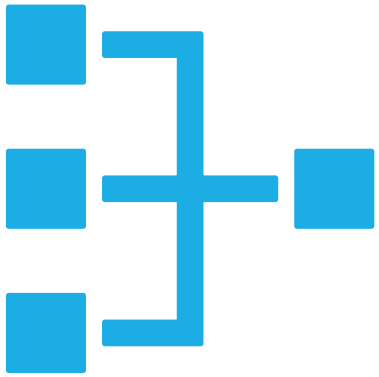
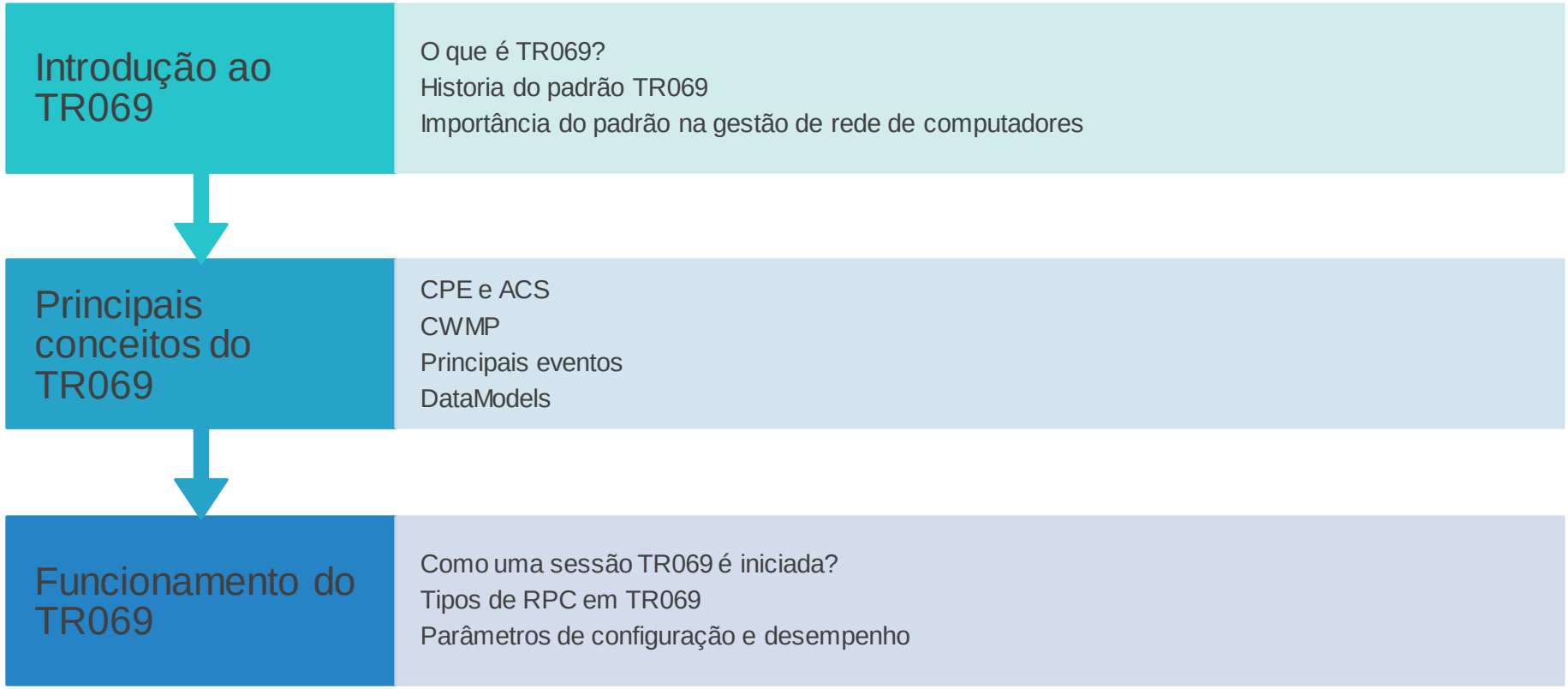


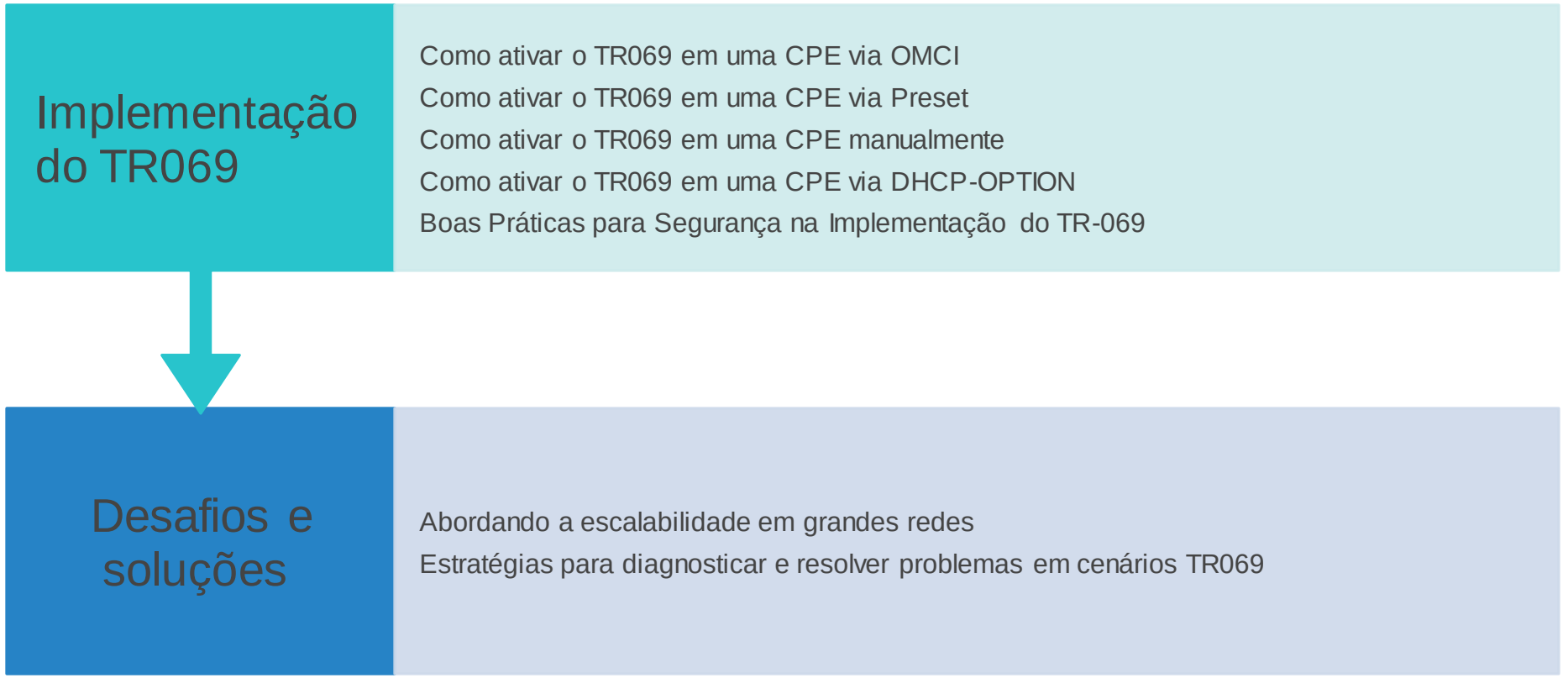
Do Conceito à Prática: TR069 e o promissor TR369 como pilares da gestão remota e eficiente de CPEs

SEMANA DE CAPACITAÇÃO - EDIÇÃO ONLINE 8

Índice I


Introdução ao TR069
O que é TR069?
Historia do padrão TR069
Importância do padrão na gestão de rede de computadores
Principais conceitos do TR069
CPE e ACS
CWMP
Principais eventos
DataModels
Funcionamento do TR069
Como uma sessão TR069 é iniciada?
Tipos de RPC em TR069
Parâmetros de configuração e desempenho

Índice II


Implementação do TR069
Como ativar o TR069 em uma CPE via OMCI
Como ativar o TR069 em uma CPE via Preset
Como ativar o TR069 em uma CPE manualmente
Como ativar o TR069 em uma CPE via DHCP-OPTION
Boas Práticas para Segurança na Implementação do TR-069
Desafios e soluções
Abordando a escalabilidade em grandes redes
Estratégias para diagnosticar e resolver problemas em cenários TR069

Indice III

Futuro do TR069

Apresentamos o USP

Por que um novo protocolo?

Quais os obstáculos do TR-069?

Comparação entre TR-069 e TR-369

Mas o USP é mais eficiente?

Gerenciamento de próxima geração é mais eficiente?

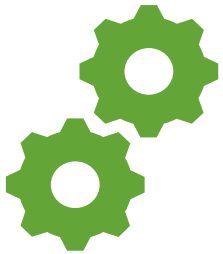
O futuro do gerenciamento remoto

Para onde corre a Indústria?

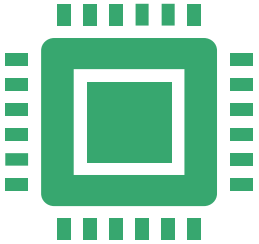
Para saber mais

Introdução ao TR069

O que é TR069



O uso do TR-069 simplifica e automatiza o processo de gerenciamento de dispositivos de rede, melhorando a eficiência operacional dos provedores de serviços enquanto oferece uma experiência mais conveniente para os usuários finais.



Em outras palavras o padrão foi criado para:

Permitir o gerenciamento remoto de dispositivos de rede.
Facilitar a atualização de firmware.
Configurar parâmetros de rede.
Realizar diagnósticos.
Fornecer suporte técnico remoto.
Entre outras funcionalidades

História do TR069

- Criado pela BroadBand fórum, para centralizar a gestão remota de dispositivos de rede, o padrão TR069 foi lançado em 2004, buscando resolver diversos problemas, como:
  - Gestão decentralizada de CPEs
  - Complexidade operacional
  - Custos elevados para treinamento e manutenção
  - Não existência de um padrão aberto
  - Cabia ao fabricante desenvolver e lançar seu protocolo de gestão remota da CPE

História do TR069

Versão 1.0:

Estabeleceu os princípios fundamentais para o gerenciamento remoto de equipamentos de cliente (CPE) em redes de banda larga.

Versão 1.1:

Introduziu melhorias e correções de bugs para aumentar a estabilidade e a interoperabilidade do protocolo.

Versão 1.2:

Adicionou suporte a diagnósticos aprimorados, gerenciamento de eventos e melhorias na segurança.

Versão 1.3:

Expandiu os recursos com suporte para operações de configuração avançada, gerenciamento de QoS e aprimoramentos na gestão de dispositivos.

Versão 1.4:

Introduziu melhorias adicionais de desempenho, segurança e estabilidade, além de suporte a novos tipos de dispositivos e serviços.

Importância do padrão na gestão de rede de computadores

Gerenciamento Remoto Simplificado:

Permite o gerenciamento remoto padronizado de dispositivos de rede.

Eficiência Operacional:

Melhora a eficiência dos provedores de serviços ao realizar operações remotamente.

Interchangeabilidade:

Substituição transparente de dispositivos, mantendo serviços contínuos e interoperabilidade entre fabricantes.

Interoperabilidade:

Garante interoperabilidade entre dispositivos de diferentes fabricantes.

Segurança Aprimorada:

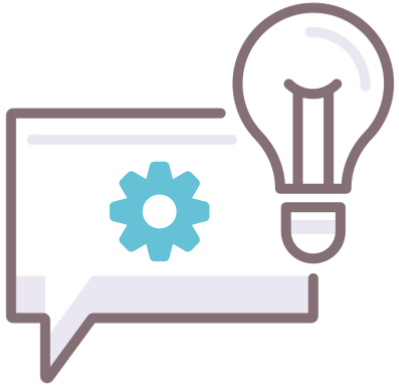
Inclui recursos de segurança, como autenticação e criptografia.

Escalabilidade:

Permite escalabilidade para lidar com grandes redes de forma eficiente.

Atualizações Contínuas:

Evolui constantemente para adicionar recursos e melhorias



Principais conceitos do TR069

ACS

ACS (Auto Configuration Server): Servidor que gerencia os dispositivos CPE. O ACS é responsável por enviar comandos, coletar informações e realizar outras operações de gerenciamento nos CPEs.

Além dos pontos citados ele pode facilitar operações como:

Provisionamento de serviços,
Diagnósticos de rede,
Atualizações de firmware e
Configurações remotas.

CPE

São dispositivos usados para acessar a internet e que são gerenciados pelo CWMP,

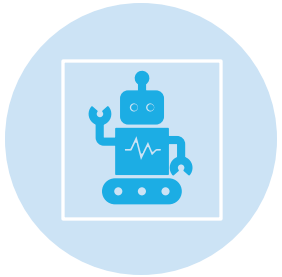
Podem estar localizados nas instalações do cliente.

Utilizados para acessar serviços de rede.

Exemplos incluem roteadores, modems, set-top boxes.

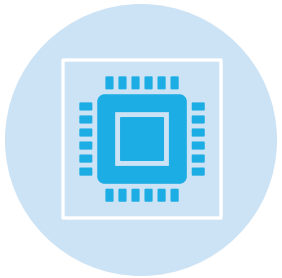
Responsáveis por estabelecer conexão com a rede do provedor de serviços

CWMP



Protocolo padronizado para gerenciamento remoto de dispositivos CPE (Customer Premises Equipment).

Estabelece comunicação entre dispositivos CPE e servidores ACS (Auto Configuration Server).



Permite configuração, diagnóstico, monitoramento e atualizações remotas de dispositivos de rede.

Facilita a entrega de serviços de forma eficiente e escalável para clientes finais pelos provedores de serviços de internet.

Datamodels

Existem hoje dois datamodels conhecidos para TR069, o TR-098 e o TR181.

No contexto histórico o TR-098 foi publicado antes que o TR181.

O desenvolvimento do TR-181 ocorreu porque o TR-098 não fornecia todas as funcionalidades e recursos necessários para atender às demandas crescentes da indústria de telecomunicações e as complexidades dos dispositivos CPE modernos.

Embora o TR-098 tenha sido um marco importante na padronização do gerenciamento remoto de dispositivos CPE, o desenvolvimento do TR-181 foi necessário, para acompanhar o mercado.

Principais Eventos

- INICIADOS PELA CPE
  - 0 BOOTSTRAP
  - 1 BOOT
  - 2 PERIODIC
  - 4 VALUE CHANGE
  - 8 DIAGNOSTIC COMPLETE
  - Quando o evento for desencadeado por uma solicitação TR-069 pelo ACS, a resposta da CPE será um evento iniciado com "M" que vem de "method", como exemplo: M.REBOOT

- INICIADOS PELO ACS
  - 6 CONNECTION REQUEST

Datamodels

Objetivo:

- Padronizar a representação das funcionalidades e configurações dos dispositivos CPE.
- Facilitar o gerenciamento remoto e interoperabilidade entre diferentes dispositivos e provedores de serviços.

Estrutura Hierárquica:

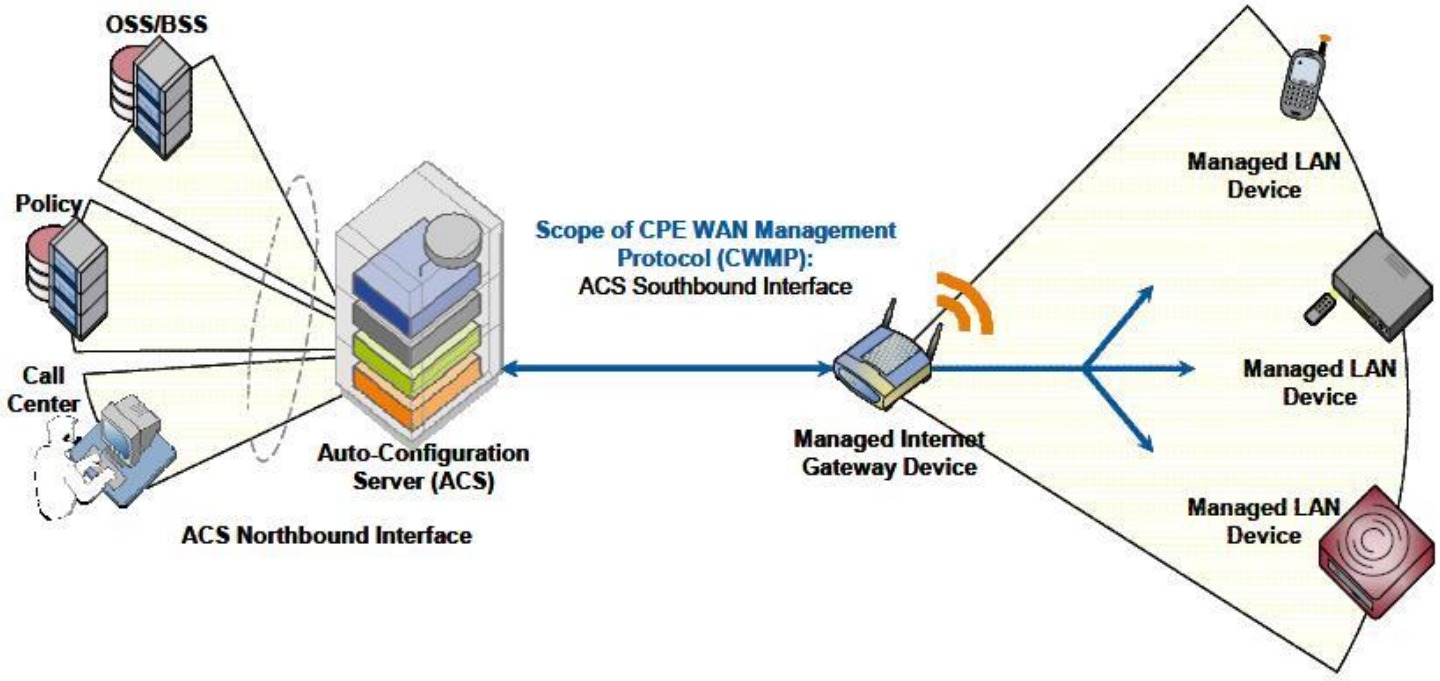
- Define uma estrutura de objetos e parâmetros que abrangem diversos aspectos do dispositivo.
- Inclui
  - configurações de rede,
  - interfaces, serviços,
  - diagnósticos,
  - entre outros.

Amplamente adotado na indústria de telecomunicações.

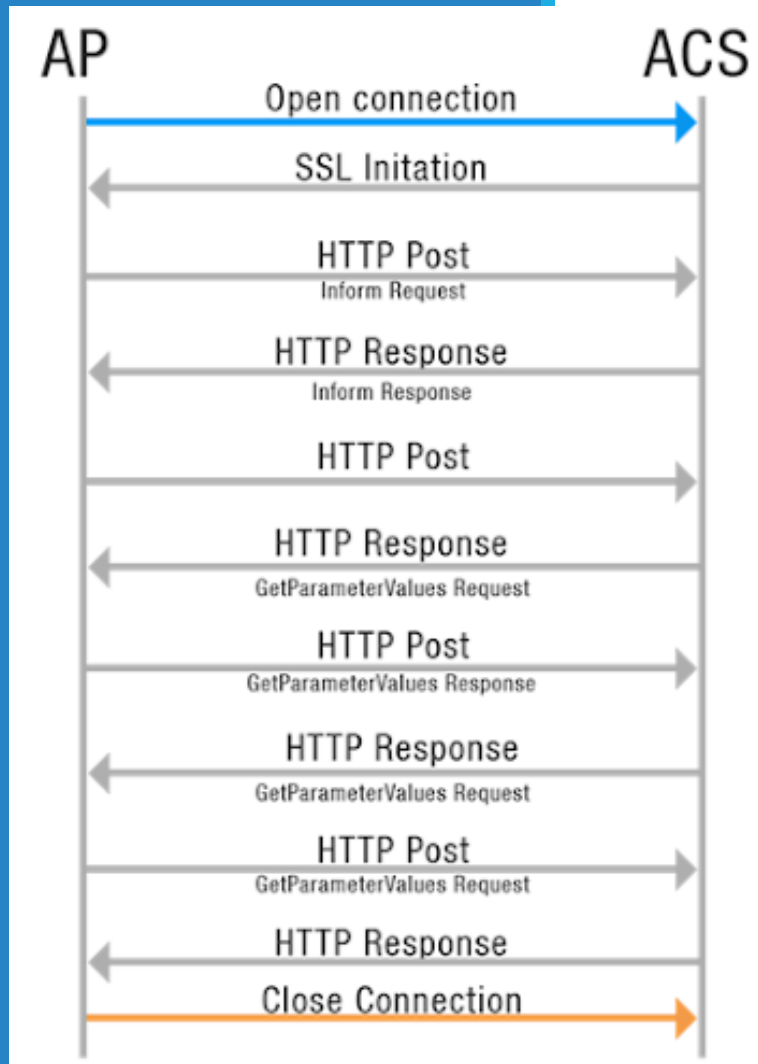
Utilizado em conjunto com protocolos de gerenciamento remoto, como TR-069 (CWMP).

All parameters

Virtual
InternetGatewayDevice.LANDevice.1.WLANConfiguration.2.X_ALU-COM_VirtualIfCfg_MaxAss…
InternetGatewayDevice.LANDevice.1.WLANConfiguration.3.X_ALU-COM_VirtualIfCfg_MaxAss…
InternetGatewayDevice.LANDevice.1.WLANConfiguration.4.X_ALU-COM_VirtualIfCfg_MaxAss…
InternetGatewayDevice.LANDevice.1.WLANConfiguration.5.X_ALU-COM_VirtualIfCfg_MaxAss…
InternetGatewayDevice.LANDevice.1.WLANConfiguration.6.X_ALU-COM_VirtualIfCfg_MaxAss…
InternetGatewayDevice.LANDevice.1.WLANConfiguration.7.X_ALU-COM_VirtualIfCfg_MaxAss…
InternetGatewayDevice.LANDevice.1.WLANConfiguration.8.X_ALU-COM_VirtualIfCfg_MaxAss…
VirtualParameters
VirtualParameters.VPdhcp



Funcionamento do TR069



Como uma sessão TR069 é iniciada

- Após obter os parâmetros básicos do ACS, o CPE inicia uma conexão TCP com o ACS.
- Se HTTPS for usado, o CPE e o ACS inicializarão o SSL para uma conexão HTTP segura.
- O CPE envia uma mensagem Inform em HTTP ou HTTPS para iniciar uma sessão CWMP.
- Após o CPE passar na autenticação, o ACS retorna uma resposta Inform para estabelecer a sessão.
- Após enviar todas as solicitações, o CPE envia uma mensagem HTTP vazia.
- Após isso o ACS esta livre para aplicar as configurações na CPE, seja de forma automática, seja de forma manual

Tipos de RPC em TR069

O CWMP usa métodos de chamada de procedimento remoto (RPC) para comunicação bidirecional entre CPE e ACS.

Os métodos RPC são encapsulados em HTTP ou HTTPS.

Os metodos RPC usados no CWMP são:

GetParameterValues
SetParameterValues
Inform
Download
Upload
Reboot
AddObject e DeleteObject

Parâmetros de configurações e desempenho

Parâmetros de Rede:

Endereço IP WAN

Endereço IP LAN

Máscara de sub-rede

Gateway padrão

Servidores DNS primário e secundário

Endereços de servidor NTP (Network Time Protocol)

Configurações de Wi-Fi:

SSID (Service Set Identifier)

Chave de segurança (WEP, WPA, WPA2)

Modo de operação (por exemplo, 802.11b/g/n/ac)

Canal de operação

Lista de dispositivos autorizados (MAC Address Filtering)

Firewall e Segurança:

Regras de firewall

Port forwarding

DMZ (Zona Desmilitarizada)

Controle de acesso

Ativação/desativação de UPnP (Universal Plug and Play)

Serviços de Rede:

Configurações DHCP (Dynamic Host Configuration Protocol)

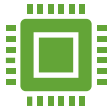
NAT (Network Address Translation)

Configurações de PPPoE (Point-to-Point Protocol over Ethernet)

Configurações de VPN (Virtual Private Network)

Atualizações de Firmware:

Parâmetros de configurações e desempenho



Utilização de Recursos:

Utilização de CPU (porcentagem)

Utilização de memória RAM (em bytes ou porcentagem)

Utilização de armazenamento (em bytes ou porcentagem)

Taxa de Transferência de Dados:

Taxa de download (em bits por segundo)

Taxa de upload (em bits por segundo)

Taxa de erros de transmissão e recepção

Latência e Tempo de Resposta:

Tempo de resposta da interface WAN

Tempo de resposta da interface LAN

Latência média da rede (em milissegundos)

Histórico de Eventos:

Registros de eventos do sistema (reinicializações, quedas de conexão, alterações de configuração)

Logs de segurança (tentativas de acesso não autorizadas, tentativas de ataque, etc.)

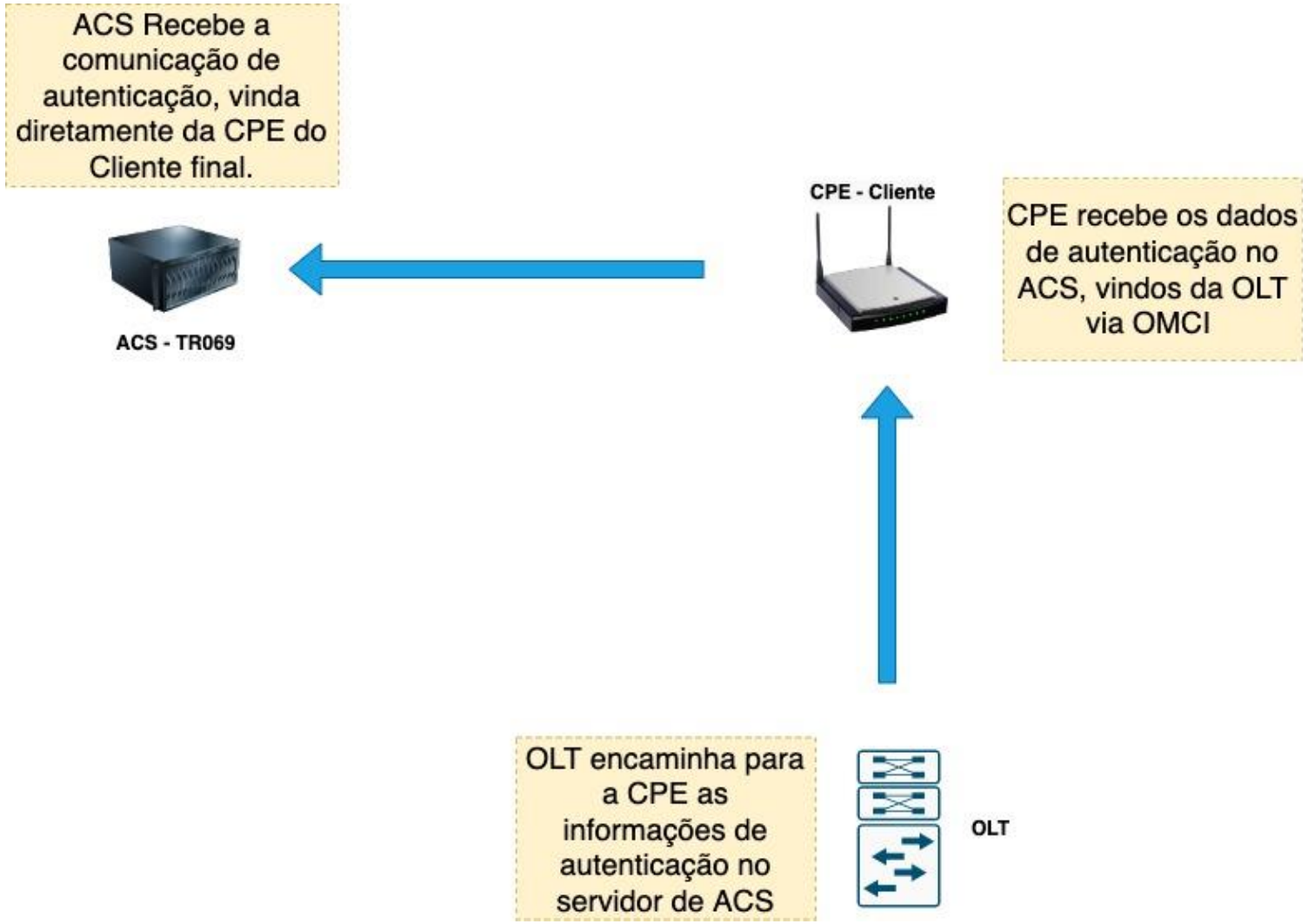
Status da Conexão:

Status da conexão WAN (ativo, inativo, conectando, desconectado)

Status da conexão LAN (ativo, inativo)

Contagem de pacotes enviados e recebido

Implementação do TR069



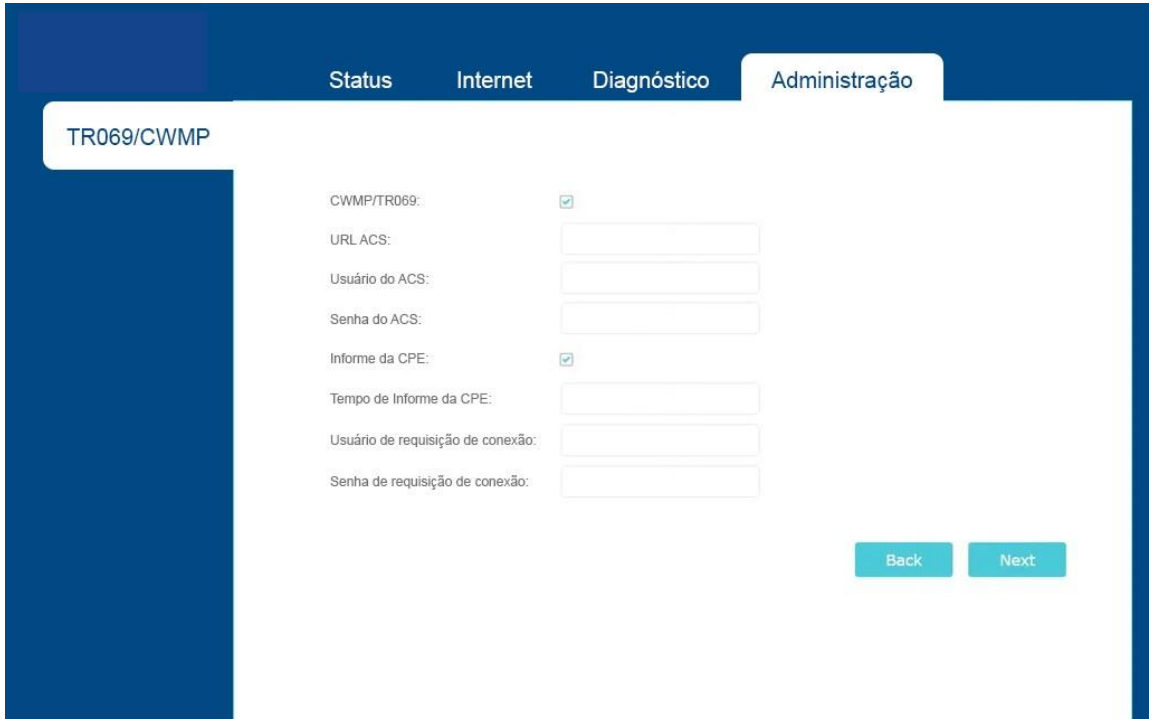
Como ativar o TR069 em uma CPE via OMCI

- Na modalidade de configuração via OLT, a entrega dos parâmetros de autenticação de ACS(TR069), é feita na OLT, e enviada a CPE via OMCI.
- Veja com seu fabricante se ele entrega as configurações de ACS para a CPE via OMCI
- Imagina um lugar onde sua OLT entrega a porta de entrada para o crescimento do seu provedor

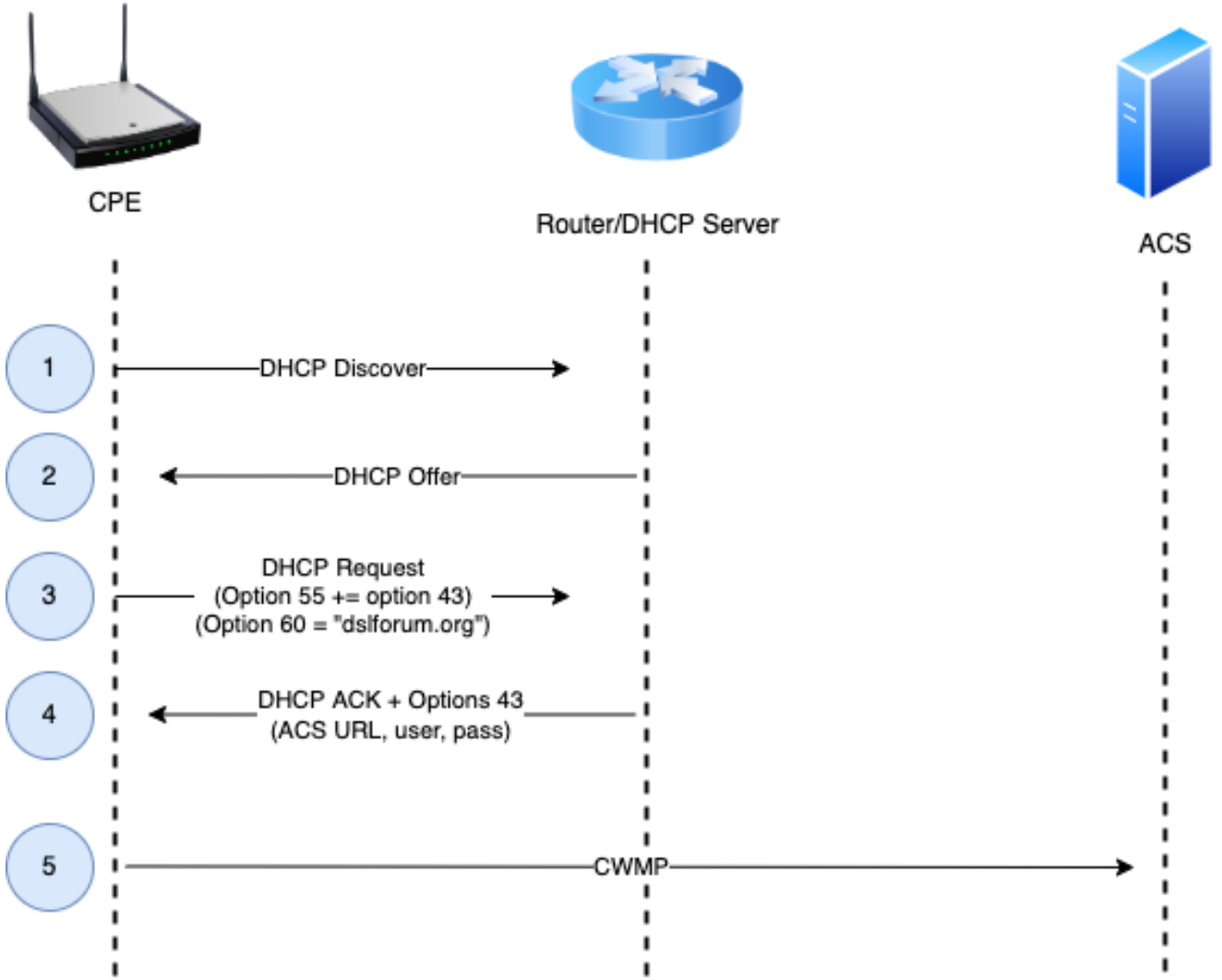
Como ativar o TR069 em uma CPE via Preset

A customização da firmware, para seu provedor, deve ser feita diretamente com o fabricante, onde o mesmo irá disponibilizar os arquivos corretos para a sua CPE, o uso de softwares ou firmwares de terceiros não é encorajado, visto que esta prática pode trazer possíveis problemas no desempenho e seguranças das CPEs

Como ativar o TR069 em uma CPE manualmente



- Na configuração manual, acessando a CPE pelo navegador, você deve localizar a tela de configuração do TR069, após isso, configure sua CPE conforme o que for pedido, cadastre o servidor e aguardar a CPE aparecer no ACS.
- As configurações necessárias são:
  - O botão CWMP deve ficar ativo
  - Intervalo de informação
  - URL ACS = http://dominio-do-server-acs:7547
  - Nome de usuário ACS
  - Senha ACS
  - Interface utilizada pelo TR-069
  - A caixa “Autenticação de solicitação de conexão”
  - Usuário de solicitação de conexão
  - Senha de solicitação de conexão
  - Caminho de solicitação de conexão
  - Se for Solicitado a porta de conexão, use a 7547



Como ativar o TR069 em uma CPE via DHCP-OPTION 43

Boas Práticas para Segurança na Implementação do TR-069

- Utilize protocolos seguros como TLS para criptografar a comunicação entre dispositivos gerenciados e o ACS.
- Evite acesso não autorizado aos dispositivos gerenciados e ao ACS.
- Configure políticas para restringir quem pode acessar e modificar configurações via TR-069.
- Mantenha todos os dispositivos atualizados com os últimos patches de segurança.
- Reduza vulnerabilidades e riscos de exploração.
- Implemente sistemas de monitoramento para detectar atividades suspeitas.
- Responda rapidamente a possíveis ameaças à segurança.
- Considere segmentar a rede para isolar dispositivos gerenciados.
- Desenvolva políticas claras sobre o uso e configuração do TR-069.
- Eduque usuários e administradores sobre a importância da segurança da rede.
- No dispositivo CPE, tenha uma WAN exclusiva para gerencia de TR069.

Desafios e soluções

Escalabilidade e desempenho eficiente em grandes redes TR069

Gerenciamento Centralizado

O TR-069 permite o gerenciamento centralizado de um grande número de dispositivos de rede, como roteadores, modems e gateways.

Facilita o provisionamento, monitoramento e configuração em larga escala.

Hierarquia de ACS

É possível implementar uma hierarquia de ACS, onde múltiplos servidores ACS podem ser organizados em uma estrutura escalável.

Distribui a carga de gerenciamento e facilita a escalabilidade horizontal.

Balanceamento de Carga

Utilize técnicas de balanceamento de carga para distribuir equitativamente as solicitações de gerenciamento entre os servidores ACS.

Garante uma distribuição eficiente de recursos e evita sobrecargas em servidores individuais.

Redundância e Failover

Implemente redundância e mecanismos de failover para garantir alta disponibilidade do sistema.

Reduz o risco de interrupções no gerenciamento, mesmo em caso de falha de hardware ou software.

Escalabilidade e desempenho eficiente em grandes redes TR069 II

Escalabilidade Vertical e Horizontal

- A arquitetura do TR-069 suporta tanto a escalabilidade vertical (adicionando recursos a um único servidor) quanto horizontal (adicionando mais servidores).
- Permite expandir a capacidade do sistema conforme a demanda da rede aumenta.

Testes de Desempenho e Dimensionamento

- Realize testes de desempenho e dimensionamento para avaliar a capacidade do sistema TR-069 em lidar com grandes volumes de dispositivos.
- Identifique potenciais gargalos e permite ajustes para otimização da escalabilidade.

Monitoramento e Otimização Contínua

- Mantenha um monitoramento constante do desempenho do sistema TR-069 em grandes redes.
- Otimize a infraestrutura conforme necessário para garantir um gerenciamento eficiente e sem interrupções.

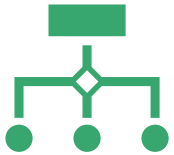
Boas práticas para o bom uso do TR069

NAT (Network address translation)

Uma rede onde a comunicação entre a CPE e o ACS, é feita atravéz de NAT, não terá uma comunicação em tempo real

Pode ser usado uma regra na PBR para que a comunicação ocorra sem NAT

Pode ser usado STUN para contornar o NAT caso tenha uma segunda CPE recebendo DHCP-LAN



Interface Type: TR069

A CPE que é classificada como ONT/ONU deve ter em sua interface, o TR069 ativo

E recomendavel que a gestão do TR069 pode ser feita em uma interface diferente de PPPoE, pois caso o cliente fique sem o PPPoE, ainda existira uma interface de gerencia na CPE

DNS

Usar um DOMINIO é altamente recomendado, pois se amanhã você precisar realocar algum IP, não terá problemas.

Estratégias para diagnosticar e resolver problemas em cenários TR069

Testes de Conformidade e Interoperabilidade

Certifique-se de que os dispositivos gerenciados estão em conformidade com os padrões TR-069 e que são interoperáveis com o ACS.

- Evita problemas causados por incompatibilidades entre dispositivos e o sistema de gerenciamento.

Colaboração com Fornecedores e Comunidade

Mantenha uma comunicação aberta com fornecedores de dispositivos e com a comunidade TR-069 para compartilhar experiências e soluções.

Aproveite o conhecimento coletivo para resolver problemas de forma mais eficaz.

Utilize produtos que tenham a certificação do BroadBand Forum para TR069

Testes de Diagnóstico Remoto

Utilize recursos de diagnóstico remoto oferecidos pelo TR-069 para identificar e isolar problemas em dispositivos gerenciados pelo ACS

- Facilita a resolução de problemas sem a necessidade de intervenção manual.

Estratégias para diagnosticar e resolver problemas em cenários TR069 II

Treinamento e Capacitação de Equipe

Capacite a equipe técnica com treinamentos específicos sobre diagnóstico e resolução de problemas em cenários TR-069.

- Garante que a equipe esteja preparada para lidar com desafios de maneira eficiente e rápida.

Registro e Monitoramento de Logs

Implemente uma estratégia de registro e monitoramento de logs na comunicação TR069.

- Isso facilita a identificação de problemas, fornecendo informações detalhadas sobre atividades e eventos.

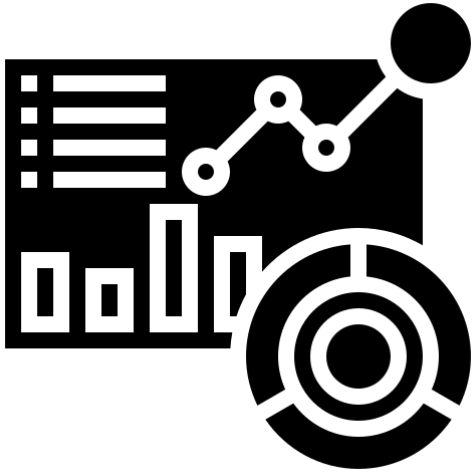
Ferramentas de Monitoramento de Rede

Utilize ferramentas de monitoramento de rede para acompanhar o tráfego e o desempenho da comunicação TR-069.

- Identifica possíveis gargalos, latências ou falhas na comunicação.

Realize análise de pacotes de rede para inspecionar o tráfego TR-069 e identificar possíveis problemas de protocolo ou comunicação.

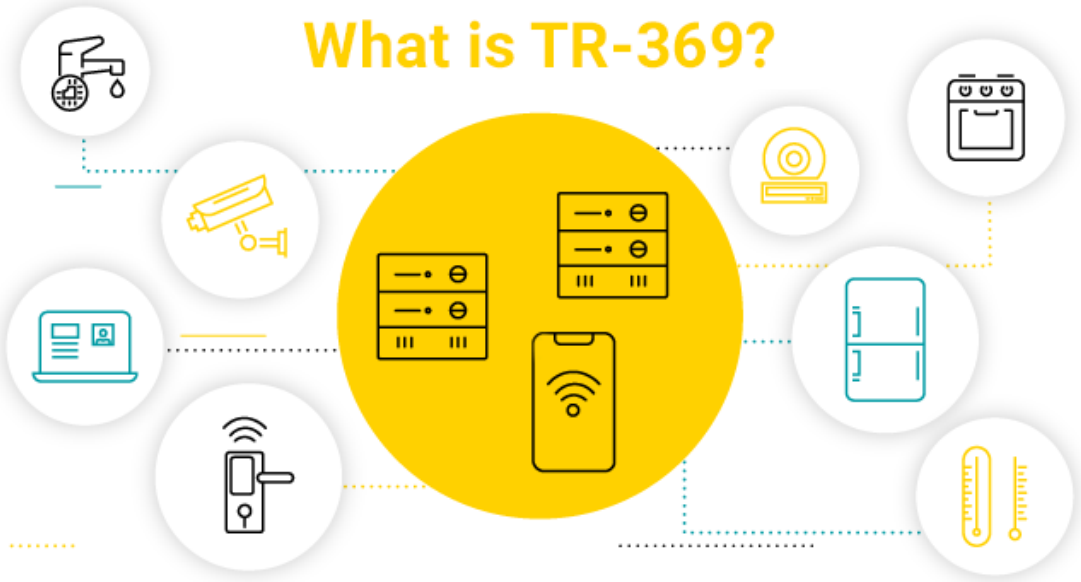
protocolo ou comunicação?



Vamos Subir um ACS?

Futuro do TR069

Apresentamos o USP



- USP - O TR-369
  - User Services Plataform
- Primeira especificação em 2018
- Se tornando o padrão de fato dos novos produtos

Por que um novo protocolo?

Diversidade de novos tipos de dispositivos

Necessidade de integração com sistemas terceiros

Escalabilidade

Modelo voltado a contemplar todos IoTs

Diversas camadas de segurança

Quais os obstáculos do TR-069?

- Protocolo mais "pesado" (message encoding & transfer protocols)
- Segurança básica
- Dependência de um único ACS
- Feito para gerenciar CPEs (e não IoTs)
- Falta de mecanismos de "real-time" de fato "real-time"
- Problemas com NAT

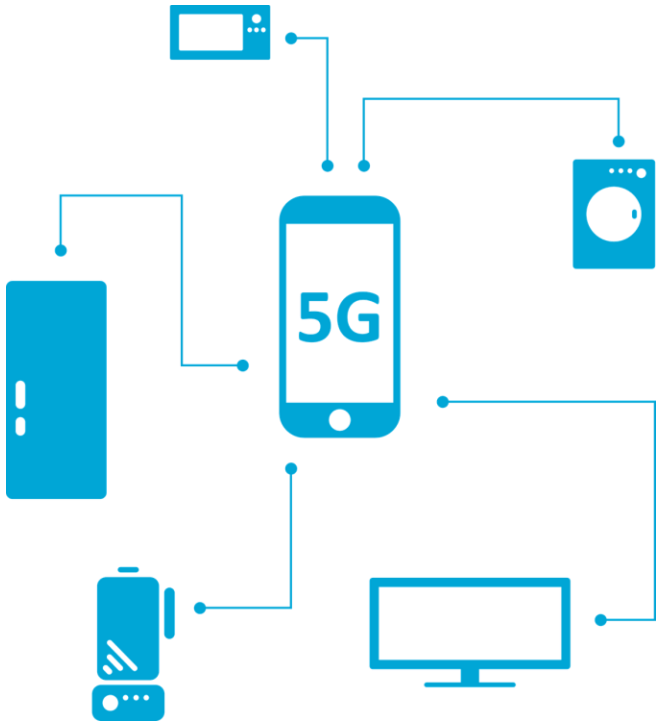
Comparação entre TR-069 e TR-369

Item	TR-369 -USP	TR-069
Protocolo de transferência de dados	MQTT Websocket STOMP CoAP Unix domain socket	HTTP
Codificação dos dados	Google ProtoBuffers	SOAP/XML
Estilo de comunicação	Sempre conectado	Baseado em eventos, com conexões esporádicas
Servidor de comunicação	Múltiplos servidores podem ser adicionados, centrais, em dispositivos móveis, etc	Depende de um único ACS
Segurança	DTLS/TLS ACLs RBAC	TLS A CPE só conversa com um único ACS

Mas o USP é mais eficiente?

Caso de uso	Tamanho da sessão em KB		
	TR069	USP	
		MQTT	Websocket
Bootstrap (tr069) / OnBoardRequest (USP)	43	9	8
Informes periódicos	6	1	1
Pedido de dados de monitoramento	18	4	4
Resposta de dados de monitoramento	6	1	1

Gerenciamento de próxima geração



- Maior flexibilidade de comunicação
- Protocolos eficientes
- Sem problemas com NAT
- Escalabilidade
- Adiciona camadas de segurança
- Pronto para Smart Home e IoTs
- Feito para se integrar a diversas plataformas
- Arquitetura modular
- Um Data Model em evolução constante

O futuro do gerenciamento remoto

Melhorar a experiência do cliente na rede interna

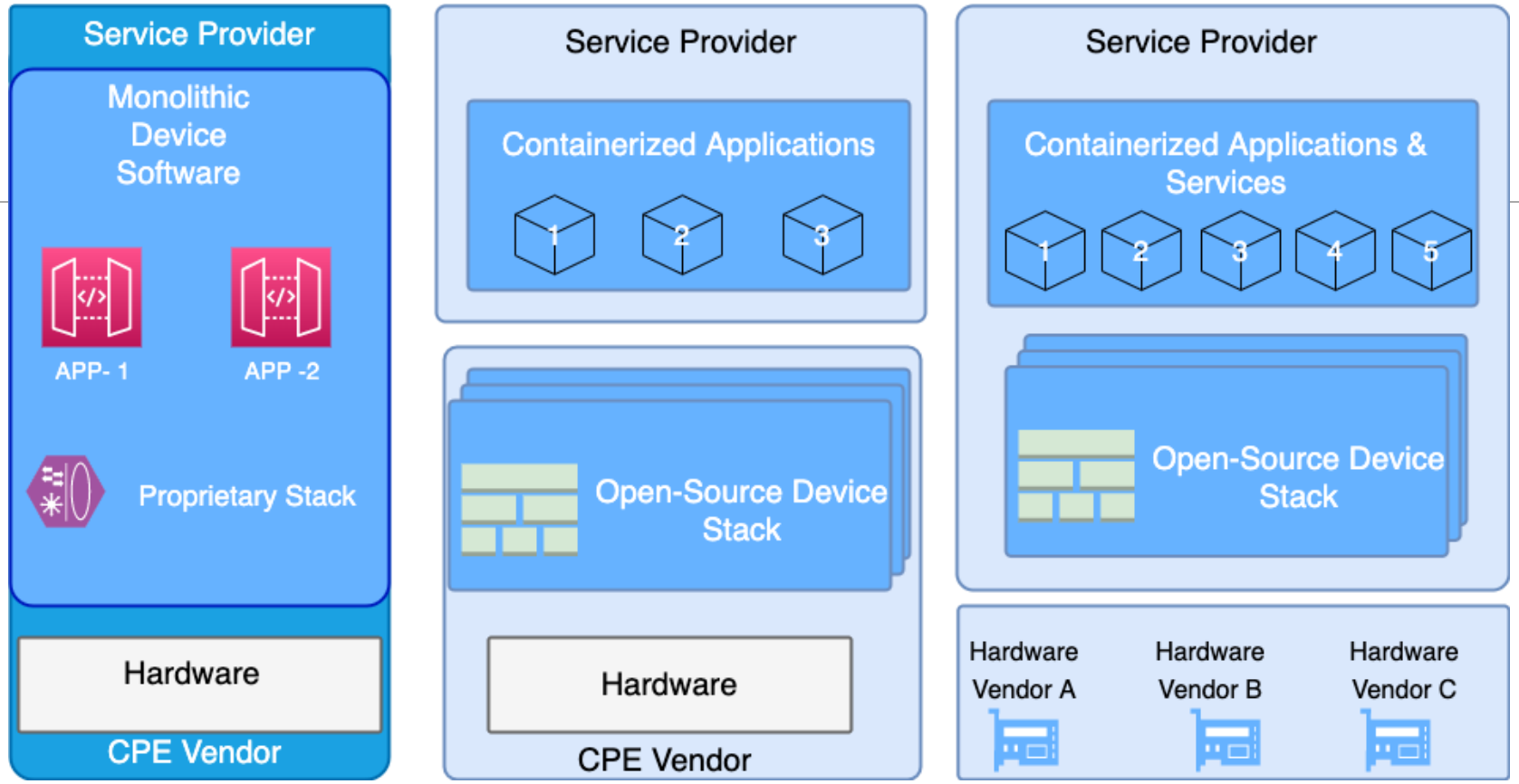
Ter plataformas distintas interoperando

A casa toda conectada, e gerenciada

Aplicações interagindo entre si

A rede interna sendo gerenciada de diversos pontos (mobile, central, outros softwares)

O USP é a resposta para estas questões



Para onde corre a Indústria?

Para saber mais

broadband forum

The User Services Platform

A standardized protocol to manage, monitor, update, and control connected devices, IoT endpoints, user services and home networks

Specification | HTML | PDF | Data Models | Test Plan | Resources | FAQ

What is USP?

The **User Services Platform** is a standardized **protocol for managing, monitoring, upgrading, and controlling connected devices**. USP allows service providers, consumer electronics manufacturers, and end users to:

- Create interoperable and vendor-independent **managed Wi-Fi systems**.
- Perform **lifecycle management** of consumer connected devices and containerized microservices.
- Support **independent applications** for application-enabled services gateways.
- Enable **IoT and consumer electronics upgradability** for critical security patches.
- Develop applications that gather the telemetry necessary to **mass data processing, AI, and machine learning**.
- **Bootstrap and configure** newly installed or purchased devices and applications.
- Let customer support **monitor and troubleshoot** connected devices, services, and home network links.

Current Version: 1.3

About this version:

This specification includes:

- Architectural overview
- Discovery mechanisms for Controllers and Agents
- Basic CRUD messages between Controllers and Agents
- Use of USP Record encapsulation for end to end integrity, security, and privacy
- Data model Objects specific to protocol functionality, object defined operations, and notifications/events
- Protocol buffers encoding schema
- Use of WebSockets, MQTT, STOMP, and UNIX Domain Sockets as message transfer protocols (MTP)
- A system for authentication and authorization
- Extensions for bulk data collection, firmware management, software module management, containerized microservices, and device proxying
- Theory of operations for using a USP Agent to control IoT devices and systems

- ✓Site oficial do TR369
  - https://usp.technology/

Obrigado!

www.made4it.com.br
comercial@made4it.com.br
(43) 3047-8300