CONSULTA PÚBLICA

PROCEDIMENTO DE MANIFESTAÇÃO DE INTERESSE

PMI CEMIG 002/2025

ANEXO I

Neste Anexo são apresentados os critérios e exigências técnicas mínimas aplicáveis a um teste de integração entre fornecedores da infraestrutura de rede Advanced Metering Infrastructure (AMI) em operação na Cemig.

1. INTRODUÇÃO

Este documento busca fornecer uma estrutura abrangente que oriente os proponentes no desenvolvimento de medidores e sistemas para compatibilidade com a planta em operação na Cemig. Serão abordados aspectos técnicos, protocolos de comunicação, formatos de dados, segurança e outros requisitos essenciais para garantir uma integração efetiva entre os sistemas de diferentes fornecedores.

O objetivo é promover a padronização e a colaboração entre os fabricantes, facilitando a integração de diferentes soluções e a expansão confiável e eficiente do AMI atualmente utilizado pela Cemig.

2. TERMINOLOGIA

Integração: Capacidade de diferentes sistemas, dispositivos ou componentes interagirem e trabalharem em conjunto de forma eficiente e eficaz. Envolve a habilidade de trocar informações e utilizar funcionalidades entre diferentes sistemas de maneira transparente, mesmo que sejam desenvolvidos por fabricantes diferentes ou utilizem tecnologias diversas. Permite a interligação de sistemas heterogêneos, garantindo a comunicação e a cooperação entre eles.

Medidor: Equipamento localizado na unidade consumidora destinado à medição de grandezas elétricas, com capacidade de realizar a conexão e desconexão de unidades consumidoras de ligação direta. O medidor possui módulo de comunicação com interface apropriada para transferência de dados de medição, controle e alarmes de forma bidirecional.

NIC (Network Interface Card): Componente de hardware embarcado no medidor que permite a conexão e a comunicação entre medidores inteligentes e a infraestrutura de rede Wi-SUN. É responsável por converter os dados de medição e outros dados relevantes em pacotes de rede compatíveis com o protocolo Wi-SUN, permitindo que esses dispositivos transmitam e recebam informações dentro da rede AMI. O NIC deve estar em conformidade com os padrões de comunicação e segurança Wi-SUN, suportar mecanismos de roteamento e encaminhamento de dados e operar eficientemente em cenários de comunicação de baixo consumo de energia e alta confiabilidade.

DCU (Data Concentrator Unit): A unidade concentradora de dados é um dispositivo de comunicação projetado para facilitar a criação de redes de área ampla de baixa potência (LPWAN - Low- Power Wide-Area Network). A DCU é composta por Gateway + Border Router (roteador de borda). Para o teste de integração, será utilizada uma DCU existente na rede AMI atual.

NMS (Network Management System): É um sistema de gerenciamento de rede que controla, monitora e gerencia todos os componentes de uma rede. Possui uma interface única para monitorar a rede, o desempenho, detectar problemas e tomar medidas de correção (análise de tráfego, gerenciamento de configurações, falhas, segurança e inventário). Para o teste de integração, será utilizado o NMS existente na rede AMI atual.

Rede FAN (Field Area Network): Compreende a infraestrutura que garante a comunicação principal wireless em medidores que se conectam em uma rede comum destinada ao tráfego de dados bidirecional de forma segura. A rede WAN (Wide Area Network) responsável pela conexão bidirecional de dados segura entre os concentradores da rede FAN e o sistema MDC.

MDC (Meter Data Collector): Sistema responsável por gerenciar a conexão dos elementos da rede de comunicação de campo, através do envio de comandos, recebimento de dados de medição e tratamento de eventos de forma a garantir a segurança e a integridade dos dados de campo. O sistema realiza a transferência dos dados para o sistema MDM. O ambiente de teste de integração será composto por MDC da rede AMI atual e o MDC do proponente.

MDM (Meter Data Management): Sistema responsável pelo gerenciamento dos dados com disponibilização para os sistemas legados.

Remote Authentication Dial In User Service (Radius): Fornece autenticação, autorização e contabilidade centralizadas para dispositivos que se conectam a uma rede. Controla o acesso a rede, verifica a identidade dos usuários e monitora o uso da rede.

Constrained Application Protocol (CoAP): Protocolo de aplicação desenvolvido para dispositivos de Internet das Coisas (IoT) que têm restrições de recursos, como capacidade limitada de processamento, memória e energia. Foi projetado para ser eficiente em termos de consumo de recursos e é adequado para dispositivos que operam em redes com restrições, como redes de sensores sem fio. Geralmente é utilizado para permitir a comunicação entre dispositivos IoT e serviços baseados na Internet, como sistemas de gerenciamento de dados e aplicativos em nuvem. As especificações do CoAP são definidas no Request for Comments -RFC 7252.

DLMS/COSEM:

Device Language Message Specification ou Distribution Line Message Specification/Companion Specification for Energy Metering (DLMS/COSEM) é um protocolo de aplicação para um conjunto de padrões que define como os dispositivos de medição e controle comunicam-se, coletam dados e interagem em redes inteligentes. Cada dispositivo de medição expõe uma coleção de objetos (leituras de medição, eventos, parâmetros de configuração etc.) que representam funcionalidades e dados específicos. O protocolo define como os dispositivos se comunicam usando mensagens padronizadas. Essas mensagens podem incluir solicitações de leitura, gravação ou execução de operações. Além disso, o DLMS/COSEM oferece recursos de segurança para proteger as comunicações e os dados. Ele suporta autenticação, criptografia e outras medidas para garantir a integridade e confidencialidade das informações transmitidas. O DLMS/COSEM permite a comunicação confiável e eficiente entre dispositivos de medição e sistemas de gerenciamento.

3. REPRESENTAÇÃO DA INTEGRAÇÃO

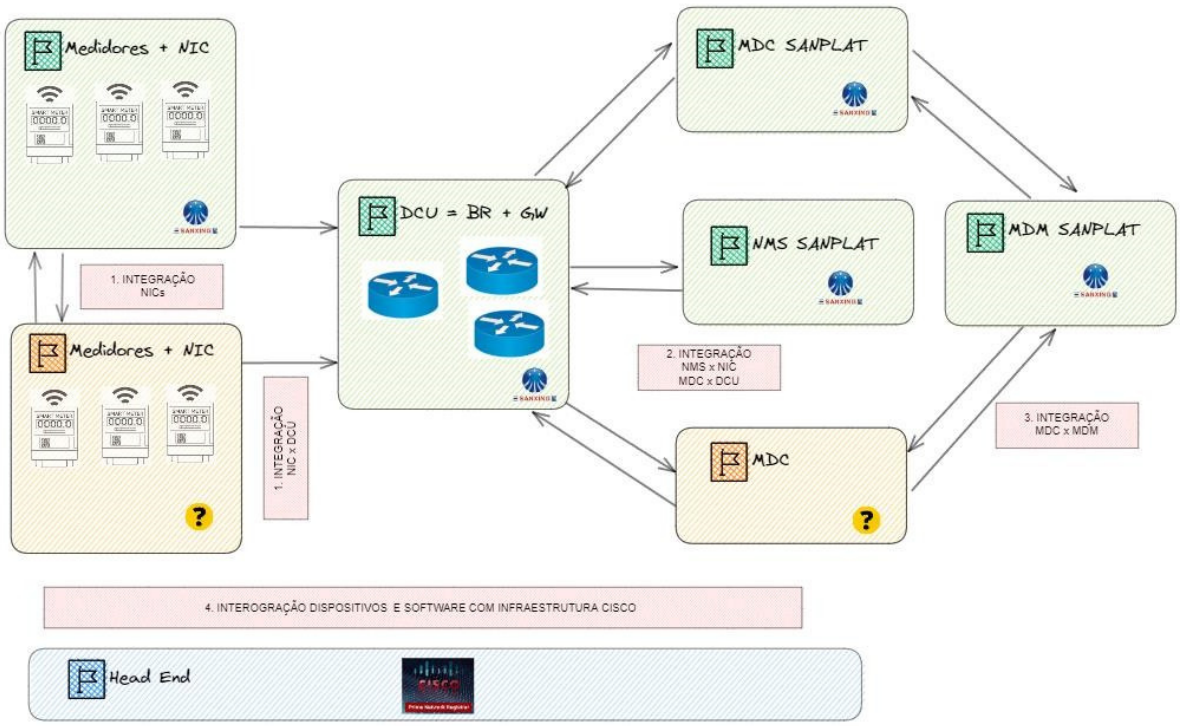

Figura 1 - Representação para integração entre fornecedores – Rede AMI

a) Medidores + NIC: O conjunto Medidores + NIC devem manter a integração com medidores + NIC de outros fabricantes e manter a integração com a DCU em operação na rede AMI atual.

b) DCU (Border Router + Gateway): A unidade concentradora de dados utilizada atualmente na rede AMI deve ter integração com medidores inteligentes e MDC próprios e de outros fabricantes. Também deve possuir integração com o NMS atual para controle da rede.

c) MDC e MDM: O novo fornecedor deverá garantir a integração entre o seu MDC e o MDM e a DCU em uso atualmente.

d) Dispositivos + software e Headend: Todos os dispositivos e softwares devem possuir integração com o Headend que possui infraestrutura Cisco, o Cisco Prime Network Registrar (CPNR).

4. ESTRUTURA DO AMBIENTE DE TESTE

Um ambiente de testes será disponibilizado pela Cemig para os proponentes conectarem seus equipamentos à rede AMI para a realização dos testes de integração.

A figura que segue, demonstra a infraestrutura do ambiente de teste. As instalações do laboratório da Cemig hospedam a FAN, os medidores e aplicativos de Headend. Para os testes o proponente deve disponibilizar sistema responsável pela coleta e tratamento dos dados (Application Server), hospedado na nuvem e que se conecta por meio de uma conexão VPN via a infraestrutura descrita abaixo.

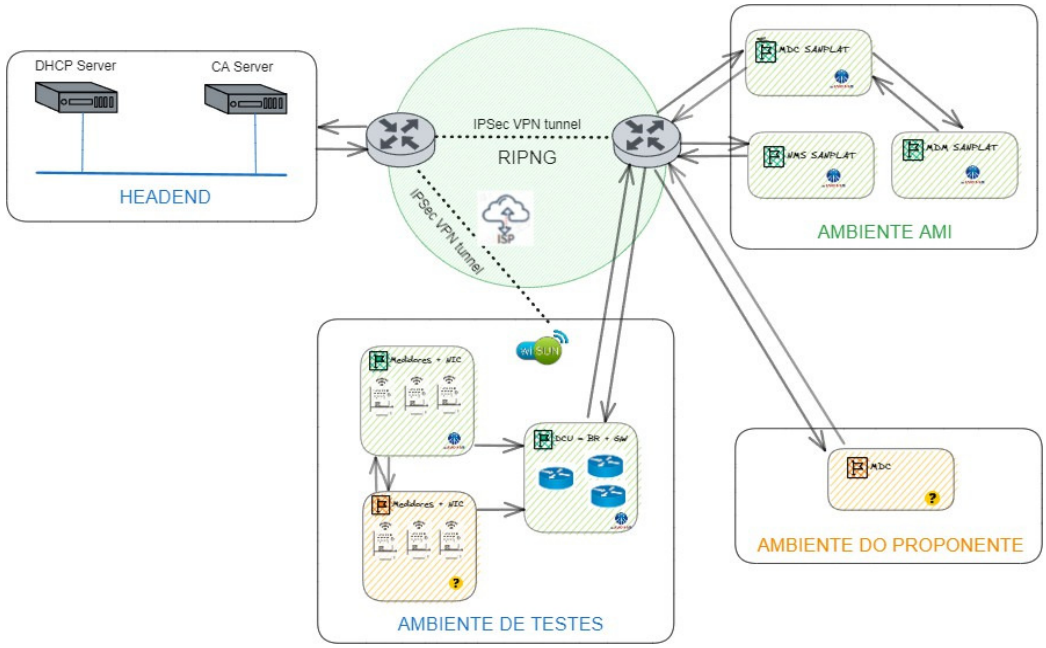

Figura 7 – Representação da estrutura do ambiente de teste de integração

Para acessar o ambiente de teste de integração, as seguintes informações deverão ser disponibilizadas pelo proponente:

a) Informações sobre os equipamentos (medidores + NIC e MDC);
b) Informações de conexão para estabelecer VPN site-to-site para acesso a aplicação.

As seguintes informações e recursos para conexão ao ambiente do teste de integração serão fornecidas pela Cemig:
a) PKI/autoridade certificadora (CA);
c) Informações para conexão ao servidor DHCP;
d) Informações para conexão ao Radius e configurações necessárias.

Todos os testes serão realizados como uma atividade conjunta entre a equipe de desenvolvimento, proponente e Cemig.

Requisitos de redes de telecomunicações

Os sistemas existentes estão implementados com protocolos de padrão aberto, não sendo utilizado nenhum protocolo proprietário na composição dos sistemas de medidores inteligentes.
Para garantir a compatibilidade do concentrador de dados com o sistema existente os seguintes parâmetros devem ser atendidos:

- Suporte ao Internet Protocol versão 4 (IPv4), conforme descrito pelo Internet Engineering Task Force (IETF) na publicação da RFC 791.

- Suporte ao Internet Protocol versão 6(IPv6), conforme descrito na Internet Engineering Task Force (IETF) na publicação da RFC 8200.
- Suporte Remote Authentication Dial In User Service (Radius), conforme descrito no Internet Engineering Task Force (IETF) na publicação da RFC 2865.
- Suporte ao Simple Certificate Enrolment Protocol (SCEP), conforme descrito na Internet Engineering Task Force (IETF) na publicação RFC 8894.
- Utilizar certificados de chave pública X.509 da International Telecommunication Union (ITU), seguindo as características definidas na ISO/IEC 9594-8:2020 e a na RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile descrito pela Network Working Group.
- Suporte a IP Security (IPsec) and Internet Key Exchange (IKE), conforme descrito na Internet Engineering Task Force (IETF) na publicação RFC 6071.
- Suporte ao Router information Protocol Next Generation (RIPng), conforme descrito na Internet Engineering Task Force (IETF) na publicação RFC 2080.
- Suporte a Tunelamento 6to4 conforme descrito no Network Working Group publicado na RFC 3056 e na Internet Engineering Task Force (IETF) RFC 6343.
- Suporte a DHCPv6, conforme Internet Engineering Task Force (IETF) na publicação RFC 8415.
- Suporte a Lightweight DHCPv6 Relay Agent (LDRA), conforme descrito na Internet EngineeringTask Force (IETF) na publicação RFC 3315.
- Compatibilidade dos medidores com a rede AMI existente.
- Suporte ao Internet Protocol versão 6(IPv6), conforme descrito na Internet Engineering Task Force (IETF) na publicação da RFC 8200.
- Suporte a DHCPv6, conforme Internet Engineering Task Force (IETF) na publicação RFC 8415.
- Todos os tuneis de criptografia, ou tunelamento de ipv6/ ipv4 da solução, devem estar implementados e compatíveis, através dos Concentradores de túneis IPSEC (Via plataforma Cisco CSR 1000V).
- Todo o escopo de entrega de IPs da solução ofertada, devem estar implementados e compatíveis usando o Servidor de DHCP/DNS (Via plataforma Cisco Prime IP Express DHCP/DNS).
- Funcionalidade de DHCP Relay devem estar implementados e compatíveis com o sistema de DHCP Server (Via plataforma Cisco Prime IP Express DHCP).
- Toda as trocas de certificados digitais entre os elementos de rede devem estar implementa-das e compatíveis com o protocolo SCEP (Via plataforma CSR 1000V SCEP).

5. PLANO DE TESTES

Os testes abrangem as seguintes áreas:

- Caracterização de RF;
- Análise e gerenciamento local;
- Conectividade RF Mesh;
- Segurança de Mesh Security;
- Aplicativo de medidores;
- Resiliência a falha e disponibilidade.

Para fins de certificação, a FAN precisará ser configurada para as seguintes topologias para diferentes cenários de teste. As topologias necessárias são descritas nos cenários de testes

Cenários de teste

Um NIC e uma FAN

Essa topologia FAN simples de um dispositivo é recomendada para validação de recursos básicos antes do teste dos recursos em topologias mais complexas.

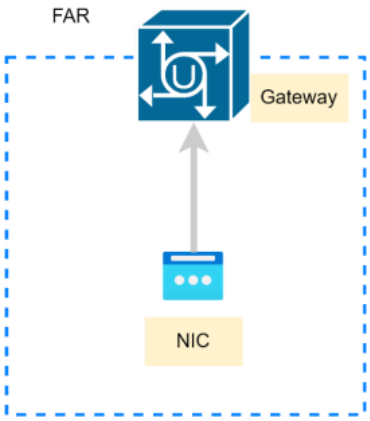

Figura 8 - Um NIC em um FAN

Detalhes do caso de teste	
Título	**Caracterização de RF** - Física RF e camada MAC - Potência de transmissão - Medir a potência de transmissão do NIC durante a operação normal
Configuração de teste	Figuras 8 e 9
Procedimento	• Deixe a configuração de potência de transmissão da NIC como padrão. • Configuração de RF: Gateway a uma distância de aproximadamente 1 metro do nó. Com 50dB de atenuação na antena. O valor RSSI aceitável deve estar na faixa de -45 dBm a -55 dBm. • Compare a potência de transmissão do NIC existente da rede com o NIC do proponente quando eles são colocados adjacentes um ao outro.
Critérios de aprovação/reprovação	Faixa de nível de sinal aceitável -45 dBm a -55 dBm.

Tabela 1 - Detalhes dos casos de teste (camadas físicas e de MAC)

Detalhes do caso de teste	
Título	**Caracterização de RF** - Teste comparativo do nível e qualidade do Sinal
Configuração de teste	Figuras 8 e 9
Procedimento	• Compare os níveis de potência de transmissão e recepção do terminal em teste com a plataforma existente na Cemig. • Coloque o terminal com 50 dB de atenuação a uma distância de aproximadamente 1 metro do Gateway. • Coloque um NIC+medidor em aplicação atualmente na mesma distância com a mesma atenuação. • Certifique-se de que ambos se unem à malha. • Certifique-se de que o RSSI para ambos os nós estejam dentro de ± 5 dB um do outro.
Critérios de aprovação/reprovação	Registro do resultado e não pode haver discrepância maior que o valor recomendado.

Tabela 2 - Detalhes do teste qualidade de sinal

Quatro NICs em uma FAN

Esta é a topologia recomendada para a maioria dos recursos, funcionalidades, segurança, gerenciamento e testes de resiliência a falhas. Deve-se notar que quatro é o número mínimo sugerido para NICs nesta topologia. É um requisito ter pelo menos 3 saltos na rede Mesh. Observe também que os NICs nesta topologia são os dispositivos do novo proponente em teste, ou seja, não uma topologia de vários dispositivos.

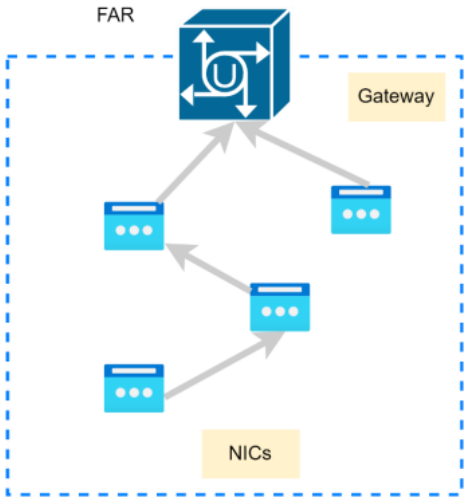

Figura 9 - Quatro NICs em uma FAN

Detalhes do caso de teste	
Título	Controle de acesso para certificado não autenticado/não confiável no dispositivo (Rejeição do dispositivo)
Configuração de teste	Figura 9
Procedimento	• Um ou mais NIC não devem ser configurados com segurança. • Certifique-se de que os NICs sem as credenciais não se juntem à malha. Todos os outros NICs confiáveis ainda devem ser capazes de ingressar e se comunicar pela malha. • Agora, carregue certificados de CA não confiável em um ou mais NICs. • Certifique-se de que os NICs não confiáveis não se juntem à malha. Todos os outros NICs confiáveis ainda devem ser capazes de ingressar e se comunicar sobre malha.
Critérios de aprovação/reprovação	Conforme observado no procedimento, não pode ocorrer conexão de NIC não confiável

Tabela 3 - Controle de acesso para certificado não autenticado/não confiável no dispositivo (Rejeição do dispositivo)

Detalhes do caso de teste	
Título	Comunicação CSMP deve funcionar entre o NMS e o NIC
Configuração de teste	Figura 9
Procedimento	• Certifique-se de que todo o provisionamento para a configuração do novo proponente esteja completo e funcionando entre o NIC e NMS. • Certifique-se de que o ambiente FAN esteja configurado para segurança, incluindo 802.1x e 802.11i.

Critérios de aprovação/reprovação	As comunicações do NMS com a NIC devem ser bem-sucedidas. Registro NMS, acessibilidade e atualizações periódicas.

Tabela 4 – Comunicação CSMP para conexão entre NMS e NIC

Detalhes do caso de teste	
Título	Atualização de firmware NMS sobre mensagens CSMP
Configuração de teste	Figura 9
Procedimento	• Certifique-se de que todo o provisionamento para a configuração do novo proponente esteja completo e funcionando entre o NIC e o NMS. • Certifique-se de que o ambiente FAN esteja configurado para segurança, incluindo 802.1x e 802.11i. • Realize uma atualização de firmware através do NMS. • Certifique-se de que o download do firmware do NIC esta utilizando mensagens unicast. • Certifique-se de que o download do firmware foi bem-sucedido. • O NIC deve executar a reinicialização. Após a conclusão do download do firmware, agende uma reinicialização. • Certifique-se de que a NIC seja reiniciado no horário agendado. • Após o reinicialização do NIC, certifique-se de que o mesmo ingresse na rede Mesh e solicitando e recebendo endereço IPv6 com sucesso. • Certifique-se de que o Gateway esteja registrado no NMS. • Verifique no NMS que a nova versão do firmware esteja correta. • Certifique-se de que todos os NICs possam se comunicar por meio de pings.
Critérios de aprovação/reprovação	Firmware do NIC atualizado com sucesso. Obs: Pode ser solicitado a atualização broadcast dos NICs.

Tabela 5 – Atualização de firmware NIC com NMS

Detalhes do caso de teste	
Título	Funcionalidade do servidor de aplicativos (leituras do medidor etc.)
Configuração de teste	Figura 9
Procedimento	• Certifique-se de que o Application Server esteja conectado ao medidor usando VPN e tem um endereço IPv6 válido e alcançável. • Certifique-se de que o roteamento esteja configurado entre o Gateway e o Application Server para acessibilidade. • Certifique-se de que servidor DHCP atenda opção para o endereço IPv6 do servidor de aplicativos específico do proponente. • Certifique-se de que o ambiente FAN esteja configurado para segurança, incluindo 802.1x e 802.11i, e os NICs estejam configurados com as credenciais, bem como todos os certificados necessários (para 802.1x, NMS e Application Server(s) se aplicável. • Certifique-se de que os NICs se juntem à malha e possam se comunicar usando pings. Verifique se os NICs foram registrados no NMS. • Se aplicável, certifique-se de que os NICs se

	registrem no Application Server. • Certifique-se de que o Gateway esteja registrado no NMS. • Certifique-se de que a conexão/conectividade entre o Application Server e o NIC foi bem-sucedido (UDP). • Certifique-se de que a funcionalidade do servidor de aplicativos seja bem-sucedida, realizando comandos, sob demanda ou leituras do medidor, notificações periódicas do NIC etc. Devem ser testadas as funcionalidades abaixo quando disponível no medidor: a. Leitura dos totalizadores atuais direta e reversa (totalizador geral e totalizadores das tarifas de Ponta, Fora Ponta, Reservado, e tarifa D) e memória de massa dos canais b. Parametrização de Data c. Parametrização de Hora d. Parametrização de feriados e. Ativação/desativação de tarifação diferenciada aos sábados f. Ativação/desativação de tarifação diferenciada aos domingos g. Parametrização de horário de ponta h. Parametrização de horário fora de ponta i. Parametrização de horário reservado j. Parametrização de horário da tarifa D k. Parametrização de Tarifa Reativa (Ativa ou Inativa) l. Parametrização de Fatura Automática m. Parametrização de Início do horário Indutivo n. Parametrização de Início do horário Capacitivo o. Alteração do horário de verão p. Abertura/fechamento do relé interno com e sem carga e com simulação de presença de tensão do lado da carga q. Ativação e desativação de medição de demanda r. Leitura dos status de alarmes dos medidores s. operação de last gasp t. Leitura de dados de Medição de Qualidade de Energia u. Verificação de atualização de dados a cada kWh alterado e a cada 15min; v. Alteração de código de registradores x. Leitura de parâmetros de qualidade
Critérios de aprovação/reprovação	O servidor de aplicativos deve ser capaz de se comunicar e realizar as operações leitura e comandos nos medidores.

Tabela 6 - Funcionalidade do servidor de aplicativos (leituras do medidor etc.)

Detalhes do caso de teste	
Título	Execução de atualizações de firmware do medidor over-the-air
Configuração de teste	Figura 9
Procedimento	• Certifique-se de que o Application Server esteja conectado ao medidor usando VPN e tem um endereço IPv6 válido e alcançável. • Certifique-se de que o roteamento esteja configurado entre o Gateway e o Application Server para acessibilidade. • Certifique-se de que servidor DHCP atenda opção para o endereço IPv6 do servidor de aplicativos específico do proponente. • Certifique-se de que o ambiente FAN esteja configurado para segurança, incluindo 802.1x e 802.11i, e os NICs estejam configurados com as credenciais, bem como todos os certificados necessários (para 802.1x, NMS e Application Server(s) se aplicável. • Certifique-se de que os NICs se juntem à malha e possam se comunicar usando pings. Verifique se os NICs foram registrados no NMS. • Se aplicável, certifique-se de que os NICs se registrem no Application Server. • Certifique-se de que o Gateway esteja registrado no NMS. • Certifique-se de que a conexão/conectividade entre o Application Server e o NIC foi bem-sucedido. • Certifique-se de que a funcionalidade do servidor de aplicativos seja bem-sucedida com atualização de fimware do medidor.
Critérios de aprovação/reprovação	O servidor de aplicativos deve ser capaz de se comunicar e realizar atualização de firmware over-the-air Obs: Pode ser solicitado a atualização broadcast dos medidores.

Tabela 7 - Execução de atualizações de firmware do medidor

Detalhes do caso de teste	
Título	Recuperação após desligamento do medidor
Configuração de teste	Figura 9
Procedimento	• Realizar desligamento do medidor • Verificar seu retorno após reenergização.
Critérios de aprovação/reprovação	O medidor deve Recuperação após falha de energia da NIC

Tabela 8 - Recuperação após falha de energia da NIC

FAN de grande escala e de múltiplos saltos (multi-hop) + NIC de vários fornecedores

Nesta topologia, o NIC DUT (Network Interface Card Device Under Test) é um dos muitos dispositivos de vários fornecedores conectados ao mesmo FAN. A topologia de teste requer a presença de vários NIC nas funções de nós de malha (mesh nodes) e nós terminais (leaf nodes). Os detalhes são registrados no teste.

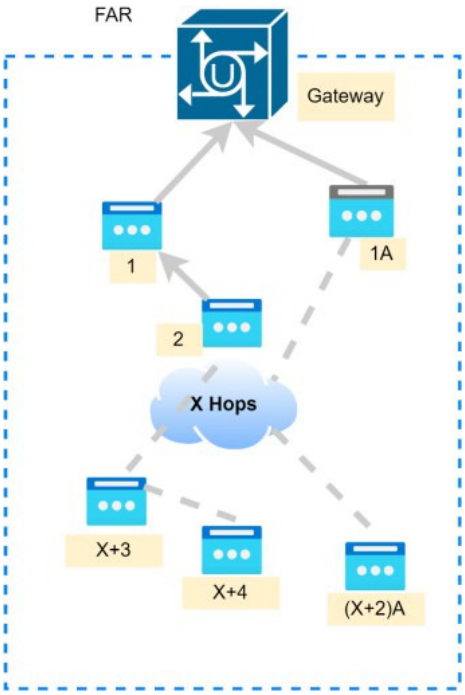

Figura 10 - NIC FAN de grande escala, multi-hop, multi-fornecedor

Detalhes do caso de teste	
Título	Teste de desempenho e escalabilidade
Configuração de teste	Figura 10

Procedimento	• Posicionar o NIC na FAN de grande escala, multi-hop e multi-dispositivo como um root da subárvore • O NIC deve realizar o encaminhamento de grandes volumes de upstream e downstream de datagramas IPv6 (usando roteamento de origem padrão) para vários destinos • Realizar uma operação remota de tráfego intenso sobre a malha (transferência de arquivo/firmware) • Realizar ao mesmo tempo upstream, downstream e uma operação de tráfego intenso (transferência de arquivo/firmware) • Testar o desempenho na coleta de dados do medidor, eficiência de encaminhamento (quedas de pacotes de ponta a ponta e valores de latência para fluxos de tráfego upstream e downstream), recursos de FAN, capacidade de gerenciamento (consultas CSMP), testes de longa duração/saturação.
Critérios de aprovação/reprovação	Realizar coleta satisfatória de dados com atualização de leituras, memória de massa e grandezas elétricas com agendamento de atualização a cada 4 horas.

Tabela 9 - desempenho e escalabilidade

Testes sem a necessidade de um cenário de testes

Detalhes do caso de teste	
Título	Atualização do firmware no campo de NIC e Medidores
Configuração de teste	N/A
Procedimento	• Deve ser disponibilizado mecanismo para atualizar o firmware em campo. • Os técnicos de campo devem atualizar o firmware de comunicação no campo.
Critérios de aprovação/reprovação	Deve ser possível atualizar o firmware de medidor e NIC em campo

Tabela 10 - Atualização do firmware no campo

Detalhes do caso de teste	
Título	Capacidade de depuração de rede por meio de pings
Configuração de teste	N/A
Procedimento	• Para o modelo PPP, a capacidade de executar ping do NIC para qualquer destino IPv6 deve estar disponível. • Certifique-se de que o ping do IPv6 do NIC para a interface WPAN do Gateway foi bem-sucedido. • Certifique-se de que o ping IPv6 para outro NIC no mesmo WPAN foi bem-sucedido.
Critérios de aprovação/reprovação	Realizar PING em nós da rede

Tabela 11 - Depuração de rede por meio de pings

Detalhes do caso de teste	
Título	Capacidade de consultar a configuração de rede
Configuração de teste	N/A
Procedimento	• O NIC deve fornecer ferramentas para consultar ou exibir a seguinte configuração de rede na NIC: - Para o modelo PPP, endereços IPv6 da interface PPP (link local e global) e tamanho do prefixo no kernel; - Tabela de roteamento na NIC; - Endereço do servidor de aplicativos: derivado do conteúdo da opção DHCP (Cada fornecedor receberá um endereço exclusivo); - O endereço IPv6 conterá o endereço do servidor de aplicativos. O NIC não deve “codificar” este índice, pois pode variar de utilitário para utilitário.
Critérios de aprovação/reprovação	Deve ser informado os valores esperados para os itens dos parâmetros acima

Tabela 12 - Consulta a configuração de rede

Detalhes do caso de teste	
Título	Capacidade de depuração por meio do CSMP
Configuração de teste	N/A
Procedimento	• Deve ser disponibilizado mecanismo para consultar CSMP TLV do kernel CM/IE. • Para o modelo PPP, a capacidade de consultar CSMP TLVs por meio da porta do host na conexão PPP deve estar disponível. • Todos os valores CSMP TLVs devem estar disponíveis para consulta.
Critérios de aprovação/reprovação	Todos os critérios descritos no procedimento devem ser disponíveis.

Tabela 13 - Depuração por meio do CSMP

Detalhes do caso de teste	
Título	Valores EUI64 organizacionalmente exclusivos para comunicação em malha. Marcação de QoS para mensagem CSMP do kernel
Procedimento	• O parceiro deve usar um identificador exclusivo organizacional (OUI) designado pela autoridade de registro IEEE para os primeiros 3 bytes do EUI-64 para todos os seus dispositivos. • Os 40 bits restantes do EUI-64 devem ser exclusivos para cada dispositivo fabricado. Documentar o procedimento de derivação EUI64 para as NICs. Através de configuração xml ou derivação algorítmica. • Observe o procedimento para derivação algorítmica do valor EUI64 e certifique-se de que o IEEE atribua o OUI que está sendo usado.
Critérios de aprovação/reprovação	Conforme observado no procedimento.

Tabela 14 - Mensagem CSMP

Belo Horizonte, 17 de setembro de 2025.