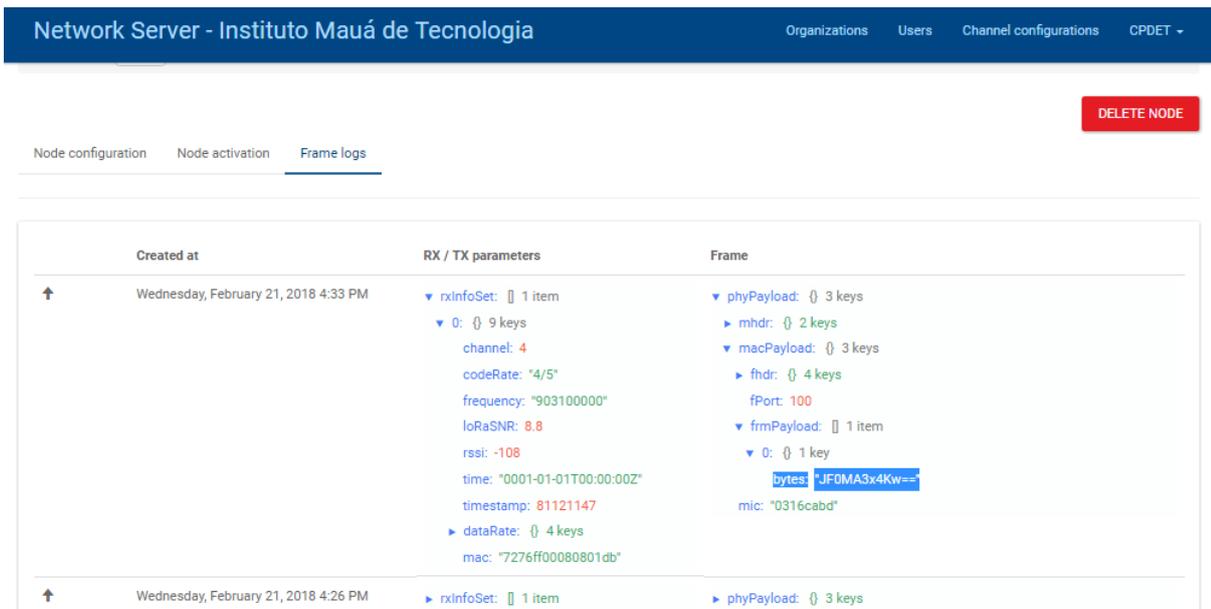
Figura 10 - Inserção de parâmetros para a ativação de *node* através de ativação do tipo ABP (Activation by Personalization).

Percebe-se que é possível gerar um número randômico através do *link generate* para cada campo. Entretanto, é preciso seguir alguns procedimentos segundo o protocolo *LoRaWAN*. O campo *device Address* deve conter 8 *bytes* em formato *hexadecimal*. Entretanto, o campo *Network session key* bem como o campo *application session key* devem possuir uma *string* em *hexadecimal* de 32 *bytes* cada uma. Estes campos, além de servir para a ativação, são as chaves de dupla criptografia necessária para descriptografar e decodificar os dados armazenados no banco de dados, referente ao payload enviado pelo node e como parâmetro de checagem de integridade da mensagem. Para saber mais sobre este processo, deve-se consultar a documentação disponível em [LoRa Alliance](#).

### 2.4.3 REGISTRO DE ATIVIDADES DO NODE

Finalizado este procedimento, e inseridos estes valores de ativação corretamente no código fonte do *node* correspondente, é possível, a partir de agora, receber os dados a serem transmitidos. Para uma rápida visualização, há uma guia denominada *frame Logs*. Nesta guia é possível visualizar os dados de *uplink* e *downlink* da comunicação entre *node-server-node*. Os dados estão por sua vez ainda criptografados no campo *frmPayload*. A Figura 11 abaixo mostra os dados deste *node* que estão chegando (*uplink*) ao servidor. Neste caso, somente há *uplinks*, visto que os dados estão sendo transmitidos sem o caráter de confirmação pelo servidor (*unconfirmed*).

Na figura a seguir também observa-se uma valor descrito como *bytes: "JF0MA3x4Kw=="*. Este valor, embora não se assemelhe com o dado enviado pelo *node* ao servidor, é o dado criptografado e codificado em *base64* armazenado no banco de dados. Somente com os valores de ativação de cada *node* será possível recuperá-lo de maneira decriptografada e decodificada.



The screenshot shows the 'Network Server - Instituto Mauá de Tecnologia' interface. The top navigation bar includes 'Organizations', 'Users', 'Channel configurations', and 'CPDET'. A 'DELETE NODE' button is visible in the top right. The main content area is titled 'Node configuration', 'Node activation', and 'Frame logs'. The 'Frame logs' section displays a table with columns for 'Created at', 'RX / TX parameters', and 'Frame'. The first row shows an uplink frame received on Wednesday, February 21, 2018, at 4:33 PM. The RX / TX parameters include channel: 4, codeRate: '4/5', frequency: '903100000', loRaSNR: 8.8, rssi: -108, time: '0001-01-01T00:00:00Z', timestamp: 81121147, dataRate: '4 keys', and mac: '7276ff00080801db'. The Frame section shows phyPayload: '3 keys', mhdr: '2 keys', macPayload: '3 keys', fhdr: '4 keys', fPort: 100, frmPayload: '1 item', and a key: 'bytes: "JF0MA3x4Kw=="'. The second row shows a downlink frame received on Wednesday, February 21, 2018, at 4:26 PM, with rxInfoSet: '1 item' and phyPayload: '3 keys'.

Figura 11 - Guia Frame logs para visualização de dados de *uplink* e *downlink*.

### 3 RECUPERAÇÃO DE DADOS DO NODE PARA APLICAÇÃO

Em relação à Figura 11 acima, a guia demonstrada serve apenas como um *debug* para que se saiba se o dado está chegando ao servidor bem como mostrar outras informações referentes ao envio. A recuperação das informações estão descritas nos documentos IMT – ACESSO AO MQTT BROKER NETWORKSERVER, para a recuperação destes dados exatamente no momento em que são enviados; no documento IMT – Acesso ao Banco de dados API REST, para recuperação de dados de histórico. Esses dois métodos estão em acordo com a mais recente tendência de retorno de informações no formato *JSON* (*JavaScript Object Notation*). Bem como ainda em EXEMPLO DE APLICAÇÃO MQTT (NODE-RED) e EXEMPLO DE APLICAÇÃO REST API (NODE-RED), são demonstradas aplicações em *Node-RED*, utilizando-se ambos os métodos.