UNIVERSIDADE FEDERAL FLUMINENSE

ESCOLA DE ENGENHARIA

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA E DE TELECOMUNICAÇÕES

MARCO ANTONIO ABI-RAMIA JUNIOR

GERENCIADOR DE ATIVOS DE PROTEÇÃO EM SUBESTAÇÕES

BASEADO NA IEC 61850

NITERÓI, RJ

2017

MARCO ANTONIO ABI-RAMIA JUNIOR
MATRÍCULA: M054.216.008

GERENCIADOR DE ATIVOS DE PROTEÇÃO EM SUBESTAÇÕES

BASEADO NA IEC 61850

Dissertação de Mestrado apresentada ao Programa de Pós Graduação em Engenharia Elétrica e Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre em Engenharia Elétrica e de Telecomunicações.

Orientadora: Prof. Natália Castro Fernandes, D.Sc.

Coorientador: Prof. Márcio Zamboti Fortes, Dr.

Niterói, RJ

2017

Ficha catalográfica automática - SDC/BEE

A148g Abi-Ramia Junior, Marco Antonio
Gerenciador de Ativos de Proteção em Subestações Baseado na IEC 61850 / Marco Antonio Abi-Ramia Junior; Natália Castro Fernandes, orientadora; Márcio Zamboti Fortes, coorientador. Niterói, 2017.
166 f.

Dissertação (mestrado)-Universidade Federal Fluminense, Niterói, 2017.

1. Gestão de Ativo. 2. Automação (Engenharia). 3. Proteção, Supervisão e Controle. 4. IEC61850. 5. Produção intelectual. I. Título II. Castro Fernandes,Natália, orientadora. III. Zamboti Fortes, Márcio, coorientador. IV. Universidade Federal Fluminense. Escola de Engenharia.

CDD -

Bibliotecária responsável: Fabiana Menezes Santos da Silva - CRB7/5274

MARCO ANTONIO ABI-RAMIA JUNIOR

GERENCIADOR DE ATIVOS DE PROTEÇÃO EM SUBESTAÇÕES

BASEADO NA IEC 61850

Dissertação de Mestrado apresentada ao Programa de Pós Graduação em Engenharia Elétrica e Telecomunicações da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Mestre em Engenharia Elétrica e de Telecomunicações.

Aprovado em 20/12/2017.

BANCA EXAMINADORA

Prof. Natália Castro Fernandes, D.Sc.

Universidade Federal Fluminense

Prof. Marcio Zamboti Fortes, Dr.

Universidade Federal Fluminense

Prof. Vitor Hugo Ferreira, D.Sc.

Universidade Federal Fluminense

Prof. Rainer Zanghi, D.Sc.

Universidade Federal Fluminense

Prof. Miguel Elias Mitre Campista, D.Sc.

Universidade Federal do Rio de Janeiro

Este trabalho é dedicado aos meus queridos pais, Marco Antonio Abi-Ramia e Helena Maria Baptista Pereira Abi-Ramia, que muito se esforçaram para me possibilitar boas oportunidades de estudos, e que sempre me apoiaram e incentivaram nas realizações de meus projetos, mesmo os mais inusitados.

AGRADECIMENTOS

A Deus, que está ao meu lado em todo os momentos de minha vida, me dando conforto, alento, coragem e força.

À Ana Maria Dore Bastos Abi-Ramia, minha esposa companheira, que nos momentos de sufoco sempre me lembrou de que sou capaz de ultrapassar os obstáculos. Obrigado pelo carinho, a paciência e por sua capacidade de me acalmar na correria da vida entre as obrigações do trabalho, estudo, família e lar.

Aos Professores da UFF, companheiros nesta caminhada, posso dizer que a minha formação, não teria sido a mesma sem a presença de vocês. Em especial, agradeço à Yona Lopes, querida amiga que me abriu portas na nesta universidade, e aos meus orientadores Natália Castro Fernandes e Márcio Zamboti Fortes, pela paciência, pelos diversos ensinamentos ao longo destes anos de mestrado e por acreditarem no meu potencial.

Aos colegas de trabalho em Furnas, Ângelo Andelnyr Sampaio Alves, Wagner Queiroga Dos Reis Santos, Filipe Fernandes Machado, Paulo Roberto Assumpção De Souza, Levi Cirqueira Santos Junior e José Geraldo Franceschett pelo suporte, ajuda, amizade e compreensão. À Adriana Barroso De Vasconcellos Moura, João Silvério Dourado Pereira e Marco Antonio Fernandes Ramos por me facilitarem a execução deste projeto.

Aos professores da UEMG, Ms.C. Alessandro de Castro Borges e Ms.C. Gualberto Rabay Filho, pelos ensinamentos, pelo apoio e pela participação determinante na minha jornada acadêmica.

A todos aqueles que participaram e colaboraram com a realização deste trabalho, o meu muito obrigado! Vencemos!

“Nada existe de tão difícil que não seja vencível.”

Júlio Cesar

“Sempre há uma saída para qualquer problema, por mais complexo e difícil que nos pareça.”

C. Torres Pastorino

“O gênio consiste em um por cento de inspiração e noventa e nove por cento de transpiração.”

Thomas Edison

“Procure ser um homem de valor, em vez de ser um homem de sucesso.”

Albert Einstein

RESUMO

Apesar da existência de toda sorte de iniciativas e esforços, além de padrões, normas e protocolos que intencionam garantir que sistemas onde coexistam *Intelligent Electronic Devices* (IEDs) de diferentes fabricantes se comuniquem de forma transparente, o problema da interoperabilidade entre equipamentos de proteção que se comunicam através de redes de dados ainda constitui um dos principais desafios para gestão técnica de plataformas de automação, proteção e controle. Depois de configurados e validados em uma estação, os equipamentos são disponibilizados para operação comercial deixando uma série de alterações e adaptações do projeto original sem registro formal, por vezes registradas de forma imprecisa, incompleta ou mesmo redundante. Esta dissertação apresenta uma proposta de sistema unificado para levantamento de ativos de proteção aderentes à norma IEC 61850, conectados a uma rede de automação, supervisão e controle. IEDs de diferentes fabricantes são identificados e tem suas funções disponíveis listadas em um relatório, sem alterar, contudo, as parametrizações de função e de operação dos IEDs. Os algoritmos utilizados para registro de ativos de proteção conectados a uma rede de dados, escritos em Python e LabView, se comunicam com peças de software comercial e se utilizam de técnicas de seleção, análise e manipulação de dados para produzir informações consistentes sobre os ativos de proteção em uma subestação. Os algoritmos desenvolvidos são baseados em duas referências principais. Uma delas é o que diz a norma IEC 61850. A outra é um estudo de como se deu a implementação desta norma por alguns fabricantes de IEDs presentes no mercado brasileiro. Foram analisados três tipos de IEDs como caso de estudo, sendo demonstrando o potencial do sistema apresentado. O sistema proposto ainda auxilia na pesquisa de defeitos, problemas de desempenho da rede e na identificação de alterações ocorridas na rede de IEDs de uma subestação.

Palavras-chave: Gerenciamento de ativos, comunicação de dados, automação de subestações, proteção, supervisão e controle, IEC 61850.

ABSTRACT

Despite the existence of all kind of initiatives and efforts, in addition to standards, norms and protocols that aim to ensure that systems with different IEDs manufacturers coexist in a transparent manner, the problem of interoperability between protection equipment communicating through data networks is still one of the main challenges for the technical management of automation, protection and control platforms. Once configured and validated, the equipment is set available for commercial operation, leaving behind a series of changes and tunings of the original project without proper and formal registration, or recorded in an imprecise, incomplete or even redundant way. This dissertation presents a proposal for a unified system for surveying protection assets adhering to the IEC 61850 standard, connected to an automation, supervision and control network. IEDs from different manufacturers are identified and have their available functions listed in a report, without, however, changing the function or operation parameterizations of the IEDs. The algorithms used for collect data over an IED network, written in Python and LabView, communicate with pieces of commercial software and use selection, analysis and data manipulation techniques to produce consistent information about protection assets in a substation. The algorithms are based on IEC 61850 and the study of how the implementation of this standard was given by some IEDs manufacturers present in the Brazilian market. As case study, three types of IEDs were analyzed, demonstrating the presented system's potential. The proposed system also assists in troubleshooting defects, network performance problems and in identifying changes occurring within a substation's IED network.

Keywords: Asset manager, data communication, substation automation, automation, supervisory, control, IEC 61850.

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

ABB	*Asea Brown Boveri*
ACSI	*Abstract Communication Service Interface*
ANSI	*American Nation Standards Institute*
ARP	*Address Resolution Protocol*
BD	Base de Dados
BlkCls	Bloqueado para Comando de Fechamento
BlkOpn	Bloqueado para Comando de Abertura
CAN	*Campus Area Network*
CBOpCap	Disponibilidade de Operação
CDC	*Common Data Class*
CF	Configuração
CID	*Configured IED Description*
CLP	Controlador Lógico Programável
CO	Controle
CSMA/CD	*Carrier Sense Multiple Access With Collision Detection*
CSWT	Controlador de Chaveamento
ctlVal	Valor do Controle
DC	Descrição
DLCI	*Data Link Connection Identifier*
DNP3	*Distributed Network Protocol*
DNS	*Domain Name System*
DoD	*Department Of Defense*
DoS	*Deny Of Service*
EMI	*Electro-Magnetic Interference*
EMS	*Energy Management System*
EPRI	*Electric Power Research Institute*
EX	Definição do Espaço para Nomes
FC	*Functional Constraints*
FDDI	*Fiber Distributed Data Interface*
FTP	*File Transfer Protocol*
GD	Geração Distribuída

GE	*General Electric*
GOOSE	*Generic Object Oriented Substation Event*
GPS	*Global Positioning System*
GSE	*Generic Substation Events*
GSSE	*Generic Substation Status Event*
HAN	*Home Area Network*
HDLC	*High-Level Data Link Control*
HTTP	Hypertext Transfer Protocol
HTTPS	*Hyper Text Transfer Protocol Secure*
ICD	*Ied Capability Description*
ICMP	*Internet Control Message Protocol*
IDS	*Intrusion Detection Systems*
IEC	*International Electrotechnical Commission*
IED	*Intelligent Electronic Device*
IEEE	*Institute of Electrical and Electronics Engineers*
IF	Interface de Rede
IGMP	*Internet Group Management Protocol*
IHM	Interface Homem Máquina
IP	*Internet Protocol*
IPng	*Internet Protocol Next Generation*
IPv4	*Internet Protocol* Vesão 4
IPv5	*Internet Protocol* Vesão 5
IPv6	*Internet Protocol* Vesão 6
ISO	*International Organization for Standardization*
LAN	*Local Area Network*
LC	*Logical Connections*
LD	*Logical Device*
LLC	*Logic Link Control*
LN	*Logical Nodes*
LOC	Bloqueado
MAC	*Media Access Control*
MAN	*Metropolitan Area Network*
MDIF	Medição Diferencial

MHAI	Medição De Harmônicos E Inter-Harmônicos
MMPM	*Manufactoring Message Protocol Machine*
MMS	*Manufacturing Message Specification*
MMTR	Contador
MMXU	Medição Operativa e Indicativa
MU	*Merging Unit*
MX	Medição
NFS	*Network File System*
ONS	Operador Nacional do Sistema
OSI	*Open System Interconnection*
PC	*Physical Connections*
PD	*Physical Devices*
PDIS	Proteção de Distância
PMU	*Phasor Measurement Units*
Pos	Posição
RREC	Religamento Automático
SAS	Sistema de Automação e Supervisão
SCADA	*Supervisory Control and Data Acquisition*
SCD	*Substation Configuration Description*
SCL	*Substation Configuration Language*
SE	Subestação
SEP	Sistema Elétrico de Potência
SG	Parâmetros de Ajuste de Grupos
SNMP	*Simple Network Management Protocol*
SSD	*System Specification Description*
SSH	*Secure Shell*
ST	*Status*
stVal	Valor do Estado
SV	Valor Amostrado
TC	Transformador de Corrente
TCP	*Transmission Contol Protocol*
TI	Tecnologia da Informação
TP	Transformador de Potencial

TrgOp	*Trigger Option*
UCA	*Utility Communications Architecture*
UDP	*User Datagram Protocol*
UML	*Unified Modeling Language*
UPA	Unidade de Proteção Alternada
UPP	Unidade de Proteção Principal
UTR	Unidade Terminal Remota
VLAN	*Virtual Local Area Network*
VPN	*Virtual Private Network*
WAN	Wide Area Network
WG11	*Workgroup 11*
WG12	*Workgroup 12*
WG1O	*Workgroup 10*

1. INTRODUÇÃO

O problema da criação e manutenção de uma relação dos ativos em uma rede de proteção, supervisão e controle de uma subestação se apresenta como uma atividade complexa. Com a crescente aplicação de estratégias de execução de empreendimentos no modelo *de turn key* e *as-built* em projetos de implantação, ou de modernização, em subestações do sistema elétrico, a reconfiguração de equipamentos de proteção, supervisão e controle em sistemas de produção e transmissão de energia elétrica também implica em atualização da documentação específica nem sempre realizada. Existem pesquisas realizadas dentro desta linha de gestão de ativos de subestações com abordagens concentradas em aspectos de desempenho dos equipamentos, priorização de manutenção e condições operacionais dos equipamentos como reportado em [1] e [2] e propostas considerando os equipamentos inteligentes disponíveis nas *smart grids* para subestações de distribuição [3]. Será considerada neste estudo a avaliação de uma subestação como um nó de conexão entre sistemas de geração e de transmissão de energia elétrica.

O aumento da concorrência e a redução das margens de lucro estão levando as empresas a encontrar caminhos para aperfeiçoar processos e reduzir custos. Ao mesmo tempo incentivos governamentais e iniciativas comunitárias encorajam o setor industrial a perseguir a sustentabilidade na operação. Isso introduziu uma mudança de paradigma aonde o foco vem mudando de simples redução de custos para uma gestão mais eficiente dos ativos [4], inclusive utilizando técnicas avançadas de computação como *Data Analytics* [5].

Ter acesso à informação certa na hora certa tem sido um problema no processo de Operação e Manutenção (OeM). Prover a habilidade de gerenciar os ativos em uma subestação não é um desafio diferente. É uma atividade que vem sendo melhorada, porém ainda se encontram muitos problemas. Tipicamente, os gerenciadores de ativos são confrontados com documentação do tipo *as-built* que frequentemente está incompleta, imprecisa e/ou redundante [1].

Diante dos desafios econômicos impostos às empresas, onde os equipamentos têm seus custos iniciais cada vez mais altos, tem-se procurado por soluções que aumentem o tempo de sua vida útil. A comunidade de pesquisadores já percebeu a necessidade de trabalhar mais próximo para prover soluções de gerência de ativos [4], cobrindo inclusive preocupações com as pegadas de gás carbônico, através do aumento do ciclo de vida e consequente diminuição no ritmo da substituição de ativos.

Os sistemas de transmissão e distribuição de energia elétrica ainda são compostos por um grande número de equipamentos e aparatos antigos, que podem ser causa da diminuição da confiabilidade do sistema, devido a sua deterioração. Sistemas de gestão de ativos podem auxiliar no plano de manutenção ótimo e no alcance da redução de custos com OeM [3].

Cada vez mais as organizações de gestão de ativos estão se apoiando em dados confiáveis para conduzir seus processos de tomada de decisão, apesar do pequeno número de pesquisas sistemáticas no campo da geração de dados confiáveis. Dados confiáveis têm claramente um impacto definido e consistente sobre a qualidade esperada de qualquer sistema. Do processo decisório aos sistemas autônomos, passando pelo controle de inventário e gestão de manutenção, nenhum processo funciona bem sem dados confiáveis [6].

1.1 MOTIVAÇÃO

A gestão de ativos é um tema relativamente novo e relevante, porém pouco trabalhado, especialmente no sistema elétrico. No Brasil, o domínio das técnicas e a disponibilidade de ferramentas para a gestão de ativos em uma subestação ainda se encontram num horizonte distante.

Os sistemas de proteção, supervisão e controle de subestações em sistemas de produção e transmissão de energia elétrica sempre foram tratados como sistemas distintos que operavam de maneira coordenada. Desta forma, os profissionais de engenharia e manutenção se dividiam em equipes especializadas, cada grupo lidando com um conjunto de especificidades bem distintas e definidas. No Brasil, o início dos anos 1990 marcou a entrada de dispositivos eletrônicos de proteção, chamados de estado sólido. Estes dispositivos começaram a substituir os relés eletromecânicos e, em sequência, foram rapidamente substituídos pelos dispositivos digitais e microprocessados.

Nos dias atuais, o fenômeno da convergência observado nos dispositivos eletrônicos de nosso uso cotidiano, como GPS (*Global Positioning System)*, telefone, computador, câmera fotográfica, rádio e TV (Televisão) em um único dispositivo chamado de *smart phone*, também ocorre nos dispositivos de supervisão, proteção, controle e automação por meio dos *Intelligent Electronic Devices* (IEDs). Os IEDs concentram os dispositivos físicos, as filosofias de proteção e as técnicas inerentes aos sistemas de proteção, controle, automação e supervisão em sistemas elétricos. Com os IEDs, veio também a necessidade de integração mais forte e completa entre as equipes de engenharia e manutenção destes sistemas, integrando inclusive as tecnologias de comunicação em rede *ethernet* com protocolo TCP/IP (*Transmission Control Protocol / Internet Protocol*).

Sempre que se desenvolve algo novo, cada fabricante presente no mercado cria projetos que carregam consigo a cultura da empresa, trazendo vantagens e argumentos fortemente justificados, novamente cada um enfatizando seu contexto. Para garantir a integração de equipamentos de diferentes fabricantes, em ambientes heterogêneos, onde precisam coexistir dispositivos tanto de proteção, de supervisão e de controle, o *International Electrotechnical Commission* (IEC) trabalhou na criação de uma norma que padronize o funcionamento destes sistemas em todos os aspectos que são necessários para garantir a interoperabilidade. Para tanto a norma define o uso de rede TCP/IP, protocolo de transporte *Manufacturing Message Specification* (MMS) e protocolo de aplicação *Generic Object Oriented Substation Event* (GOOSE) entre outros. É a norma IEC 61850.

Apesar da existência da Norma é difícil saber o que se encontra de fato dentro de uma subestação, em termos de equipamentos e funções lógicas, em especial após projetos de atualização consecutivos feitos por diferentes empresas.

Esse problema dificulta que novas atualizações sejam feitas por diversos motivos técnicos e até administrativos. Por exemplo, dificultando que empresas fornecedoras de serviços e produtos, participantes de um certame de concorrência pelo menor preço, possam concorrer em condição de igualdade e de preço justo nas licitações abertas no mercado brasileiro de energia elétrica, já que não se sabe a priori exatamente quais elementos e quais funções estariam disponíveis em equipamentos que a concessionária contratante já possui naquela subestação, objeto de ampliação ou modernização. Estes fatores causam dificuldades e eventualmente prejuízos às concessionárias.

A interferência humana também é uma preocupação, pois frequentemente é apontada como principal causa de falhas. Detectar essas falhas auxilia no rápido reestabelecimento do sistema e permite que se produzam ações para que não voltem a acontecer.

Contudo, não existe uma ferramenta de levantamento e diagnóstico de uma subestação que seja interoperável entre diferentes fabricantes. Essa é a motivação principal para este trabalho.

1.2 OBJETIVOS

O principal objetivo deste trabalho é apresentar uma ferramenta de levantamento de ativos de proteção em uma subestação baseada na norma IEC 61850, que seja interoperável entre diferentes fabricantes. Para atingir este objetivo, um usuário do sistema deverá obter previamente as devidas credenciais de segurança e de trâmites formais para acessar (fisicamente ou remotamente) a rede de supervisão e controle de uma subestação, observando-

se as políticas de segurança das instalações. A partir deste ponto o sistema será capaz de identificar dispositivos de rede conectados, identificar e quantificar os IEDs, obter marcas e modelos, listar suas funções de proteção disponíveis, e os *datasets* de proteção publicados na rede.

Para atingir o objetivo de gerenciar ativos de proteção, foram desenvolvidas as seguintes funcionalidades:

- Descobrir, em uma rede TCP/IP, de quais dispositivos estão *online*,
- Mapear endereços IP utilizados e livres (não utilizados) nesta rede.
- Identificar, dentre os endereços IP ativos, os endereços físicos *Media Access Control* (MAC) associados e, quando disponível, identificar também o fabricante da interface de rede e o sistema operacional embarcado em cada *host* da rede sob análise.
- Identificar dos *hosts* que respondem ao protocolo MMS.
- Identificar dos *hosts* MMS que implementam a norma IEC 61850 (Dispositivos Físicos) recuperando o fabricante do dispositivo, modelo, e *firmware* instalado.
- Mapear automaticamente os pontos presentes nos IEDs:
    - Relacionar os Dispositivos Lógicos dos Dispositivos Físicos;
    - Buscar no Dispositivo Lógico de proteção os Nós Lógicos disponíveis;
    - Buscar os *Datasets* que estão configurados no IED;
    - Exibir os atributos presentes em cada *Dataset* para publicação na rede;
- Gerar um arquivo de registro contendo os dados levantados nas pesquisas descritas acima, para arquivamento.
- Comparar os registros feitos.

De posse deste conjunto de dados e destas funcionalidades, o sistema torna possível investigar alguns tipos de problemas na rede de IEDs como: pesquisa de motivos para mau funcionamento e pesquisa de possibilidades de melhoria no desempenho da rede. Estas questões serão discutidas e detalhadas nos próximos capítulos.

1.3 PRINCIPAIS CONTRIBUIÇÕES

Este trabalho apresenta um sistema de *software* que se propõe a auxiliar na gestão de ativos de proteção aderentes à norma IEC 61850. Seu objetivo principal é fornecer coletar dados atualizados, únicos e relevantes gerando informação consistente para sistemas de gestão de ativos.

Como objetivos secundários, pretende-se disponibilizar uma série de funcionalidades que permitam a análise da rede e a pesquisa de problemas de comunicação, considerando a norma IEC 61850.

Assim, o sistema proposto se apresenta como uma ferramenta de pesquisa e registro para redes de IEDs com as seguintes vantagens:

- Permite, para pesquisa de defeitos, detecção de alterações no sistema, tanto em nível físico (troca de equipamentos) quanto lógico (troca de configurações) a partir da Comparação de registros de ativos, mostrando as diferenças encontradas.
- Faz análise quantitativa sobre o registro de configurações de IEDs, como:
    - Quantos pontos ou funções estão disponíveis, quantos e quais estão em uso.
    - Quantos IEDs existem da rede
    - Classificação por marca, modelo e funções de proteção.
- Pesquisa e determina mudanças ocorridas na rede, por ocasião da substituição de um IED, da reconfiguração de IEDs e de alterações na estrutura da rede de supervisão, automação e controle de uma subestação.
- Faz análises visando a melhoria de fluxo de dados e congestionamento de redes de desempenho crítico como estas, onde existem restrições severas de tempo, através da identificação de *datasets* que estejam sendo publicados por padrão e que não tenham seu uso efetivo.
- Levantamento de informações de proteção de IEDs de qualquer fabricante, desde que seja aderente às especificações da norma IEC 61850.

Esta proposta não resolve completamente o problema da gestão de ativos, se limitando a coletar informações únicas, relevantes e consistentes para alimentar outros sistemas de gestão, sejam eles manuais ou automatizados.

1.4 ESTRUTURA DO DOCUMENTO

Este documento está dividido em seis capítulos, contando com este capítulo introdutório ao tema central deste trabalho, que inclui a caracterização do problema e sua contextualização, bem como objetivos, motivações e contribuições, além da estrutura do

mesmo, que será agora apresentada, organizada de forma a proporcionar ao leitor uma sequência lógica dos tópicos apresentados:

- No Capítulo 2, "FUNDAMENTAÇÃO TEÓRICA", são apresentados alguns conceitos com o intuito de introduzir o leitor no tema abordado e ainda apresenta o estado da arte, apresentando o sistema de geração e transmissão de energia elétrica, os sistemas de proteção de equipamentos de subestações, a norma IEC 61850, o protocolo MMS e seus serviços, além dos desafios atuais na comunicação entre IEDs, tópicos importantes para mapear, discutir e definir pontos que podem ser factíveis naquele momento de estudo, além de se definir o melhor caminho a percorrer.
- O Capítulo 3, "PROPOSTA", apresenta a teoria que será aplicada e a técnica, bem como uma visão em alto nível do sistema, organizado em blocos funcionais.
- O Capítulo 4, "IMPLEMENTAÇÃO DA PROPOSTA", dedica-se a apresentar os métodos utilizados para a realização das atividades necessárias para o alcance dos objetivos definidos, os critérios e premissas adotados no desenvolvimento deste trabalho.
- No Capítulo 5, "VALIDAÇÃO DA PROPOSTA", mostram-se os resultados dos testes realizados com base na teoria descrita, telas de interface e resultados obtidos, comparando ensaios realizados em ambientes diferentes.
- O Capítulo 6, "CONCLUSÕES", apresenta as principais conclusões deste trabalho, comentando as contribuições efetivamente alcançadas. Em seguida, "TRABALHOS FUTUROS" apresentam-se propostas de desenvolvimento do trabalho e sugestões para a continuidade deste trabalho e apontando recomendações para possíveis aplicações da metodologia aqui descrita.

Por fim, têm-se os Anexos, que contém: os resultados dos processos de *port scanning* nas duas redes ensaiadas e um exemplo de relatório contendo dados extraídos de um dos IEDs

Assim chega-se ao fim deste capítulo introdutório, no próximo serão apresentados alguns conceitos e o estado da arte relativo a este trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 SISTEMAS DE GERAÇÃO E TRANSMISSÃO DE ENERGIA ELÉTRICA

Sistemas de geração e transmissão de energia elétrica possuem alta complexidade devido aos seus inúmeros componentes: unidades geradoras, linhas de transmissão, subestações (SEs) elevadoras/abaixadoras, disjuntores, transformadores, chaves seccionadoras e ainda sistemas auxiliares a seu funcionamento, além dos sistemas Proteção, Automação, Supervisão e Controle dos equipamentos. A Figura 1 apresenta uma ilustração tradicional de um sistema elétrico de potência (SEP). No caso brasileiro, o mesmo deve ser projetado para suportar contingências segundo critérios operacionais e de planejamento como, por exemplo, suportar a abertura de uma linha de transmissão após a ocorrência de um curto-circuito. Um dos critérios adotados é o denominado "N-1" [7], onde o sistema planejado deve suportar a princípio contingência simples (defeito/falta de um elemento temporário de geração ou transmissão) sem que haja perda de carga, tanto durante o período transitório quanto no novo estado de equilíbrio resultante da ocorrência.

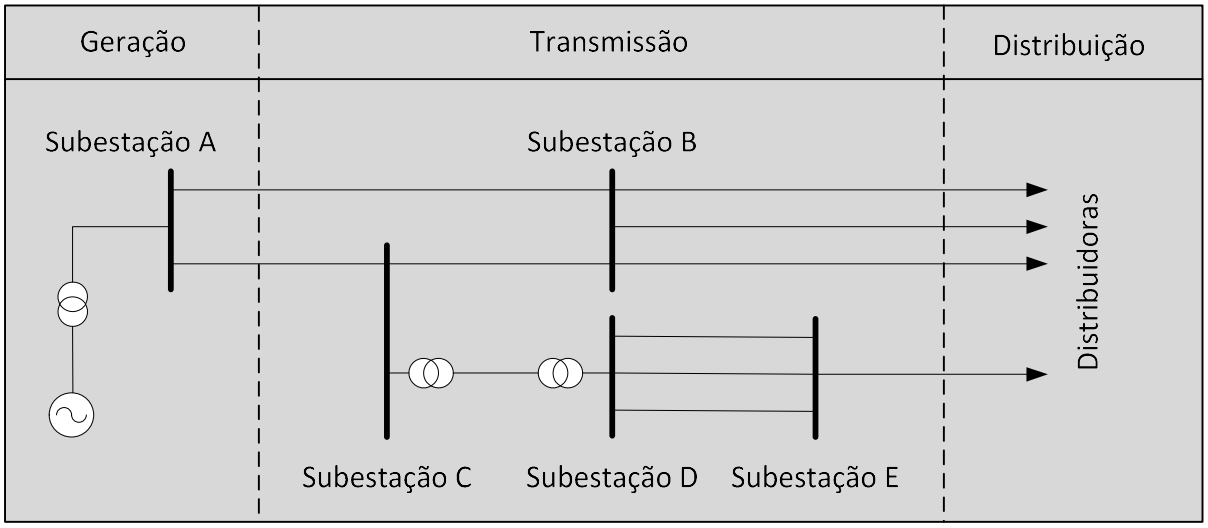


Figura 1 – Caracterização do Sistema Elétrico de Potência

De acordo com [8], cabe ressaltar que apesar deste esquema ser realizado em grande parte do Brasil, é possível que esse formato seja alterado com o advento das redes inteligentes, a popularização da geração distribuída (GD) e a inserção de unidades geradoras em unidades consumidoras. As linhas de transmissão (LTs) são, dentre todas as partes do SEP, os componentes que apresentam maior vulnerabilidade e maior grau de probabilidade de ocorrência de eventos que comprometam sua integridade, tendo em vista sua exposição a

intempéries que aumentam sua vulnerabilidade a descargas atmosféricas e por estarem cada vez mais operando nos seus limites. Logo, o principal objetivo dos sistemas de proteção de LTs é impedir que esses eventos em sua área de atuação comprometam justamente sua integridade/disponibilidade e a estabilidade do sistema.

No período de 1º de agosto de 2014 a 31 de julho de 2015, Agência Nacional de Energia Elétrica, ANEEL, registrou em seu relatório anual [9] 3.386 desligamentos forçados, de origem interna ou secundária, em equipamentos e linhas de transmissão da Rede Básica e da Rede Complementar do Sistema Interligado Nacional – SIN, ocorridos. A Figura 2 [9] mostra a estratificação desses desligamentos.

Por meio dessa estratificação percebe-se que a maior parte dos desligamentos ocorreu em linhas de transmissão e quase todos na Rede Básica.

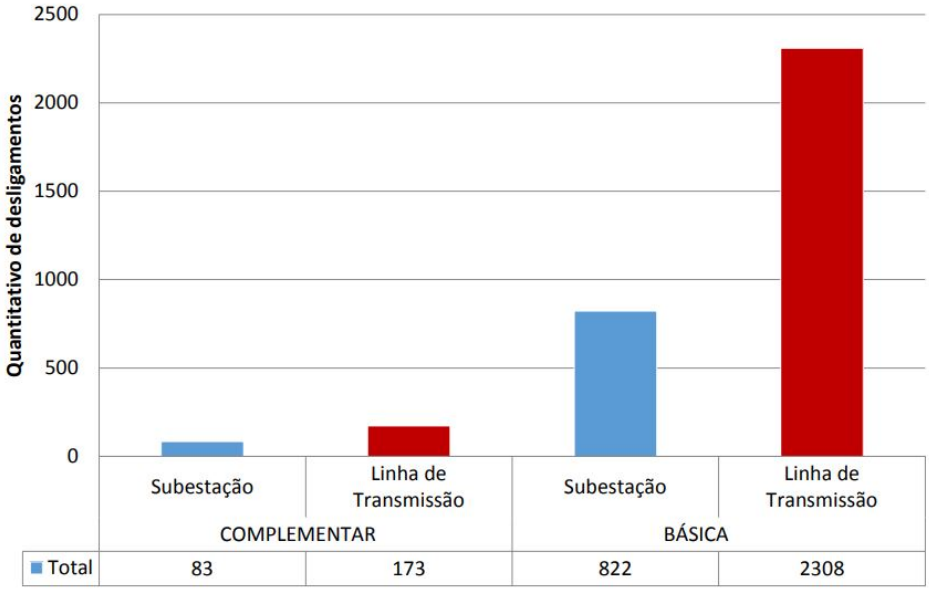


Figura 2 - Estratificação dos desligamentos por rede

Com relação às classificações dos desligamentos, a Figura 3 [9] demonstra a situação no período. Percebe-se que, somadas, as causas indeterminadas, as descargas atmosféricas e as falhas humanas foram responsáveis por mais da metade das ocorrências no período.

Esta questão demonstra a importância do sistema de proteção de LTs. Dentro deste contexto, o problema de análise e diagnóstico de oscilografias de perturbações em LTs vem sendo objeto de estudo da literatura técnica ao longo dos últimos anos, com foco nos sistemas baseados em Inteligência Computacional.

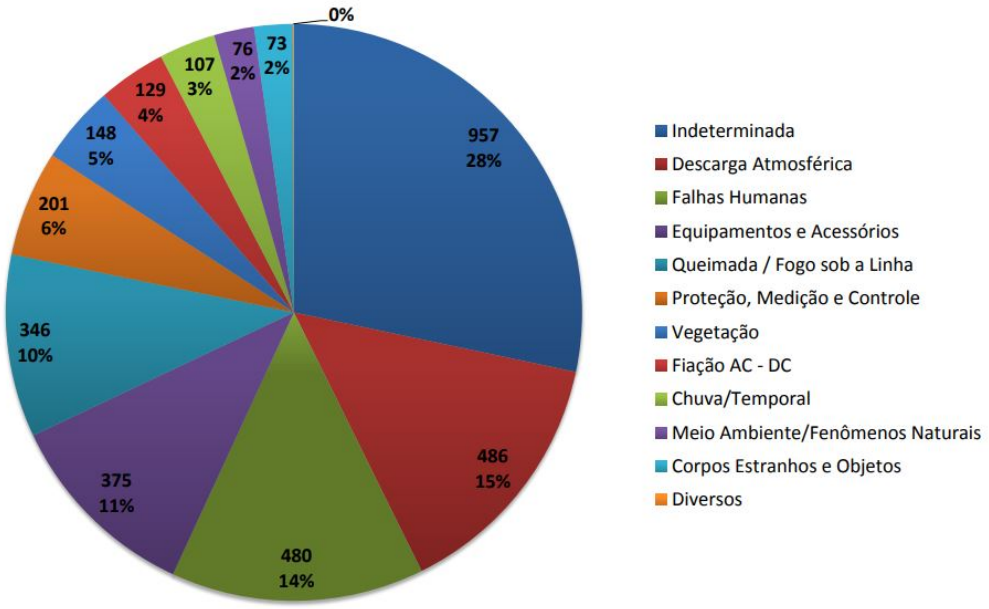


Figura 3 - Estratificação dos desligamentos por motivo

Fortes [10] e [11] apresenta um panorama das aplicações baseadas em sistemas inteligentes para diagnóstico de falhas em linhas de transmissão. A maioria das propostas trata de etapas distintas do problema de diagnóstico (detecção do instante de início do evento, classificação do tipo de distúrbio e localização da eventual falta). Além desta abordagem estanque do problema, boa parte das técnicas fornece diagnósticos de difícil interpretação, muitas vezes desprovidos de probabilidades associadas a cada decisão tomada. A consolidação destes módulos em uma ferramenta integrada incluindo as etapas de detecção, classificação e localização de falhas, e que forneça relatórios qualitativos sobre os eventos analisados é um desafio, principalmente no setor elétrico nacional, onde o presente estudo pretende deixar sua contribuição.

2.2 PROTEÇÃO DE SISTEMAS ELÉTRICOS DE POTÊNCIA

Os sistemas elétricos de potência são constituídos por conjunto de equipamentos como geradores, transformadores, disjuntores, linhas de transmissão, e distribuição cujo principal objetivo é fornecer energia elétrica aos consumidores de forma confiável, econômica e ininterrupta [12].

A proteção de sistemas elétricos tem por objetivo isolar um equipamento defeituoso, uma situação de falha ou de sobrecarga, de forma rápida e confiável, comprometendo a menor parcela possível da rede elétrica, evitando perdas de carga, protegendo equipamentos e

também preservando a condição física das pessoas. Para isso certos requisitos devem ser preenchidos: confiabilidade, sensibilidade, velocidade e seletividade.

As principais causas de defeito são:

- **Sobrecarga:** quando a corrente de carga de um equipamento ultrapassa seu valor nominal, e que provoca aumento de temperatura dos equipamentos;
- **Curto-circuito:** quando ocorre falha para terra, através de descargas por circuitos de baixa impedância, por rompimento de dielétrico, descargas atmosféricas, galhos de árvores, entre outros fatores como: queda de torres ao solo ou de objetos nos cabos condutores;
- **Surtos:** são tensões ou correntes elevadas provocadas principalmente por corrente de magnetização de transformador, partida de motor, chaveamentos de bancos de capacitores, rejeição de carga, etc.

A proteção de sistemas é normalmente implementada através dos chamados esquemas de proteção, que são comandados por relés. Estes relés de proteção tem por finalidade identificar os defeitos, localizá-los da maneira mais precisa possível, promover o isolamento elétrico do defeito abrindo disjuntores e ainda emitir alertas ao operador da subestação.

Os primeiros relés de proteção eram de tecnologia eletromecânica, normalmente com uma função específica (uni função). O sistema de supervisão e controle associado era constituído por chaves de controle e chaves seletoras, lâmpadas indicadoras, painel mímico, instrumentos de medição indicativa, valores analógicos e um ou mais anunciadores de alarme.

Os dispositivos de controle eram distribuídos em painéis de controle, e os relés em painéis de proteção. Em tensões de 138 kV até 345 kV utilizava-se, em geral, um painel de controle e um painel de proteção para cada saída de linha ou para cada transformador, além de um ou mais painéis para as funções comuns a cada tipo de equipamento. Nas subestações de 500 kV e 765 kV, a quantidade de relés e dispositivos de controle era tal que cada saída de linha ou transformador requeria, muitas vezes, dois painéis de controle e dois painéis de proteção. Todos esses painéis eram localizados numa casa de controle que, em alguns casos, precisava ser ampliada para comportar mais painéis e cabos.

Nas subestações e usinas de maior porte, um grande espaço era necessário para acomodar todos esses painéis, aumentando o custo das edificações necessárias para abrigá-los.

As diferentes lógicas utilizadas nos circuitos de controle e intertravamento eram efetuadas por ligação física de contatos em série e em paralelo, através de fios. Era necessário um conjunto independente de contatos auxiliares dos disjuntores e chaves seccionadoras, o

que aumentava muito a cablagem. Como alternativa podiam-se utilizar relés auxiliares, porém este método também trazia desvantagem, aumentando a fiação interna e custo dos painéis.

Tendo em vista as distâncias envolvidas e o grande número de cabos por equipamento protegido, seja de geração, de transmissão, de transformação ou outros, estas subestações e usinas requeriam, muitas vezes, dezenas ou até centenas de quilômetros de cabos de controle, bem como as respectivas estruturas para contê-los, como eletrodutos, dutos, canaletas e bandejas. Todos estes fatores oneravam o custo das instalações e eram fatores complicadores para a manutenção.

Como os níveis de tensão em um sistema de produção e transmissão de energia elétrica são normalmente elevados, os relés operam com mais segurança quando energizados por transformadores de tensão e corrente. Os transformadores de potencial (TP) e de corrente (TC) são transformadores destinados apenas a alimentar os equipamentos de medição, controle e proteção. Os equipamentos de proteção encontrados em um sistema elétrico de potência são basicamente os relés, TCs, TPs, banco de baterias, disjuntores e contatos auxiliares.

Esses equipamentos exigiam cuidados na instalação e no seu ajuste, pois pequenas peças mecânicas, comparáveis à mecânica de relojoaria, eram utilizadas na sua montagem, além dos relés suportarem apenas uma ou duas funções de proteção, o que exigia utilização de diversos relés para funções de retaguarda, mais cabos e mais espaço físico dentro dos painéis. A Figura 4 [13] mostra alguns relés eletromecânicos.

Figura 4 - Relés eletromecânicos

Estes relés ainda são encontrados em diversas concessionárias de energia elétrica no Brasil. Porém estão sendo gradativamente substituídos por equipamentos mais modernos devido à falta de peças de reposição e à falta de mão de obra especializada no mercado de trabalho, uma vez que esta tecnologia está se tornando cada vez mais obsoleta.

Com o desenvolvimento dos semicondutores, surgiram os primeiros relés eletrônicos, também chamados de relés estáticos, por não possuírem partes móveis. Estes relés exigiam cuidados de instalação, como por exemplo, um melhor controle de temperatura, da umidade e de interferências eletromagnéticas.

Os elementos básicos que constituem um relé eletrônico (Figura 5 [14]) são: a unidade conversora, as unidades de medição e de saída bem como a fonte de alimentação. Eles não ganharam vasta utilização no setor elétrico devido a pouca aceitação e ao rápido aparecimento dos relés digitais.

Figura 5 - Exemplo de relé eletrônico.

Com a evolução dos microprocessadores, surgiram os primeiros relés digitais. esses equipamentos utilizam em seus algoritmos os princípios dinâmicos dos antigos relés eletromecânicos e os evoluídos conceitos da eletrônica digital. Os relés digitais atuais são chamados de IEDs que, além das funções de proteção, possuem funcionalidades adicionais de outros equipamentos, como medição de grandezas analógicas, monitoramento de disjuntores, comutadores de *tap*, monitores de qualidade de energia, medição fasorial com *Phasor Measurement Units* (PMUs), Controladores Lógico-Programáveis (CLPs), reguladores de tensão, alarmes, e o mais importante: a capacidade de se comunicar em rede, característica que seus antecessores nunca possuíram, considerando a evolução tecnológica.

Os IEDs (Figura 6 [15]) computadores por essência. Um tipo especial de computador, com hardware projetado para suportar ambientes industriais agressivos, no que se refere a ruídos e oscilações na alimentação elétrica, interferência eletromagnética, temperatura, umidade e vibração. Podem desempenhar diversas funções de proteção, supervisão e controle, superando em muito as capacidades e funcionalidades dos relés que foram seus antecessores na escalada tecnológica. IEDs são capazes de se comunicar em rede com sistemas de supervisão e controle e também podem se comunicar uns com os outros. Assim podem enviar e receber valores para uso em suas lógicas de operação, bem como enviar e receber comandos para os disjuntores aos quais estejam associados.

Figura 6 - Exemplo de IED.

Os relés digitais estão hoje sendo bastante utilizados em novos projetos de sistemas elétricos de potência e na substituição de relés eletromecânicos e estáticos. Algumas de suas vantagens são: velocidade, confiabilidade, integração digital e flexibilidade funcional.

2.3 A NORMA IEC 61850

A automação de subestações demanda a implantação de uma rede de comunicação de dados e computadores, envolvendo telecomunicações e computação, para a integração de dispositivos com medição, controle e proteção, conforme a necessidade crescente de consolidar e disseminar, de forma rápida e precisa, informações provenientes do sistema elétrico de potência (SEP).

Esta integração envolve uma grande diversidade de fabricantes, equipamentos, gerações de tecnologia, redes de comunicação, arquiteturas, softwares, protocolos de comunicação, e como consequência, alto custo para obtenção de uniformidade de seus dados.

No ambiente da automação, o elevado número de protocolos proprietários e não proprietários tem representado um desafio para conexão entre equipamentos de fabricantes distintos. Alguns exemplos de protocolos mais utilizados são: *Distributed Network Protocol* (DNP3), MODBUS, HART, CONTROLNET, 60870-5-103, PROFIBUS, FILEDBUS, UCA2, LON, DEVICENET, 60870-5-101/4 e PROFINET.

Em 1988 o EPRI (*Eletric Power Research Institute*) iniciou atividades para definição de uma arquitetura de comunicação para concessionárias de energia elétrica, UCA (*Utility Communications Architecture*). Com base nestes estudos a versão 2.0 da arquitetura foi publicada pelo IEEE (*Institute of Electrical and Electronics Engineers*) como o relatório técnico TR1550, 1989, definindo dois contextos de comunicação [16]:

- Comunicação entre centros de controle;

- Comunicação entre dispositivos de campo.

Paralelamente, a IEC (*International Electrotechnical Commission*) reconheceu a necessidade de normalizar as interfaces para os dispositivos de telecontrole, por meio da série de normas IEC-60870-5, através dos comitês técnicos IEC-TC57 e IEC-TC95 [17]:

- IEC-60870-5-101: trouxe a inovação para a padronização da comunicação entre unidades terminais remotas (UTRs) e centros de controle para o sistema de potência;
- IEC-60870-5-103: padronização da comunicação serial de dispositivos de proteção digital;
- IEC-60870-5-104: a comunicação em redes *Local Area Network* e *Wide Area Network* (LAN e WAN), baseado no uso de redes *ethernet* com protocolo TCP/IP.

Este protocolo utiliza o modelo mestre-escravo, com a restrição de um pequeno número de funções e modelo de dados padronizado [17].

Em 1994, reconheceu-se a necessidade de uma padronização mais geral cobrindo redes de comunicação e sistemas em subestações, e foram criados os grupos de trabalho WG1O, WG11e WG12, conectados ao Comitê Técnico IEC-TC57 [27]. Esses três grupos reuniram especialistas de vários países com experiência nos protocolos, segundo a norma IEC-60870-5 e a UCA 2.0. A IEC e o EPRI concordaram então em ter uma única normalização, o padrão IEC-61850, Redes de Comunicação e Sistemas em Subestações [19], estabelecendo o modelo de dados e a pilha de protocolos para troca de informações.

A norma IEC-61850 foi organizada em 10 partes, todas aprovadas e com estado de padrão internacional, conforme descreve a Tabela 1.

A parte 1 da norma IEC-61850 [19] descreve como premissa a interoperabilidade na troca de informações entre dispositivos de fabricantes distintos, como, por exemplo, IEDs, sendo que a comunicação deve suportar as funções operativas das subestações, e garantir entre outras, as seguintes características:

- A comunicação baseada no perfil de padrões já existentes (IEC/IEEE/ISO/OSI);
- A utilização de protocolos abertos com suporte à autodescrição dos dispositivos, o que deve permitir a adição de novas funcionalidades;

- A utilização de uma estrutura de dados (*data object*) que represente informações específicas, por exemplo, estados e medições, relativas às necessidades da indústria de energia elétrica;
- A sintaxe e semântica das informações devem basear-se no uso de objetos de dados comuns relativos ao sistema de potência;
- Suportar futuros desenvolvimentos tecnológicos.

Tabela 1 - Documentos que definem a Norma IEC 61850 [19]

Característica	**Parte**	**Descrição**	**Publicação**
Aspectos do Sistema	1	Introdução e Visão Geral	04/2003
	2	Glossário	01/2002
	3	Requisitos Gerais	01/2002
	4	Gerenciamento de Sistema e Projeto	01/2002
	5	Requisitos de Comunicação para Funções e Modelos de Dispositivos	07/2003
Configuração	6	Linguagem de Configuração para IEDs de Subestações Elétricas (SCL)	03/2004
Estrutura de Comunicação Básica para Equipamentos de Subestações e Alimentadores	7.1	Princípios e Modelos	07/2003
	7.2	Serviços de Interface de Comunicação Abstrata (ACSI)	05/2003
	7.3	Classe de Dados Comum (CDC)	05/2003
	7.4	Classes de Nós Lógicos e de Dados Compatíveis	05/2003
Mapeamento de Serviços de Comunicação Específicos	8.1	Mapeamento para MMS (ISO/IEC 9506 Parte 1 and Parte 2) e para ISO/IEC 8802-3	05/2004
	9.1	Valores Amostrais sobre Enlace Serial Unidirecional *Multidrop* Ponto-a-Ponto	05/2003
	9.2	Valores Amostrais sobre ISO/IEC 8802-3	04/2004
Ensaios	10	Testes de Conformidade	06/2005

Adicionalmente, as operadoras do sistema de energia elétrica também requerem como objetivo a intercambiabilidade entre IEDs de fabricantes distintos, ou seja, a substituição de

equipamentos de um fabricante por outro, sem necessidade de alterações nos demais dispositivos constituintes do sistema.

Embora inicialmente o padrão IEC-61850 tenha sido concebido apenas para uso interno às subestações, estudos estão sendo realizados para utilizá-lo também na comunicação entre subestações, e subestação – centro de controle.

Mackiewicz [20] esboça que a estrutura da norma IEC-61850 utiliza o conceito de definição abstrata para acomodamento de dados e serviços, isto é, objetos e serviços são criados independentemente de qualquer outro protocolo, permitindo neste entretempo, mapeá-los para diversas regras de comunicação que atendam os dados e serviços requeridos.

2.3.1 REQUISITOS GERAIS

A parte 3 da norma IEC-61850 define requisitos gerais da comunicação em rede, com ênfase para as exigências de qualidade e recomendações específicas sobre a relevância de outras normas e especificações. As minúcias desta parte referem-se a requisitos, como por exemplo, [21]: no requisito de confiabilidade o padrão exige que a falha de um componente de comunicação não afete a operabilidade do sistema e que o monitoramento e controle local sejam mantidos. Dependendo dos requisitos de confiabilidade e da filosofia de operação, redundância de diferentes níveis pode ser aplicada.

Os demais requisitos da comunicação estão na parte 3 da norma IEC-61850 [21].

2.3.2 GERENCIAMENTO DO PROJETO E SISTEMA

As especificações pertencentes à parte 4 da norma IEC-61850 descrevem as exigências básicas de gerenciamento do projeto e sistema para automação da subestação com respeito ao processo de engenharia e às ferramentas de suporte, ao ciclo de vida de todo sistema e dos IEDs e à garantia de qualidade iniciada com o estágio de desenvolvimento e terminada com o abandono e desmantelamento do Sistema de Automação e Supervisão (SAS) e seus IEDs [22].

2.3.3 REQUISITOS DE COMUNICAÇÃO

A norma IEC-61850, parte 5, especifica os requisitos para comunicação das funções implementadas nos diversos níveis do SAS, e para o modelo de dispositivos.

As funções referem-se a tarefas que devem ser executadas na subestação, por exemplo: controle, monitoração e proteção dos equipamentos da subestação. Essas funções podem ser logicamente alocadas nos três diferentes níveis hierárquicos de uma subestação:

- Nível de processo: aquisição de dados dos equipamentos de alta tensão;
- Nível de *bay*: proteção e automação;
- Nível de estação: supervisão e telecontrole.

Neste contexto, o objetivo da norma IEC-61850 é fornecer interoperabilidade entre os IEDs de diferentes fabricantes, ou mais precisamente, entre as funções desempenhadas nos níveis hierárquicos da subestação, que residem em dispositivos físicos distintos [23].

2.3.4 NÓ LÓGICO, LN (*LOGICAL NODE*)

Na automação de uma subestação os protocolos mais tradicionais normalmente definem como os bytes serão transmitidos, utilizando um conceito orientado a sinais ou mensagens, pelo qual cada mensagem ou sinal representa um ponto de medição ou um dado como, por exemplo, uma informação de estado ou um valor numérico [23]. Isto requer que o engenheiro de sistemas configure e mapeie os sinais manualmente, elemento por elemento, endereço por endereço.

Um IED que forneça conformidade com a norma IEC-61850 é formado, inicialmente, por um *hardware* que se conecta ao sistema de comunicação de dados, através de um endereço de rede (físico e lógico), e o conjunto de funções representadas em modelos de *software* por classes que caracterizam seu comportamento. Este modelo é concebido segundo os conceitos da programação orientada a objetos, onde existem as figuras das classes com seus métodos e suas propriedades. As classes contam com os conceitos de poliformismo e herança. Desta forma os objetos, que são instâncias vivas das classes, podem conter outros objetos aninhados carregando dados de maneira categorizada.

As funções de um SAS como supervisão, controle e proteção dos dispositivos primários e do próprio SEP, foram identificadas e separadas em subfunções, que são descritas como um grupo de dados e serviços associados em classes, formando um nó lógico (LN). Por sua vez, um conjunto de LNs forma um dispositivo lógico, *Logical Device* (LD), que reside no dispositivo físico (IED), conforme ilustra a Figura 7 [23].

Este modelo de dados é tratado, armazenado, codificado e decodificado segundo a lógica do *firmware* embarcado do IED. O *firmware* é um *software* por essência, que tem a função de controlar o funcionamento de todo o *hardware* e os eventos que ocorrem no IED, de maneira similar ao que fazem os sistemas operacionais em um computador pessoal.

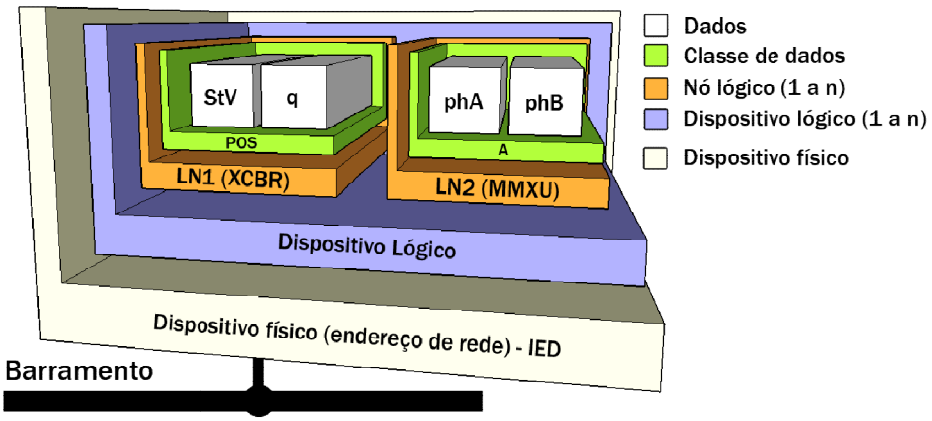


Figura 7 – Modelo de dados

A Norma define todas as especificações necessárias para a compreensão e implementação destas classes.

Os nós lógicos são congregados em grupos, que por sua vez são identificados por indicadores, conforme Tabela 2 [23].

Cada LN possui uma denominação, iniciada pelo grupo indicador e um sufixo pode ser utilizado para o nome do nó, e possibilitar a diferenciação de nós lógicos com o mesmo nome. Como exemplo, Mackiewicz [20] supõe a existência de duas entradas de medição em um equipamento para aferir dois alimentadores trifásicos. O nome padronizado para um nó lógico de medição é MMXU. Para diferenciar as medições de cada um dos alimentadores, a IEC 61850 adiciona o sufixo 1 e 2 aos nomes, procedendo à identificação como MMXU1 e MMXU2.

Tabela 2 – Grupos de LN (parcial)

Grupo Indicador	Grupo de Nó Lógico
A	Controle Automático
C	Controle Supervisionado
G	Função Genérica
I	Interfaces e Arquivamento
L	Sistema de Nó Lógico
M	Contador e Medição
P	Função de Proteção
R	Função Relacionada a Proteção

A representação de um disjuntor é denominada XCBR, indicador X (disjuntor e seccionadora) e CBR (*circuit breaker*), conforme ilustra a Figura 8.

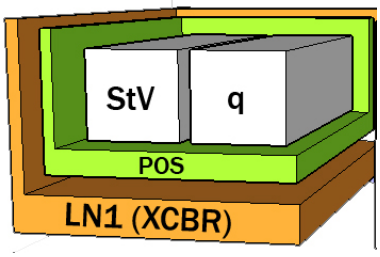


Figura 8 – Nó lógico XCBR

O elemento de dado associado, Pos, é diferente de um simples ponto de estado do disjuntor. Segundo Gurjão, Souza e Carmo [24], Pos tem vários atributos de controle, substituição, configuração, descrição e extensão, como Pos.ctlVal, que representa um controle e pode ser um comando de abertura ou fechamento. O Pos.stVal que representa a posição real de um disjuntor, podendo assumir os seguintes estados: transição, aberto, fechado ou defeito.

2.3.5 LINGUAGEM DE CONFIGURAÇÃO

Diante de possibilidades distintas de uso dos nós lógicos em diferentes dispositivos, se faz necessário uma estratégia que atribua o caminho que a informação deve seguir. A definição desta estrutura está descrita na parte 6 da norma IEC-61850, que especifica uma linguagem de descrição formal de configuração para sistemas de automação de subestações, conhecida como *Substation Configuration Language* (SCL).

Esta linguagem permite a configuração dos IEDs com seus respectivos parâmetros, além da configuração de funções de subestações. De acordo com a IEC-61850-5 e IEC-61850-7x. Cada equipamento deve prover um arquivo SCL que descreva sua própria configuração, com base na *Extended Markaup Language* (XML) versão 1.0.

A configuração SCL é composta por arquivos que contêm dados da subestação, das relações dos equipamentos de manobra, da funcionalidade dos IEDs e de todos os serviços de comunicação, permitindo a troca de informações de configuração entre ferramentas de fabricantes distintos [25].

A SCL em toda a sua extensão descreve modelos, como os citados por Gurjão, Souza e Carmo [24] em referência à Norma [25].

2.3.6 ESTRUTURA DE COMUNICAÇÃO

A estrutura de comunicação prevista na norma IEC-61850 utiliza o conceito de "definição abstrata" para acomodação de dados e serviços, permitindo mapeá-los para outros protocolos que atendam os dados e serviços requeridos. A parte 7.1 da Norma especifica os princípios e modelos necessários para compreender as seções posteriores [26]. As partes 7.2 e 7.4 da Norma definem os serviços abstratos e os objetos de dados abstratos respectivamente.

Conforme Mackiewicz [20], os objetos de dados são compostos de partes comuns, como: estados, medições e controle. O conceito de *Common Data Classes* (CDC) foi desenvolvido utilizando-se de blocos comuns para compor objetos de dados maiores, de acordo com a parte 7.3 da Norma.

2.3.7 SERVIÇO DE INTERFACE DE COMUNICAÇÃO ABSTRATA, ACSI

A parte 7.2 da norma IEC-61850 define o serviço de interface de comunicação abstrata (ACSI) como um modelo de classe hierárquica de todas as informações que podem ser acessadas e trocadas, implantando a cooperação entre os vários dispositivos do sistema.

O ACSI dispõe das seguintes interfaces abstratas [27]:

- A interface abstrata que descreve a comunicação entre um cliente e um servidor remoto;
- A interface de comunicação para sistemas cujo tempo na troca de dados é um fator crítico.

Esta parte da norma IEC-61850 também pode ser aplicada para descrever modelos de dispositivos e funções para atividades adicionais [27], tais como: a troca de informações entre subestações, a troca de informações entre subestações e centro de controle, a troca de informações entre o ambiente de campo e o centro de controle e troca de informações para medição.

2.3.8 CLASSE COMUM DE DADOS, CDC

O elemento de dados característico de um nó lógico é definido de acordo com a especificação de uma classe comum de dados (*Common Data Class*, CDC), descrita na norma IEC-61850, parte 7.3. Cada CDC tem um nome definido e determina o tipo de estrutura dos dados, dentro de um nó lógico, como, por exemplo, informação de estado, medição, parametrização ou controle [28] (Tabela 3).

Tabela 3 – CDCs citadas no padrão IEC-61850 parte 7.3

Nome	Tipo da Informação	Descrição
ACT	Estado	Proteção ativa
SAV	Medição	Valor análogo
SPC	Controle	Posição única controlável
CURVE	Parametrização	Parametrização de curva
LPL	Supervisão	Identificador do Nó Lógico

2.3.9 COMPATIBILIDADE ENTRE NÓS LÓGICOS E CLASSES DE DADOS

A parte 7.4 da norma IEC-61850 [29] especifica os modelos de informação dos dispositivos e funções relacionadas para aplicações em subestações. Em especial, estabelece a compatibilidade dos nomes dos nós lógicos e o nome dos dados para comunicação entre IEDs, possibilitando a interoperabilidade na comunicação.

Santos [30] salienta que o padrão não se restringe apenas aos LNs previstos, suporta novos LNs que podem ser criados por usuários seguindo os padrões estabelecidos na parte 4 da Norma.

2.3.10 MAPEAMENTO DE SERVIÇOS DE COMUNICAÇÃO ESPECÍFICOS

A parte 8.1 da norma IEC-61850 especifica um método de troca de dados com, ou sem restrições críticas de tempo, através de uma LAN, tendo como objetivo o fornecimento de instruções e especificações detalhadas quanto aos mecanismos e as regras necessárias para implementar os serviços, objetos e algoritmos apontados no padrão IEC-61850, partes 7.2, 7.3 e 7.4, quanto ao uso da norma ISO 9506 (MMS).

Os serviços e o protocolo MMS são especificados para operar sobre as camadas do modelo OSI e compatíveis com os perfis de comunicação do TCP/IP. A utilização do MMS permite o uso de arquiteturas centralizadas e distribuídas, e inclui a troca de dados seja de estado, operações de controle ou notificações em tempo real [31].

2.3.11 PILHA DE PROTOCOLOS E TIPOS DE MENSAGEM

Na especificação da norma IEC-61850, foram definidos dois perfis (*profiles*), ou conjuntos de padrões escolhidos para se implementar um determinado protocolo, dividindo as sete camadas do modelo OSI (*Open System Interconnection*) em dois grupos, o "*Application Profile* (*A-Profile*)" que engloba as três camadas superiores (aplicação, apresentação e sessão)

e o "*Transport Profile* (*T-Profile*)" que agrupa as quatro camadas inferiores restantes (transporte, rede, enlace e física) [44]. Várias combinações de *A-Profile* e *T-Profile* podem ser executadas com o intuito de permitir a troca de determinados tipos de informações e serviços.

A Tabela 4 explicita quais camadas do modelo OSI tem protocolos descritos pela norma IEC-61850, para cada combinação supracitada, de acordo com o respectivo *profile*. A parte 8.1 da Norma mostra os protocolos apontados [31].

Observa-se na Tabela 4 que somente as duas primeiras camadas, física e de enlace, são comuns a todos os serviços e suas respectivas mensagens, sendo que na camada física utilizam-se os padrões de rede do tipo *Ethernet*. As células em cinza: *Time Sync*, SV (Sample *Values*) e GOOSE não possuem regras estabelecidas pela norma IEC 61850 nestas camadas. As mensagens GOOSE e GSEE são mensagens que sofrem restrições severas de tempo e usam apenas os endereços MAC.

Tabela 4 – Combinações de serviços dos protocolos, padrão IEC-61850 parte 8.1

Profile **A ou T**	**Camada do modelo OSI**	**Serviço Cliente/Servidor (OSI)**	**Time Sync**	**SV**	**GOOSE**	**GSEE**
A	Aplicação	**X**	**X**	**X**	**X**	**X**
	Apresentação	**X**		**X**	**X**	**X**
	Sessão	**X**				**X**
T	Transporte	**X**	**X**			**X**
	Rede	**X**	**X**			**X**
	Enlace	**X**	**X**	**X**	**X**	**X**
	Física	**X**	**X**	**X**	**X**	**X**

2.3.12 MENSAGENS GOOSE (*GENERIC OBJECT ORIENTED SUBSTATION EVENT*)

As mensagens denominadas GSE (*Generic Substation Events*) podem ser classificadas em GOOSE (*Generic Object Oriented Substation Event*) e GSSE (*Generic Substation Status Event*). Pereira [32] cita que nas mensagens GOOSE, a informação é configurável e pode utilizar um grupo de dados (*data set*) que permite a um receptor tomar ciência que um estado foi modificado e o instante da alteração. Já as mensagens GSSE somente suportam uma estrutura fixa de informação de estado, a qual é publicada e disponibilizada na rede.

Bastos e Castro [33] descrevem que a mensagem GOOSE foi implementada como um protocolo não orientado a conexão, contendo em seu cabeçalho as informações de endereço e nome do emissor, tempo do evento que disparou a mensagem GOOSE e o tempo esperado para a nova mensagem.

Uma grande vantagem das mensagens GOOSE é permitir a interligação entre dois ou mais IEDs através da rede, intercambiando mensagens com alta velocidade e substituindo as diversas ligações por meio de fios metálicos, pela rede local de comunicação.

2.3.13 SISTEMA DE TESTE BASEADO NA IEC 61850

A parte 10 da norma IEC-61850 [34] tem como objetivo assegurar que todos os seus modelos e serviços sejam executados corretamente, na busca por melhorar as possibilidades para a interoperabilidade entre os dispositivos do sistema de automação.

Conforme especificação de Paulino [35] um sistema de teste baseado na norma IEC 61850 deve permitir um ensaio apropriado, adequado às exigências do sistema de supervisão, controle e proteção, e simular as características da subestação e do sistema elétrico em questão.

2.4 PROTOCOLO MMS (*MANUFACTURING MESSAGE SPECIFICATION)*

A norma IEC 61850 define o uso do MMS porque seus são especificados para operar sobre sistemas em conformidade com as definições do modelo OSI e do protocolo TCP. Além disso, o uso do MMS permite provisionar suporte para arquiteturas de sistemas centralizados ou distribuídos. O protocolo MMS inclui a troca de dados em tempo real, operações de controle e notificação por relatórios. A norma IEC 61850 especifica o mapeamento de objetos e serviços da ACSI para o MMS [31].

O objetivo da proposta MMS [36], [37] e [38] é definir um protocolo de aplicação com os serviços de mensagem necessários para a comunicação entre dispositivos industriais programáveis e controladores de célula em um ambiente de manufatura integrado por computador. A norma que define o MMS [39] é constituída de duas partes distintas: os serviços MMS e a máquina de protocolo.

2.4.1 OS SERVIÇOS MMS

A primeira parte da norma define 86 serviços que normalizam a comunicação de mensagens para comando e controle remoto de dispositivos industriais. Estes serviços são agrupados da seguinte forma [37], [38]: gerência das associações MMS, informação sobre

dispositivos remotos, gerência de recursos de dispositivos remotos, carregamento e execução à distância de programa, acesso a variáveis remotas, gerência à distância de semáforos, gerência à distância de eventos, gerência distribuída de relatório, comunicação com operador remoto e transferência de arquivos.

Quando um usuário MMS (cliente) requisita um serviço MMS qualquer, este fica representado no servidor de serviço MMS por uma instância do serviço até o fim do tratamento. A Figura 9 mostra como são trocadas as mensagens entre os serviços MMS.

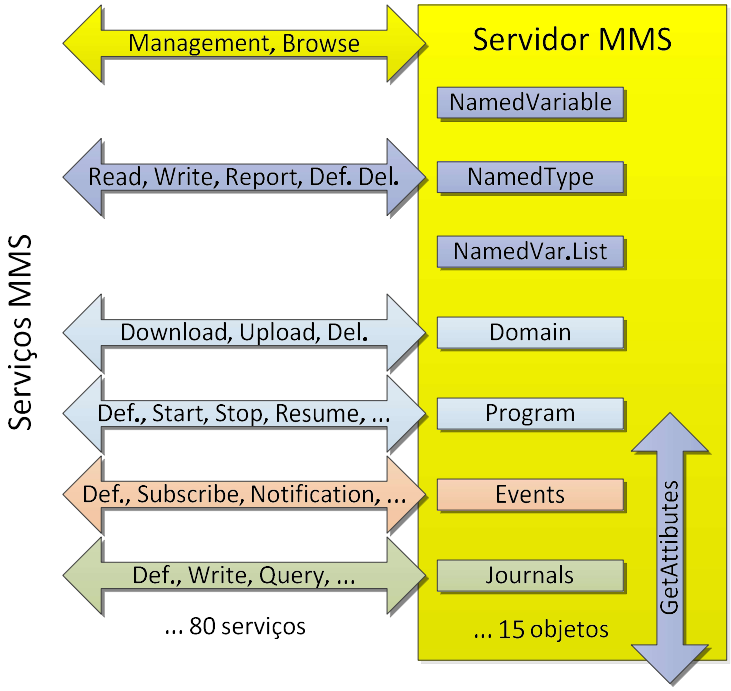


Figura 9 - Troca de mensagens dos serviços MMS

2.4.2 A MÁQUINA DE PROTOCOLO MMS

A segunda parte das especificações MMS descreve a máquina de protocolo MMS associada aos serviços descritos anteriormente.

Os procedimentos do protocolo MMS são suportados por uma máquina de protocolo chamada MMPM (*Manufacturing Message Protocol Machine*). As principais funções da MMPM são:

- Codificação: construir campo a campo as mensagens recebidas do cliente MMS;
- Decodificação: analisar as mensagens recebidas e fornecer os parâmetros a serem passados para o cliente MMS;
- MMPM deve gerenciar todas as instâncias em curso dos serviços requisitados;

A MMPM deve gerenciar todas as associações de aplicação.

Os serviços *INITIATE* e *ABORT* permitem estabelecer e abortar uma associação de aplicação entre dois atores MMS; Qualquer outra requisição de serviço não será atendida pelo servidor MMS se não participa de associação de aplicação previamente estabelecida. Um terceiro serviço chamado *CONCLUDE* permite terminar a associação de aplicação entre cliente e servidor.

A utilização dos serviços MMS será discutida na apresentação do algoritmo desenvolvido neste estudo.

2.5 DESAFIOS NA COMUNICAÇÃO ENTRE IEDS

Os equipamentos que compõe o sistema elétrico nacional tais como: Linhas de Transmissão, Geradores, Transformadores, Disjuntores entre outros, são guarnecidos de sistemas de proteção e controle que evoluíram de um modelo onde predominavam dispositivos eletromecânicos, para um estágio intermediário onde estes dispositivos passaram a ser eletrônicos, ou estáticos, coexistindo com os antigos dispositivos eletromecânicos. Atualmente estes dispositivos de proteção e controle se encontram em um terceiro estágio na sua linha da evolução tecnológica, onde são agora microprocessados e chamados de inteligentes. Os IEDs são dispositivos capazes de agregar, além das funções de proteção e controle de equipamentos do sistema elétrico, as funções de automação, comunicação via rede ethernet ou óptica, e supervisão remota através de sistemas supervisórios em camadas.

Preiss e Wegmann [40] falam de problemas do mundo real que surgiram com estas novas capacidades dos IEDs, que abriram uma infinidade de novas possibilidades e desafios que a Norma IEC 61850 veio organizar. A capacidade de comunicação via rede entre IEDs eliminou a grande quantidade de fiação física entre dispositivos e equipamentos que operam de forma coordenada, substituindo uma grande quantidade de cabeamento em painéis por um único condutoramento de comunicação digital elétrico, ou óptico. A supervisão dos sistemas de IEDs pode ser agrupada em camadas, onde a primeira delas é a aquisição de dados, que posteriormente trabalhados por aplicações computacionais de aquisição de dados, supervisão e controle - *Supervisory Control And Data Acquisition* (SCADA) e também aplicações de gerenciamento de energia - *Energy Management System* (EMS), são transformados em informações.

Os dados gerados pelos IEDs de uma estação podem ser trabalhados e supervisionados na sala de controle de nível local, através de sistemas SCADA, gerando informações de uma estação. As informações das estações com seus IEDs podem entrar como dados em

agrupamentos de Centros de Controle regionais, gerando informações de ilhas elétricas ainda em aplicações SCADA. As informações destes centros de controle regionais podem ser trabalhadas e agrupadas em um centro de controle de cada concessionária de energia elétrica, gerando informações por concessionária, onde aparecem as aplicações de gerenciamento de energia - EMS. As informações dos centros de controle de cada concessionária podem ser agrupadas e supervisionadas pelo Operador Nacional do Sistema (ONS), gerando assim o conhecimento de todas as informações pertinentes ao Sistema Interligado Nacional também em EMS. Tudo começa no IED e sua correta parametrização para seu funcionamento coordenado e fornecimento de dados.

Porém cada fabricante destes IEDs tem sua interpretação da Norma IEC 61850 de acordo com a cultura empresarial individual. Não é incomum encontrar aplicações que sejam criadas e personalizadas por profissionais, ou ligados ao domínio da engenharia elétrica ou ligados ao domínio da engenharia de software e, raramente criadas usufruindo uma plena, rica e necessária fusão destes domínios de conhecimento. Esta é, provavelmente, a maior razão dos problemas de interoperabilidade entre IEDs de fabricantes diferentes. Assim cada fabricante desenvolveu sua ferramenta de software que programa, parametriza e configura seus dispositivos microcontrolados para exercer as funções de proteção, controle, automação, supervisão e comunicação de maneira singular, o que dificulta o planejamento da interoperabilidade destes IEDs. Não é raro que, quando um IED de um fabricante operar em coordenação com outro IED de fabricante diferente do primeiro, apareçam as dificuldades. Acrescentar que, segundo experiência profissional em Furnas e observações pessoais em outras empresas do setor elétrico, esta é uma situação bastante comum no cenário brasileiro. Os problemas são particularmente evidentes quando se toca na questão das nomenclaturas e do processo de comunicação entre IEDs.

Yun et. al [41] abordam o problema da dificuldade dos engenheiros em parametrizar IEDs através da edição direta dos arquivos de configuração em linguagem SCL, e propõe como solução uma ferramenta de software visual, baseada em elementos vetoriais, que alinham o fluxo de trabalho. Apostolov [42] comenta a mesma dificuldade enfrentada pelos engenheiros, dada a complexidade da linguagem SCL, e sugere o desenvolvimento de uma estrutura formalizada que permita a descrição dos diferentes elementos e suas relações. Holbach et. al [43] abordam o problema da interoperabilidade e desenvolvem um estudo envolvendo a geradora e transmissora americana TVA e os fabricantes GE, ABB, Siemens e Areva, proporcionando o amadurecimento da implementação da norma IEC 61850. A multinacional Siemens desenvolveu o *software* IEC *Browser* [45]. Este aplicativo permite

explorar os LN de IEDs, porém não descobre a rede de automaticamente e, a troca de conexão de um IED para outro é feita de maneira manual. O projeto *open source* colaborativo *IEDExplorer* [46] também se propõe a explorar LNs em IEDs aderentes à norma IEC 61850, se valendo dos recursos do protocolo MMS.Este sistema permite inspecionar variáveis em estrutura de árvore, ler valores, criar ou apagar listas de variáveis, ativar e ler relatórios do tipo *buffered* e *unbuffered*, ler arquivos e capturar pacotes MMS, além de escrever em variáveis e enviar comandos ao IED. No entanto este sistema também não dispõe de um mecanismo capaz de se conectar a múltiplos IEDs em sequência, nem descobre a rede de maneira automática. A empresa Omicron, outra multinacional, oferece no mercado o software *IEDScout* [47], que também oferece uma série de funcionalidades ligadas à exploração de funções e configurações de IEDs, permitindo aos engenheiros enxergarem o que existe configurado dentro do IED e seus parâmetros de comunicação. Mas este programa, como os anteriores, também não permite explorar a rede e recuperar automaticamente estas informações. Vicente [48] apresenta um estudo que avalia a segurança de redes quando a configuração de funções de supervisão e proteção trocam informações entre agentes distintos. Utilizando o serviço de mensagens prioritárias previsto na norma IEC 61850 em substituição aos relés auxiliares e ao painel de interface, que utilizam cabos de cobre, e tendo a segurança como ponto principal da discussão quando se deseja conectar duas redes de comunicação de empresas diferentes. O estudo ressalta que algumas tecnologias que já são amplamente utilizadas na área de Tecnologia da Informação podem ser aplicadas em sistemas baseados na IEC 61850 sem impactar significantemente no desempenho e nos custos. Kostic et. al [49] apresentam uma proposta de modelagem mais elegante em UML (*Unified Modeling Language*) da norma IEC 61850 que se apresenta de maneira bastante complexa, e sugere que o conceito da Norma pode ser aplicado em outros ambientes além da geração, transmissão e distribuição de energia elétrica. Hoga et. al [50] abordam as questões da interoperabilidade entre equipamentos de fabricantes ou de gerações diferentes, do ciclo de vida e da substituição dos equipamentos, da preocupação com menores custos substituição, de treinamento e de manutenção de sistemas de automação em subestações. Esses estudos apontam a complexidade e o interesse de pesquisa nessa área.

3 PROPOSTA

As atuais tecnologias em sistemas de informação oferecem algumas soluções que podem ser aplicadas para auxiliar na superação dos problemas encontrados na gestão de ativos em uma rede de proteção de uma subestação.

O objetivo principal deste trabalho é prover uma ferramenta de software que seja capaz de produzir um relatório de ativos de proteção em uma subestação automatizada segundo os preceitos da norma IEC 61850. Esta ferramenta deve ser capaz de:

- Descobrir os IEDs na rede;
- Descobrir as funções de proteção e *datasets* ativos em cada IED;
- Gerar um relatório que represente uma imagem do que foi encontrado na rede.

A Figura 10 apresenta um fluxograma básico do método proposto.

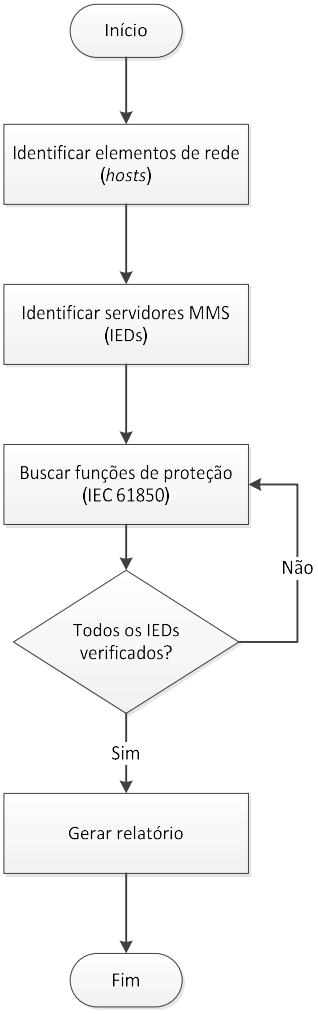


Figura 10 - Fluxograma do método proposto.

Como objetivo secundário, esta ferramenta auxilia na depuração de alguns tipos de problema de comunicação e de desempenho da rede. Isso é possível porque o sistema exibe informações como:

- Quantos e quais IEDs estão ativos na rede;
- Quantos datasets estão configurados;
- O conteúdo dos datasets;

- As funções de proteção disponíveis.

Além disso, é possível comparar os relatórios gerados, o que também auxilia na pesquisa de falhas ou de melhoria de desempenho da rede.

Para atingir os objetivos deste trabalho foram desenvolvidas aplicações específicas que se combinam com aplicações conhecidas e disponíveis no mercado.

O trabalho foi dividido em quatro módulos:

- netScanner, que recolhe as requisições do usuário;
- nMap, que realiza a descoberta da rede de comunicação;
- get61850nodes, que realiza o levantamento dos IEDs conectados no sistema; e
- Relatórios, que executa a comparação de relatórios para realização de diagnósticos.

A Figura 11 ilustra como o sistema foi dividido em módulos e como os módulos se relacionam.

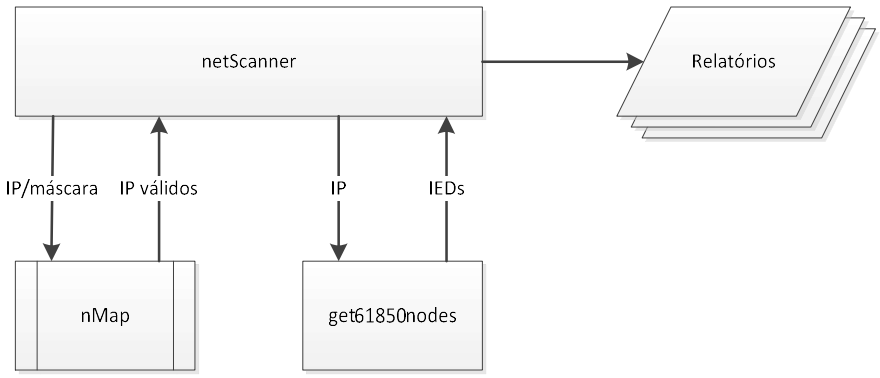


Figura 11 - Módulos do sistema

Apesar de abrir diversas possibilidades de uso, que serão exploradas no capítulo 6, a proposta se limita a coletar dados referentes à rede de IEDs e suas respectivas configurações no que se refere aos elementos previstos na norma IEC 61850.

3.1 MÓDULO NETSCANNER

O módulo netScanner providencia as interfaces com o usuário bem como com os demais módulos do sistema: nMap e get61850nodes.

As interfaces com o usuário são três:

- Interface principal;
- Interface de comparação de *hosts*;

- Interface de comparação de configurações de IEDs.

A interface principal recebe como entrada do usuário a placa de rede a ser utilizada, ou seja, a interface de rede do computador que executa o sistema que está de fato conectada à rede de automação onde será feito o levantamento de ativos. Como saída, a interface principal envia parâmetros de configuração para o módulo nMap e para o módulo get61850nodes. Para o usuário a interface principal exibe informações sobre os hosts, IEDs e demais elementos de rede descobertos.

A interface de comparação de *hosts* recebe como entrada do usuário duas pastas que contenham relatórios gerados pelo sistema de gerenciamento de ativos. Como saída, a interface apresenta as diferenças encontradas.

A interface de comparação de configurações de IEDs recebe como entrada do usuário dois arquivos de configuração de IEDs gerados pelo sistema de gerenciamento de ativos. Como saída, a interface apresenta as diferenças de configuração encontradas.

De posse dos dados obtidos com o nMap, o módulo netScanner faz os devidos tratamentos e aciona o módulo get61850nodes, passando os parâmetros necessários para o descobrimento dos IEDs.

3.2 MÓDULO NMAP

O módulo nMap faz a varredura da rede, o *port scanning*. Recebe do módulo netScanner a rede (endereço IP e máscara de sub-rede) como entrada e retorna os resultados do *port scanning* ao netScanner para tratamento dos dados obtidos. Este módulo trabalha no nível do protocolo TCP/IP, informando ao sistema endereços IP e MAC descobertos na rede.

3.3 PORT SCANNING

Os *port scanners* são ferramentas utilizadas para a obtenção de informações referentes aos serviços que são acessíveis e definidas por meio de mapeamento das portas TCP. Com as informações obtidas através do *port scanning*, evita-se o desperdício de esforço a exploração de serviços inexistentes, de modo que se podem concentrar os esforços em utilizar técnicas sobre serviços específicos, que podem ser de fato explorados [44].

Algumas características que tornam o nMap muito poderoso são o *scanning* paralelo, a detecção do estado de *hosts* pelos *pings* paralelos, a detecção de filtragem de portas e a flexibilidade na especificação de portas e alvos. Além disso, o nMap informa o estado de cada porta identificada como aberta (que aceita conexões), filtrada (existe um *firewall* que impede que o nMap determine se a porta está aberta ou não) ou não filtrada.

Segundo Aslan [44], o nMap tem sido usado para explorar falhas de segurança em diversos estudos e levantar vulnerabilidades em redes de computadores.

Para que as organizações detectem a ação destes *scanners*, os sistemas de detecção de intrusão (IDS) podem ser utilizados. Esse tipo de sistema faz o reconhecimento de padrões de *scanning*, de forma a alertar o administrador de segurança sobre tentativas de mapeamento da rede da organização.

Portanto o uso do nMap deve sempre ser acordado com a supervisão de rede, para evitar que o uso do sistema gere possíveis alertas de violação nos sistemas de segurança.

3.4 MÓDULO GET61850NODES

O módulo get61850nodes trabalha com o protocolo MMS na camada de aplicação do protocolo TCP/IP. Recebe do módulo netScanner, como entrada, uma lista de endereços IP ativos e parte para a etapa de descobrimento dos IEDs. Como saída, o módulo get61850nodes devolve ao módulo netScanner informações como: marca, modelo, versão de *firmware*, funções de proteção e *datasets* disponíveis.

Para descobrir quais elementos de rede são IEDs a partir de uma lista de endereços IP, o módulo get61850nodes cria uma instância de cliente MMS e tenta se conectar a um suposto servidor MMS em cada endereço IP da lista recebida. Para isso o módulo utiliza o serviço MMS *initiate*. Os elementos cujos endereços IP responderem positivamente a esta tentativa de conexão são prováveis IEDs. Em seguida é enviado o comando *identify* que recebe do servidor MMS as informações de marca, modelo e versão de *firmware*. A descrição detalhada da metodologia adotada para o descobrimento dos IEDs e posterior inventário das funções disponíveis será discutida no capítulo 6.

Por fim, o módulo get61850nodes reúne e organiza todos os dados obtidos sobre os IEDs gerando como saída um relatório completo para arquivamento. Outra saída gerada por este módulo é um relatório consolidado reunindo o endereço IP da lista recebida como entrada associado à marca, modelo e versão de firmware descobertos. Esta saída é enviada ao módulo netScanner.

Tanto a norma IEC 61850 quanto o protocolo MMS preveem a inclusão de parâmetros de configuração de funcionamento e operação dos relés, como as distâncias das zonas de atuação para relés 21, valores de *pick up* e *drop out* para relés de sobrecorrente, dentre outros. Porém alguns fabricantes ainda não programaram estas funcionalidades em seus equipamentos de acordo com o modelo proposto pela Norma. Mesmo para os modelos de equipamentos cujos fabricantes disponibilizam esta modelagem, muitas equipes de engenharia

e de projeto ainda não as utilizam. Desta forma, este trabalho se limitou a buscar as informações que se encontram disponíveis e utilizadas.

O relatório completo, contendo as funções de proteção e *datasets* descobertos fica arquivado para consulta futura e também para possibilitar comparação, apontando diferenças encontradas em caso de modificações feitas em dispositivos de rede ou em configurações de proteção em IEDs.

Os relatórios gerados obedecem à seguinte organização:

- Os relatórios são armazenados em diretórios.
- Cada novo teste na rede gera um novo diretório.
- Dentro dos diretórios são criados arquivos contendo dados coletados dos IEDs.
- Cada arquivo representa um IED.

Desta forma, quando se comparam conteúdos de diretórios de relatórios, as diferenças representam IEDs removidos ou inseridos na rede. Do mesmo modo, quando se comparam conteúdos de arquivos, as diferenças encontradas se referem a alterações de configuração de um IED. Estas comparações são efetuadas no módulo "*netScanner*".

4 IMPLEMENTAÇÃO DA PROPOSTA

Existem diversas ferramentas de *software* e linguagens de programação disponíveis no mercado que podem auxiliar no alcance dos objetivos definidos neste trabalho. Algumas opções foram objeto de análise e posterior escolha. Dentre elas destacam-se as linguagens de programação Lazarus, Delphi, C#, Java, LabView e Python. Dentre as ferramentas de apoio foram analisados os *softwares* Zabbix, Visual SNMP e nMap. Cada linguagem de programação, e cada ferramenta de *software* analisada, apresentam um conjunto de vantagens e desvantagens para as atividades aqui desempenhadas. Foi escolhida uma combinação das linguagens de programação Python 2.7 e LabView 2013 por apresentarem uma combinação de facilidades, pacotes e bibliotecas mais favoráveis ao contexto do experimento. A linguagem Python e sua biblioteca gráfica QT formaram a combinação ideal para a produção das interfaces gráficas para o usuário e para integração dos módulos do sistema, bem como para a produção das lógicas de controle e de manipulação de dados possibilitando a geração dos relatórios de ativos da subestação. A linguagem LabView trouxe a facilidade de se realizar a comunicação com os IEDs no nível do protocolo MMS através de suas bibliotecas de funções MMS. E finalmente, para descobrir todos os elementos de rede foi utilizada a técnica de *port scanning*. Foi escolhido para esta finalidade o *software* nMap. O fator de

maior influência para a escolha desta combinação da ferramenta nMap e destas linguagens de programação: LabView, Python e QT foi o fato de que todas elas estão publicadas em versões para as duas principais plataformas de sistemas operacionais: *Windows* e *Linux*. Portanto com estas escolhas, o sistema de gerenciamento de ativos para subestações é um sistema portável entre sistemas operacionais.

Para iniciar a compreensão da ideia, serão apresentados três diagramas na *Unified Modeling Language* (UML).

A Figura 12 apresenta um diagrama de caso de uso em UML, que dispõe as possibilidades de uso do sistema.

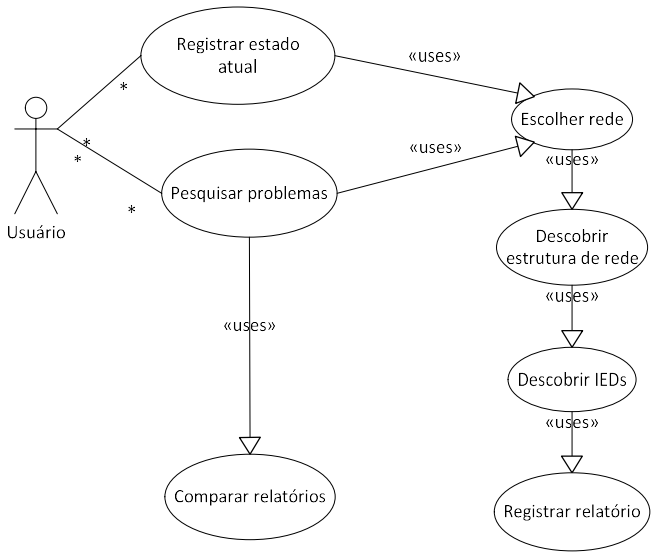


Figura 12 - Diagrama de caso de uso

O usuário pode executar uma rotina completa de registro dos ativos da rede de IEDs ou pode apenas solicitar a comparação de relatórios previamente criados, para pesquisar problemas ou simplesmente verificar se houve alguma alteração no sistema em uma data em especial.

A Figura 13 apresenta um diagrama de sequência em UML, que ilustra como os eventos ocorrem no tempo. Nesta figura aparecem ordenados os eventos que orientam o funcionamento do sistema e a sequência que os módulos de software respeitam durante suas interações.

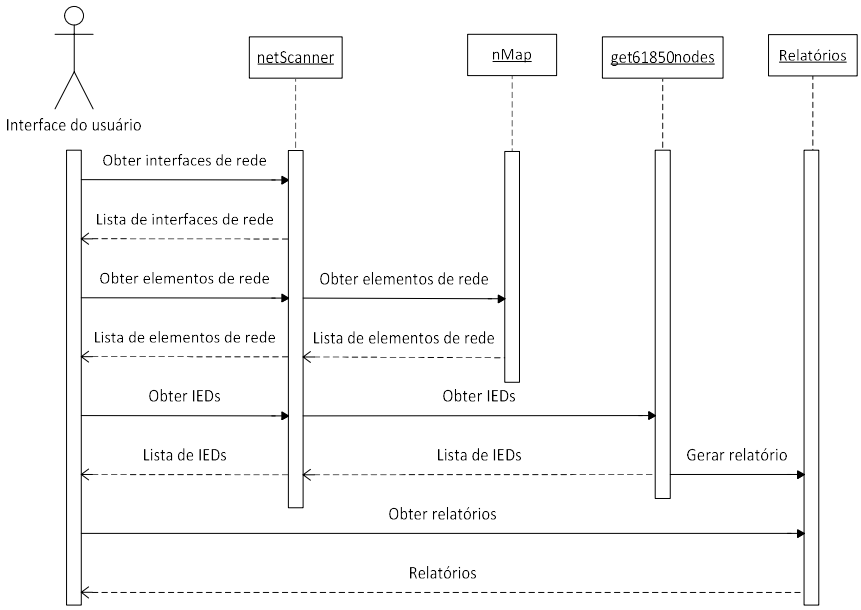


Figura 13 - Diagrama de sequência

Por fim, a Figura 14 apresenta um diagrama de atividade em UML que ilustra uma das atividades do sistema: a atividade de comparar relatórios.

A cada vez que o sistema é executado com a finalidade de gerar um novo registro de ativos de proteção na subestação, é gerado um diretório identificado com data e hora correntes.

Dentro deste diretório são colocados arquivos referentes aos hosts e aos IEDs encontrados na rede. Desta forma é possível realizar dois tipos de comparação:

- Comparação de estruturas de rede, onde são confrontados os arquivos presentes em cada diretório. Neste caso, a existência de arquivos diferentes indica uma alteração física na rede
- Comparação de configuração de IED, onde são confrontados os conteúdos dos arquivos. Neste caso, a existência de conteúdos diferentes indica uma alteração lógica na rede, alterações de conteúdo ou de alguma parametrização nos IEDs.

As diferenças eventualmente encontradas são exibidas na interface gráfica no programa netScanner.

Quando nenhuma diferença é encontrada, o sistema exibe mensagens informando que o conteúdo dos diretórios comparados, ou dos arquivos comparados, são idênticos.

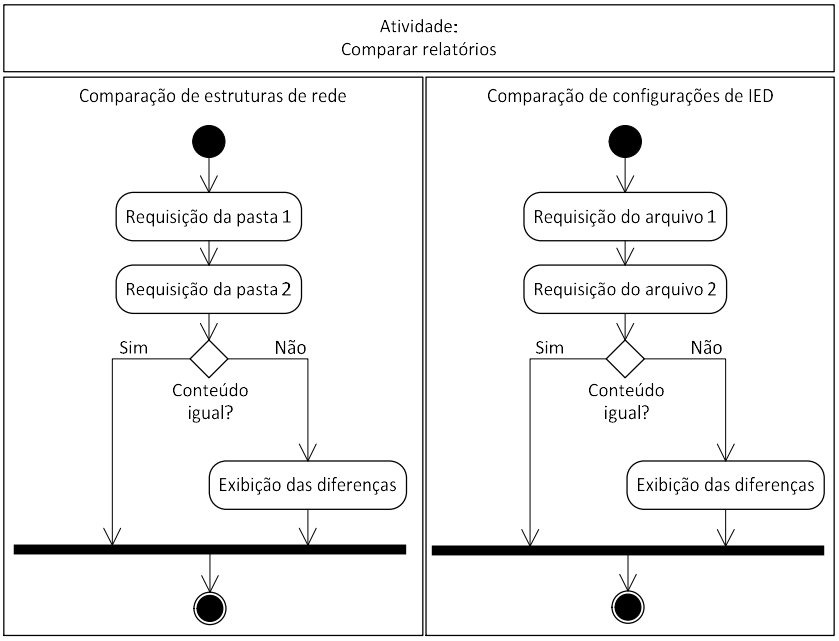


Figura 14 - Diagrama de atividade

Para distribuir o sistema foi compilado um pacote de instalação que inclui todos os pré-requisitos necessários para seu pronto funcionamento. Isso inclui o *runtime* do LabView e do Python, bem como o *software* nMap. Assim a instalação deste sistema fica simples para os usuários. As licenças de uso destes softwares são livres para uso acadêmico e não comercial, conforme documentação disponível nos sítios de internet de cada fornecedor citado.

4.1 DETALHAMENTO

Para a composição do sistema foram escritos dois programas: o primeiro programa se chama *netScanner* e o segundo programa se chama *get61850nodes*. O programa *netscanner* se comunica com nMap para descobrir a rede, e se comunica com o programa *get61850nodes* para descobrir os IEDs, como mostra a Figura 15.

O programa netScanner está listado no anexo 5 e foi integralmente escrito para este estudo, utilizando as bibliotecas padrão do Python 2.7 e do QT3. O programa nMap é uma ferramenta pronta. O programa get61850nodes está listado no anexo 6 e foi integralmente desenvolvido para este estudo, utilizando as bibliotecas padrão do Labview 2013 e o *toolkit* de bibliotecas para o protocolo MMS.

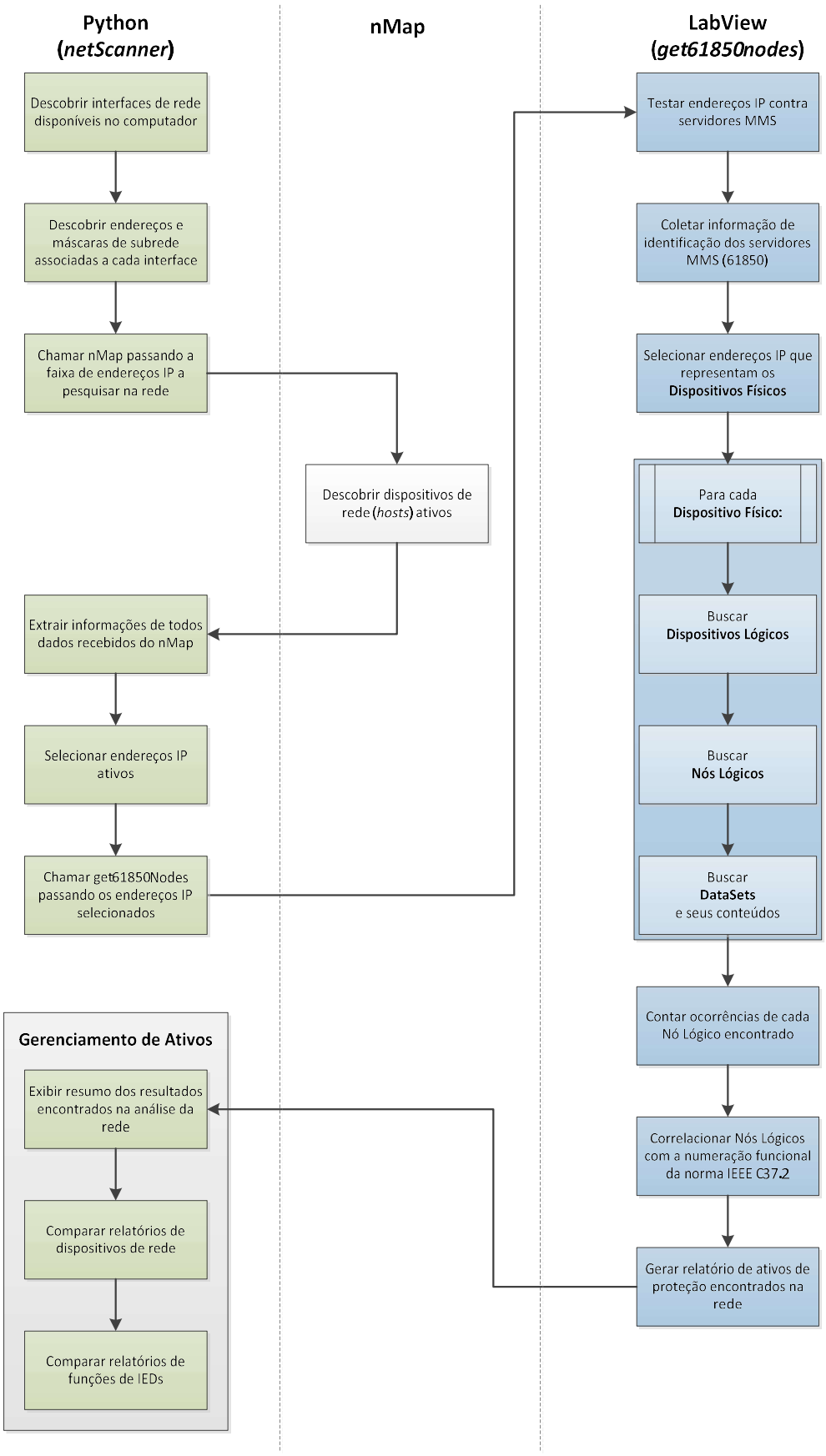


Figura 15 - Esquema de funcionamento do sistema

O programa netScanner é a parte do sistema escrita em Python e QT (Figura 16), que tem a finalidade de permitir ao usuário a escolha de alguns parâmetros que serão passados ao nMap para que se possa iniciar o processo de *port scanning* na rede. Além disso, o netScanner recolhe e organiza os resultados obtidos com o nMap e organiza os parâmetros necessários para a chamada do segundo programa desenvolvido para este sistema: o get61850nodes.

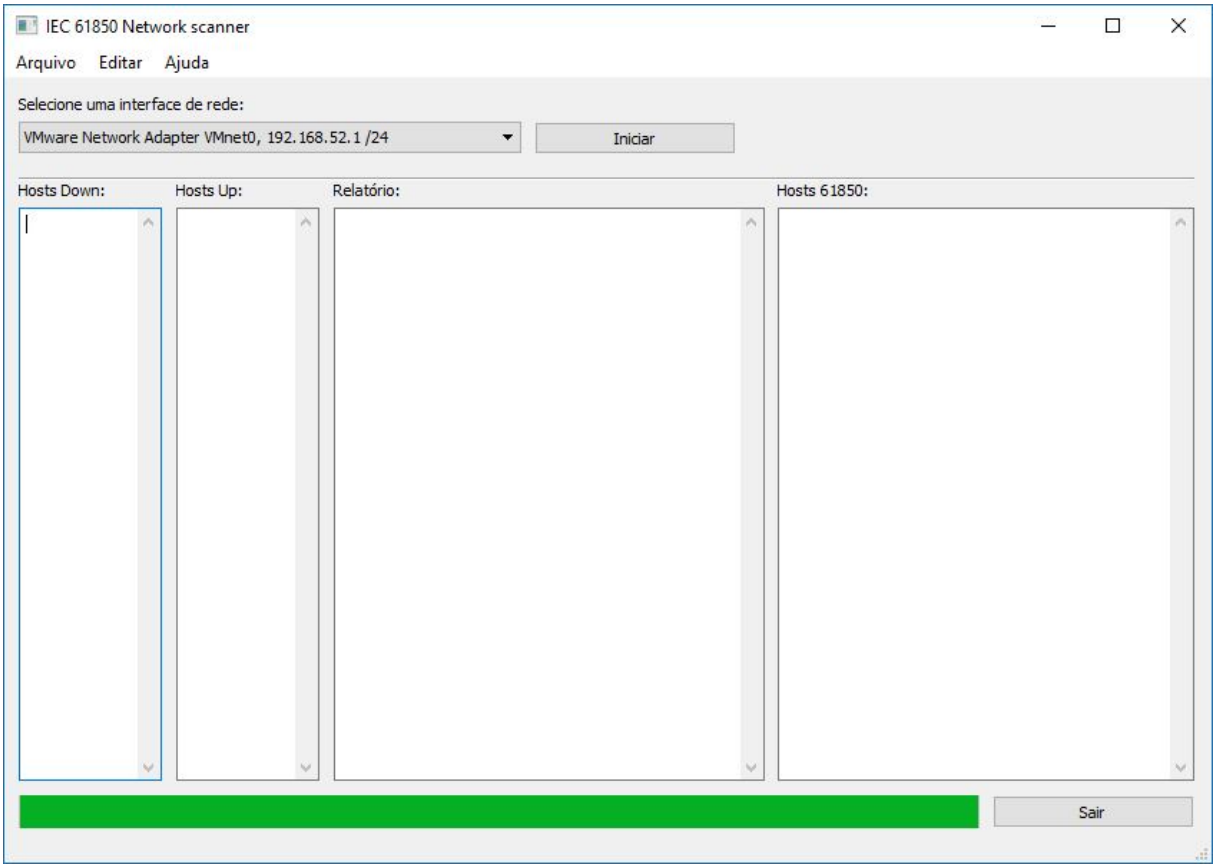


Figura 16 - Interface gráfica do programa netScanner

Atualmente é muito comum o uso de *notebooks* ou outros computadores que apresentem mais de uma interface de rede, inclusive de máquinas virtuais que eventualmente estejam instaladas no computador de testes, hospedeiro do sistema de gerenciamento de ativos. Por exemplo, um *notebook* costuma apresentar pelo menos duas interfaces de rede: uma para redes ethernet e uma para redes sem fio (802.11x).

Ao se iniciar o módulo netScanner, o programa interroga o sistema operacional solicitando as interfaces de rede disponíveis. No sistema operacional *Windows* esta etapa é realizada utilizando o comanto "netsh". A Figura 17 mostra o retorno do sistema operacional para o comando "netsh".

```
Configuration for interface "Local Area Connection* 12"
    DHCP enabled:                         Yes
    InterfaceMetric:                      25

Configuration for interface "Ethernet"
    DHCP enabled:                         No
    IP Address:                           192.168.1.1
    Subnet Prefix:                        192.168.1.0/24 (mask 255.255.255.0)
    InterfaceMetric:                      35

Configuration for interface "VMware Network Adapter VMnet0"
    DHCP enabled:                         No
    IP Address:                           192.168.52.1
    Subnet Prefix:                        192.168.52.0/24 (mask 255.255.255.0)
    InterfaceMetric:                      35

Configuration for interface "VMware Network Adapter VMnet8"
    DHCP enabled:                         No
    IP Address:                           192.168.5.1
    Subnet Prefix:                        192.168.5.0/24 (mask 255.255.255.0)
    InterfaceMetric:                      35

Configuration for interface "Ethernet 2"
    DHCP enabled:                         Yes
    InterfaceMetric:                      35

Configuration for interface "Wi-Fi"
    DHCP enabled:                         Yes
    IP Address:                           172.16.10.146
    Subnet Prefix:                        172.16.10.0/24 (mask 255.255.255.0)
    Default Gateway:                      172.16.10.1
    Gateway Metric:                       0
    InterfaceMetric:                      55
```

Figura 17 - Resultado do "netsh" em um sistema operacional *Windows*.

No sistema operacional *Linux* esta etapa é realizada utilizando o comando "ifconfig", cuja resposta está ilustrada na Figura 18.

```
eth0      Link encap:Ethernet  Endereço de HW 00:0C:29:0D:54:91
          BROADCASTMULTICAST  MTU:1500  Métrica:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          IRQ:67 Endereço de E/S:0x2024

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          UP LOOPBACKRUNNING  MTU:16436  Métrica:1
          RX packets:1367 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1367 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:0
          RX bytes:99905 (97.5 KiB)  TX bytes:99905 (97.5 KiB)
```

Figura 18 - Resultado do "ifconfig" em um sistema operacional *Linux*.

Quando o programa netScanner recebe a lista de interfaces de rede disponibilizada pelo sistema operacional se inicia o tratamento de dados que identifica as interfaces ativas. As

interfaces ativas são aquelas que estão conectadas a uma rede e que possuem endereço IP e máscara de sub-rede configurados.

Este conjunto de interfaces ativas é apresentado ao usuário que deverá, a partir deste ponto, informar ao programa qual das interfaces de rede disponíveis em seu equipamento está de fato conectada à rede de automação, como mostra a Figura 19.

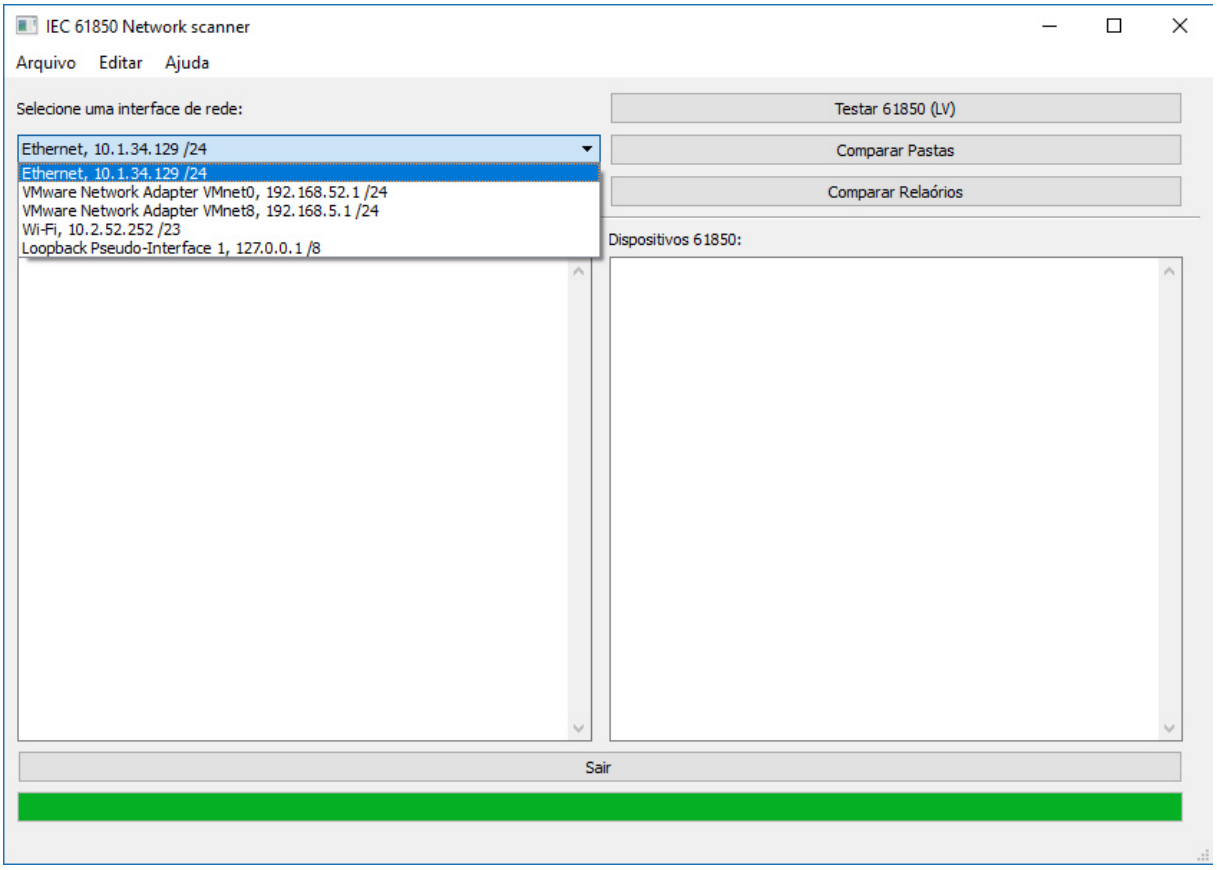


Figura 19 - Seleção de interfaces de rede

Neste momento o módulo netScanner está pronto para se comunicar com o módulo nMap e dar início ao *port scanning* na rede. Quando o usuário clica no botão "Iniciar" que aparece na Figura 20, é iniciado o processo de *port scanning* do nMap sobre a rede selecionada.

O módulo do nMap recebe do programa netScanner a rede e a máscara de sub-rede que deverá ser pesquisada. De posse desta informação inicia-se a busca por todos os elementos de rede que estejam conectados e que possuem, portanto, interfaces de rede configurada com um endereço IP e um endereço MAC.

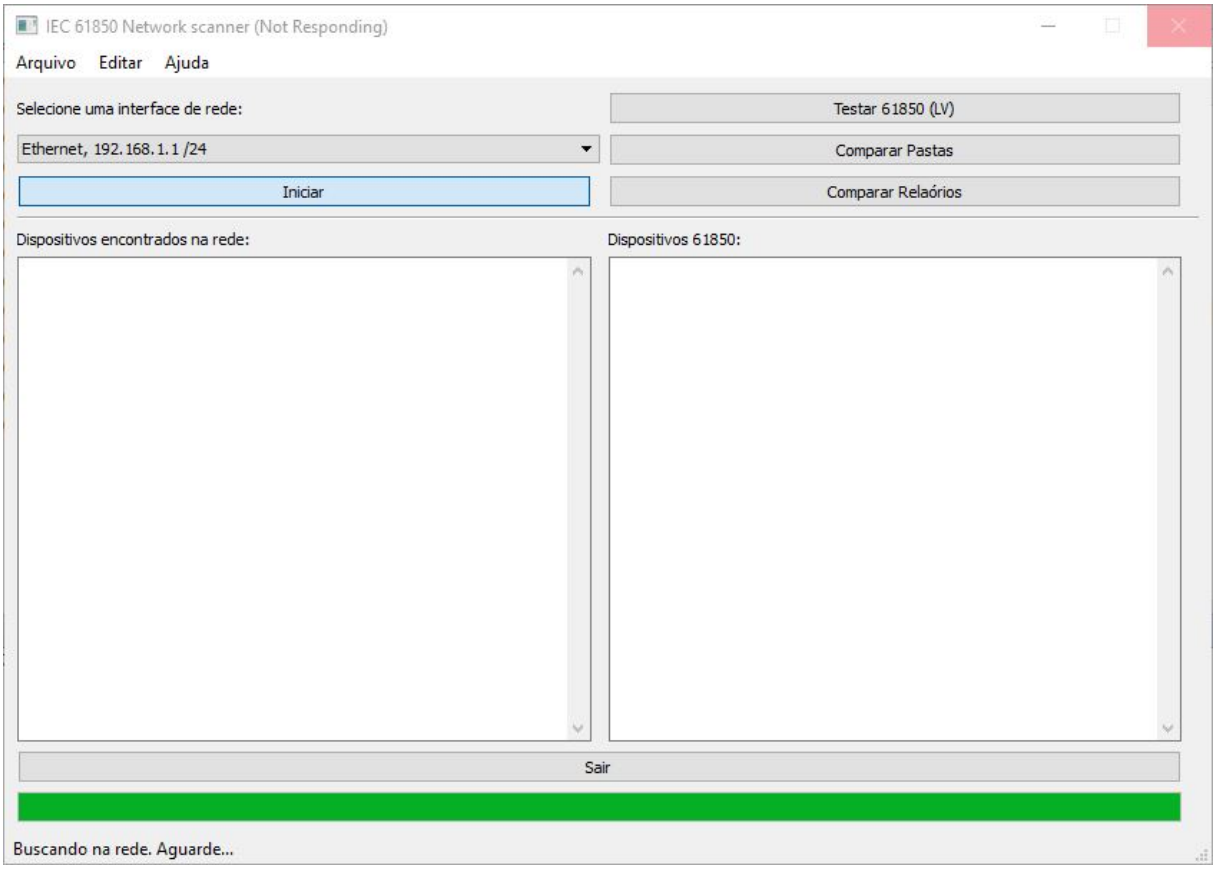


Figura 20 - Tela inicial do *netScanner*

A listagem de retorno deste processo é bastante extensa e pode ser vista no Anexo 1 (para a rede de testes 1) e no Anexo 2 (para a rede de testes 2).

Ao fim do processo de pesquisa na rede executado pelo nMap o controle do sistema volta ao módulo netScanner.

A próxima etapa é garimpar os dados da listagem de retorno do nMap e extrair algumas informações importantes para a continuidade do processo de descobrimento de IEDs. A Figura 21 mostra tais informações extraídas da rede de testes 1. São elas:

- Endereço IP;
- Endereço MAC;
- Fabricante da interface de rede;
- Sistema operacional embarcado.

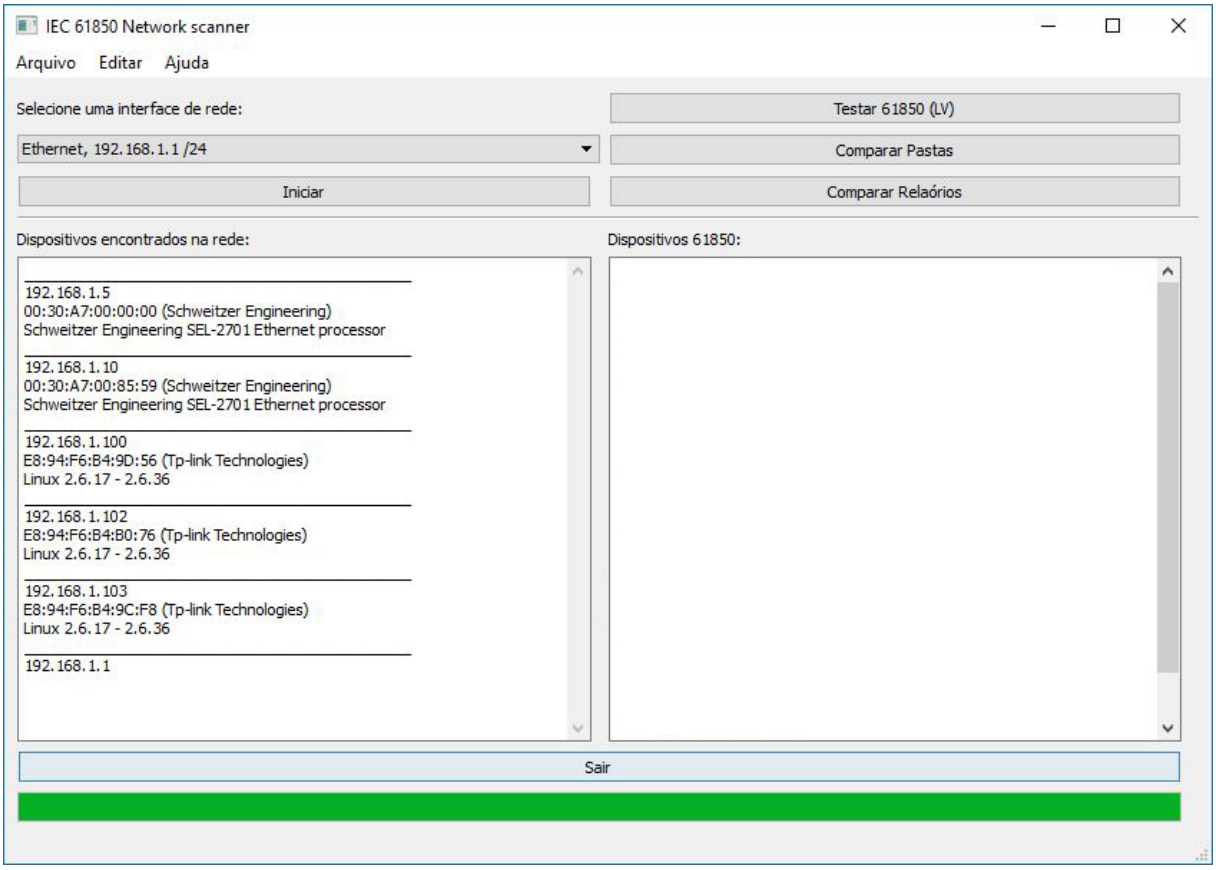


Figura 21 - Retorno do nMap filtrado, para a rede de testes 1

Em alguns casos, sistemas de segurança presentes nos *hosts* previnem certos tipos de consultas feitas pelo nMap, pois levantam suspeita de ataque cibernético. Isso pode fazer com que não se consigam alguns dados desta lista apresentada na Figura 21 acima, porém, o dado mais importante para o processo é o endereço IP. Conseguir o endereço IP dos equipamentos é uma atividade que não apresenta dificuldade nestes testes. Os endereços IP descobertos nesta etapa se referem todo e qualquer dispositivo de rede ou *host* conectado e ativo.

A próxima etapa, seguindo o fluxograma da Figura 15 é acionar o módulo get61850nodes, passando para ele os endereços IP descobertos na rede para identificar entre eles se existem IEDs.

O programa get61850nodes foi escrito em LabView e se destina a identificar dentre os dispositivos de rede (*hosts*) identificados pelo nMap, quais são IEDs (Figura 22) e ainda, dentre os IEDs quais são as funções de proteção disponíveis e os *datasets* preparados para publicação na rede.

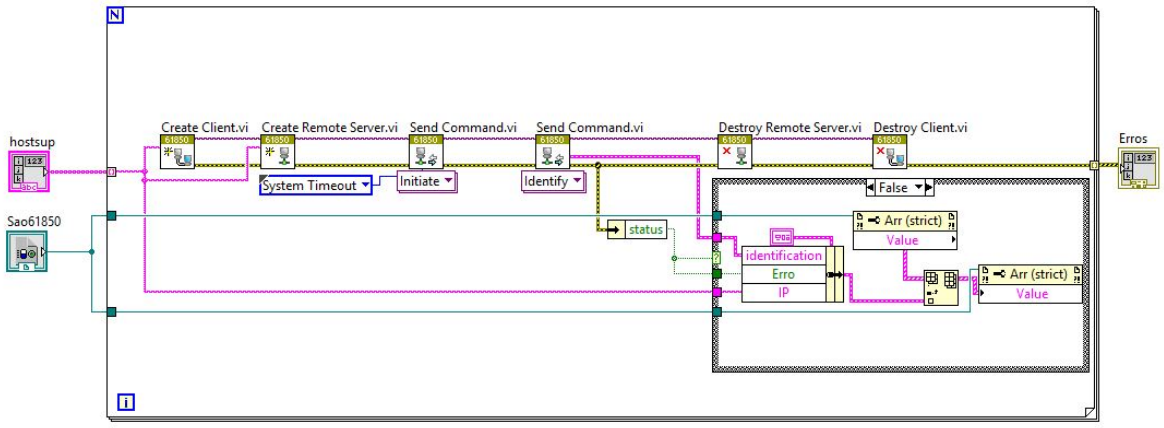


Figura 22 - Código LabView que descobre os servidores MMS na rede.

Este programa funciona de maneira transparente ao usuário, de forma que não é necessária interação com interfaces gráficas ou textuais.

Ao receber uma lista de endereços IP, o primeiro passo do programa é fazer a identificação dos IEDs na rede (*Logical Devices*), e depois buscar os nós lógicos (LN) de proteção, disponíveis em cada IED como mostra a Figura 23.

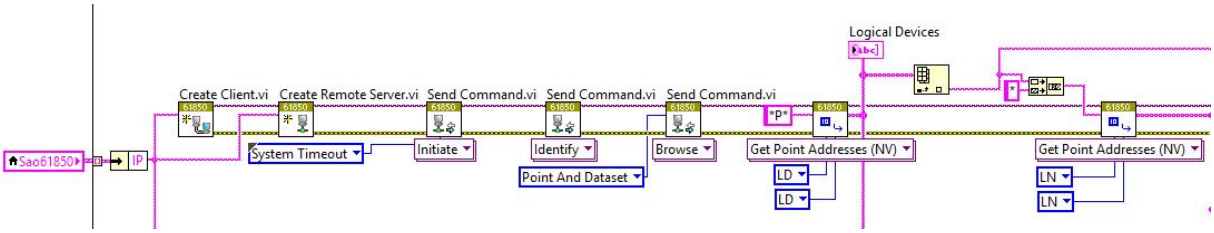


Figura 23 - Código LabView que descobre os LN de proteção.

A identificação dos IEDs é feita com o uso dos serviços MMS *initiate, e identify*. O módulo get61850nodes cria um cliente MMS no computador onde está rodando. Este cliente testa cada endereço IP recebido do módulo anterior, tentando criar uma conexão com um possível servidor MMS. Em seguida envia os comandos de início e de identificação. O comando de início (*initiate*) inicia a conexão no protocolo MMS. O comando de identificação (*identify*) solicita ao servidor MMS uma mensagem padronizada pelo protocolo que contém o nome do fabricante, o modelo do equipamento e a versão do *firmware* instalado, conforme mostra a Figura 24.

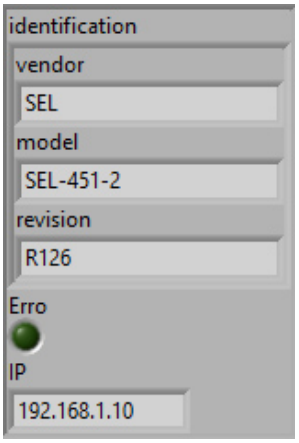


Figura 24 - Resposta do servidor MMS ao comando *identify*

Caso o *host* não responda às solicitações do cliente este endereço IP será descartado, pois não se trata de um IED. Caso o host responda positivamente à conexão e aos comandos de início e de identificação, o módulo get61850nodes assume que o endereço IP testado pertence a um servidor MMS e que este é um IED. Ainda, quando a resposta é positiva, o programa coleta os dados do fabricante, modelo e versão do *firmware* do IED. Após isto o programa busca no servidor MMS do IED quais são os LD e os LN de proteção disponíveis (Figura 25) e armazena a resposta em memória.

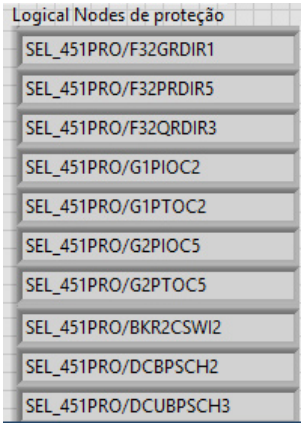


Figura 25 - Resposta do IED: LN de proteção

A Figura 26 mostra o próximo passo, que é a busca dos *datasets* publicáveis e seus conteúdos.

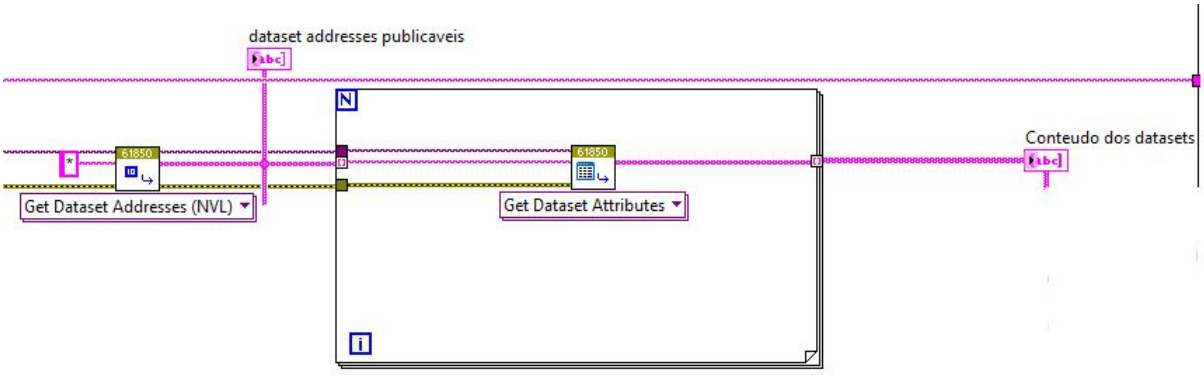


Figura 26 - Código LabView que descobre os datasets.

A Figura 27 ilustra a resposta do IED para a consulta aos conteúdos dos *datasets* de proteção preparados para publicação.

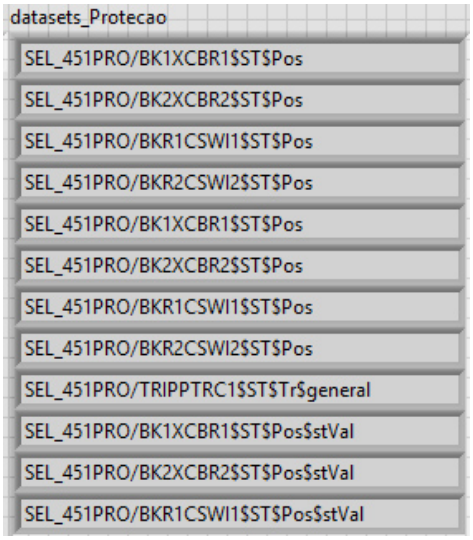


Figura 27 - Conteúdo dos *Datasets* de proteção enviados pelo IED

Estes dados são armazenados em memória para posterior composição do relatório de cada IED.

O módulo get61850nodes conta as ocorrências de cada *Logical Node* recebido do IED e faz a correspondência com as funções de proteção da norma ANSI (*American National Standards Institute*)/IEEE (*Institute of Electrical and Electronics Engineers*) C37.2-1996 (IEEE *Standard Electrical Power System Device Function Numbers and Contact Designations*) de acordo com a Tabela 5, como ilustra a Figura 28.

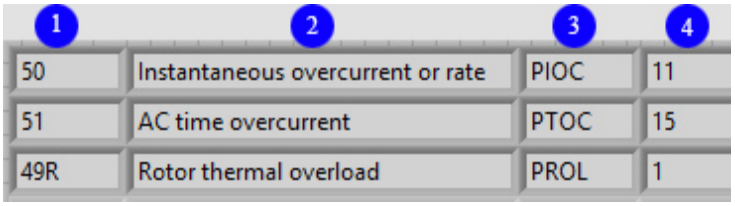


Figura 28 - Número de ocorrências de LN x função de proteção ANSI.

Onde:

1. Numeração da função de proteção ANSI
2. Descritivo da função de proteção ANSI
3. LN
4. Número de ocorrências do LN

Tabela 5 - Correspondência entre LN e funções ANSI (parcial).

Functionality	**IEEE C37.2 *reference***	***Defined in* IEC 61850-5**	***Modeled in* IEC 61850-7-4**
Distance	21	PDIS	PDIS, PSCH
Volt per Hz	24	PVPH	PVPH
(Time) Under voltage	27	PTUV	PTUV
Directional power /reverse power	32	PDPR	PDOP, PDUP
Loss of field/under excitation	40	PUEX	PDUP
Reverse phase or phase balance current	46	PPBR	PTOC
Phase sequence voltage	47	PPBV	PTOV
Thermal overload	49	PTTR	PTTR
Rotor thermal overload	49R	PROL	PTTR
Instantaneous over current or rate of rise	50	PIOC	PIOC
AC time over current	51	PTOC	PTOC
Voltage controlled/dependent time over current	51V	PVOC	PVOC
(Time) Overvoltage	59	PTOV	PTOV
Voltage or current balance	60	PVCB	PTOV, PTOC
Earth fault / Ground detection	64	PHIZ	PHIZ
Rotor earth fault	64R	PREF	PTOC
Stator earth fault	64S	PSEF	PTOC
Interturn fault	64W	PITF	PTOC
AC directional over current	67	PDOC	PTOC
DC time over current	76	PDCO	PTOC
Phase angle or out-of-step	78	PPAM	PPAM
Frequency	81	PFRQ	PTOF, PTUF, PFRC
Carrier or pilot wire protection	85	RCPW	PSCH
Differential	87	PDIF	PDIF

Depois destes passos, o programa gera os relatórios contendo todas as informações encontradas sobre os elementos de rede e sobre os IEDs da rede de automação da estação. Em seguida os dados adquiridos e o controle do processo são devolvidos ao programa netScanner.

Por fim, o programa netScanner recolhe os dados dos IEDs obtidos pelo módulo get61850nodes e gera um resumo do relatório de ativos de proteção encontrados na rede de automação, contendo marca, modelo, versão do *firmware* e o endereço IP de cada IED encontrado.

5 VALIDAÇÃO DA PROPOSTA

Para este estudo foram montadas duas redes distintas de IEDs de teste. Foram utilizados dois laboratórios diferentes, com o objetivo de validar o experimento em ambientes distintos, no que se refere ao tamanho das redes, ao número de elementos conectados e contando ainda com uma maior diversidade de fabricantes e de modelos de equipamentos, tanto para *hosts* e dispositivos de rede quanto para IEDs.

A primeira rede (rede de testes 01) foi montada em um dos laboratórios da UFF, contando com dois modelos de IEDs de um mesmo fabricante e dispositivos de rede associados, como mostram a Figura 29 e a Figura 30. A Figura 29 mostra o diagrama da rede de teste 1.

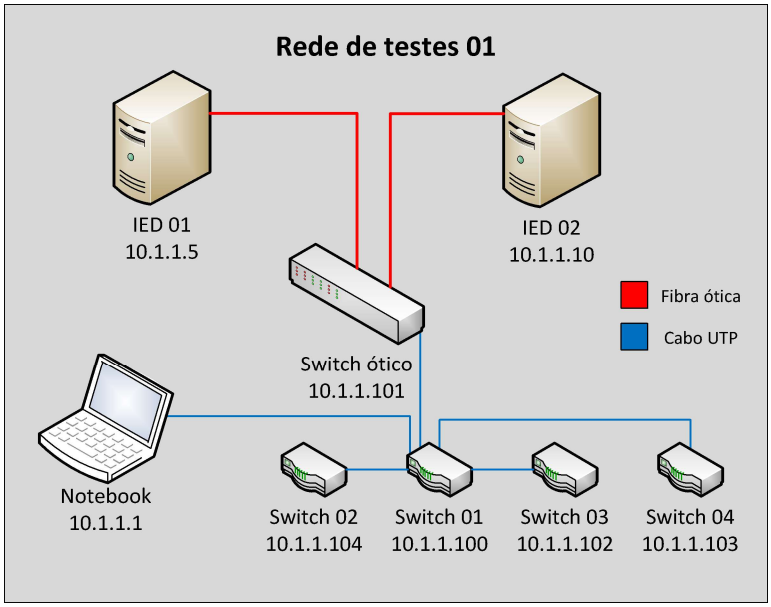


Figura 29 - Rede de testes 01: Diagrama

A Figura 30 mostra o arranjo físico da rede de testes 1.

Figura 30 - Rede de testes 01: Arranjo Físico

A segunda rede, (rede de testes 2) foi montada em um dos laboratórios de Furnas e conta com outros dois IEDs de outro fabricante, diferentes da rede de testes 1 e diversos outros equipamentos conforme a Figura 31 e a Figura 32. Os equipamentos que se encontram dedicados a atividades que não são objeto deste estudo também foram detectados com sucesso na etapa de identificação e mapeamento da rede como um todo.

A Figura 31 mostra o diagrama da rede de teste 2.

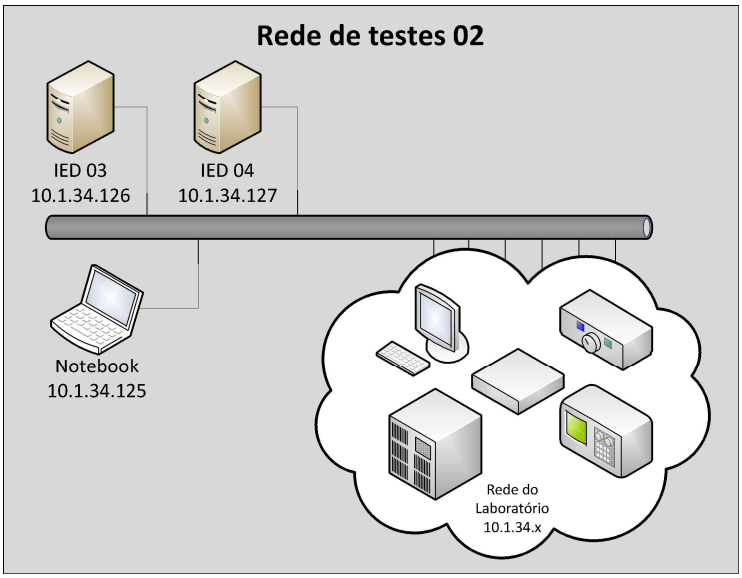


Figura 31 - Rede de testes 02: Diagrama

A Figura 32 mostra o arranjo físico da rede de testes 2.

Figura 32 - Rede de testes 2: Arranjo físico

A Figura 33 mostra o resultado do processo quando executado na rede de testes 1.

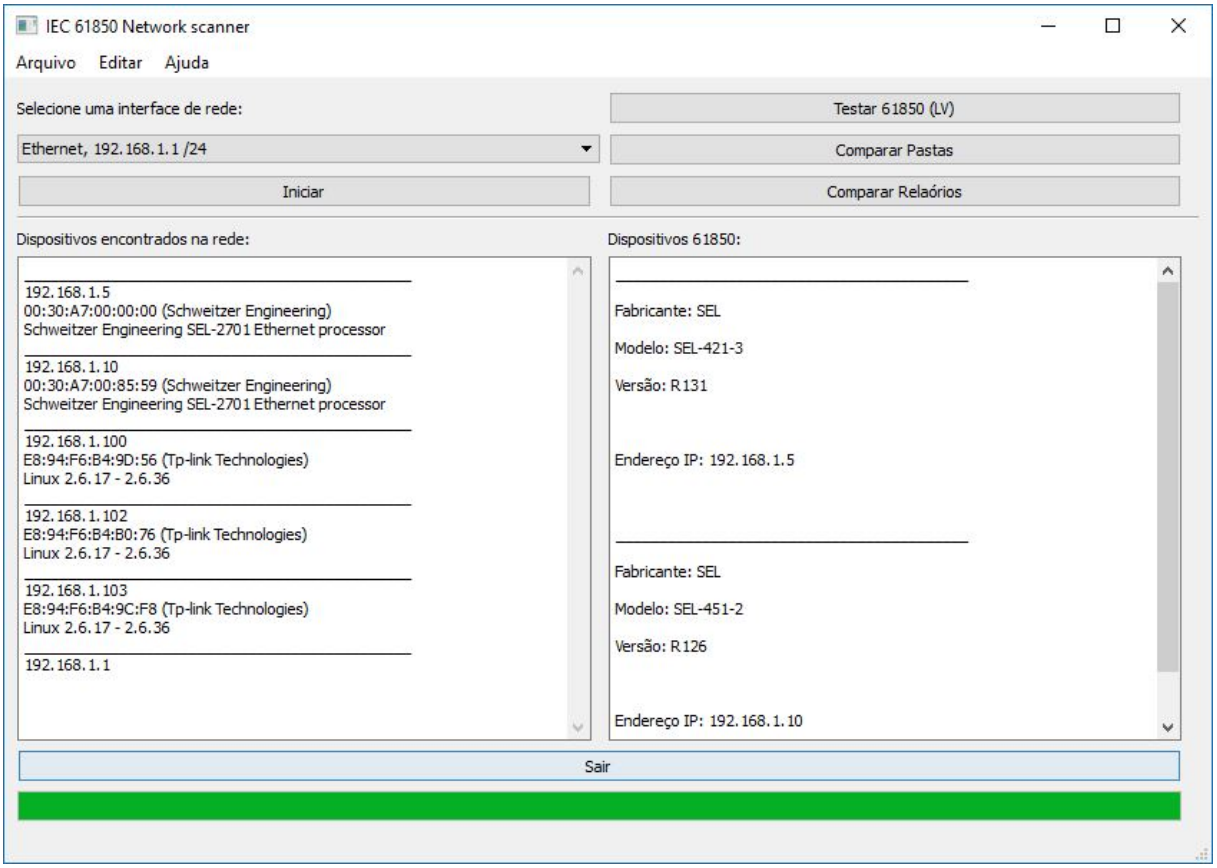


Figura 33 - Resumo do relatório apresentado para a rede de testes 1.

A Figura 34 mostra o resultado do processo quando executado na rede de testes 2.

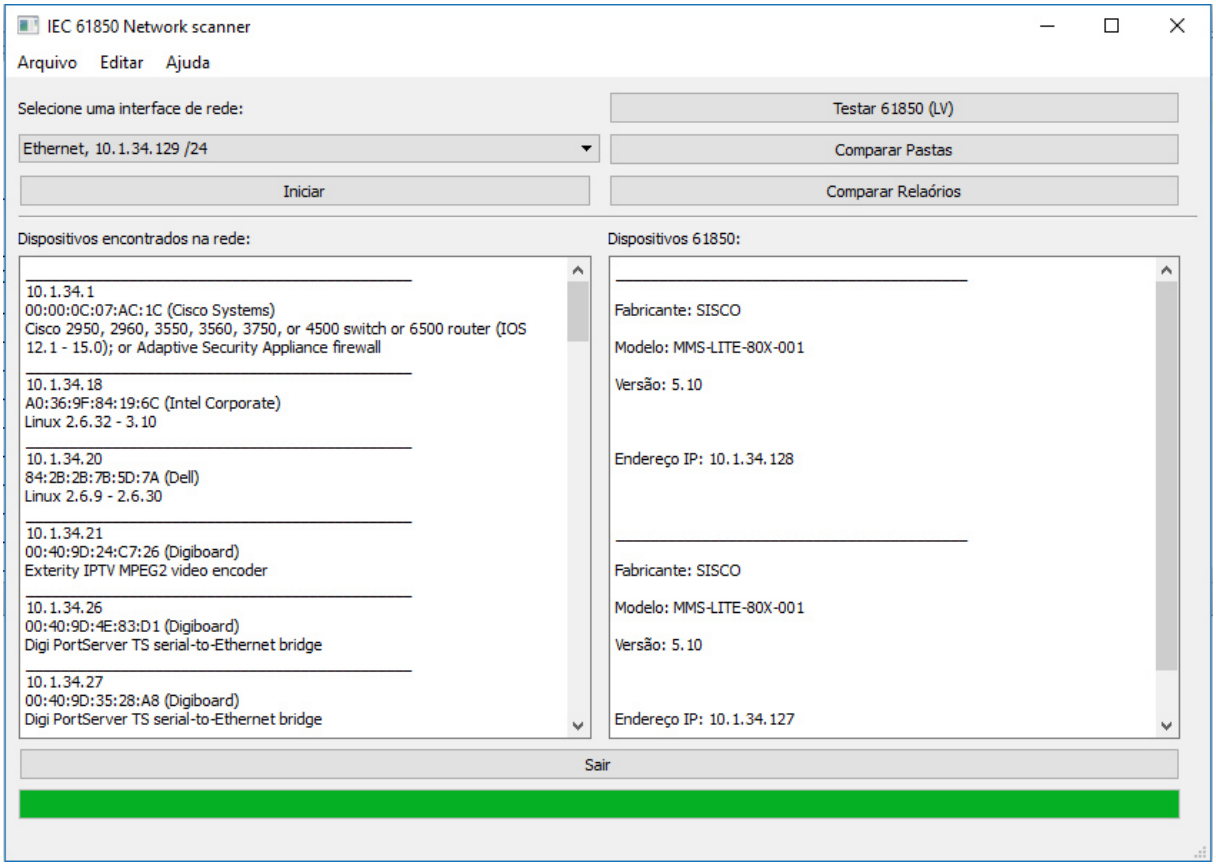


Figura 34 - Resumo do relatório apresentado para a rede de testes 2.

A comparação de relatórios aparece nas figuras 32 e 33. Os relatórios gerados podem ser comparados com a finalidade de localizar diferenças na rede como mostra a Figura 35, ou nos IEDs (em *Logical Nodes* ou em *Datasets*) como mostra a Figura 36.

Quando um IED é removido da rede, o arquivo que o representa aparece somente na lista da esquerda. Quando um IED é incluído na rede, o arquivo que o representa aparece somente na lista da Direita. A figura 32 mostra a retirada de um IED da rede e a colocação de outro IED, visto que o arquivo que aparece na listagem da direita não existia na esquerda e o da esquerda por sua vez também não existia na direita. Isto representa a substituição de um IED por outro.

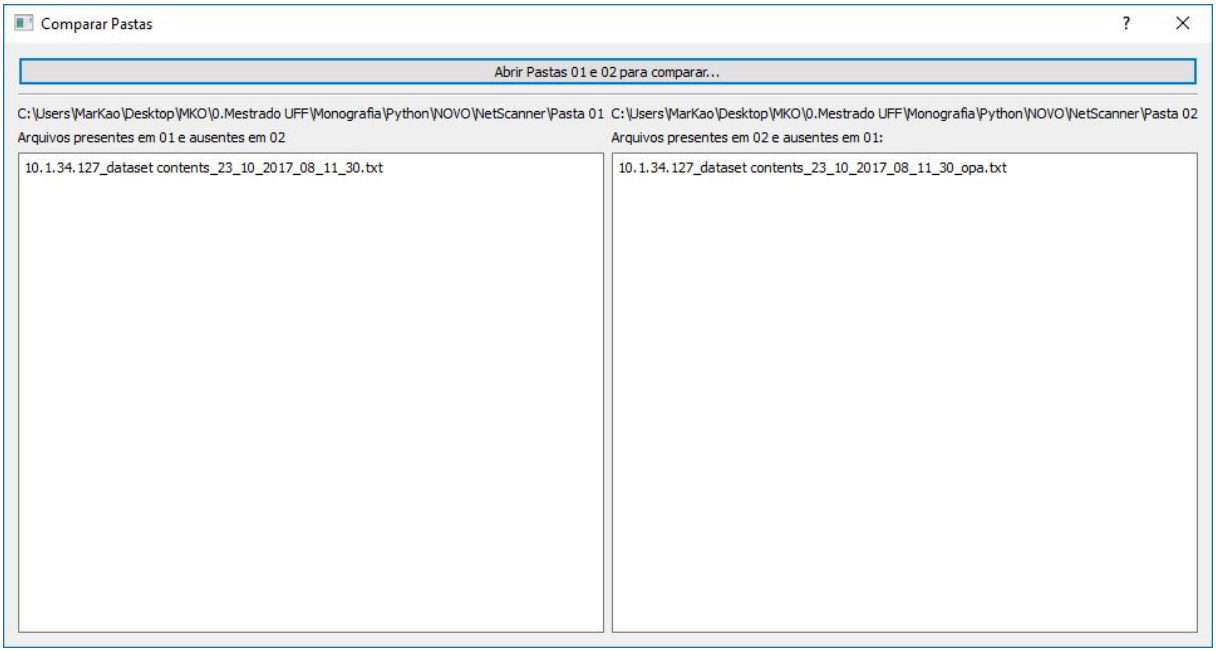


Figura 35 - Detecção da modificação na presença de dispositivos na rede.

Na Figura 35 está ilustrada uma situação de diferença encontrada entre duas pastas de relatórios gerados anteriormente. Quando os dados coletados dos IEDs geram relatórios iguais, e estes são confrontados neste sistema, o programa exibe uma mensagem informando que os conteúdos das pastas são idênticos.

A Figura 36 mostra todas as diferenças de configuração de proteção encontradas no IED.

Estas diferenças sugerem que o IED foi substituído. Elas mostram que um modelo de IED foi substituído por outro modelo que está com a parametrização muito diferente, indicando que o mesmo não está configurado para exercer exatamente as mesmas funções que seu antecessor. Quando os dados colhidos de um IED são comparados com os de outro IED e não aparecem diferenças, o sistema exibe mensagem informando que os arquivos são idênticos.

Para que se tenha uma boa rastreabilidade dos eventos ocorridos nos ativos da rede do SAS é recomendável executar um registro de relatório a cada intervenção técnica executada na rede, ou nos IEDs. Pode-se ainda, por meio do estabelecimento de procedimentos de uso, definir um período regular de registros do estado da rede de IEDs a fim de detectar falhas ou problemas oriundos de eventos imprevistos.

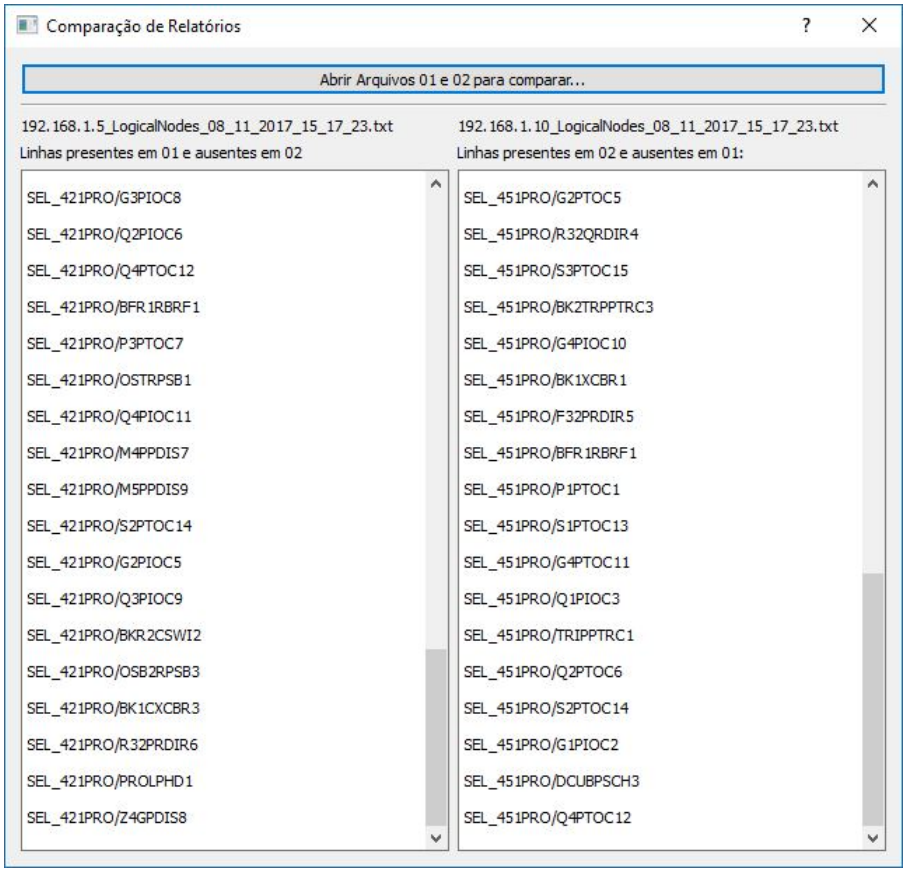


Figura 36 - Detecção de modificação nas configurações de um IED

6 CONCLUSÃO

A partir dos passos descritos neste trabalho, com a varredura de uma rede TCP/IP e o descobrimento de servidores MMS, foi possível inventariar automaticamente os IEDs de uma rede de automação em subestações.

Para se ter acesso à rede de IEDs é preciso uma série de autorizações. Observa-se a existência de ritos formais. Por questões de segurança, não raramente estas redes são redes isoladas, portanto é necessário acesso físico aos equipamentos. É comum que se obtenham documentos que autorizem a entrada na estação e a conexão de um notebook no *switch* de acesso à rede e a execução do trabalho. Normalmente estes documentos são programados com antecedência, envolvem aprovação de entidades internas às organizações ou mesmo externas, como o ONS. Os documentos descrevem o trabalho a ser executado, o tempo necessário para execução, e um plano de contingência em caso de eventual emergência durante a execução do trabalho.

O sistema proposto provou ser uma ferramenta útil para auxiliar na gestão de ativos de proteção aderentes à norma IEC 61850 em subestações, podendo alimentar sistemas de gestão

que necessitam de dados de entrada confiáveis, atualizados, únicos e consistentes, contribuindo para as pesquisas na área de gestão de ativos.

Este sistema provê um modo automatizado de monitorar a plataforma existente em uma instalação elétrica (subestação), tanto no nível de equipamentos (*hardware*) quanto de configuração (*software*). IEDs mais novos, conformes com a norma IEC 61850 e corretamente configurados foram corretamente detectados e puderam ter suas configurações lidas corretamente. IEDs mais antigos, com problemas de conformidade com a norma IEC 61850 e outros dispositivos conectados à rede, não aderentes à norma IEC 61850 foram detectados como *hosts* de rede ou mesmo como IEDs, porém com um conjunto bastante limitado de informações lidas pelo sistema.

Com este sistema é possível, mediante as devidas credenciais relativas às questões de segurança cibernética, contar com a facilidade de conectar um notebook em uma rede de automação, proteção e controle de uma subestação e, ao clique de um botão, efetuar o levantamento de todos os elementos conectados e suas funções de proteção ativas. Além disso, é possível descobrir os *datasets* publicados na rede e é possível salvar o estado da rede encontrado.

O objetivo principal deste trabalho foi atingido através do desenvolvimento dos programas netScanner e get61850nodes, e da aplicação da metodologia descrita, com a integração da ferramenta de software nMap ao sistema. Foi possível descobrir todos os elementos presentes em todas as redes de automação montadas para testes, e foi possível salvar um relatório contendo o estado da rede e de seus elementos, bem como as funções de proteção disponíveis e os datasets publicados.

A validação do sistema ocorreu com sucesso em duas redes distintas, cada uma com configurações diferentes, elementos diferentes, fabricantes diferentes, modelos diferentes e IEDs diferentes. Foi possível, em todos os cenários ensaiados, proceder todos os testes necessários para identificação dos elementos da rede, no que se refere aos hosts, inclusive os IEDs, e elementos associados como switches e roteadores.

O sistema se mostrou eficaz na identificação dos Dispositivos Físicos, dos Dispositivos Lógicos, dos Nós Lógicos e dos datasets de cada IED em todas as situações testadas.

Os relatórios gerados são suficientes para o registro de ativos e configurações de IEDs relativas à norma IEC 61850. Servem para auxiliar as equipes de engenharia e de manutenção tanto para registro dos ativos de proteção presentes em uma estação, bem como de suas

configurações disponíveis, quanto para identificação de alterações na rede ou nas configurações.

O sistema também se mostrou útil para apoiar a análise de fatores que podem impactar no desempenho da rede de automação, como, por exemplo, a identificação de *datasets* que podem representar mensagens GOOSE ou SV e que possam estar publicados sem necessidade, ocupando banda em uma rede que preza pelo alto desempenho e se submete a rígidos limites de atraso na propagação de mensagens, ditados pela norma IEC 61850.

O objetivo secundário, o de auxiliar nas pesquisas de problemas de comunicação, também foi alcançado quando o sistema apresentou uma forma de comparar os resultados obtidos em duas ocasiões diferentes.

Desta forma, se considerarmos a possibilidade de que o sistema seja executado com uma determinada periodicidade, existirá registro temporal, com data e hora em que foram criados, permitindo a determinação mais exata do "quando", do "onde" e do "porquê" alguma mudança ocorreu na rede.

O programa nMap tomou uma boa fatia do tempo total de cada ensaio realizado com o sistema.

Na rede de testes 1, a menor das redes ensaiadas, o processo se concluiu em aproximadamente 2 minutos.

Na rede de testes 2, muito maior em hosts, o processo se concluiu em aproximadamente 20 minutos.

Estes tempos foram considerados razoáveis, observando que:

- A velocidade não é um fator crítico neste sistema;
- Aproximadamente 90% destes tempos foram consumidos pelo programa nMap;
- O processo do nMap estava configurado para realizar mais testes contra os *hosts* do que o necessário para recuperar seus endereços IP e;
- É possível melhorar os tempos do nMap.

Ainda sobre o desempenho do sistema, é importante ressaltar que não foram contabilizados possíveis impactos no uso da banda da rede durante a execução do nMap, tendo em vista que o sistema proposto não se destina a monitoramento contínuo, em tempo real, da rede de IEDs.

O código fonte do sistema está disponível na plataforma colaborativa *GitHub* em https://github.com/marcoarj/NetScanner.

6.1 TRABALHOS FUTUROS

Este trabalho deixa algumas portas abertas para avançar no seu desenvolvimento.

A Norma prevê muitas situações que ainda não são aplicadas pelas equipes de engenharia e projeto das empresas de energia elétrica no Brasil.

Uma das funcionalidades mais interessante de se conseguir alcançar no futuro é a de buscar pela rede, de maneira automática, da mesma forma que foi conduzido este trabalho, os parâmetros de operação e funcionamento dos IEDs de proteção. Apesar da técnica já existir, isso só será possível quando, de fato, este recurso estiver em uso pelas empresas do setor elétrico.

Quando ocorrer uma maior adesão das empresas de energia elétrica ao modelo proposto pela norma IEC 61850, tanto por parte dos fabricantes quanto por parte das equipes de engenharia e projetos, será possível expandir as funcionalidades deste sistema. Desta forma será possível incluir nos relatórios mais informações úteis como, por exemplo, os ajustes das funções de proteção e outras parametrizações inerentes ao funcionamento dos IEDs.

É possível avançar no que se refere aos relatórios. Até o presente momento, os relatórios são de uso interno do programa. São relatórios de texto plano. É possível modelar os relatórios de acordo com novas necessidades, incluindo ou excluindo dados a pesquisar nos IEDs. É possível também prover uma modelagem para um relatório impresso, formatado de acordo com os padrões de layout e tipográficos adequados para determinado ambiente corporativo ou de pesquisa, conforme a necessidade.

Outro avanço a se considerar é a melhoria do tempo de execução do processo de *port scanning* utilizando o nMap. O processo de descoberta da rede tomou um tempo relativamente alto para sua conclusão durante os testes de validação. O processo de *port scanning* do nMap é o maior consumidor de tempo do sistema proposto. Em redes onde existem mais computadores ou servidores rodando sistemas operacionais *Windows* e *Linux* o nMap gasta mais tempo para terminar o seu processo, pois, na configuração utilizada, o programa investiga diferentes fragilidades de segurança em cada *host.* Existem diversas opções de chamada do programa nMap, diferentes das opções utilizadas nos ensaios conduzidos e descritos neste documento. O *software* nMap é um dos *port scanners* mais utilizados e pode ser empregado para realizar a auditoria de *firewalls* e de sistemas de detecção de intrusão, os *Intrusion Detection systems* (IDS). Este software também é capaz de determinar se um sistema tem falhas de implementação da pilha TCP/IP, que possam ser exploradas em ataques do tipo DoS (*Deny of Service* - Negação de Serviço). Além de mapear

as portas abertas dos sistemas, ele pode identificar o sistema operacional utilizado pelo alvo. Existem também opções de execução para informar sobre o número de sequência dos pacotes TCP, o usuário que está executando cada serviço relativo a uma determinada porta e o nome DNS (*Domain Name System*), entre outras. Cada uma destas funções toma um tempo de execução do nMap na rede, e nem todas elas são necessárias no contexto deste trabalho. É interessante avaliar outras opções de chamada do nMap disponíveis, de forma que se obtenham os resultados necessários em um tempo reduzido.

Outra possibilidade que se apresenta como trabalho futuro é o desenvolvimento de interfaces com o usuário mais dinâmicas e intuitivas, bem como a integração com ambiente *web* para consultas remotas e através de dispositivos móveis, como *tablets* e *smartphones*.

Também é possível evoluir a proposta de gestão de ativos e promover a integração com bases de dados relacionais para alimentar sistemas de suporte à tomada de decisão, de *business intelligence* (BI) e de inventário automático.

É possível desenvolver módulos que ampliem as utilidades deste sistema para o monitoramento online, integrando com sistemas SCADA, permitindo assim monitoramento da rede de IEDs a partir de centros de controle de sistema elétrico, ou de centros de controle de telecomunicações.

Pensando em um cenário de estudos e ajustes de proteção, seria possível adicionar módulos que permitam ainda a integração com redes de oscilografia e a configuração remota dos IEDs, tanto na parte relativa à comunicação segundo os preceitos da norma IEC 61850 quanto na parte relativa aos ajustes de operação e funcionamento dos dispositivos.

BIBLIOGRAFIA

[1] CHOOBINEH, M., MOHAGHEGHI S., A multi-objective optimization framework for energy and asset management in an industrial Microgrid, Journal of Cleaner Production 139, Elsevier, 2016

[2] LOVE P. E.D., ZHOU, J., Matthews J., Luo H., Systems information modelling: Enabling digital asset management, Advances in Engineering Software 102, elsevier, 2016

[3] CAMPOS, J., SHARMA, P., GABIRIA, U. G., JANTUNEN, E., BAGLEE, D., A big data analytical architecture for the Asset Management, The 9th CIRP IPSS Conference: Circular Perspectives on Product/Service-Systems, Procedia CIRP 64, Science Direct, Elsevier, 2017

[4] PARLIKAD, A. K., JAFARI, M., Challenges in infrastructure asset management, IFAC-PapersOnLine 49-28, Science Direct, elsevier, 2016

[5] HANAI, M., KOJIMA, H., HAYAKAWA, N., SHINODA, K., OKUBO, H., Integration of Asset Management and Smart Grid with Intelligent Grid Management System, IEEE Transactions on Dielectrics and Electrical Insulation Vol. 20, No. 6, IEEE, December 2013

[6] BROUS, P., HERDER, P., JANSSEN, M., Towards Modelling Data Infrastructures in the Asset Management Domain, Procedia Computer Science 61, Science Direct, Elsevier, 2015

[7] ONS, Operador Nacional do Sistema Elétrico, Submódulo 23.3 – Diretrizes e Critérios para Estudos Elétricos, Resolução Normativa n° 756/16, 16 de dezembro de 2016. Disponível em: <http://extranet.ons.org.br/operacao/prdocme.nsf/videntificadorlogico/4D565277AFFCC26783258099003DEA96/$file/Subm%C3%B3dulo%2023.3.pdf?openelement> Acesso em: 12/11/17

[8] LAZZARETTI, A. E., Segmentação, Classificação e Detecção de Novas Classes de Eventos em Oscilografias de Redes de Distribuição de Energia Elétrica. Tese de Doutorado - Curso de Engenharia Elétrica e Informática Industrial, Universidade Federal do Paraná, Curitiba, 2015

[9] Relatório de Análise : desligamentos forçados do Sistema de Transmissão / Agência Nacional de Energia Elétrica. – Brasília : ANEEL, 2016.

[10] FERREIRA, V.H., ZANGHI, R., FORTES, M.Z., SOTELO, G.G., SILVA, R.B.M., SOUZA, J.C.S., GUIMARÃES, C.H.C., GOMES Jr, S., A survey on intelligent system application to fault diagnosis in electric power system transmission lines, Electric Power Systems Research, Volume 136, Elsevier, 2016.

[11] FORTES, M.Z., FERREIRA, V.H., ZANGHI, R., Fault Diagnosis in Transmission Lines: Trends and Main Research Areas, IEEE Latin America Transactions, Volume: 13, Issue: 10, IEEE, 2015

[12] GERALDO, K.,. Proteção de Sistemas Elétricos de Potência. Vol. 1 e 2, 1999

[13] http://www.ebah.com.br/content/ABAAAfCLEAH/geracao-transmissao-energia-2012-protecao-por-reles?part=6, acessado em 08/11/2016

[14] http://www.ebah.com.br/content/ABAAAgMlgAK/modulo-07-rele-sobrecorrente, acessado em 08/11/2016

[15] https://selinc.com/pt/products/421/, acessado em 08/11/2016

[16] OLIVEIRA, P. R. P., et al. Sistemas abertos de supervisão e controle e subestações de energia. In : Congresso de Inovação Tecnológica em Energia Elétrica, II CITENEL, Salvador, 2003.

[17] RODRIGUES, J.R.M., Primeira subestação em funcionamento com IEC 61850. In : Simpósio de Automação de Sistemas Elétricos, VI SIMPASE, São Paulo, 2005.

[18] MESMAEKER, I., BRAND, K.P. e BRUNNER, C.. How to use IEC 61850 in protection and automation. In : ELECTRA - CIGRE, 2005. ISSN: 1286-1146.

[19] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC-61850, part 1: introduction and overview. 2003. IEC/TR 61850-1:2003(E).

[20] MACKIEWICZ, R. E., Overview of IEC 61850 and benefits. IEEE : 0-7803-9193-4/06, 2006.

[21] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC-61850, part 3: general requirements. 2002. CEI/IEC 61850-3:2002

[22] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC-61850, Part 4: system and project management. 2002. CEI/IEC 61850-4:2002.

[23] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC-61850, part 5: communication requirements for functions and device models. 2003. IEC 61850-5:2003(E).

[24] GURJÃO, E. C., SOUZA, B. A. e CARMO, U. A., A comunicação entre equipamentos de proteção na norma IEC 61850. São Paulo : Eletricidade Moderna, 2007. pp. 148-157. Vol. 397.

[25] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC-61850, part 6: substation automation system configuration description language. 2004. IEC 61850-6:2004(E).

[26] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 61850, part 7.1: basic communication structure for substation and feeder equipment - principles and models. 2003. IEC 61850-7-1:2003(E).

[27] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 61850, part 7.2: basic communication structure for substation and feeder equipment - abstract communication service interface (ACSI). 2003. IEC 61850-7- 2:2003(E).

[28] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC-61850, part 7.3: basic communication structure for substation and feeder equipment – common data classes. 2003. IEC 61850-7-3:2003(E).

[29] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC-61850, part 7.4: basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes. 2003. IEC 61850-7-4:2003(E).

[30] SANTOS, A. A., Automação elétrica com a IEC-61850. Universidade do Estado do Rio de Janeiro, Universidade Petrobras. Monografia de Especialização em Automação Industrial, Rio de Janeiro, 2007

[31] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC-61850, part 8.1: specific communication service mapping (SCSM) – mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3. 2004. IEC 61850-8- 1:2004(E).

[32] PEREIRA, A. C., Automação de subestações e usinas: estado da arte e tendências utilizando a norma IEC 61850. Simpósio de Automação de Sistemas Elétricos, VII SIMPASE, Salvador, 2007

[33] BASTOS, M. R. e CASTRO, E.. A evolução dos sistemas de proteção e controle com a IEC 61850. São Paulo : Eletricidade Moderna, 2005. pp. 168- 177. Vol. 374.

[34] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC-61850, part 10: conformance testing. 2005. IEC 61850-10:2005(E).

[35] PAULINO, M. E. C., Testes de conformidade em relés multifuncionais baseados na IEC 61850. In : Seminário Técnico de Proteção e Controle, VIII STPC, Rio de Janeiro, 2005.

[36] NEVES JÚNIOR, F., VALADIER, J. C., O protocolo de comunicação MMS para redes locias industriais, Curso de pós-graduação em informática industrial, CPGII

[37] MENDES, M.J., Magalhães, M, Redes Locais Industriais e Projeto de Padronização MAP/TOP, SBA: Controle e Automação, Vol. 2, n. 1, pp56-70, 1988

[38] TOMLINSON, J., Farb, H., Manufaturing Message Specification (MMS) Services, Open System Data Transfer, 1988

[39] INTERNATIONAL STANDARD ORGANIZATION, Manufacturing Message Specification, ISO/DIS 9506, agosto de 1988

[40] PREISS, O., WEGMANN, A., Towards a composition model problem based on IEC61850, Journal of Systems and Software, Volume 65, Elsevier, 2003.

[41] YUN, P. et. al, Research on IED Configurator Based on IEC 61850, International Conference on Control, Automation and Systems Engineering (CASE), IEEE, 2011

[42] APOSTOLOV, A. P. e PAULINO, M. E. C. Testes de sistemas de automação de subestações complexos baseados na IEC 61850. Simpósio de Automação de Sistemas Elétricos, VII SIMPASE, Salvador, 2007.

[43] HOLBACH, J. et. al, Status on the first IEC61850 based protection and control, multi-vendor project in the United States, Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, IEEE, 2007

[44] ASLAN, Ö., SAMET, R., Mitigating Cyber Security Attacks by being Aware of Vulnerabilities and Bugs, International Conference on Cyberworlds, IEEE, 2017

[45] http://w3.siemens.com/smartgrid/global/en/products-systems-solutions/protection/engineering-evaluation-diagnostic-software/pages/iec-browser.aspx, acessado em 08/11/2017

[46] https://sourceforge.net/projects/iedexplorer/, acessado em 08/11/2017

[47] https://www.omicronenergy.com/en/products/iedscout/, acessado em 08/11/2017

[48] VICENTE, Décio Tomasulo de, Aplicação dos padrões da norma IEC 61850 a subestações compartilhadas de transmissão/distribuição de energia elétrica, 10.11606/D.3.2011.tde-09032012-151057, USP, São Paulo, 2011

[49] KOSTIC, T., PREISS O., FREI, C., Understanding and using the IEC 61850: a case for meta-modelling, Computer Standards & Interfaces, Volume 27, Issue 6, Elsevier, 2005

[50] HOGA, C., WONG, G., IEC 61850: open communication in practice in substations, Power Systems Conference and Exposition. IEEE PES, DOI: 10.1109/PSCE.2004.1397694, IEEE, 2004.

ANEXO 1 - RESULTADOS NO NMAP PARA A REDE DE TESTES 1

```
Starting Nmap 7.50 ( https://nmap.org ) at 2017-09-20 16:04 E. South America Standard Time
NSE: Loaded 144 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:04
Completed NSE at 16:04, 0.00s elapsed
Initiating NSE at 16:04
Completed NSE at 16:04, 0.00s elapsed
Initiating ARP Ping Scan at 16:04
Scanning 254 hosts [1 port/host]
Completed ARP Ping Scan at 16:04, 2.40s elapsed (254 total hosts)
Initiating Parallel DNS resolution of 254 hosts. at 16:04
Completed Parallel DNS resolution of 254 hosts. at 16:04, 5.51s elapsed
Nmap scan report for 192.168.1.0 [host down]
Nmap scan report for 192.168.1.3 [host down]
Nmap scan report for 192.168.1.4 [host down]
Nmap scan report for 192.168.1.6 [host down]
Nmap scan report for 192.168.1.7 [host down]
Nmap scan report for 192.168.1.8 [host down]
Nmap scan report for 192.168.1.9 [host down]
Nmap scan report for 192.168.1.11 [host down]
Nmap scan report for 192.168.1.12 [host down]
Nmap scan report for 192.168.1.13 [host down]
Nmap scan report for 192.168.1.14 [host down]
Nmap scan report for 192.168.1.15 [host down]
Nmap scan report for 192.168.1.16 [host down]
Nmap scan report for 192.168.1.17 [host down]
Nmap scan report for 192.168.1.18 [host down]
Nmap scan report for 192.168.1.19 [host down]
Nmap scan report for 192.168.1.20 [host down]
Nmap scan report for 192.168.1.21 [host down]
Nmap scan report for 192.168.1.22 [host down]
Nmap scan report for 192.168.1.23 [host down]
Nmap scan report for 192.168.1.24 [host down]
Nmap scan report for 192.168.1.25 [host down]
Nmap scan report for 192.168.1.26 [host down]
Nmap scan report for 192.168.1.27 [host down]
Nmap scan report for 192.168.1.28 [host down]
Nmap scan report for 192.168.1.29 [host down]
Nmap scan report for 192.168.1.30 [host down]
Nmap scan report for 192.168.1.31 [host down]
Nmap scan report for 192.168.1.32 [host down]
Nmap scan report for 192.168.1.33 [host down]
Nmap scan report for 192.168.1.34 [host down]
Nmap scan report for 192.168.1.35 [host down]
Nmap scan report for 192.168.1.36 [host down]
Nmap scan report for 192.168.1.37 [host down]
Nmap scan report for 192.168.1.38 [host down]
Nmap scan report for 192.168.1.39 [host down]
Nmap scan report for 192.168.1.40 [host down]
Nmap scan report for 192.168.1.41 [host down]
Nmap scan report for 192.168.1.42 [host down]
Nmap scan report for 192.168.1.43 [host down]
Nmap scan report for 192.168.1.44 [host down]
Nmap scan report for 192.168.1.45 [host down]
Nmap scan report for 192.168.1.46 [host down]
Nmap scan report for 192.168.1.47 [host down]
Nmap scan report for 192.168.1.48 [host down]
Nmap scan report for 192.168.1.49 [host down]
Nmap scan report for 192.168.1.50 [host down]
Nmap scan report for 192.168.1.51 [host down]
Nmap scan report for 192.168.1.52 [host down]
Nmap scan report for 192.168.1.53 [host down]
Nmap scan report for 192.168.1.54 [host down]
Nmap scan report for 192.168.1.55 [host down]
Nmap scan report for 192.168.1.56 [host down]
Nmap scan report for 192.168.1.57 [host down]
Nmap scan report for 192.168.1.58 [host down]
Nmap scan report for 192.168.1.59 [host down]
Nmap scan report for 192.168.1.60 [host down]
Nmap scan report for 192.168.1.61 [host down]
Nmap scan report for 192.168.1.62 [host down]
Nmap scan report for 192.168.1.63 [host down]
Nmap scan report for 192.168.1.64 [host down]
Nmap scan report for 192.168.1.65 [host down]
```

Nmap scan report for 192.168.1.66 [host down]
Nmap scan report for 192.168.1.67 [host down]
Nmap scan report for 192.168.1.68 [host down]
Nmap scan report for 192.168.1.69 [host down]
Nmap scan report for 192.168.1.70 [host down]
Nmap scan report for 192.168.1.71 [host down]
Nmap scan report for 192.168.1.72 [host down]
Nmap scan report for 192.168.1.73 [host down]
Nmap scan report for 192.168.1.74 [host down]
Nmap scan report for 192.168.1.75 [host down]
Nmap scan report for 192.168.1.76 [host down]
Nmap scan report for 192.168.1.77 [host down]
Nmap scan report for 192.168.1.78 [host down]
Nmap scan report for 192.168.1.79 [host down]
Nmap scan report for 192.168.1.80 [host down]
Nmap scan report for 192.168.1.81 [host down]
Nmap scan report for 192.168.1.82 [host down]
Nmap scan report for 192.168.1.83 [host down]
Nmap scan report for 192.168.1.84 [host down]
Nmap scan report for 192.168.1.85 [host down]
Nmap scan report for 192.168.1.86 [host down]
Nmap scan report for 192.168.1.87 [host down]
Nmap scan report for 192.168.1.88 [host down]
Nmap scan report for 192.168.1.89 [host down]
Nmap scan report for 192.168.1.90 [host down]
Nmap scan report for 192.168.1.91 [host down]
Nmap scan report for 192.168.1.92 [host down]
Nmap scan report for 192.168.1.93 [host down]
Nmap scan report for 192.168.1.94 [host down]
Nmap scan report for 192.168.1.95 [host down]
Nmap scan report for 192.168.1.96 [host down]
Nmap scan report for 192.168.1.97 [host down]
Nmap scan report for 192.168.1.98 [host down]
Nmap scan report for 192.168.1.99 [host down]
Nmap scan report for 192.168.1.104 [host down]
Nmap scan report for 192.168.1.105 [host down]
Nmap scan report for 192.168.1.106 [host down]
Nmap scan report for 192.168.1.107 [host down]
Nmap scan report for 192.168.1.108 [host down]
Nmap scan report for 192.168.1.109 [host down]
Nmap scan report for 192.168.1.110 [host down]
Nmap scan report for 192.168.1.111 [host down]
Nmap scan report for 192.168.1.112 [host down]
Nmap scan report for 192.168.1.113 [host down]
Nmap scan report for 192.168.1.114 [host down]
Nmap scan report for 192.168.1.115 [host down]
Nmap scan report for 192.168.1.116 [host down]
Nmap scan report for 192.168.1.117 [host down]
Nmap scan report for 192.168.1.118 [host down]
Nmap scan report for 192.168.1.119 [host down]
Nmap scan report for 192.168.1.120 [host down]
Nmap scan report for 192.168.1.121 [host down]
Nmap scan report for 192.168.1.122 [host down]
Nmap scan report for 192.168.1.123 [host down]
Nmap scan report for 192.168.1.124 [host down]
Nmap scan report for 192.168.1.125 [host down]
Nmap scan report for 192.168.1.126 [host down]
Nmap scan report for 192.168.1.127 [host down]
Nmap scan report for 192.168.1.128 [host down]
Nmap scan report for 192.168.1.129 [host down]
Nmap scan report for 192.168.1.130 [host down]
Nmap scan report for 192.168.1.131 [host down]
Nmap scan report for 192.168.1.132 [host down]
Nmap scan report for 192.168.1.133 [host down]
Nmap scan report for 192.168.1.134 [host down]
Nmap scan report for 192.168.1.135 [host down]
Nmap scan report for 192.168.1.136 [host down]
Nmap scan report for 192.168.1.137 [host down]
Nmap scan report for 192.168.1.138 [host down]
Nmap scan report for 192.168.1.139 [host down]
Nmap scan report for 192.168.1.140 [host down]
Nmap scan report for 192.168.1.141 [host down]
Nmap scan report for 192.168.1.142 [host down]
Nmap scan report for 192.168.1.143 [host down]
Nmap scan report for 192.168.1.144 [host down]
Nmap scan report for 192.168.1.145 [host down]
Nmap scan report for 192.168.1.146 [host down]

Nmap scan report for 192.168.1.147 [host down]
Nmap scan report for 192.168.1.148 [host down]
Nmap scan report for 192.168.1.149 [host down]
Nmap scan report for 192.168.1.150 [host down]
Nmap scan report for 192.168.1.151 [host down]
Nmap scan report for 192.168.1.152 [host down]
Nmap scan report for 192.168.1.153 [host down]
Nmap scan report for 192.168.1.154 [host down]
Nmap scan report for 192.168.1.155 [host down]
Nmap scan report for 192.168.1.156 [host down]
Nmap scan report for 192.168.1.157 [host down]
Nmap scan report for 192.168.1.158 [host down]
Nmap scan report for 192.168.1.159 [host down]
Nmap scan report for 192.168.1.160 [host down]
Nmap scan report for 192.168.1.161 [host down]
Nmap scan report for 192.168.1.162 [host down]
Nmap scan report for 192.168.1.163 [host down]
Nmap scan report for 192.168.1.164 [host down]
Nmap scan report for 192.168.1.165 [host down]
Nmap scan report for 192.168.1.166 [host down]
Nmap scan report for 192.168.1.167 [host down]
Nmap scan report for 192.168.1.168 [host down]
Nmap scan report for 192.168.1.169 [host down]
Nmap scan report for 192.168.1.170 [host down]
Nmap scan report for 192.168.1.171 [host down]
Nmap scan report for 192.168.1.172 [host down]
Nmap scan report for 192.168.1.173 [host down]
Nmap scan report for 192.168.1.174 [host down]
Nmap scan report for 192.168.1.175 [host down]
Nmap scan report for 192.168.1.176 [host down]
Nmap scan report for 192.168.1.177 [host down]
Nmap scan report for 192.168.1.178 [host down]
Nmap scan report for 192.168.1.179 [host down]
Nmap scan report for 192.168.1.180 [host down]
Nmap scan report for 192.168.1.181 [host down]
Nmap scan report for 192.168.1.182 [host down]
Nmap scan report for 192.168.1.183 [host down]
Nmap scan report for 192.168.1.184 [host down]
Nmap scan report for 192.168.1.185 [host down]
Nmap scan report for 192.168.1.186 [host down]
Nmap scan report for 192.168.1.187 [host down]
Nmap scan report for 192.168.1.188 [host down]
Nmap scan report for 192.168.1.189 [host down]
Nmap scan report for 192.168.1.190 [host down]
Nmap scan report for 192.168.1.191 [host down]
Nmap scan report for 192.168.1.192 [host down]
Nmap scan report for 192.168.1.193 [host down]
Nmap scan report for 192.168.1.194 [host down]
Nmap scan report for 192.168.1.195 [host down]
Nmap scan report for 192.168.1.196 [host down]
Nmap scan report for 192.168.1.197 [host down]
Nmap scan report for 192.168.1.198 [host down]
Nmap scan report for 192.168.1.199 [host down]
Nmap scan report for 192.168.1.200 [host down]
Nmap scan report for 192.168.1.201 [host down]
Nmap scan report for 192.168.1.202 [host down]
Nmap scan report for 192.168.1.203 [host down]
Nmap scan report for 192.168.1.204 [host down]
Nmap scan report for 192.168.1.205 [host down]
Nmap scan report for 192.168.1.206 [host down]
Nmap scan report for 192.168.1.207 [host down]
Nmap scan report for 192.168.1.208 [host down]
Nmap scan report for 192.168.1.209 [host down]
Nmap scan report for 192.168.1.210 [host down]
Nmap scan report for 192.168.1.211 [host down]
Nmap scan report for 192.168.1.212 [host down]
Nmap scan report for 192.168.1.213 [host down]
Nmap scan report for 192.168.1.214 [host down]
Nmap scan report for 192.168.1.215 [host down]
Nmap scan report for 192.168.1.216 [host down]
Nmap scan report for 192.168.1.217 [host down]
Nmap scan report for 192.168.1.218 [host down]
Nmap scan report for 192.168.1.219 [host down]
Nmap scan report for 192.168.1.220 [host down]
Nmap scan report for 192.168.1.221 [host down]
Nmap scan report for 192.168.1.222 [host down]
Nmap scan report for 192.168.1.223 [host down]

```
Nmap scan report for 192.168.1.224 [host down]
Nmap scan report for 192.168.1.225 [host down]
Nmap scan report for 192.168.1.226 [host down]
Nmap scan report for 192.168.1.227 [host down]
Nmap scan report for 192.168.1.228 [host down]
Nmap scan report for 192.168.1.229 [host down]
Nmap scan report for 192.168.1.230 [host down]
Nmap scan report for 192.168.1.231 [host down]
Nmap scan report for 192.168.1.232 [host down]
Nmap scan report for 192.168.1.233 [host down]
Nmap scan report for 192.168.1.234 [host down]
Nmap scan report for 192.168.1.235 [host down]
Nmap scan report for 192.168.1.236 [host down]
Nmap scan report for 192.168.1.237 [host down]
Nmap scan report for 192.168.1.238 [host down]
Nmap scan report for 192.168.1.239 [host down]
Nmap scan report for 192.168.1.240 [host down]
Nmap scan report for 192.168.1.241 [host down]
Nmap scan report for 192.168.1.242 [host down]
Nmap scan report for 192.168.1.243 [host down]
Nmap scan report for 192.168.1.244 [host down]
Nmap scan report for 192.168.1.245 [host down]
Nmap scan report for 192.168.1.246 [host down]
Nmap scan report for 192.168.1.247 [host down]
Nmap scan report for 192.168.1.248 [host down]
Nmap scan report for 192.168.1.249 [host down]
Nmap scan report for 192.168.1.250 [host down]
Nmap scan report for 192.168.1.251 [host down]
Nmap scan report for 192.168.1.252 [host down]
Nmap scan report for 192.168.1.253 [host down]
Nmap scan report for 192.168.1.254 [host down]
Nmap scan report for 192.168.1.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 16:04
Completed Parallel DNS resolution of 1 host. at 16:04, 0.01s elapsed
Initiating NULL Scan at 16:04
Scanning 6 hosts [1000 ports/host]
Completed NULL Scan against 192.168.1.103 in 5.27s (5 hosts left)
Completed NULL Scan against 192.168.1.5 in 5.29s (4 hosts left)
Completed NULL Scan against 192.168.1.102 in 5.29s (3 hosts left)
Completed NULL Scan against 192.168.1.10 in 5.31s (2 hosts left)
Completed NULL Scan against 192.168.1.100 in 5.31s (1 host left)
Completed NULL Scan at 16:04, 17.55s elapsed (6000 total ports)
Initiating Service scan at 16:04
Scanning 23 services on 6 hosts
Discovered open port 21/tcp on 192.168.1.5
Discovered open|filtered port 21/tcp on 192.168.1.5 is actually open
Discovered open port 21/tcp on 192.168.1.10
Discovered open|filtered port 21/tcp on 192.168.1.10 is actually open
Discovered open port 80/tcp on 192.168.1.100
Discovered open|filtered port 80/tcp on 192.168.1.100 is actually open
Discovered open port 1900/tcp on 192.168.1.100
Discovered open|filtered port 1900/tcp on 192.168.1.100 is actually open
Discovered open port 20005/tcp on 192.168.1.100
Discovered open|filtered port 20005/tcp on 192.168.1.100 is actually open
Discovered open port 49152/tcp on 192.168.1.100
Discovered open|filtered port 49152/tcp on 192.168.1.100 is actually open
Discovered open port 22/tcp on 192.168.1.101
Discovered open|filtered port 22/tcp on 192.168.1.101 is actually open
Discovered open port 1900/tcp on 192.168.1.102
Discovered open|filtered port 1900/tcp on 192.168.1.102 is actually open
Discovered open port 80/tcp on 192.168.1.102
Discovered open|filtered port 80/tcp on 192.168.1.102 is actually open
Discovered open port 20005/tcp on 192.168.1.102
Discovered open|filtered port 20005/tcp on 192.168.1.102 is actually open
Discovered open port 23/tcp on 192.168.1.5
Discovered open|filtered port 23/tcp on 192.168.1.5 is actually open
Discovered open port 1024/tcp on 192.168.1.5
Discovered open|filtered port 1024/tcp on 192.168.1.5 is actually open
Discovered open port 23/tcp on 192.168.1.10
Discovered open|filtered port 23/tcp on 192.168.1.10 is actually open
Discovered open port 1024/tcp on 192.168.1.10
Discovered open|filtered port 1024/tcp on 192.168.1.10 is actually open
Discovered open port 49152/tcp on 192.168.1.102
Discovered open|filtered port 49152/tcp on 192.168.1.102 is actually open
Discovered open port 80/tcp on 192.168.1.103
Discovered open|filtered port 80/tcp on 192.168.1.103 is actually open
Discovered open port 1900/tcp on 192.168.1.103
```

```
Discovered open|filtered port 1900/tcp on 192.168.1.103 is actually open
Discovered open port 20005/tcp on 192.168.1.103
Discovered open|filtered port 20005/tcp on 192.168.1.103 is actually open
Discovered open port 49152/tcp on 192.168.1.103
Discovered open|filtered port 49152/tcp on 192.168.1.103 is actually open
Discovered open port 23/tcp on 192.168.1.101
Discovered open|filtered port 23/tcp on 192.168.1.101 is actually open
Discovered open port 80/tcp on 192.168.1.101
Discovered open|filtered port 80/tcp on 192.168.1.101 is actually open
Discovered open port 161/tcp on 192.168.1.101
Discovered open|filtered port 161/tcp on 192.168.1.101 is actually open
Discovered open port 443/tcp on 192.168.1.101
Discovered open|filtered port 443/tcp on 192.168.1.101 is actually open
Completed Service scan at 16:05, 25.42s elapsed (23 services on 6 hosts)
Initiating OS detection (try #1) against 6 hosts
Retrying OS detection (try #2) against 3 hosts
NSE: Script scanning 6 hosts.
Initiating NSE at 16:05
Completed NSE at 16:06, 61.62s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 1.42s elapsed
Nmap scan report for 192.168.1.5
Host is up (0.011s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp?
| fingerprint-strings:
|   GenericLines:
|     220 FTP SERVER:
|     Syntax error, command unrecognized.
|   Help:
|     220 FTP SERVER:
|     HELP command not implemented, or not allowed.
|   NULL:
|_    220 FTP SERVER:
|_ftp-anon: ERROR: Script execution failed (use -d to debug)
|_ftp-bounce: no banner
23/tcp   open  telnet?
| fingerprint-strings:
|   GenericLines, NULL:
|     HOST TERMINAL SERVER:
|     SEL-421 Date: 09/20/2017 Time: 17:13:04.418
|     Serial Number: 2001285094
|   tn3270:
|     HOST TERMINAL SERVER:
|     SEL-421 Date: 09/20/2017 Time: 17:13:15.146
|_    Serial Number: 2001285094
1024/tcp open  kdm?
| fingerprint-strings:
|   FourOhFourRequest:
|     Service is not available at this time, try back later.
|   NULL:
|_    Service has been disabled.
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port21-TCP:V=7.50%I=7%D=9/20%Time=59C2BBD8%P=i686-pc-windows-windows%r(
SF:NULL,11,"220\x20FTP\x20SERVER:\r\n")%r(GenericLines,3A,"220\x20FTP\x20S
SF:ERVER:\r\n500\x20Syntax\x20error,\x20command\x20unrecognized\.\r\n")%r(
SF:Help,44,"220\x20FTP\x20SERVER:\r\n502\x20HELP\x20command\x20not\x20impl
SF:emented,\x20or\x20not\x20allowed\.\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port23-TCP:V=7.50%I=7%D=9/20%Time=59C2BBD8%P=i686-pc-windows-windows%r(
SF:NULL,C6,"\xff\xfd\0\xff\xfd\x03\xff\xfb\0\xff\xfb\x01\xff\xfb\x03HOST\x
SF:20TERMINAL\x20SERVER:\r\n\r\nSEL-421\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20Date:\x2009/20/2017\x20\x20Time:\
SF:x2017:13:04\.418\r\nSE\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20Serial\x20Number:\x20200128
SF:5094\r\n\r\n\x02\r\n=\x03")%r(GenericLines,D4,"\xff\xfd\0\xff\xfd\x03\x
SF:ff\xfb\0\xff\xfb\x01\xff\xfb\x03HOST\x20TERMINAL\x20SERVER:\r\n\r\nSEL-
SF:421\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20Date:\x2009/20/2017\x20\x20Time:\x2017:13:04\.418\r\nSE\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
```

```
SF:x20\x20\x20Serial\x20Number:\x202001285094\r\n\r\n\x02\r\n=\x03\r\n\x02
SF:\r\n=\x03\r\n\x02\r\n=\x03")%r(tn3270,D7,"\xff\xfd\0\xff\xfd\x03\xff\xf
SF:b\0\xff\xfb\x01\xff\xfb\x03HOST\x20TERMINAL\x20SERVER:\r\n\xff\xfe\x18\
SF:xff\xfd\x19\xff\xfb\x19\xff\xfd\0\xff\xfb\0\r\nSEL-421\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20Date:\x2009/20/
SF:2017\x20\x20Time:\x2017:13:15\.146\r\nSE\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20Serial\x2
SF:0Number:\x202001285094\r\n\r\n\x02\r\n=\x03\xff\xef");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1024-TCP:V=7.50%I=7%D=9/20%Time=59C2BBD2%P=i686-pc-windows-windows%
SF:r(NULL,1E,"\r\n\r\nService\x20has\x20been\x20disabled\.")%r(FourOhFourR
SF:equest,3C,"\r\n\r\nService\x20is\x20not\x20available\x20at\x20this\x20t
SF:ime,\x20try\x20back\x20later\.\r\n");
MAC Address: 00:30:A7:00:00:00 (Schweitzer Engineering)
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (87%)
OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   11.39 ms 192.168.1.5

Nmap scan report for 192.168.1.10
Host is up (0.0082s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp?
| fingerprint-strings:
|   GenericLines:
|     220 FTP SERVER:
|     Syntax error, command unrecognized.
|   Help:
|     220 FTP SERVER:
|     HELP command not implemented, or not allowed.
|   NULL:
|_    220 FTP SERVER:
|_ftp-anon: ERROR: Script execution failed (use -d to debug)
|_ftp-bounce: no banner
23/tcp   open  telnet?
| fingerprint-strings:
|   GenericLines, NULL:
|     HOST TERMINAL SERVER:
|     SEL-451 Date: 09/20/2017 Time: 16:10:14.754
|     Serial Number: 2007310197
|   tn3270:
|     HOST TERMINAL SERVER:
|     SEL-451 Date: 09/20/2017 Time: 16:10:25.797
|_    Serial Number: 2007310197
1024/tcp open  kdm?
| fingerprint-strings:
|   DNSVersionBindReq, GenericLines, HTTPOptions, LPDString:
|     Service is not available at this time, try back later.
|   NULL:
|_    Service has been disabled.
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port21-TCP:V=7.50%I=7%D=9/20%Time=59C2BBD8%P=i686-pc-windows-windows%r(
SF:NULL,11,"220\x20FTP\x20SERVER:\r\n")%r(GenericLines,3A,"220\x20FTP\x20S
SF:ERVER:\r\n500\x20Syntax\x20error,\x20command\x20unrecognized\.\r\n")%r(
SF:Help,44,"220\x20FTP\x20SERVER:\r\n502\x20HELP\x20command\x20not\x20impl
SF:emented,\x20or\x20not\x20allowed\.\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port23-TCP:V=7.50%I=7%D=9/20%Time=59C2BBD8%P=i686-pc-windows-windows%r(
SF:NULL,C6,"\xff\xfd\0\xff\xfd\x03\xff\xfb\0\xff\xfb\x01\xff\xfb\x03HOST\x
SF:20TERMINAL\x20SERVER:\r\n\r\nSEL-451\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20Date:\x2009/20/2017\x20\x20Time:\
SF:x2016:10:14\.754\r\nSE\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20Serial\x20Number:\x20200731
SF:0197\r\n\r\n\x02\r\n=\x03")%r(GenericLines,D4,"\xff\xfd\0\xff\xfd\x03\x
```

```
SF:ff\xfb\0\xff\xfb\x01\xff\xfb\x03HOST\x20TERMINAL\x20SERVER:\r\n\r\nSEL-
SF:451\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20Date:\x2009/20/2017\x20\x20Time:\x2016:10:14\.754\r\nSE\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20Serial\x20Number:\x202007310197\r\n\r\n\x02\r\n=\x03\r\n\x02
SF:\r\n=\x03\r\n\x02\r\n=\x03")%r(tn3270,D7,"\xff\xfd\0\xff\xfd\x03\xff\xf
SF:b\0\xff\xfb\x01\xff\xfb\x03HOST\x20TERMINAL\x20SERVER:\r\n\xff\xfe\x18\
SF:xff\xfd\x19\xff\xfb\x19\xff\xfd\0\xff\xfb\0\r\nSEL-451\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20Date:\x2009/20/
SF:2017\x20\x20Time:\x2016:10:25\.797\r\nSE\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20Serial\x2
SF:0Number:\x202007310197\r\n\r\n\x02\r\n=\x03\xff\xef");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1024-TCP:V=7.50%I=7%D=9/20%Time=59C2BBD2%P=i686-pc-windows-windows%
SF:r(NULL,1E,"\r\n\r\nService\x20has\x20been\x20disabled\.")%r(GenericLine
SF:s,3C,"\r\n\r\nService\x20is\x20not\x20available\x20at\x20this\x20time,\
SF:x20try\x20back\x20later\.\r\n")%r(HTTPOptions,3C,"\r\n\r\nService\x20is
SF:\x20not\x20available\x20at\x20this\x20time,\x20try\x20back\x20later\.\r
SF:\n")%r(DNSVersionBindReq,3C,"\r\n\r\nService\x20is\x20not\x20available\
SF:x20at\x20this\x20time,\x20try\x20back\x20later\.\r\n")%r(LPDString,3C,"
SF:\r\n\r\nService\x20is\x20not\x20available\x20at\x20this\x20time,\x20try
SF:\x20back\x20later\.\r\n");
MAC Address: 00:30:A7:00:85:59 (Schweitzer Engineering)
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (87%)
OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   8.21 ms 192.168.1.10

Nmap scan report for 192.168.1.100
Host is up (0.0021s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    TP-LINK WR842ND WAP http config
| http-auth:
| HTTP/1.1 401 N/A\x0D
|_  Basic realm=TP-LINK Wireless N Router WR842ND
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Router Webserver
|_http-title: Login Incorrect
1900/tcp  open  upnp    ipOS upnpd (TP-LINK TL-WR842ND WAP 2.0; UPnP 1.0)
20005/tcp open  btx?
49152/tcp open  upnp    Portable SDK for UPnP devices 1.6.6 (Linux 2.6.31--LSDK-9.2.0_U5.508; UPnP 1.0)
MAC Address: E8:94:F6:B4:9D:56 (Tp-link Technologies)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Uptime guess: 0.857 days (since Tue Sep 19 19:32:50 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: ipOS 7.0, Linux; Device: WAP; CPE: cpe:/h:tp-link:wr842nd, cpe:/h:tp-link:tl-wr842nd, cpe:/o:ubicom:ipos:7.0,
cpe:/o:linux:linux_kernel:2.6.31--lsdk-9.2.0_u5.508

TRACEROUTE
HOP RTT     ADDRESS
1   2.13 ms 192.168.1.100

Nmap scan report for 192.168.1.101
Host is up (0.14s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  tcpwrapped
23/tcp  open  telnet?
| fingerprint-strings:
|   GenericLines:
```

```
|    Copyright (c) 2001-2006 GarrettCom Inc All rights reserved.
|    RESTRICTED RIGHTS
|    ----------------
|    Use, duplication or disclosure is subject to U.S. Government restrictions
|    forth in Sub-division (b)(3)(ii) of the rights in Technical Data and
|    Computer Software clause at 52.227-7013.
|    GarrettCom, Inc.
|    47823 Westinghouse Drive
|    Fremont CA 94539-9072
|    www.garrettcom.com
|    Magnum 6K25e Version: 4.1.5
|    Login :
|    Login :
|  NULL:
|    Copyright (c) 2001-2006 GarrettCom Inc All rights reserved.
|    RESTRICTED RIGHTS
|    ----------------
|    Use, duplication or disclosure is subject to U.S. Government restrictions
|    forth in Sub-division (b)(3)(ii) of the rights in Technical Data and
|    Computer Software clause at 52.227-7013.
|    GarrettCom, Inc.
|    47823 Westinghouse Drive
|    Fremont CA 94539-9072
|    www.garrettcom.com
|    Magnum 6K25e Version: 4.1.5
|_   Login :
80/tcp  open  http      GoAhead WebServer
|_http-server-header: GoAhead-Webs
161/tcp open  snmp?
443/tcp open  ssl/https?
| http-methods:
|_  Supported Methods: HEAD
| ssl-cert: Subject: commonName=Software Group/organizationName=Garrettcom
Inc./stateOrProvinceName=CA/countryName=US
| Issuer: commonName=Software Group/organizationName=Garrettcom Inc./stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2006-12-11T20:33:09
| Not valid after:  2016-12-08T20:33:09
| MD5:   8403 17ca fbef 348f dab6 bed5 c9ca 37c2
|_SHA-1: 1673 1c9a b4d1 0de8 352e 0649 55e5 a168 d7f8 7eeb
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port23-TCP:V=7.50%I=7%D=9/20%Time=59C2BBD8%P=i686-pc-windows-windows%r(
SF:NULL,1DA,"\xff\xfd\x18\xff\xfb\x05\xff\xfb\x03\xff\xfb\x01\x1b\[2J\x1b\
SF:[H\n\rCopyright\x20\(c\)\x202001-2006\x20GarrettCom\x20Inc\x20All\x20ri
SF:ghts\x20reserved\.\r\n\r\nRESTRICTED\x20RIGHTS\n\r----------\n\r
SF:Use,\x20duplication\x20or\x20disclosure\x20\x20is\x20subject\x20to\x20\
SF:x20U\.S\.\x20Government\x20restrictions\x20\n\ras\x20set\x20forth\x20in
SF:\x20Sub-division\x20\(b\)\(3\)\(ii\)\x20of\x20the\x20rights\x20in\x20Te
SF:chnical\x20Data\x20and\x20\n\rComputer\x20Software\x20clause\x20at\x205
SF:2\.227-7013\.\n\r\n\r\x20\x20\x20GarrettCom,\x20Inc\.\n\r\x20\x20\x2047
SF:823\x20Westinghouse\x20Drive\n\r\x20\x20\x20Fremont\x20CA\x2094539-9072
SF:\n\r\x20\x20\x20USA\x20\n\n\r\x20\x20\x20www\.garrettcom\.com\n\n\rMagn
SF:um\x206K25e\x20Version:\x204\.1\.5\n\r\n\rLogin\x20\x20\x20\x20:\x20")%
SF:r(GenericLines,1E9,"\xff\xfd\x18\xff\xfb\x05\xff\xfb\x03\xff\xfb\x01\x1
SF:b\[2J\x1b\[H\n\rCopyright\x20\(c\)\x202001-2006\x20GarrettCom\x20Inc\x2
SF:0All\x20rights\x20reserved\.\r\n\r\nRESTRICTED\x20RIGHTS\n\r----------
SF:------\n\rUse,\x20duplication\x20or\x20disclosure\x20\x20is\x20subject\
SF:x20to\x20\x20U\.S\.\x20Government\x20restrictions\x20\n\ras\x20set\x20f
SF:orth\x20in\x20Sub-division\x20\(b\)\(3\)\(ii\)\x20of\x20the\x20rights\x
SF:20in\x20Technical\x20Data\x20and\x20\n\rComputer\x20Software\x20clause\
SF:x20at\x2052\.227-7013\.\n\r\n\r\x20\x20\x20GarrettCom,\x20Inc\.\n\r\x20
SF:\x20\x2047823\x20Westinghouse\x20Drive\n\r\x20\x20\x20Fremont\x20CA\x20
SF:94539-9072\n\r\x20\x20\x20USA\x20\n\n\r\x20\x20\x20www\.garrettcom\.com
SF:\n\n\rMagnum\x206K25e\x20Version:\x204\.1\.5\n\r\n\rLogin\x20\x20\x20\x
SF:20:\x20\n\r\n\rLogin\x20\x20\x20\x20:\x20");
MAC Address: 00:20:06:28:3F:80 (Garrett Communications)
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (87%)
OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
```

```
HOP RTT       ADDRESS
1   136.66 ms 192.168.1.101

Nmap scan report for 192.168.1.102
Host is up (0.0030s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    TP-LINK WR842ND WAP http config
| http-auth:
| HTTP/1.1 401 N/A\x0D
|_  Basic realm=TP-LINK Wireless N Router WR842ND
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Router Webserver
|_http-title: Login Incorrect
1900/tcp  open  upnp    ipOS upnpd (TP-LINK TL-WR842ND WAP 2.0; UPnP 1.0)
20005/tcp open  btx?
49152/tcp open  upnp    Portable SDK for UPnP devices 1.6.6 (Linux 2.6.31--LSDK-9.2.0_U5.508; UPnP 1.0)
MAC Address: E8:94:F6:B4:B0:76 (Tp-link Technologies)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Uptime guess: 0.864 days (since Tue Sep 19 19:22:55 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: ipOS 7.0, Linux; Device: WAP; CPE: cpe:/h:tp-link:wr842nd, cpe:/h:tp-link:tl-wr842nd, cpe:/o:ubicom:ipos:7.0,
cpe:/o:linux:linux_kernel:2.6.31--lsdk-9.2.0_u5.508

TRACEROUTE
HOP RTT     ADDRESS
1   2.98 ms 192.168.1.102

Nmap scan report for 192.168.1.103
Host is up (0.0034s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    TP-LINK WR842ND WAP http config
| http-auth:
| HTTP/1.1 401 N/A\x0D
|_  Basic realm=TP-LINK Wireless N Router WR842ND
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Router Webserver
|_http-title: Login Incorrect
1900/tcp  open  upnp    ipOS upnpd (TP-LINK TL-WR842ND WAP 2.0; UPnP 1.0)
20005/tcp open  btx?
49152/tcp open  upnp    Portable SDK for UPnP devices 1.6.6 (Linux 2.6.31--LSDK-9.2.0_U5.508; UPnP 1.0)
MAC Address: E8:94:F6:B4:9C:F8 (Tp-link Technologies)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.17 - 2.6.36
Uptime guess: 0.857 days (since Tue Sep 19 19:32:50 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=200 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: ipOS 7.0, Linux; Device: WAP; CPE: cpe:/h:tp-link:wr842nd, cpe:/h:tp-link:tl-wr842nd, cpe:/o:ubicom:ipos:7.0,
cpe:/o:linux:linux_kernel:2.6.31--lsdk-9.2.0_u5.508

TRACEROUTE
HOP RTT     ADDRESS
1   3.39 ms 192.168.1.103

Initiating ARP Ping Scan at 16:06
Scanning 192.168.1.2 [1 port]
Completed ARP Ping Scan at 16:06, 0.41s elapsed (1 total hosts)
Nmap scan report for 192.168.1.2 [host down]
Skipping NULL Scan against 192.168.1.1 because Windows does not support scanning your own machine (localhost) this way.
Initiating Service scan at 16:06
Skipping OS Scan against 192.168.1.1 because it doesn't work against your own machine (localhost)
NSE: Script scanning 192.168.1.1.
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
```

Nmap scan report for 192.168.1.1
Host is up.

PORT	STATE	SERVICE	VERSION
1/tcp	unknown	tcpmux	
3/tcp	unknown	compressnet	
4/tcp	unknown	unknown	
6/tcp	unknown	unknown	
7/tcp	unknown	echo	
9/tcp	unknown	discard	
13/tcp	unknown	daytime	
17/tcp	unknown	qotd	
19/tcp	unknown	chargen	
20/tcp	unknown	ftp-data	
21/tcp	unknown	ftp	
22/tcp	unknown	ssh	
23/tcp	unknown	telnet	
24/tcp	unknown	priv-mail	
25/tcp	unknown	smtp	
26/tcp	unknown	rsftp	
30/tcp	unknown	unknown	
32/tcp	unknown	unknown	
33/tcp	unknown	dsp	
37/tcp	unknown	time	
42/tcp	unknown	nameserver	
43/tcp	unknown	whois	
49/tcp	unknown	tacacs	
53/tcp	unknown	domain	
70/tcp	unknown	gopher	
79/tcp	unknown	finger	
80/tcp	unknown	http	
81/tcp	unknown	hosts2-ns	
82/tcp	unknown	xfer	
83/tcp	unknown	mit-ml-dev	
84/tcp	unknown	ctf	
85/tcp	unknown	mit-ml-dev	
88/tcp	unknown	kerberos-sec	
89/tcp	unknown	su-mit-tg	
90/tcp	unknown	dnsix	
99/tcp	unknown	metagram	
100/tcp	unknown	newacct	
106/tcp	unknown	pop3pw	
109/tcp	unknown	pop2	
110/tcp	unknown	pop3	
111/tcp	unknown	rpcbind	
113/tcp	unknown	ident	
119/tcp	unknown	nntp	
125/tcp	unknown	locus-map	
135/tcp	unknown	msrpc	
139/tcp	unknown	netbios-ssn	
143/tcp	unknown	imap	
144/tcp	unknown	news	
146/tcp	unknown	iso-tp0	
161/tcp	unknown	snmp	
163/tcp	unknown	cmip-man	
179/tcp	unknown	bgp	
199/tcp	unknown	smux	
211/tcp	unknown	914c-g	
212/tcp	unknown	anet	
222/tcp	unknown	rsh-spx	
254/tcp	unknown	unknown	
255/tcp	unknown	unknown	
256/tcp	unknown	fw1-secureremote	
259/tcp	unknown	esro-gen	
264/tcp	unknown	bgmp	
280/tcp	unknown	http-mgmt	
301/tcp	unknown	unknown	
306/tcp	unknown	unknown	
311/tcp	unknown	asip-webadmin	
340/tcp	unknown	unknown	
366/tcp	unknown	odmr	
389/tcp	unknown	ldap	
406/tcp	unknown	imsp	
407/tcp	unknown	timbuktu	
416/tcp	unknown	silverplatter	
417/tcp	unknown	onmux	
425/tcp	unknown	icad-el	

427/tcp unknown svrloc
443/tcp unknown https
444/tcp unknown snpp
445/tcp unknown microsoft-ds
458/tcp unknown appleqtc
464/tcp unknown kpasswd5
465/tcp unknown smtps
481/tcp unknown dvs
497/tcp unknown retrospect
500/tcp unknown isakmp
512/tcp unknown exec
513/tcp unknown login
514/tcp unknown shell
515/tcp unknown printer
524/tcp unknown ncp
541/tcp unknown uucp-rlogin
543/tcp unknown klogin
544/tcp unknown kshell
545/tcp unknown ekshell
548/tcp unknown afp
554/tcp unknown rtsp
555/tcp unknown dsf
563/tcp unknown snews
587/tcp unknown submission
593/tcp unknown http-rpc-epmap
616/tcp unknown sco-sysmgr
617/tcp unknown sco-dtmgr
625/tcp unknown apple-xsrvr-admin
631/tcp unknown ipp
636/tcp unknown ldapssl
646/tcp unknown ldp
648/tcp unknown rrp
666/tcp unknown doom
667/tcp unknown disclose
668/tcp unknown mecomm
683/tcp unknown corba-iiop
687/tcp unknown asipregistry
691/tcp unknown resvc
700/tcp unknown epp
705/tcp unknown agentx
711/tcp unknown cisco-tdp
714/tcp unknown iris-xpcs
720/tcp unknown unknown
722/tcp unknown unknown
726/tcp unknown unknown
749/tcp unknown kerberos-adm
765/tcp unknown webster
777/tcp unknown multiling-http
783/tcp unknown spamassassin
787/tcp unknown qsc
800/tcp unknown mdbs_daemon
801/tcp unknown device
808/tcp unknown ccproxy-http
843/tcp unknown unknown
873/tcp unknown rsync
880/tcp unknown unknown
888/tcp unknown accessbuilder
898/tcp unknown sun-manageconsole
900/tcp unknown omginitialrefs
901/tcp unknown samba-swat
902/tcp unknown iss-realsecure
903/tcp unknown iss-console-mgr
911/tcp unknown xact-backup
912/tcp unknown apex-mesh
981/tcp unknown unknown
987/tcp unknown unknown
990/tcp unknown ftps
992/tcp unknown telnets
993/tcp unknown imaps
995/tcp unknown pop3s
999/tcp unknown garcon
1000/tcp unknown cadlock
1001/tcp unknown webpush
1002/tcp unknown windows-icfw
1007/tcp unknown unknown
1009/tcp unknown unknown
1010/tcp unknown surf

1011/tcp unknown unknown
1021/tcp unknown exp1
1022/tcp unknown exp2
1023/tcp unknown netvenuechat
1024/tcp unknown kdm
1025/tcp unknown NFS-or-IIS
1026/tcp unknown LSA-or-nterm
1027/tcp unknown IIS
1028/tcp unknown unknown
1029/tcp unknown ms-lsa
1030/tcp unknown iad1
1031/tcp unknown iad2
1032/tcp unknown iad3
1033/tcp unknown netinfo
1034/tcp unknown zincite-a
1035/tcp unknown multidropper
1036/tcp unknown nsstp
1037/tcp unknown ams
1038/tcp unknown mtqp
1039/tcp unknown sbl
1040/tcp unknown netsaint
1041/tcp unknown danf-ak2
1042/tcp unknown afrog
1043/tcp unknown boinc
1044/tcp unknown dcutility
1045/tcp unknown fpitp
1046/tcp unknown wfremotertm
1047/tcp unknown neod1
1048/tcp unknown neod2
1049/tcp unknown td-postman
1050/tcp unknown java-or-OTGfileshare
1051/tcp unknown optima-vnet
1052/tcp unknown ddt
1053/tcp unknown remote-as
1054/tcp unknown brvread
1055/tcp unknown ansyslmd
1056/tcp unknown vfo
1057/tcp unknown startron
1058/tcp unknown nim
1059/tcp unknown nimreg
1060/tcp unknown polestar
1061/tcp unknown kiosk
1062/tcp unknown veracity
1063/tcp unknown kyoceranetdev
1064/tcp unknown jstel
1065/tcp unknown syscomlan
1066/tcp unknown fpo-fns
1067/tcp unknown instl_boots
1068/tcp unknown instl_bootc
1069/tcp unknown cognex-insight
1070/tcp unknown gmrupdateserv
1071/tcp unknown bsquare-voip
1072/tcp unknown cardax
1073/tcp unknown bridgecontrol
1074/tcp unknown warmspotMgmt
1075/tcp unknown rdrmshc
1076/tcp unknown sns_credit
1077/tcp unknown imgames
1078/tcp unknown avocent-proxy
1079/tcp unknown asprovatalk
1080/tcp unknown socks
1081/tcp unknown pvuniwien
1082/tcp unknown amt-esd-prot
1083/tcp unknown ansoft-lm-1
1084/tcp unknown ansoft-lm-2
1085/tcp unknown webobjects
1086/tcp unknown cplscrambler-lg
1087/tcp unknown cplscrambler-in
1088/tcp unknown cplscrambler-al
1089/tcp unknown ff-annunc
1090/tcp unknown ff-fms
1091/tcp unknown ff-sm
1092/tcp unknown obrpd
1093/tcp unknown proofd
1094/tcp unknown rootd
1095/tcp unknown nicelink
1096/tcp unknown cnrprotocol

1097/tcp unknown sunclustermgr
1098/tcp unknown rmiactivation
1099/tcp unknown rmiregistry
1100/tcp unknown mctp
1102/tcp unknown adobeserver-1
1104/tcp unknown xrl
1105/tcp unknown ftranhc
1106/tcp unknown isoipsigport-1
1107/tcp unknown isoipsigport-2
1108/tcp unknown ratio-adp
1110/tcp unknown nfsd-status
1111/tcp unknown lmsocialserver
1112/tcp unknown msql
1113/tcp unknown ltp-deepspace
1114/tcp unknown mini-sql
1117/tcp unknown ardus-mtrns
1119/tcp unknown bnetgame
1121/tcp unknown rmpp
1122/tcp unknown availant-mgr
1123/tcp unknown murray
1124/tcp unknown hpvmmcontrol
1126/tcp unknown hpvmmdata
1130/tcp unknown casp
1131/tcp unknown caspssl
1132/tcp unknown kvm-via-ip
1137/tcp unknown trim
1138/tcp unknown encrypted_admin
1141/tcp unknown mxomss
1145/tcp unknown x9-icue
1147/tcp unknown capioverlan
1148/tcp unknown elfiq-repl
1149/tcp unknown bvtsonar
1151/tcp unknown unizensus
1152/tcp unknown winpoplanmess
1154/tcp unknown resacommunity
1163/tcp unknown sddp
1164/tcp unknown qsm-proxy
1165/tcp unknown qsm-gui
1166/tcp unknown qsm-remote
1169/tcp unknown tripwire
1174/tcp unknown fnet-remote-ui
1175/tcp unknown dossier
1183/tcp unknown llsurfup-http
1185/tcp unknown catchpole
1186/tcp unknown mysql-cluster
1187/tcp unknown alias
1192/tcp unknown caids-sensor
1198/tcp unknown cajo-discovery
1199/tcp unknown dmidi
1201/tcp unknown nucleus-sand
1213/tcp unknown mpc-lifenet
1216/tcp unknown etebac5
1217/tcp unknown hpss-ndapi
1218/tcp unknown aeroflight-ads
1233/tcp unknown univ-appserver
1234/tcp unknown hotline
1236/tcp unknown bvcontrol
1244/tcp unknown isbconference1
1247/tcp unknown visionpyramid
1248/tcp unknown hermes
1259/tcp unknown opennl-voice
1271/tcp unknown excw
1272/tcp unknown cspmlockmgr
1277/tcp unknown miva-mqs
1287/tcp unknown routematch
1296/tcp unknown dproxy
1300/tcp unknown h323hostcallsc
1301/tcp unknown ci3-software-1
1309/tcp unknown jtag-server
1310/tcp unknown husky
1311/tcp unknown rxmon
1322/tcp unknown novation
1328/tcp unknown ewall
1334/tcp unknown writesrv
1352/tcp unknown lotusnotes
1417/tcp unknown timbuktu-srv1
1433/tcp unknown ms-sql-s

1434/tcp unknown ms-sql-m
1443/tcp unknown ies-lm
1455/tcp unknown esl-lm
1461/tcp unknown ibm_wrless_lan
1494/tcp unknown citrix-ica
1500/tcp unknown vlsi-lm
1501/tcp unknown sas-3
1503/tcp unknown imtc-mcs
1521/tcp unknown oracle
1524/tcp unknown ingreslock
1533/tcp unknown virtual-places
1556/tcp unknown veritas_pbx
1580/tcp unknown tn-tl-r1
1583/tcp unknown simbaexpress
1594/tcp unknown sixtrak
1600/tcp unknown issd
1641/tcp unknown invision
1658/tcp unknown sixnetudr
1666/tcp unknown netview-aix-6
1687/tcp unknown nsjtp-ctrl
1688/tcp unknown nsjtp-data
1700/tcp unknown mps-raft
1717/tcp unknown fj-hdnet
1718/tcp unknown h323gatedisc
1719/tcp unknown h323gatestat
1720/tcp unknown h323q931
1721/tcp unknown caicci
1723/tcp unknown pptp
1755/tcp unknown wms
1761/tcp unknown landesk-rc
1782/tcp unknown hp-hcip
1783/tcp unknown unknown
1801/tcp unknown msmq
1805/tcp unknown enl-name
1812/tcp unknown radius
1839/tcp unknown netopia-vo1
1840/tcp unknown netopia-vo2
1862/tcp unknown mysql-cm-agent
1863/tcp unknown msnp
1864/tcp unknown paradym-31
1875/tcp unknown westell-stats
1900/tcp unknown upnp
1914/tcp unknown elm-momentum
1935/tcp unknown rtmp
1947/tcp unknown sentinelsrm
1971/tcp unknown netop-school
1972/tcp unknown intersys-cache
1974/tcp unknown drp
1984/tcp unknown bigbrother
1998/tcp unknown x25-svc-port
1999/tcp unknown tcp-id-port
2000/tcp unknown cisco-sccp
2001/tcp unknown dc
2002/tcp unknown globe
2003/tcp unknown finger
2004/tcp unknown mailbox
2005/tcp unknown deslogin
2006/tcp unknown invokator
2007/tcp unknown dectalk
2008/tcp unknown conf
2009/tcp unknown news
2010/tcp unknown search
2013/tcp unknown raid-am
2020/tcp unknown xinupageserver
2021/tcp unknown servexec
2022/tcp unknown down
2030/tcp unknown device2
2033/tcp unknown glogger
2034/tcp unknown scoremgr
2035/tcp unknown imsldoc
2038/tcp unknown objectmanager
2040/tcp unknown lam
2041/tcp unknown interbase
2042/tcp unknown isis
2043/tcp unknown isis-bcast
2045/tcp unknown cdfunc
2046/tcp unknown sdfunc

2047/tcp unknown dls
2048/tcp unknown dls-monitor
2049/tcp unknown nfs
2065/tcp unknown dlsrpn
2068/tcp unknown avocentkvm
2099/tcp unknown h2250-annex-g
2100/tcp unknown amiganetfs
2103/tcp unknown zephyr-clt
2105/tcp unknown eklogin
2106/tcp unknown ekshell
2107/tcp unknown msmq-mgmt
2111/tcp unknown kx
2119/tcp unknown gsigatekeeper
2121/tcp unknown ccproxy-ftp
2126/tcp unknown pktcable-cops
2135/tcp unknown gris
2144/tcp unknown lv-ffx
2160/tcp unknown apc-2160
2161/tcp unknown apc-agent
2170/tcp unknown eyetv
2179/tcp unknown vmrdp
2190/tcp unknown tivoconnect
2191/tcp unknown tvbus
2196/tcp unknown unknown
2200/tcp unknown ici
2222/tcp unknown EtherNetIP-1
2251/tcp unknown dif-port
2260/tcp unknown apc-2260
2288/tcp unknown netml
2301/tcp unknown compaqdiag
2323/tcp unknown 3d-nfsd
2366/tcp unknown qip-login
2381/tcp unknown compaq-https
2382/tcp unknown ms-olap3
2383/tcp unknown ms-olap4
2393/tcp unknown ms-olap1
2394/tcp unknown ms-olap2
2399/tcp unknown fmpro-fdal
2401/tcp unknown cvspserver
2492/tcp unknown groove
2500/tcp unknown rtsserv
2522/tcp unknown windb
2525/tcp unknown ms-v-worlds
2557/tcp unknown nicetec-mgmt
2601/tcp unknown zebra
2602/tcp unknown ripd
2604/tcp unknown ospfd
2605/tcp unknown bgpd
2607/tcp unknown connection
2608/tcp unknown wag-service
2638/tcp unknown sybase
2701/tcp unknown sms-rcinfo
2702/tcp unknown sms-xfer
2710/tcp unknown sso-service
2717/tcp unknown pn-requester
2718/tcp unknown pn-requester2
2725/tcp unknown msolap-ptp2
2800/tcp unknown acc-raid
2809/tcp unknown corbaloc
2811/tcp unknown gsiftp
2869/tcp unknown icslap
2875/tcp unknown dxmessagebase2
2909/tcp unknown funk-dialout
2910/tcp unknown tdaccess
2920/tcp unknown roboeda
2967/tcp unknown symantec-av
2968/tcp unknown enpp
2998/tcp unknown iss-realsec
3000/tcp unknown ppp
3001/tcp unknown nessus
3003/tcp unknown cgms
3005/tcp unknown deslogin
3006/tcp unknown deslogind
3007/tcp unknown lotusmtap
3011/tcp unknown trusted-web
3013/tcp unknown gilatskysurfer
3017/tcp unknown event_listener

3030/tcp unknown arepa-cas
3031/tcp unknown eppc
3052/tcp unknown powerchute
3071/tcp unknown csd-mgmt-port
3077/tcp unknown orbix-loc-ssl
3128/tcp unknown squid-http
3168/tcp unknown poweronnud
3211/tcp unknown avsecuremgmt
3221/tcp unknown xnm-clear-text
3260/tcp unknown iscsi
3261/tcp unknown winshadow
3268/tcp unknown globalcatLDAP
3269/tcp unknown globalcatLDAPssl
3283/tcp unknown netassistant
3300/tcp unknown ceph
3301/tcp unknown unknown
3306/tcp unknown mysql
3322/tcp unknown active-net
3323/tcp unknown active-net
3324/tcp unknown active-net
3325/tcp unknown active-net
3333/tcp unknown dec-notes
3351/tcp unknown btrieve
3367/tcp unknown satvid-datalnk
3369/tcp unknown satvid-datalnk
3370/tcp unknown satvid-datalnk
3371/tcp unknown satvid-datalnk
3372/tcp unknown msdtc
3389/tcp unknown ms-wbt-server
3390/tcp unknown dsc
3404/tcp unknown unknown
3476/tcp unknown nppmp
3493/tcp unknown nut
3517/tcp unknown 802-11-iapp
3527/tcp unknown beserver-msg-q
3546/tcp unknown unknown
3551/tcp unknown apcupsd
3580/tcp unknown nati-svrloc
3659/tcp unknown apple-sasl
3689/tcp unknown rendezvous
3690/tcp unknown svn
3703/tcp unknown adobeserver-3
3737/tcp unknown xpanel
3766/tcp unknown sitewatch-s
3784/tcp unknown bfd-control
3800/tcp unknown pwgpsi
3801/tcp unknown ibm-mgr
3809/tcp unknown apocd
3814/tcp unknown neto-dcs
3826/tcp unknown wormux
3827/tcp unknown netmpi
3828/tcp unknown neteh
3851/tcp unknown spectraport
3869/tcp unknown ovsam-mgmt
3871/tcp unknown avocent-adsap
3878/tcp unknown fotogcad
3880/tcp unknown igrs
3889/tcp unknown dandv-tester
3905/tcp unknown mupdate
3914/tcp unknown listcrt-port-2
3918/tcp unknown pktcablemmcops
3920/tcp unknown exasoftport1
3945/tcp unknown emcads
3971/tcp unknown lanrevserver
3986/tcp unknown mapper-ws_ethd
3995/tcp unknown iss-mgmt-ssl
3998/tcp unknown dnx
4000/tcp unknown remoteanything
4001/tcp unknown newoak
4002/tcp unknown mlchat-proxy
4003/tcp unknown pxc-splr-ft
4004/tcp unknown pxc-roid
4005/tcp unknown pxc-pin
4006/tcp unknown pxc-spvr
4045/tcp unknown lockd
4111/tcp unknown xgrid
4125/tcp unknown rww

4126/tcp unknown ddrepl
4129/tcp unknown nuauth
4224/tcp unknown xtell
4242/tcp unknown vrml-multi-use
4279/tcp unknown vrml-multi-use
4321/tcp unknown rwhois
4343/tcp unknown unicall
4443/tcp unknown pharos
4444/tcp unknown krb524
4445/tcp unknown upnotifyp
4446/tcp unknown n1-fwp
4449/tcp unknown privatewire
4550/tcp unknown gds-adppiw-db
4567/tcp unknown tram
4662/tcp unknown edonkey
4848/tcp unknown appserv-http
4899/tcp unknown radmin
4900/tcp unknown hfcs
4998/tcp unknown maybe-veritas
5000/tcp unknown upnp
5001/tcp unknown commplex-link
5002/tcp unknown rfe
5003/tcp unknown filemaker
5004/tcp unknown avt-profile-1
5009/tcp unknown airport-admin
5030/tcp unknown surfpass
5033/tcp unknown jtnetd-server
5050/tcp unknown mmcc
5051/tcp unknown ida-agent
5054/tcp unknown rlm-admin
5060/tcp unknown sip
5061/tcp unknown sip-tls
5080/tcp unknown onscreen
5087/tcp unknown biotic
5100/tcp unknown admd
5101/tcp unknown admdog
5102/tcp unknown admeng
5120/tcp unknown barracuda-bbs
5190/tcp unknown aol
5200/tcp unknown targus-getdata
5214/tcp unknown unknown
5221/tcp unknown 3exmp
5222/tcp unknown xmpp-client
5225/tcp unknown hp-server
5226/tcp unknown hp-status
5269/tcp unknown xmpp-server
5280/tcp unknown xmpp-bosh
5298/tcp unknown presence
5357/tcp unknown wsdapi
5405/tcp unknown pcduo
5414/tcp unknown statusd
5431/tcp unknown park-agent
5432/tcp unknown postgresql
5440/tcp unknown unknown
5500/tcp unknown hotline
5510/tcp unknown secureidprop
5544/tcp unknown unknown
5550/tcp unknown sdadmind
5555/tcp unknown freeciv
5560/tcp unknown isqlplus
5566/tcp unknown westec-connect
5631/tcp unknown pcanywheredata
5633/tcp unknown beorl
5666/tcp unknown nrpe
5678/tcp unknown rrac
5679/tcp unknown activesync
5718/tcp unknown dpm
5730/tcp unknown unieng
5800/tcp unknown vnc-http
5801/tcp unknown vnc-http-1
5802/tcp unknown vnc-http-2
5810/tcp unknown unknown
5811/tcp unknown unknown
5815/tcp unknown unknown
5822/tcp unknown unknown
5825/tcp unknown unknown
5850/tcp unknown unknown

5859/tcp unknown wherehoo
5862/tcp unknown unknown
5877/tcp unknown unknown
5900/tcp unknown vnc
5901/tcp unknown vnc-1
5902/tcp unknown vnc-2
5903/tcp unknown vnc-3
5904/tcp unknown unknown
5906/tcp unknown unknown
5907/tcp unknown unknown
5910/tcp unknown cm
5911/tcp unknown cpdlc
5915/tcp unknown unknown
5922/tcp unknown unknown
5925/tcp unknown unknown
5950/tcp unknown unknown
5952/tcp unknown unknown
5959/tcp unknown unknown
5960/tcp unknown unknown
5961/tcp unknown unknown
5962/tcp unknown unknown
5963/tcp unknown indy
5987/tcp unknown wbem-rmi
5988/tcp unknown wbem-http
5989/tcp unknown wbem-https
5998/tcp unknown ncd-diag
5999/tcp unknown ncd-conf
6000/tcp unknown X11
6001/tcp unknown X11:1
6002/tcp unknown X11:2
6003/tcp unknown X11:3
6004/tcp unknown X11:4
6005/tcp unknown X11:5
6006/tcp unknown X11:6
6007/tcp unknown X11:7
6009/tcp unknown X11:9
6025/tcp unknown x11
6059/tcp unknown X11:59
6100/tcp unknown synchronet-db
6101/tcp unknown backupexec
6106/tcp unknown isdninfo
6112/tcp unknown dtspc
6123/tcp unknown backup-express
6129/tcp unknown unknown
6156/tcp unknown unknown
6346/tcp unknown gnutella
6389/tcp unknown clariion-evr01
6502/tcp unknown netop-rc
6510/tcp unknown mcer-port
6543/tcp unknown mythtv
6547/tcp unknown powerchuteplus
6565/tcp unknown unknown
6566/tcp unknown sane-port
6567/tcp unknown esp
6580/tcp unknown parsec-master
6646/tcp unknown unknown
6666/tcp unknown irc
6667/tcp unknown irc
6668/tcp unknown irc
6669/tcp unknown irc
6689/tcp unknown tsa
6692/tcp unknown unknown
6699/tcp unknown napster
6779/tcp unknown unknown
6788/tcp unknown smc-http
6789/tcp unknown ibm-db2-admin
6792/tcp unknown unknown
6839/tcp unknown unknown
6881/tcp unknown bittorrent-tracker
6901/tcp unknown jetstream
6969/tcp unknown acmsoda
7000/tcp unknown afs3-fileserver
7001/tcp unknown afs3-callback
7002/tcp unknown afs3-prserver
7004/tcp unknown afs3-kaserver
7007/tcp unknown afs3-bos
7019/tcp unknown doceri-ctl

7025/tcp unknown vmsvc-2
7070/tcp unknown realserver
7100/tcp unknown font-service
7103/tcp unknown unknown
7106/tcp unknown unknown
7200/tcp unknown fodms
7201/tcp unknown dlip
7402/tcp unknown rtps-dd-mt
7435/tcp unknown unknown
7443/tcp unknown oracleas-https
7496/tcp unknown unknown
7512/tcp unknown unknown
7625/tcp unknown unknown
7627/tcp unknown soap-http
7676/tcp unknown imqbrokerd
7741/tcp unknown scriptview
7777/tcp unknown cbt
7778/tcp unknown interwise
7800/tcp unknown asr
7911/tcp unknown unknown
7920/tcp unknown unknown
7921/tcp unknown unknown
7937/tcp unknown nsrexecd
7938/tcp unknown lgtomapper
7999/tcp unknown irdmi2
8000/tcp unknown http-alt
8001/tcp unknown vcom-tunnel
8002/tcp unknown teradataordbms
8007/tcp unknown ajp12
8008/tcp unknown http
8009/tcp unknown ajp13
8010/tcp unknown xmpp
8011/tcp unknown unknown
8021/tcp unknown ftp-proxy
8022/tcp unknown oa-system
8031/tcp unknown unknown
8042/tcp unknown fs-agent
8045/tcp unknown unknown
8080/tcp unknown http-proxy
8081/tcp unknown blackice-icecap
8082/tcp unknown blackice-alerts
8083/tcp unknown us-srv
8084/tcp unknown unknown
8085/tcp unknown unknown
8086/tcp unknown d-s-n
8087/tcp unknown simplifymedia
8088/tcp unknown radan-http
8089/tcp unknown unknown
8090/tcp unknown opsmessaging
8093/tcp unknown unknown
8099/tcp unknown unknown
8100/tcp unknown xprint-server
8180/tcp unknown unknown
8181/tcp unknown intermapper
8192/tcp unknown sophos
8193/tcp unknown sophos
8194/tcp unknown sophos
8200/tcp unknown trivnet1
8222/tcp unknown unknown
8254/tcp unknown unknown
8290/tcp unknown unknown
8291/tcp unknown unknown
8292/tcp unknown blp3
8300/tcp unknown tmi
8333/tcp unknown bitcoin
8383/tcp unknown m2mservices
8400/tcp unknown cvd
8402/tcp unknown abarsd
8443/tcp unknown https-alt
8500/tcp unknown fmtp
8600/tcp unknown asterix
8649/tcp unknown unknown
8651/tcp unknown unknown
8652/tcp unknown unknown
8654/tcp unknown unknown
8701/tcp unknown unknown
8800/tcp unknown sunwebadmin

8873/tcp unknown dxspider
8888/tcp unknown sun-answerbook
8899/tcp unknown ospf-lite
8994/tcp unknown unknown
9000/tcp unknown cslistener
9001/tcp unknown tor-orport
9002/tcp unknown dynamid
9003/tcp unknown unknown
9009/tcp unknown pichat
9010/tcp unknown sdr
9011/tcp unknown unknown
9040/tcp unknown tor-trans
9050/tcp unknown tor-socks
9071/tcp unknown unknown
9080/tcp unknown glrpc
9081/tcp unknown unknown
9090/tcp unknown zeus-admin
9091/tcp unknown xmltec-xmlmail
9099/tcp unknown unknown
9100/tcp unknown jetdirect
9101/tcp unknown jetdirect
9102/tcp unknown jetdirect
9103/tcp unknown jetdirect
9110/tcp unknown unknown
9111/tcp unknown DragonIDSConsole
9200/tcp unknown wap-wsp
9207/tcp unknown wap-vcal-s
9220/tcp unknown unknown
9290/tcp unknown unknown
9415/tcp unknown unknown
9418/tcp unknown git
9485/tcp unknown unknown
9500/tcp unknown ismserver
9502/tcp unknown unknown
9503/tcp unknown unknown
9535/tcp unknown man
9575/tcp unknown unknown
9593/tcp unknown cba8
9594/tcp unknown msgsys
9595/tcp unknown pds
9618/tcp unknown condor
9666/tcp unknown zoomcp
9876/tcp unknown sd
9877/tcp unknown unknown
9878/tcp unknown kca-service
9898/tcp unknown monkeycom
9900/tcp unknown iua
9917/tcp unknown unknown
9929/tcp unknown nping-echo
9943/tcp unknown unknown
9944/tcp unknown unknown
9968/tcp unknown unknown
9998/tcp unknown distinct32
9999/tcp unknown abyss
10000/tcp unknown snet-sensor-mgmt
10001/tcp unknown scp-config
10002/tcp unknown documentum
10003/tcp unknown documentum_s
10004/tcp unknown emcrmirccd
10009/tcp unknown swdtp-sv
10010/tcp unknown rxapi
10012/tcp unknown unknown
10024/tcp unknown unknown
10025/tcp unknown unknown
10082/tcp unknown amandaidx
10180/tcp unknown unknown
10215/tcp unknown unknown
10243/tcp unknown unknown
10566/tcp unknown unknown
10616/tcp unknown unknown
10617/tcp unknown unknown
10621/tcp unknown unknown
10626/tcp unknown unknown
10628/tcp unknown unknown
10629/tcp unknown unknown
10778/tcp unknown unknown
11110/tcp unknown sgi-soap

11111/tcp unknown vce
11967/tcp unknown sysinfo-sp
12000/tcp unknown cce4x
12174/tcp unknown unknown
12265/tcp unknown unknown
12345/tcp unknown netbus
13456/tcp unknown unknown
13722/tcp unknown netbackup
13782/tcp unknown netbackup
13783/tcp unknown netbackup
14000/tcp unknown scotty-ft
14238/tcp unknown unknown
14441/tcp unknown unknown
14442/tcp unknown unknown
15000/tcp unknown hydap
15002/tcp unknown onep-tls
15003/tcp unknown unknown
15004/tcp unknown unknown
15660/tcp unknown bex-xr
15742/tcp unknown unknown
16000/tcp unknown fmsas
16001/tcp unknown fmsascon
16012/tcp unknown unknown
16016/tcp unknown unknown
16018/tcp unknown unknown
16080/tcp unknown osxwebadmin
16113/tcp unknown unknown
16992/tcp unknown amt-soap-http
16993/tcp unknown amt-soap-https
17877/tcp unknown unknown
17988/tcp unknown unknown
18040/tcp unknown unknown
18101/tcp unknown unknown
18988/tcp unknown unknown
19101/tcp unknown unknown
19283/tcp unknown keysrvr
19315/tcp unknown keyshadow
19350/tcp unknown unknown
19780/tcp unknown unknown
19801/tcp unknown unknown
19842/tcp unknown unknown
20000/tcp unknown dnp
20005/tcp unknown btx
20031/tcp unknown unknown
20221/tcp unknown unknown
20222/tcp unknown ipulse-ics
20828/tcp unknown unknown
21571/tcp unknown unknown
22939/tcp unknown unknown
23502/tcp unknown unknown
24444/tcp unknown unknown
24800/tcp unknown unknown
25734/tcp unknown unknown
25735/tcp unknown unknown
26214/tcp unknown unknown
27000/tcp unknown flexlm0
27352/tcp unknown unknown
27353/tcp unknown unknown
27355/tcp unknown unknown
27356/tcp unknown unknown
27715/tcp unknown unknown
28201/tcp unknown unknown
30000/tcp unknown ndmps
30718/tcp unknown unknown
30951/tcp unknown unknown
31038/tcp unknown unknown
31337/tcp unknown Elite
32768/tcp unknown filenet-tms
32769/tcp unknown filenet-rpc
32770/tcp unknown sometimes-rpc3
32771/tcp unknown sometimes-rpc5
32772/tcp unknown sometimes-rpc7
32773/tcp unknown sometimes-rpc9
32774/tcp unknown sometimes-rpc11
32775/tcp unknown sometimes-rpc13
32776/tcp unknown sometimes-rpc15
32777/tcp unknown sometimes-rpc17

32778/tcp unknown sometimes-rpc19
32779/tcp unknown sometimes-rpc21
32780/tcp unknown sometimes-rpc23
32781/tcp unknown unknown
32782/tcp unknown unknown
32783/tcp unknown unknown
32784/tcp unknown unknown
32785/tcp unknown unknown
33354/tcp unknown unknown
33899/tcp unknown unknown
34571/tcp unknown unknown
34572/tcp unknown unknown
34573/tcp unknown unknown
35500/tcp unknown unknown
38292/tcp unknown landesk-cba
40193/tcp unknown unknown
40911/tcp unknown unknown
41511/tcp unknown unknown
42510/tcp unknown caerpc
44176/tcp unknown unknown
44442/tcp unknown coldfusion-auth
44443/tcp unknown coldfusion-auth
44501/tcp unknown unknown
45100/tcp unknown unknown
48080/tcp unknown unknown
49152/tcp unknown unknown
49153/tcp unknown unknown
49154/tcp unknown unknown
49155/tcp unknown unknown
49156/tcp unknown unknown
49157/tcp unknown unknown
49158/tcp unknown unknown
49159/tcp unknown unknown
49160/tcp unknown unknown
49161/tcp unknown unknown
49163/tcp unknown unknown
49165/tcp unknown unknown
49167/tcp unknown unknown
49175/tcp unknown unknown
49176/tcp unknown unknown
49400/tcp unknown compaqdiag
49999/tcp unknown unknown
50000/tcp unknown ibm-db2
50001/tcp unknown unknown
50002/tcp unknown iiimsf
50003/tcp unknown unknown
50006/tcp unknown unknown
50300/tcp unknown unknown
50389/tcp unknown unknown
50500/tcp unknown unknown
50636/tcp unknown unknown
50800/tcp unknown unknown
51103/tcp unknown unknown
51493/tcp unknown unknown
52673/tcp unknown unknown
52822/tcp unknown unknown
52848/tcp unknown unknown
52869/tcp unknown unknown
54045/tcp unknown unknown
54328/tcp unknown unknown
55055/tcp unknown unknown
55056/tcp unknown unknown
55555/tcp unknown unknown
55600/tcp unknown unknown
56737/tcp unknown unknown
56738/tcp unknown unknown
57294/tcp unknown unknown
57797/tcp unknown unknown
58080/tcp unknown unknown
60020/tcp unknown unknown
60443/tcp unknown unknown
61532/tcp unknown unknown
61900/tcp unknown unknown
62078/tcp unknown iphone-sync
63331/tcp unknown unknown
64623/tcp unknown unknown
64680/tcp unknown unknown

```
65000/tcp unknown unknown
65129/tcp unknown unknown
65389/tcp unknown unknown

NSE: Script Post-scanning.
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 129.04 seconds
        Raw packets sent: 7156 (302.518KB) | Rcvd: 6059 (244.850KB)
```

ANEXO 2 - RESULTADOS NO NMAP PARA A REDE DE TESTES 2

```
Starting Nmap 7.50 ( https://nmap.org ) at 2017-12-08 10:06 E. South America Daylight Time
NSE: Loaded 144 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:06
Completed NSE at 10:06, 0.01s elapsed
Initiating NSE at 10:06
Completed NSE at 10:06, 0.00s elapsed
Initiating ARP Ping Scan at 10:06
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 10:07, 1.85s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 10:07
Completed Parallel DNS resolution of 255 hosts. at 10:07, 16.50s elapsed
Nmap scan report for 10.1.34.0 [host down]
Nmap scan report for 10.1.34.2 [host down]
Nmap scan report for 10.1.34.3 [host down]
Nmap scan report for 10.1.34.4 [host down]
Nmap scan report for 10.1.34.5 [host down]
Nmap scan report for 10.1.34.6 [host down]
Nmap scan report for 10.1.34.7 [host down]
Nmap scan report for 10.1.34.8 [host down]
Nmap scan report for 10.1.34.9 [host down]
Nmap scan report for 10.1.34.10 [host down]
Nmap scan report for 10.1.34.11 [host down]
Nmap scan report for 10.1.34.12 [host down]
Nmap scan report for 10.1.34.13 [host down]
Nmap scan report for 10.1.34.14 [host down]
Nmap scan report for 10.1.34.15 [host down]
Nmap scan report for 10.1.34.16 [host down]
Nmap scan report for 10.1.34.17 [host down]
Nmap scan report for 10.1.34.19 [host down]
Nmap scan report for 10.1.34.22 [host down]
Nmap scan report for 10.1.34.23 [host down]
Nmap scan report for 10.1.34.24 [host down]
Nmap scan report for 10.1.34.25 [host down]
Nmap scan report for 10.1.34.29 [host down]
Nmap scan report for 10.1.34.30 [host down]
Nmap scan report for 10.1.34.32 [host down]
Nmap scan report for 10.1.34.33 [host down]
Nmap scan report for 10.1.34.34 [host down]
Nmap scan report for 10.1.34.35 [host down]
Nmap scan report for 10.1.34.36 [host down]
Nmap scan report for 10.1.34.37 [host down]
Nmap scan report for 10.1.34.38 [host down]
Nmap scan report for 10.1.34.39 [host down]
Nmap scan report for 10.1.34.40 [host down]
Nmap scan report for 10.1.34.41 [host down]
Nmap scan report for 10.1.34.42 [host down]
Nmap scan report for 10.1.34.43 [host down]
Nmap scan report for 10.1.34.44 [host down]
Nmap scan report for 10.1.34.45 [host down]
Nmap scan report for 10.1.34.46 [host down]
Nmap scan report for 10.1.34.47 [host down]
Nmap scan report for 10.1.34.48 [host down]
Nmap scan report for 10.1.34.49 [host down]
Nmap scan report for 10.1.34.50 [host down]
Nmap scan report for 10.1.34.51 [host down]
Nmap scan report for 10.1.34.52 [host down]
Nmap scan report for 10.1.34.53 [host down]
Nmap scan report for 10.1.34.54 [host down]
Nmap scan report for 10.1.34.55 [host down]
Nmap scan report for 10.1.34.56 [host down]
Nmap scan report for 10.1.34.57 [host down]
Nmap scan report for 10.1.34.58 [host down]
Nmap scan report for 10.1.34.59 [host down]
Nmap scan report for 10.1.34.61 [host down]
Nmap scan report for 10.1.34.62 [host down]
Nmap scan report for 10.1.34.63 [host down]
Nmap scan report for 10.1.34.64 [host down]
Nmap scan report for 10.1.34.65 [host down]
Nmap scan report for 10.1.34.66 [host down]
Nmap scan report for 10.1.34.67 [host down]
Nmap scan report for 10.1.34.68 [host down]
Nmap scan report for 10.1.34.69 [host down]
Nmap scan report for 10.1.34.70 [host down]
```

Nmap scan report for 10.1.34.74 [host down]
Nmap scan report for 10.1.34.78 [host down]
Nmap scan report for 10.1.34.79 [host down]
Nmap scan report for 10.1.34.80 [host down]
Nmap scan report for 10.1.34.82 [host down]
Nmap scan report for 10.1.34.84 [host down]
Nmap scan report for 10.1.34.86 [host down]
Nmap scan report for 10.1.34.88 [host down]
Nmap scan report for 10.1.34.90 [host down]
Nmap scan report for 10.1.34.91 [host down]
Nmap scan report for 10.1.34.92 [host down]
Nmap scan report for 10.1.34.93 [host down]
Nmap scan report for 10.1.34.94 [host down]
Nmap scan report for 10.1.34.95 [host down]
Nmap scan report for 10.1.34.96 [host down]
Nmap scan report for 10.1.34.98 [host down]
Nmap scan report for 10.1.34.103 [host down]
Nmap scan report for 10.1.34.104 [host down]
Nmap scan report for 10.1.34.105 [host down]
Nmap scan report for 10.1.34.106 [host down]
Nmap scan report for 10.1.34.107 [host down]
Nmap scan report for 10.1.34.108 [host down]
Nmap scan report for 10.1.34.109 [host down]
Nmap scan report for 10.1.34.110 [host down]
Nmap scan report for 10.1.34.112 [host down]
Nmap scan report for 10.1.34.113 [host down]
Nmap scan report for 10.1.34.114 [host down]
Nmap scan report for 10.1.34.115 [host down]
Nmap scan report for 10.1.34.116 [host down]
Nmap scan report for 10.1.34.117 [host down]
Nmap scan report for 10.1.34.118 [host down]
Nmap scan report for 10.1.34.119 [host down]
Nmap scan report for 10.1.34.120 [host down]
Nmap scan report for 10.1.34.121 [host down]
Nmap scan report for 10.1.34.122 [host down]
Nmap scan report for 10.1.34.123 [host down]
Nmap scan report for 10.1.34.124 [host down]
Nmap scan report for 10.1.34.125 [host down]
Nmap scan report for 10.1.34.130 [host down]
Nmap scan report for 10.1.34.131 [host down]
Nmap scan report for 10.1.34.132 [host down]
Nmap scan report for 10.1.34.133 [host down]
Nmap scan report for 10.1.34.134 [host down]
Nmap scan report for 10.1.34.135 [host down]
Nmap scan report for 10.1.34.136 [host down]
Nmap scan report for 10.1.34.137 [host down]
Nmap scan report for 10.1.34.138 [host down]
Nmap scan report for 10.1.34.139 [host down]
Nmap scan report for 10.1.34.140 [host down]
Nmap scan report for 10.1.34.141 [host down]
Nmap scan report for 10.1.34.142 [host down]
Nmap scan report for 10.1.34.143 [host down]
Nmap scan report for 10.1.34.144 [host down]
Nmap scan report for 10.1.34.145 [host down]
Nmap scan report for 10.1.34.146 [host down]
Nmap scan report for 10.1.34.147 [host down]
Nmap scan report for 10.1.34.148 [host down]
Nmap scan report for 10.1.34.149 [host down]
Nmap scan report for 10.1.34.150 [host down]
Nmap scan report for 10.1.34.154 [host down]
Nmap scan report for 10.1.34.155 [host down]
Nmap scan report for 10.1.34.156 [host down]
Nmap scan report for 10.1.34.157 [host down]
Nmap scan report for 10.1.34.158 [host down]
Nmap scan report for 10.1.34.159 [host down]
Nmap scan report for 10.1.34.160 [host down]
Nmap scan report for 10.1.34.161 [host down]
Nmap scan report for 10.1.34.162 [host down]
Nmap scan report for 10.1.34.163 [host down]
Nmap scan report for 10.1.34.164 [host down]
Nmap scan report for 10.1.34.165 [host down]
Nmap scan report for 10.1.34.166 [host down]
Nmap scan report for 10.1.34.167 [host down]
Nmap scan report for 10.1.34.168 [host down]
Nmap scan report for 10.1.34.169 [host down]
Nmap scan report for 10.1.34.170 [host down]
Nmap scan report for 10.1.34.171 [host down]

```
Nmap scan report for 10.1.34.172 [host down]
Nmap scan report for 10.1.34.173 [host down]
Nmap scan report for 10.1.34.174 [host down]
Nmap scan report for 10.1.34.175 [host down]
Nmap scan report for 10.1.34.176 [host down]
Nmap scan report for 10.1.34.177 [host down]
Nmap scan report for 10.1.34.178 [host down]
Nmap scan report for 10.1.34.179 [host down]
Nmap scan report for 10.1.34.180 [host down]
Nmap scan report for 10.1.34.181 [host down]
Nmap scan report for 10.1.34.182 [host down]
Nmap scan report for 10.1.34.183 [host down]
Nmap scan report for 10.1.34.184 [host down]
Nmap scan report for 10.1.34.185 [host down]
Nmap scan report for 10.1.34.186 [host down]
Nmap scan report for 10.1.34.187 [host down]
Nmap scan report for 10.1.34.188 [host down]
Nmap scan report for 10.1.34.189 [host down]
Nmap scan report for 10.1.34.190 [host down]
Nmap scan report for 10.1.34.191 [host down]
Nmap scan report for 10.1.34.192 [host down]
Nmap scan report for 10.1.34.193 [host down]
Nmap scan report for 10.1.34.194 [host down]
Nmap scan report for 10.1.34.196 [host down]
Nmap scan report for 10.1.34.197 [host down]
Nmap scan report for 10.1.34.198 [host down]
Nmap scan report for 10.1.34.199 [host down]
Nmap scan report for 10.1.34.200 [host down]
Nmap scan report for 10.1.34.202 [host down]
Nmap scan report for 10.1.34.203 [host down]
Nmap scan report for 10.1.34.204 [host down]
Nmap scan report for 10.1.34.205 [host down]
Nmap scan report for 10.1.34.206 [host down]
Nmap scan report for 10.1.34.207 [host down]
Nmap scan report for 10.1.34.208 [host down]
Nmap scan report for 10.1.34.209 [host down]
Nmap scan report for 10.1.34.210 [host down]
Nmap scan report for 10.1.34.211 [host down]
Nmap scan report for 10.1.34.212 [host down]
Nmap scan report for 10.1.34.213 [host down]
Nmap scan report for 10.1.34.214 [host down]
Nmap scan report for 10.1.34.215 [host down]
Nmap scan report for 10.1.34.216 [host down]
Nmap scan report for 10.1.34.217 [host down]
Nmap scan report for 10.1.34.218 [host down]
Nmap scan report for 10.1.34.219 [host down]
Nmap scan report for 10.1.34.220 [host down]
Nmap scan report for 10.1.34.221 [host down]
Nmap scan report for 10.1.34.222 [host down]
Nmap scan report for 10.1.34.223 [host down]
Nmap scan report for 10.1.34.224 [host down]
Nmap scan report for 10.1.34.226 [host down]
Nmap scan report for 10.1.34.227 [host down]
Nmap scan report for 10.1.34.228 [host down]
Nmap scan report for 10.1.34.229 [host down]
Nmap scan report for 10.1.34.231 [host down]
Nmap scan report for 10.1.34.232 [host down]
Nmap scan report for 10.1.34.234 [host down]
Nmap scan report for 10.1.34.235 [host down]
Nmap scan report for 10.1.34.236 [host down]
Nmap scan report for 10.1.34.237 [host down]
Nmap scan report for 10.1.34.238 [host down]
Nmap scan report for 10.1.34.239 [host down]
Nmap scan report for 10.1.34.240 [host down]
Nmap scan report for 10.1.34.241 [host down]
Nmap scan report for 10.1.34.242 [host down]
Nmap scan report for 10.1.34.245 [host down]
Nmap scan report for 10.1.34.246 [host down]
Nmap scan report for 10.1.34.249 [host down]
Nmap scan report for 10.1.34.251 [host down]
Nmap scan report for 10.1.34.252 [host down]
Nmap scan report for 10.1.34.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 10:07
Completed Parallel DNS resolution of 1 host. at 10:07, 16.50s elapsed
Initiating SYN Stealth Scan at 10:07
Scanning 44 hosts [1000 ports/host]
Discovered open port 443/tcp on 10.1.34.27
```

Discovered open port 443/tcp on 10.1.34.31
Discovered open port 443/tcp on 10.1.34.26
Discovered open port 443/tcp on 10.1.34.28
Discovered open port 443/tcp on 10.1.34.100
Discovered open port 443/tcp on 10.1.34.126
Discovered open port 443/tcp on 10.1.34.127
Discovered open port 443/tcp on 10.1.34.128
Discovered open port 443/tcp on 10.1.34.21
Discovered open port 135/tcp on 10.1.34.153
Discovered open port 135/tcp on 10.1.34.225
Discovered open port 135/tcp on 10.1.34.233
Discovered open port 445/tcp on 10.1.34.225
Discovered open port 445/tcp on 10.1.34.233
Discovered open port 22/tcp on 10.1.34.18
Discovered open port 22/tcp on 10.1.34.20
Discovered open port 22/tcp on 10.1.34.21
Discovered open port 22/tcp on 10.1.34.26
Discovered open port 22/tcp on 10.1.34.28
Discovered open port 22/tcp on 10.1.34.76
Discovered open port 22/tcp on 10.1.34.77
Discovered open port 22/tcp on 10.1.34.27
Discovered open port 22/tcp on 10.1.34.85
Discovered open port 22/tcp on 10.1.34.87
Discovered open port 22/tcp on 10.1.34.89
Discovered open port 22/tcp on 10.1.34.97
Discovered open port 22/tcp on 10.1.34.99
Discovered open port 22/tcp on 10.1.34.100
Discovered open port 22/tcp on 10.1.34.111
Discovered open port 22/tcp on 10.1.34.195
Discovered open port 22/tcp on 10.1.34.201
Discovered open port 22/tcp on 10.1.34.250
Discovered open port 22/tcp on 10.1.34.71
Discovered open port 22/tcp on 10.1.34.72
Discovered open port 22/tcp on 10.1.34.81
Discovered open port 22/tcp on 10.1.34.31
Discovered open port 22/tcp on 10.1.34.83
Discovered open port 22/tcp on 10.1.34.101
Discovered open port 22/tcp on 10.1.34.102
Discovered open port 22/tcp on 10.1.34.73
Discovered open port 22/tcp on 10.1.34.75
Discovered open port 80/tcp on 10.1.34.21
Discovered open port 80/tcp on 10.1.34.27
Discovered open port 80/tcp on 10.1.34.26
Discovered open port 80/tcp on 10.1.34.201
Discovered open port 80/tcp on 10.1.34.151
Discovered open port 80/tcp on 10.1.34.250
Discovered open port 80/tcp on 10.1.34.60
Discovered open port 80/tcp on 10.1.34.100
Discovered open port 80/tcp on 10.1.34.28
Discovered open port 80/tcp on 10.1.34.152
Discovered open port 80/tcp on 10.1.34.254
Discovered open port 80/tcp on 10.1.34.31
Discovered open port 23/tcp on 10.1.34.77
Discovered open port 23/tcp on 10.1.34.26
Discovered open port 23/tcp on 10.1.34.27
Discovered open port 23/tcp on 10.1.34.151
Discovered open port 23/tcp on 10.1.34.20
Discovered open port 23/tcp on 10.1.34.253
Discovered open port 23/tcp on 10.1.34.60
Discovered open port 23/tcp on 10.1.34.72
Discovered open port 23/tcp on 10.1.34.28
Discovered open port 23/tcp on 10.1.34.89
Discovered open port 23/tcp on 10.1.34.102
Discovered open port 23/tcp on 10.1.34.152
Discovered open port 23/tcp on 10.1.34.230
Discovered open port 23/tcp on 10.1.34.75
Discovered open port 23/tcp on 10.1.34.31
Discovered open port 23/tcp on 10.1.34.254
Discovered open port 21/tcp on 10.1.34.76
Discovered open port 21/tcp on 10.1.34.85
Discovered open port 21/tcp on 10.1.34.111
Discovered open port 21/tcp on 10.1.34.151
Discovered open port 111/tcp on 10.1.34.18
Discovered open port 21/tcp on 10.1.34.20
Discovered open port 21/tcp on 10.1.34.71
Discovered open port 21/tcp on 10.1.34.60
Discovered open port 111/tcp on 10.1.34.76

Discovered open port 21/tcp on 10.1.34.77
Discovered open port 111/tcp on 10.1.34.85
Discovered open port 21/tcp on 10.1.34.83
Discovered open port 111/tcp on 10.1.34.97
Discovered open port 21/tcp on 10.1.34.87
Discovered open port 21/tcp on 10.1.34.89
Discovered open port 111/tcp on 10.1.34.99
Discovered open port 111/tcp on 10.1.34.111
Discovered open port 21/tcp on 10.1.34.102
Discovered open port 111/tcp on 10.1.34.151
Discovered open port 21/tcp on 10.1.34.152
Discovered open port 111/tcp on 10.1.34.201
Discovered open port 111/tcp on 10.1.34.20
Discovered open port 111/tcp on 10.1.34.71
Discovered open port 111/tcp on 10.1.34.60
Discovered open port 21/tcp on 10.1.34.72
Discovered open port 21/tcp on 10.1.34.75
Discovered open port 111/tcp on 10.1.34.77
Discovered open port 111/tcp on 10.1.34.83
Discovered open port 21/tcp on 10.1.34.81
Discovered open port 111/tcp on 10.1.34.87
Discovered open port 111/tcp on 10.1.34.89
Discovered open port 111/tcp on 10.1.34.100
Discovered open port 111/tcp on 10.1.34.102
Discovered open port 111/tcp on 10.1.34.195
Discovered open port 111/tcp on 10.1.34.152
Discovered open port 21/tcp on 10.1.34.230
Discovered open port 111/tcp on 10.1.34.72
Discovered open port 111/tcp on 10.1.34.81
Discovered open port 111/tcp on 10.1.34.101
Discovered open port 139/tcp on 10.1.34.225
Discovered open port 139/tcp on 10.1.34.233
Discovered open port 3306/tcp on 10.1.34.250
Discovered open port 111/tcp on 10.1.34.75
Discovered open port 21/tcp on 10.1.34.73
Discovered open port 111/tcp on 10.1.34.73
Discovered open port 8000/tcp on 10.1.34.18
Discovered open port 8000/tcp on 10.1.34.76
Discovered open port 8000/tcp on 10.1.34.195
Discovered open port 443/tcp on 10.1.34.248
Discovered open port 443/tcp on 10.1.34.247
Discovered open port 445/tcp on 10.1.34.153
Discovered open port 80/tcp on 10.1.34.243
Discovered open port 80/tcp on 10.1.34.248
Discovered open port 80/tcp on 10.1.34.247
Discovered open port 80/tcp on 10.1.34.244
Discovered open port 23/tcp on 10.1.34.243
Discovered open port 23/tcp on 10.1.34.244
Discovered open port 23/tcp on 10.1.34.247
Discovered open port 23/tcp on 10.1.34.248
Discovered open port 23/tcp on 10.1.34.1
Discovered open port 139/tcp on 10.1.34.153
Discovered open port 49155/tcp on 10.1.34.225
Discovered open port 49154/tcp on 10.1.34.225
Discovered open port 2049/tcp on 10.1.34.97
Discovered open port 2049/tcp on 10.1.34.99
Discovered open port 2049/tcp on 10.1.34.100
Discovered open port 7200/tcp on 10.1.34.76
Discovered open port 9090/tcp on 10.1.34.89
Discovered open port 9090/tcp on 10.1.34.102
Discovered open port 9090/tcp on 10.1.34.85
Discovered open port 9090/tcp on 10.1.34.83
Discovered open port 9090/tcp on 10.1.34.81
Discovered open port 9090/tcp on 10.1.34.87
Discovered open port 514/tcp on 10.1.34.26
Discovered open port 514/tcp on 10.1.34.89
Discovered open port 514/tcp on 10.1.34.102
Discovered open port 514/tcp on 10.1.34.195
Discovered open port 514/tcp on 10.1.34.85
Discovered open port 514/tcp on 10.1.34.18
Discovered open port 514/tcp on 10.1.34.111
Discovered open port 514/tcp on 10.1.34.76
Discovered open port 514/tcp on 10.1.34.77
Discovered open port 514/tcp on 10.1.34.20
Discovered open port 514/tcp on 10.1.34.27
Discovered open port 514/tcp on 10.1.34.75
Discovered open port 514/tcp on 10.1.34.101

Discovered open port 514/tcp on 10.1.34.73
Discovered open port 514/tcp on 10.1.34.83
Discovered open port 514/tcp on 10.1.34.71
Discovered open port 514/tcp on 10.1.34.31
Discovered open port 514/tcp on 10.1.34.28
Discovered open port 514/tcp on 10.1.34.81
Discovered open port 514/tcp on 10.1.34.72
Discovered open port 514/tcp on 10.1.34.87
Discovered open port 1023/tcp on 10.1.34.20
Discovered open port 49152/tcp on 10.1.34.225
Discovered open port 11111/tcp on 10.1.34.76
Discovered open port 11111/tcp on 10.1.34.75
Discovered open port 11111/tcp on 10.1.34.77
Discovered open port 11111/tcp on 10.1.34.20
Discovered open port 11111/tcp on 10.1.34.73
Discovered open port 11111/tcp on 10.1.34.72
Discovered open port 1027/tcp on 10.1.34.26
Discovered open port 5432/tcp on 10.1.34.89
Discovered open port 5432/tcp on 10.1.34.102
Discovered open port 5432/tcp on 10.1.34.195
Discovered open port 5432/tcp on 10.1.34.75
Discovered open port 5432/tcp on 10.1.34.201
Discovered open port 5432/tcp on 10.1.34.85
Discovered open port 5432/tcp on 10.1.34.76
Discovered open port 5432/tcp on 10.1.34.111
Discovered open port 1027/tcp on 10.1.34.31
Discovered open port 5432/tcp on 10.1.34.83
Discovered open port 1027/tcp on 10.1.34.27
Discovered open port 5432/tcp on 10.1.34.101
Discovered open port 5432/tcp on 10.1.34.73
Discovered open port 5432/tcp on 10.1.34.18
Discovered open port 5432/tcp on 10.1.34.77
Discovered open port 5432/tcp on 10.1.34.20
Discovered open port 5432/tcp on 10.1.34.81
Discovered open port 5432/tcp on 10.1.34.71
Discovered open port 1027/tcp on 10.1.34.28
Discovered open port 5432/tcp on 10.1.34.72
Discovered open port 5432/tcp on 10.1.34.87
Discovered open port 8100/tcp on 10.1.34.195
Discovered open port 49156/tcp on 10.1.34.225
Discovered open port 8100/tcp on 10.1.34.18
Discovered open port 902/tcp on 10.1.34.75
Discovered open port 50000/tcp on 10.1.34.26
Discovered open port 902/tcp on 10.1.34.73
Discovered open port 902/tcp on 10.1.34.20
Discovered open port 902/tcp on 10.1.34.77
Discovered open port 50000/tcp on 10.1.34.31
Discovered open port 50000/tcp on 10.1.34.27
Discovered open port 902/tcp on 10.1.34.72
Discovered open port 50000/tcp on 10.1.34.28
Discovered open port 1100/tcp on 10.1.34.151
Discovered open port 1100/tcp on 10.1.34.60
Discovered open port 1100/tcp on 10.1.34.152
Discovered open port 5989/tcp on 10.1.34.102
Discovered open port 5989/tcp on 10.1.34.89
Discovered open port 7777/tcp on 10.1.34.230
Discovered open port 5989/tcp on 10.1.34.75
Discovered open port 5989/tcp on 10.1.34.73
Discovered open port 5989/tcp on 10.1.34.77
Discovered open port 5989/tcp on 10.1.34.20
Discovered open port 5989/tcp on 10.1.34.72
Discovered open port 49153/tcp on 10.1.34.225
Discovered open port 9/tcp on 10.1.34.230
Discovered open port 6000/tcp on 10.1.34.75
Discovered open port 6000/tcp on 10.1.34.201
Discovered open port 6000/tcp on 10.1.34.83
Discovered open port 6000/tcp on 10.1.34.85
Discovered open port 6000/tcp on 10.1.34.73
Discovered open port 6000/tcp on 10.1.34.111
Discovered open port 6000/tcp on 10.1.34.76
Discovered open port 513/tcp on 10.1.34.26
Discovered open port 6000/tcp on 10.1.34.81
Discovered open port 6000/tcp on 10.1.34.77
Discovered open port 6000/tcp on 10.1.34.20
Discovered open port 6000/tcp on 10.1.34.71
Discovered open port 513/tcp on 10.1.34.31
Discovered open port 6000/tcp on 10.1.34.72

```
Discovered open port 6000/tcp on 10.1.34.101
Discovered open port 513/tcp on 10.1.34.27
Discovered open port 6000/tcp on 10.1.34.87
Discovered open port 513/tcp on 10.1.34.28
Discovered open port 37/tcp on 10.1.34.75
Discovered open port 37/tcp on 10.1.34.73
Discovered open port 37/tcp on 10.1.34.99
Discovered open port 37/tcp on 10.1.34.195
Discovered open port 37/tcp on 10.1.34.111
Discovered open port 37/tcp on 10.1.34.76
Discovered open port 37/tcp on 10.1.34.77
Discovered open port 37/tcp on 10.1.34.18
Discovered open port 37/tcp on 10.1.34.71
Discovered open port 37/tcp on 10.1.34.101
Discovered open port 515/tcp on 10.1.34.26
Discovered open port 515/tcp on 10.1.34.31
Discovered open port 515/tcp on 10.1.34.27
Discovered open port 515/tcp on 10.1.34.28
Completed SYN Stealth Scan against 10.1.34.253 in 41.46s (43 hosts left)
Completed SYN Stealth Scan against 10.1.34.26 in 42.20s (42 hosts left)
Completed SYN Stealth Scan against 10.1.34.89 in 42.25s (41 hosts left)
Completed SYN Stealth Scan against 10.1.34.97 in 42.25s (40 hosts left)
Completed SYN Stealth Scan against 10.1.34.151 in 42.33s (39 hosts left)
Completed SYN Stealth Scan against 10.1.34.250 in 42.33s (38 hosts left)
Completed SYN Stealth Scan against 10.1.34.102 in 42.38s (37 hosts left)
Completed SYN Stealth Scan against 10.1.34.233 in 42.42s (36 hosts left)
Completed SYN Stealth Scan against 10.1.34.73 in 42.47s (35 hosts left)
Completed SYN Stealth Scan against 10.1.34.83 in 42.47s (34 hosts left)
Completed SYN Stealth Scan against 10.1.34.75 in 42.51s (33 hosts left)
Completed SYN Stealth Scan against 10.1.34.60 in 42.60s (32 hosts left)
Completed SYN Stealth Scan against 10.1.34.81 in 42.60s (31 hosts left)
Completed SYN Stealth Scan against 10.1.34.85 in 42.60s (30 hosts left)
Completed SYN Stealth Scan against 10.1.34.99 in 42.60s (29 hosts left)
Completed SYN Stealth Scan against 10.1.34.152 in 42.60s (28 hosts left)
Completed SYN Stealth Scan against 10.1.34.254 in 42.60s (27 hosts left)
Completed SYN Stealth Scan against 10.1.34.111 in 42.65s (26 hosts left)
Completed SYN Stealth Scan against 10.1.34.195 in 42.65s (25 hosts left)
Completed SYN Stealth Scan against 10.1.34.201 in 42.65s (24 hosts left)
Completed SYN Stealth Scan against 10.1.34.225 in 42.65s (23 hosts left)
Completed SYN Stealth Scan against 10.1.34.31 in 42.74s (22 hosts left)
Completed SYN Stealth Scan against 10.1.34.77 in 42.74s (21 hosts left)
Completed SYN Stealth Scan against 10.1.34.100 in 42.78s (20 hosts left)
Completed SYN Stealth Scan against 10.1.34.76 in 42.81s (19 hosts left)
Completed SYN Stealth Scan against 10.1.34.27 in 42.97s (18 hosts left)
Discovered open port 7000/tcp on 10.1.34.21
Completed SYN Stealth Scan against 10.1.34.18 in 43.04s (17 hosts left)
Completed SYN Stealth Scan against 10.1.34.71 in 43.04s (16 hosts left)
Completed SYN Stealth Scan against 10.1.34.20 in 43.06s (15 hosts left)
Completed SYN Stealth Scan against 10.1.34.72 in 43.09s (14 hosts left)
Completed SYN Stealth Scan against 10.1.34.230 in 43.11s (13 hosts left)
Completed SYN Stealth Scan against 10.1.34.101 in 43.17s (12 hosts left)
Completed SYN Stealth Scan against 10.1.34.87 in 43.19s (11 hosts left)
Completed SYN Stealth Scan against 10.1.34.1 in 43.21s (10 hosts left)
Completed SYN Stealth Scan against 10.1.34.28 in 43.21s (9 hosts left)
Completed SYN Stealth Scan against 10.1.34.21 in 43.26s (8 hosts left)
Completed SYN Stealth Scan against 10.1.34.247 in 43.27s (7 hosts left)
Completed SYN Stealth Scan against 10.1.34.248 in 43.34s (6 hosts left)
Completed SYN Stealth Scan against 10.1.34.243 in 43.35s (5 hosts left)
Completed SYN Stealth Scan against 10.1.34.244 in 43.35s (4 hosts left)
Completed SYN Stealth Scan against 10.1.34.128 in 43.44s (3 hosts left)
Completed SYN Stealth Scan against 10.1.34.127 in 43.46s (2 hosts left)
Completed SYN Stealth Scan against 10.1.34.153 in 43.50s (1 host left)
Completed SYN Stealth Scan at 10:08, 43.53s elapsed (44000 total ports)
Initiating Service scan at 10:08
Scanning 251 services on 44 hosts
Service scan Timing: About 39.04% done; ETC: 10:09 (0:00:48 remaining)
Service scan Timing: About 70.92% done; ETC: 10:10 (0:00:34 remaining)
Completed Service scan at 10:12, 245.49s elapsed (251 services on 44 hosts)
Initiating OS detection (try #1) against 44 hosts
Retrying OS detection (try #2) against 2 hosts
Retrying OS detection (try #3) against 10.1.34.26
Retrying OS detection (try #4) against 10.1.34.26
WARNING: OS didn't match until try #4
NSE: Script scanning 44 hosts.
Initiating NSE at 10:12
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
```

```
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
NSE: [ftp-bounce] Couldn't resolve scanme.nmap.org, scanning 10.0.0.1 instead.
Completed NSE at 10:23, 610.27s elapsed
Initiating NSE at 10:23
Completed NSE at 10:23, 4.14s elapsed
Nmap scan report for 10.1.34.1
Host is up (0.11s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Cisco router telnetd
MAC Address: 00:00:0C:07:AC:1C (Cisco Systems)
Device type: switch|router|firewall
Running: Cisco IOS 12.X|15.X, Cisco embedded
OS CPE: cpe:/h:cisco:catalyst_2950 cpe:/h:cisco:catalyst_2960 cpe:/h:cisco:catalyst_3550 cpe:/h:cisco:catalyst_3560
cpe:/h:cisco:catalyst_3750 cpe:/h:cisco:catalyst_4500 cpe:/o:cisco:ios:12 cpe:/o:cisco:ios:15
OS details: Cisco 2950, 2960, 3550, 3560, 3750, or 4500 switch or 6500 router (IOS 12.1 - 15.0); or Adaptive Security Appliance
firewall
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT       ADDRESS
1   114.59 ms 10.1.34.1

Nmap scan report for 10.1.34.18
Host is up (0.092s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|_  2048 20:53:d0:8b:c3:0c:e3:ce:88:df:55:9b:79:a7:93:34 (RSA)
37/tcp   open  time          (32 bits)
|_rfc868-time: 2017-12-08T12:12:51
111/tcp  open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100024  1         41660/tcp  status
|_  100024  1         50622/udp  status
514/tcp  open  shell?
5432/tcp open  postgresql    PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
8000/tcp open  tcpwrapped
8100/tcp open  xprint-server?
MAC Address: A0:36:9F:84:19:6C (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 9.841 days (since Tue Nov 28 14:11:27 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT     ADDRESS
1   92.05 ms 10.1.34.18

Nmap scan report for 10.1.34.20
Host is up (0.10s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE    VERSION
```

```
21/tcp    open  ftp        vsftpd 2.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 May 25  2010 pub
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 9f:49:4b:c2:6a:59:e7:7e:7d:c2:e5:b9:ac:33:d2:d5 (DSA)
|_  2048 cc:3c:2f:76:61:7e:4d:8e:b9:c7:64:6f:91:bd:01:86 (RSA)
23/tcp    open  telnet     BSD-derived telnetd
111/tcp   open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|   100000  2           111/udp  rpcbind
|   100024  1          1020/udp  status
|_  100024  1          1023/tcp  status
514/tcp   open  shell?
902/tcp   open  nagios-nsca Nagios NSCA
1023/tcp  open  status     1 (RPC #100024)
5432/tcp  open  postgresql  PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
5989/tcp  open  ssl/http   Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd
| http-methods:
|_  Supported Methods: POST
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=sagesrv1/organizationName=The Open
Group/stateOrProvinceName=Berkshire/countryName=UK
| Issuer: commonName=sagesrv1/organizationName=The Open Group/stateOrProvinceName=Berkshire/countryName=UK
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2014-07-31T12:15:43
| Not valid after:  2024-07-28T12:15:43
| MD5:   e36e ae5f aacc b200 becc 3b03 89d6 da9c
|_SHA-1: e63f 7b2f e94c 4168 51df 95de 14aa f3fd 298a 939c
|_ssl-date: 2017-12-08T12:13:31+00:00; -1s from scanner time.
6000/tcp  open  X11        (access denied)
11111/tcp open  ssl/vce?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos,
LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions,
SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, X11Probe:
|     <?xml version="1.0"?>
|_    <Clients_SSL_certificate_required/>
| ssl-cert: Subject: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Issuer: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2014-07-31T12:47:35
| Not valid after:  2019-07-30T12:47:35
| MD5:   821a d5d9 88fb 13d0 6462 8f4f 24d8 41f0
|_SHA-1: 9520 c96b 0515 ebd8 c08c 8e44 3b56 2644 18fd 3211
|_ssl-date: 2017-12-08T12:12:52+00:00; -1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port11111-TCP:V=7.50%T=SSL%I=7%D=12/8%Time=5A2A80CE%P=i686-pc-windows-w
SF:indows%r(NULL,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certifica
SF:te_required/>\n")%r(GenericLines,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(GetRequest,3A,"<\?xml\x20version
SF:=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(HTTPOptions,3A,
SF:"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")
SF:%r(RTSPRequest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certific
SF:ate_required/>\n")%r(RPCCheck,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clien
SF:ts_SSL_certificate_required/>\n")%r(DNSVersionBindReq,3A,"<\?xml\x20ver
SF:sion=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(DNSStatusRe
SF:quest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_requi
SF:red/>\n")%r(Help,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certif
```

```
SF:icate_required/>\n")%r(SSLSessionReq,3A,"<\?xml\x20version=\"1\.0\"\?>\
SF:n<Clients_SSL_certificate_required/>\n")%r(TLSSessionReq,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(Kerberos
SF:,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>
SF:\n")%r(SMBProgNeg,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certi
SF:ficate_required/>\n")%r(X11Probe,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(FourOhFourRequest,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LPDStrin
SF:g,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/
SF:>\n")%r(LDAPSearchReq,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_c
SF:ertificate_required/>\n")%r(LDAPBindReq,3A,"<\?xml\x20version=\"1\.0\"\
SF:?>\n<Clients_SSL_certificate_required/>\n")%r(SIPOptions,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LANDesk-
SF:RC,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required
SF:/>\n")%r(TerminalServer,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL
SF:_certificate_required/>\n")%r(NCP,3A,"<\?xml\x20version=\"1\.0\"\?>\n<C
SF:lients_SSL_certificate_required/>\n")%r(NotesRPC,3A,"<\?xml\x20version=
SF:\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n");
MAC Address: 84:2B:2B:7B:5D:7A (Dell)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Uptime guess: 0.077 days (since Fri Dec 08 08:32:41 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=194 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT       ADDRESS
1   103.22 ms 10.1.34.20

Nmap scan report for 10.1.34.21
Host is up (0.090s latency).
Not shown: 995 closed ports
PORT     STATE    SERVICE  VERSION
22/tcp   open     ssh      OpenSSH 4.0 (protocol 2.0)
| ssh-hostkey:
|   1024 86:fc:3d:e9:6d:4c:96:9f:a2:6b:17:73:70:94:5a:44 (DSA)
|_  1024 c1:70:ab:52:48:ab:e5:dc:47:9c:94:ed:99:6f:94:4f (RSA)
23/tcp   filtered telnet
80/tcp   open     http     GoAhead WebServer
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: GoAhead-Webs
| http-title: Digi Configuration and Management
|_Requested resource was http://10.1.34.21/reboot.asp?mode=4&page=https://10.1.34.21:443/login.asp
443/tcp  open     ssl/http GoAhead WebServer
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: GoAhead-Webs
| http-title: Digi Configuration and Management
|_Requested resource was https://10.1.34.21/login.asp
| ssl-cert: Subject: commonName=Digi CM/organizationName=Digi
International/stateOrProvinceName=Minnesota/countryName=US
| Issuer: commonName=Digi International/organizationName=Digi
International/stateOrProvinceName=Minnesota/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2004-03-22T04:04:12
| Not valid after:  2014-03-21T04:04:12
| MD5:   0b38 845a 466e 1b51 1f25 c2f8 16b9 5f03
|_SHA-1: db1a a365 35ac b2b5 b061 3083 a8c3 a0da 5708 6244
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
```

```
7000/tcp open     telnet   Enterasys XSR Security Router telnetd
MAC Address: 00:40:9D:24:C7:26 (Digiboard)
Device type: media device
Running: Exterity embedded
OS details: Exterity IPTV MPEG2 video encoder
Uptime guess: 107.972 days (since Tue Aug 22 10:02:55 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Device: router

TRACEROUTE
HOP RTT      ADDRESS
1   90.14 ms 10.1.34.21

Nmap scan report for 10.1.34.26
Host is up (0.0074s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-SSH_2.0
23/tcp    open  telnet     (Usually a Cisco/3com switch)
80/tcp    open  http       Allegro RomPager 3.12
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=PortServer TS 4 MEI
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: Allegro-Software-RomPager/3.12
|_http-title: PortServer TS 4 MEI Configuration and Management
443/tcp   open  ssl/https?
513/tcp   open  login?
514/tcp   open  shell?
515/tcp   open  printer?
1027/tcp  open  IIS?
50000/tcp open  tcpwrapped
|_drda-info: TIMEOUT
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port22-TCP:V=7.50%I=7%D=12/8%Time=5A2A80BD%P=i686-pc-windows-windows%r(
SF:NULL,10,"SSH-2\.0-SSH_2\.0\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1027-TCP:V=7.50%I=7%D=12/8%Time=5A2A80C2%P=i686-pc-windows-windows%
SF:r(SMBProgNeg,7,"\x15\x03\x01\0\x02\x02F");
MAC Address: 00:40:9D:4E:83:D1 (Digiboard)
Device type: bridge
Running: Digi embedded
OS details: Digi PortServer TS serial-to-Ethernet bridge
Network Distance: 1 hop
Service Info: OS: IOS; Device: switch; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT     ADDRESS
1   7.37 ms 10.1.34.26

Nmap scan report for 10.1.34.27
Host is up (0.030s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-SSH_2.0
| ssh-hostkey:
|_  512 48:aa:ac:8c:1e:26:d4:9c:9d:a6:b3:3e:bc:57:7a:2e (DSA)
23/tcp    open  telnet     (Usually a Cisco/3com switch)
80/tcp    open  http       Allegro-Software-RomPager/3.12
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=PortServer TS 4 MEI
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: Allegro-Software-RomPager/3.12
|_http-title: PortServer TS 4 MEI Configuration and Management
```

```
443/tcp   open  ssl/https?
513/tcp   open  login?
514/tcp   open  shell?
515/tcp   open  printer?
1027/tcp  open  ssl/IIS?
50000/tcp open  tcpwrapped
|_drda-info: TIMEOUT
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port22-TCP:V=7.50%I=7%D=12/8%Time=5A2A80BA%P=i686-pc-windows-windows%r(
SF:NULL,10,"SSH-2\.0-SSH_2\.0\n");
MAC Address: 00:40:9D:35:28:A8 (Digiboard)
Device type: bridge
Running: Digi embedded
OS details: Digi PortServer TS serial-to-Ethernet bridge
Network Distance: 1 hop
Service Info: OS: IOS; Device: switch; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT     ADDRESS
1   30.08 ms 10.1.34.27

Nmap scan report for 10.1.34.28
Host is up (0.024s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-SSH_2.0
23/tcp    open  telnet     (Usually a Cisco/3com switch)
80/tcp    open  http       Allegro RomPager 3.12
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=PortServer TS 4 MEI
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: Allegro-Software-RomPager/3.12
|_http-title: PortServer TS 4 MEI Configuration and Management
443/tcp   open  ssl/https?
513/tcp   open  login?
514/tcp   open  shell?
515/tcp   open  printer?
1027/tcp  open  IIS?
50000/tcp open  tcpwrapped
|_drda-info: TIMEOUT
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port22-TCP:V=7.50%I=7%D=12/8%Time=5A2A80BD%P=i686-pc-windows-windows%r(
SF:NULL,10,"SSH-2\.0-SSH_2\.0\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1027-TCP:V=7.50%I=7%D=12/8%Time=5A2A80C5%P=i686-pc-windows-windows%
SF:r(SMBProgNeg,7,"\x15\x03\x01\0\x02\x02F");
MAC Address: 00:40:9D:4E:83:5E (Digiboard)
Device type: bridge
Running: Digi embedded
OS details: Digi PortServer TS serial-to-Ethernet bridge
Network Distance: 1 hop
Service Info: OS: IOS; Device: switch; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT     ADDRESS
1   23.92 ms 10.1.34.28

Nmap scan report for 10.1.34.31
Host is up (0.035s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-SSH_2.0
| ssh-hostkey:
|_  512 30:10:29:a0:08:fa:68:fa:5c:d6:c9:fb:1c:0d:0d:c3 (DSA)
23/tcp    open  telnet     (Usually a Cisco/3com switch)
80/tcp    open  http       Allegro RomPager 3.12
```

```
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=PortServer TS 4 MEI
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: Allegro-Software-RomPager/3.12
|_http-title: PortServer TS 4 MEI Configuration and Management
443/tcp   open  ssl/https?
513/tcp   open  login?
514/tcp   open  shell?
515/tcp   open  printer?
1027/tcp  open  ssl/IIS?
50000/tcp open  tcpwrapped
|_drda-info: TIMEOUT
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port22-TCP:V=7.50%I=7%D=12/8%Time=5A2A80C0%P=i686-pc-windows-windows%r(
SF:NULL,10,"SSH-2\.0-SSH_2\.0\n");
MAC Address: 00:40:9D:45:60:59 (Digiboard)
Device type: bridge
Running: Digi embedded
OS details: Digi PortServer TS serial-to-Ethernet bridge
Network Distance: 1 hop
Service Info: OS: IOS; Device: switch; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT      ADDRESS
1   35.21 ms 10.1.34.31

Nmap scan report for 10.1.34.60
Host is up (0.11s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Tornado vxWorks ftpd 5.5.1
23/tcp   open  telnet  VxWorks telnetd
80/tcp   open  http    WindWeb 4.00
|_http-favicon: Unknown favicon MD5: E5A839BF2CADB92C294E4D04E69DA7FA
| http-methods:
|_  Supported Methods: GET
|_http-title: webCAT-Login
111/tcp  open  rpcbind 2 (RPC #100000)
|_rpcinfo:
1100/tcp open  mctp?
MAC Address: 00:50:C2:28:20:29 (Ieee Registration Authority)
Device type: general purpose
Running: Wind River VxWorks
OS CPE: cpe:/o:windriver:vxworks
OS details: VxWorks
Uptime guess: 14.895 days (since Thu Nov 23 12:54:05 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=157 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: VxWorks; CPE: cpe:/o:windriver:vxworks

TRACEROUTE
HOP RTT      ADDRESS
1   113.27 ms 10.1.34.60

Nmap scan report for 10.1.34.71
Host is up (0.11s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 May 24  2008 pub
22/tcp   open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 7b:e4:55:06:31:19:71:e3:d5:99:0c:1e:eb:e9:df:95 (DSA)
|_  2048 93:d1:fb:09:23:d6:f4:21:86:5b:88:3e:86:57:29:af (RSA)
37/tcp   open  time       (32 bits)
|_rfc868-time: 2017-12-08T12:13:37
111/tcp  open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|_  100000  2           111/udp  rpcbind
514/tcp  open  shell?
```

```
5432/tcp open  postgresql PostgreSQL DB 8.2.5 - 8.2.19
6000/tcp open  X11        X.Org (open)
MAC Address: 00:15:17:CD:EE:9A (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Uptime guess: 9.599 days (since Tue Nov 28 20:00:47 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=197 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

Host script results:
|_clock-skew: mean: 2s, deviation: 0s, median: 2s

TRACEROUTE
HOP RTT       ADDRESS
1   112.43 ms 10.1.34.71

Nmap scan report for 10.1.34.72
Host is up (0.12s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE         VERSION
21/tcp    open  ftp             vsftpd 2.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Jan 09  2013 pub
22/tcp    open  ssh             OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 cf:3f:88:24:a9:b9:e7:52:da:b4:91:12:82:b5:26:c6 (DSA)
|_  2048 a2:2f:cb:a2:82:3c:64:11:e8:17:76:14:36:14:ed:ff (RSA)
23/tcp    open  telnet          BSD-derived telnetd
111/tcp   open  rpcbind         2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|   100000  2           111/udp  rpcbind
|   100024  1           659/udp  status
|_  100024  1           662/tcp  status
514/tcp   open  shell?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5432/tcp  open  postgresql      PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
5989/tcp  open  ssl/http        Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd
| http-methods:
|_  Supported Methods: POST
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=The Open
Group/stateOrProvinceName=Berkshire/countryName=UK
| Issuer: commonName=localhost.localdomain/organizationName=The Open
Group/stateOrProvinceName=Berkshire/countryName=UK
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2014-10-03T18:53:49
| Not valid after:  2024-09-30T18:53:49
| MD5:   1ce4 ff19 5a93 58ef 8a2b 5873 0508 4bdb
|_SHA-1: a73c fe60 07e4 1344 6de1 2a1c b5c6 8b3c 6920 2dcb
|_ssl-date: 2017-12-08T12:27:24+00:00; +12m34s from scanner time.
6000/tcp  open  X11             X.Org (open)
11111/tcp open  ssl/vce?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos,
LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions,
SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, X11Probe:
|     <?xml version="1.0"?>
|_    <Clients_SSL_certificate_required/>
| ssl-cert: Subject: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Issuer: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2014-10-03T18:52:51
| Not valid after:  2019-10-02T18:52:51
| MD5:   a4cf b400 349e b6ae e23d f693 2fb2 0d89
|_SHA-1: 6284 1e8e c438 fbca c053 f21e be20 40da 0bcb 08ed
```

```
|_ssl-date: 2017-12-08T12:26:24+00:00; +12m35s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port11111-TCP:V=7.50%T=SSL%I=7%D=12/8%Time=5A2A80E1%P=i686-pc-windows-w
SF:indows%r(NULL,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certifica
SF:te_required/>\n")%r(GenericLines,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(GetRequest,3A,"<\?xml\x20version
SF:=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(HTTPOptions,3A,
SF:"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")
SF:%r(RTSPRequest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certific
SF:ate_required/>\n")%r(RPCCheck,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clien
SF:ts_SSL_certificate_required/>\n")%r(DNSVersionBindReq,3A,"<\?xml\x20ver
SF:sion=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(DNSStatusRe
SF:quest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_requi
SF:red/>\n")%r(Help,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certif
SF:icate_required/>\n")%r(SSLSessionReq,3A,"<\?xml\x20version=\"1\.0\"\?>\
SF:n<Clients_SSL_certificate_required/>\n")%r(TLSSessionReq,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(Kerberos
SF:,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>
SF:\n")%r(SMBProgNeg,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certi
SF:ficate_required/>\n")%r(X11Probe,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(FourOhFourRequest,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LPDStrin
SF:g,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/
SF:>\n")%r(LDAPSearchReq,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_c
SF:ertificate_required/>\n")%r(LDAPBindReq,3A,"<\?xml\x20version=\"1\.0\"\
SF:?>\n<Clients_SSL_certificate_required/>\n")%r(SIPOptions,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LANDesk-
SF:RC,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required
SF:/>\n")%r(TerminalServer,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL
SF:_certificate_required/>\n")%r(NCP,3A,"<\?xml\x20version=\"1\.0\"\?>\n<C
SF:lients_SSL_certificate_required/>\n")%r(NotesRPC,3A,"<\?xml\x20version=
SF:\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n");
MAC Address: 00:1B:21:85:52:62 (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.32
Uptime guess: 3.273 days (since Tue Dec 05 03:49:18 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 12m34s, deviation: 0s, median: 12m33s

TRACEROUTE
HOP RTT       ADDRESS
1   116.57 ms 10.1.34.72

Nmap scan report for 10.1.34.73
Host is up (0.12s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Jan 09  2013 pub
22/tcp    open  ssh         OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 2b:7b:b1:30:4b:b0:05:98:26:d8:d7:e2:0d:84:22:20 (DSA)
|_  2048 e8:59:7e:d5:f0:5a:02:5f:68:41:24:80:46:a6:75:23 (RSA)
37/tcp    open  time        (32 bits)
|_rfc868-time: 2017-12-08T12:14:38
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
```

```
|_  100000  2          111/udp  rpcbind
514/tcp   open  shell?
902/tcp   open  nagios-nsca Nagios NSCA
5432/tcp  open  postgresql  PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
5989/tcp  open  ssl/http    Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd
| http-methods:
|_  Supported Methods: POST
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=srv1/organizationName=The Open
Group/stateOrProvinceName=Berkshire/countryName=UK
| Issuer: commonName=srv1/organizationName=The Open Group/stateOrProvinceName=Berkshire/countryName=UK
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-07-18T12:32:01
| Not valid after:  2027-07-16T12:32:01
| MD5:   f4d1 2d05 b960 9906 c182 c831 e34f f963
|_SHA-1: d162 f835 15ee 217d 8333 f41d 9cd9 18e3 3e7c b001
|_ssl-date: 2017-12-08T12:14:48+00:00; -1s from scanner time.
6000/tcp  open  X11         (access denied)
11111/tcp open  ssl/vce?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos,
LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions,
SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, X11Probe:
|     <?xml version="1.0"?>
|_    <Clients_SSL_certificate_required/>
| ssl-cert: Subject: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Issuer: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-07-18T15:37:19
| Not valid after:  2022-07-17T15:37:19
| MD5:   b2a6 d9ad 32fe bbb3 d959 a08a 17b1 4982
|_SHA-1: a02f 3dc3 b068 f308 68ba 8856 29b2 4f77 bbe1 5992
|_ssl-date: 2017-12-08T12:14:40+00:00; -1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port11111-TCP:V=7.50%T=SSL%I=7%D=12/8%Time=5A2A80E4%P=i686-pc-windows-w
SF:indows%r(NULL,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certifica
SF:te_required/>\n")%r(GenericLines,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(GetRequest,3A,"<\?xml\x20version
SF:=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(HTTPOptions,3A,
SF:"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")
SF:%r(RTSPRequest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certific
SF:ate_required/>\n")%r(RPCCheck,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clien
SF:ts_SSL_certificate_required/>\n")%r(DNSVersionBindReq,3A,"<\?xml\x20ver
SF:sion=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(DNSStatusRe
SF:quest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_requi
SF:red/>\n")%r(Help,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certif
SF:icate_required/>\n")%r(SSLSessionReq,3A,"<\?xml\x20version=\"1\.0\"\?>\
SF:n<Clients_SSL_certificate_required/>\n")%r(TLSSessionReq,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(Kerberos
SF:,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>
SF:\n")%r(SMBProgNeg,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certi
SF:ficate_required/>\n")%r(X11Probe,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(FourOhFourRequest,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LPDStrin
SF:g,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/
SF:>\n")%r(LDAPSearchReq,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_c
SF:ertificate_required/>\n")%r(LDAPBindReq,3A,"<\?xml\x20version=\"1\.0\"\
SF:?>\n<Clients_SSL_certificate_required/>\n")%r(SIPOptions,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LANDesk-
SF:RC,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required
SF:/>\n")%r(TerminalServer,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL
```

```
SF:_certificate_required/>\n")%r(NCP,3A,"<\?xml\x20version=\"1\.0\"\?>\n<C
SF:lients_SSL_certificate_required/>\n")%r(NotesRPC,3A,"<\?xml\x20version=
SF:\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n");
MAC Address: 00:23:AE:B9:B4:34 (Dell)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.32
Uptime guess: 9.660 days (since Tue Nov 28 18:32:18 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT       ADDRESS
1   119.31 ms 10.1.34.73

Nmap scan report for 10.1.34.75
Host is up (0.12s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE         VERSION
21/tcp    open  ftp             vsftpd 2.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 May 25  2010 pub
22/tcp    open  ssh             OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 7e:12:c0:39:3b:8a:81:b7:05:6a:16:8c:ba:b8:05:b3 (DSA)
|_  2048 b1:4d:6a:62:13:60:75:66:3d:00:db:26:42:5c:07:b5 (RSA)
23/tcp    open  telnet          BSD-derived telnetd
37/tcp    open  time            (32 bits)
|_rfc868-time: 2017-12-08T12:13:30
111/tcp   open  rpcbind         2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|   100000  2           111/udp  rpcbind
|   100024  1           929/udp  status
|_  100024  1           932/tcp  status
514/tcp   open  shell?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5432/tcp  open  postgresql      PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
5989/tcp  open  ssl/http        Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd
| http-methods:
|_  Supported Methods: POST
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=sagesrv1/organizationName=The Open
Group/stateOrProvinceName=Berkshire/countryName=UK
| Issuer: commonName=sagesrv1/organizationName=The Open Group/stateOrProvinceName=Berkshire/countryName=UK
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-11-28T14:48:27
| Not valid after:  2021-11-25T14:48:27
| MD5:   b2c5 637d 4de0 39a4 d21d 8a3b a29a 13e8
|_SHA-1: d151 d019 0265 a5a3 e3f9 1ca3 8e47 a92e 9e7e a74f
|_ssl-date: 2017-12-08T12:13:07+00:00; -1s from scanner time.
6000/tcp  open  X11             (access denied)
11111/tcp open  ssl/vce?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos,
LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions,
SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, X11Probe:
|     <?xml version="1.0"?>
|_    <Clients_SSL_certificate_required/>
| ssl-cert: Subject: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Issuer: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-11-28T15:01:32
| Not valid after:  2016-11-26T15:01:32
```

```
| MD5:   299e 9eff 4f54 28db 82a9 d05e 4345 d203
|_SHA-1: ae6d 0ab3 93e9 9a51 30b6 376f 584f 0465 4b29 4066
|_ssl-date: 2017-12-08T12:14:48+00:00; -1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port11111-TCP:V=7.50%T=SSL%I=7%D=12/8%Time=5A2A80E5%P=i686-pc-windows-w
SF:indows%r(NULL,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certifica
SF:te_required/>\n")%r(GenericLines,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(GetRequest,3A,"<\?xml\x20version
SF:=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(HTTPOptions,3A,
SF:"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")
SF:%r(RTSPRequest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certific
SF:ate_required/>\n")%r(RPCCheck,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clien
SF:ts_SSL_certificate_required/>\n")%r(DNSVersionBindReq,3A,"<\?xml\x20ver
SF:sion=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(DNSStatusRe
SF:quest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_requi
SF:red/>\n")%r(Help,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certif
SF:icate_required/>\n")%r(SSLSessionReq,3A,"<\?xml\x20version=\"1\.0\"\?>\
SF:n<Clients_SSL_certificate_required/>\n")%r(TLSSessionReq,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(Kerberos
SF:,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>
SF:\n")%r(SMBProgNeg,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certi
SF:ficate_required/>\n")%r(X11Probe,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(FourOhFourRequest,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LPDStrin
SF:g,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/
SF:>\n")%r(LDAPSearchReq,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_c
SF:ertificate_required/>\n")%r(LDAPBindReq,3A,"<\?xml\x20version=\"1\.0\"\
SF:?>\n<Clients_SSL_certificate_required/>\n")%r(SIPOptions,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LANDesk-
SF:RC,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required
SF:/>\n")%r(TerminalServer,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL
SF:_certificate_required/>\n")%r(NCP,3A,"<\?xml\x20version=\"1\.0\"\?>\n<C
SF:lients_SSL_certificate_required/>\n")%r(NotesRPC,3A,"<\?xml\x20version=
SF:\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n");
MAC Address: 00:1B:21:80:D8:10 (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Uptime guess: 7.807 days (since Thu Nov 30 15:00:25 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=196 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT      ADDRESS
1   118.68 ms 10.1.34.75

Nmap scan report for 10.1.34.76
Host is up (0.12s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        vsftpd 2.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 May 24  2008 pub
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 c2:99:53:b8:ef:d5:4a:28:0f:05:cc:85:a5:2f:28:98 (DSA)
|_  2048 60:3c:a0:12:7a:cc:b8:86:18:04:95:fc:d0:d2:90:35 (RSA)
37/tcp    open  time       (32 bits)
|_rfc868-time: 2017-12-08T12:16:21
111/tcp   open  rpcbind    2 (RPC #100000)
| rpcinfo:
```

```
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|_  100000  2           111/udp  rpcbind
514/tcp   open  shell?
5432/tcp  open  postgresql PostgreSQL DB 8.2.5 - 8.2.19
6000/tcp  open  X11       X.Org (open)
7200/tcp  open  fodms?
8000/tcp  open  http-alt?
11111/tcp open  ssl/vce?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos,
LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions,
SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, X11Probe:
|     <?xml version="1.0"?>
|_    <Clients_SSL_certificate_required/>
| ssl-cert: Subject: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Issuer: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-04-29T13:27:20
| Not valid after:  2015-04-28T13:27:20
| MD5:   8c10 b443 8381 c4ec 2c60 d9fe 9042 776d
|_SHA-1: 0398 8dba af4a b56f 6613 2b3d 61a9 e42d a1b2 e342
|_ssl-date: 2017-12-08T12:14:51+00:00; +1m57s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port11111-TCP:V=7.50%T=SSL%I=7%D=12/8%Time=5A2A80E7%P=i686-pc-windows-w
SF:indows%r(NULL,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certifica
SF:te_required/>\n")%r(GenericLines,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(GetRequest,3A,"<\?xml\x20version
SF:=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(HTTPOptions,3A,
SF:"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")
SF:%r(RTSPRequest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certific
SF:ate_required/>\n")%r(RPCCheck,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clien
SF:ts_SSL_certificate_required/>\n")%r(DNSVersionBindReq,3A,"<\?xml\x20ver
SF:sion=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(DNSStatusRe
SF:quest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_requi
SF:red/>\n")%r(Help,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certif
SF:icate_required/>\n")%r(SSLSessionReq,3A,"<\?xml\x20version=\"1\.0\"\?>\
SF:n<Clients_SSL_certificate_required/>\n")%r(TLSSessionReq,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(Kerberos
SF:,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>
SF:\n")%r(SMBProgNeg,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certi
SF:ficate_required/>\n")%r(X11Probe,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(FourOhFourRequest,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LPDStrin
SF:g,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/
SF:>\n")%r(LDAPSearchReq,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_c
SF:ertificate_required/>\n")%r(LDAPBindReq,3A,"<\?xml\x20version=\"1\.0\"\
SF:?>\n<Clients_SSL_certificate_required/>\n")%r(SIPOptions,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LANDesk-
SF:RC,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required
SF:/>\n")%r(TerminalServer,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL
SF:_certificate_required/>\n")%r(NCP,3A,"<\?xml\x20version=\"1\.0\"\?>\n<C
SF:lients_SSL_certificate_required/>\n")%r(NotesRPC,3A,"<\?xml\x20version=
SF:\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n");
MAC Address: 00:23:AE:B9:B4:92 (Dell)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Uptime guess: 9.517 days (since Tue Nov 28 21:59:20 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=200 (Good luck!)
IP ID Sequence Generation: All zeros
```

```
Service Info: OS: Unix

Host script results:
|_clock-skew: mean: 1m56s, deviation: 0s, median: 1m56s

TRACEROUTE
HOP RTT       ADDRESS
1   119.14 ms 10.1.34.76

Nmap scan report for 10.1.34.77
Host is up (0.12s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 May 25  2010 pub
22/tcp    open  ssh            OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 7e:12:c0:39:3b:8a:81:b7:05:6a:16:8c:ba:b8:05:b3 (DSA)
|_  2048 b1:4d:6a:62:13:60:75:66:3d:00:db:26:42:5c:07:b5 (RSA)
23/tcp    open  telnet         BSD-derived telnetd
37/tcp    open  time           (32 bits)
|_rfc868-time: 2017-12-08T12:12:54
111/tcp   open  rpcbind        2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|   100000  2           111/udp  rpcbind
|   100024  1           959/udp  status
|_  100024  1           962/tcp  status
514/tcp   open  shell?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5432/tcp  open  postgresql     PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
5989/tcp  open  ssl/http       Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd
| http-methods:
|_  Supported Methods: POST
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=sagesrv1/organizationName=The Open
Group/stateOrProvinceName=Berkshire/countryName=UK
| Issuer: commonName=sagesrv1/organizationName=The Open Group/stateOrProvinceName=Berkshire/countryName=UK
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-11-28T14:48:27
| Not valid after:  2021-11-25T14:48:27
| MD5:   b2c5 637d 4de0 39a4 d21d 8a3b a29a 13e8
|_SHA-1: d151 d019 0265 a5a3 e3f9 1ca3 8e47 a92e 9e7e a74f
|_ssl-date: 2017-12-08T12:15:14+00:00; -1s from scanner time.
6000/tcp  open  X11            X.Org (open)
11111/tcp open  ssl/vce?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos,
LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions,
SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, X11Probe:
|     <?xml version="1.0"?>
|_    <Clients_SSL_certificate_required/>
| ssl-cert: Subject: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Issuer: commonName=Common Name/organizationName=Organization Name/stateOrProvinceName=State or
Province/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-11-28T15:01:32
| Not valid after:  2016-11-26T15:01:32
| MD5:   299e 9eff 4f54 28db 82a9 d05e 4345 d203
|_SHA-1: ae6d 0ab3 93e9 9a51 30b6 376f 584f 0465 4b29 4066
|_ssl-date: 2017-12-08T12:13:31+00:00; -1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
```

```
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port11111-TCP:V=7.50%T=SSL%I=7%D=12/8%Time=5A2A80EA%P=i686-pc-windows-w
SF:indows%r(NULL,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certifica
SF:te_required/>\n")%r(GenericLines,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(GetRequest,3A,"<\?xml\x20version
SF:=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(HTTPOptions,3A,
SF:"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")
SF:%r(RTSPRequest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certific
SF:ate_required/>\n")%r(RPCCheck,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clien
SF:ts_SSL_certificate_required/>\n")%r(DNSVersionBindReq,3A,"<\?xml\x20ver
SF:sion=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(DNSStatusRe
SF:quest,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_requi
SF:red/>\n")%r(Help,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certif
SF:icate_required/>\n")%r(SSLSessionReq,3A,"<\?xml\x20version=\"1\.0\"\?>\
SF:n<Clients_SSL_certificate_required/>\n")%r(TLSSessionReq,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(Kerberos
SF:,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>
SF:\n")%r(SMBProgNeg,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certi
SF:ficate_required/>\n")%r(X11Probe,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Cl
SF:ients_SSL_certificate_required/>\n")%r(FourOhFourRequest,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LPDStrin
SF:g,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/
SF:>\n")%r(LDAPSearchReq,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_c
SF:ertificate_required/>\n")%r(LDAPBindReq,3A,"<\?xml\x20version=\"1\.0\"\
SF:?>\n<Clients_SSL_certificate_required/>\n")%r(SIPOptions,3A,"<\?xml\x20
SF:version=\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n")%r(LANDesk-
SF:RC,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL_certificate_required
SF:/>\n")%r(TerminalServer,3A,"<\?xml\x20version=\"1\.0\"\?>\n<Clients_SSL
SF:_certificate_required/>\n")%r(NCP,3A,"<\?xml\x20version=\"1\.0\"\?>\n<C
SF:lients_SSL_certificate_required/>\n")%r(NotesRPC,3A,"<\?xml\x20version=
SF:\"1\.0\"\?>\n<Clients_SSL_certificate_required/>\n");
MAC Address: 00:15:17:F4:10:1F (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Uptime guess: 24.752 days (since Mon Nov 13 16:20:34 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT      ADDRESS
1   124.21 ms 10.1.34.77

Nmap scan report for 10.1.34.81
Host is up (0.12s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.2.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 May 11  2016 pub
22/tcp   open  ssh        OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 96:54:ca:5a:e2:11:14:26:e1:08:2a:da:58:de:8f:cc (DSA)
|_  2048 ed:46:b7:1e:0a:6c:66:f6:c3:b6:a7:5c:5f:7a:55:1f (RSA)
111/tcp  open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|_  100000  2,3,4       111/udp  rpcbind
514/tcp  open  shell?
5432/tcp open  postgresql PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
6000/tcp open  X11        (access denied)
9090/tcp open  http       Jetty
|_hadoop-datanode-info:
|_hadoop-jobtracker-info:
|_hadoop-tasktracker-info:
|_hbase-master-info:
|_http-favicon: Unknown favicon MD5: E4888EE8491B4EB75501996E41AF6460
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

```
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:50:56:95:76:00 (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 29.762 days (since Wed Nov 08 16:05:13 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE
HOP RTT       ADDRESS
1   118.24 ms 10.1.34.81

Nmap scan report for 10.1.34.83
Host is up (0.12s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.2.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 May 11  2016 pub
22/tcp   open  ssh        OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 96:54:ca:5a:e2:11:14:26:e1:08:2a:da:58:de:8f:cc (DSA)
|_  2048 ed:46:b7:1e:0a:6c:66:f6:c3:b6:a7:5c:5f:7a:55:1f (RSA)
111/tcp  open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|_  100000  2,3,4        111/udp  rpcbind
514/tcp  open  shell?
5432/tcp open  postgresql PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
6000/tcp open  X11        (access denied)
9090/tcp open  http       Jetty
|_hadoop-datanode-info:
|_hadoop-jobtracker-info:
|_hadoop-tasktracker-info:
|_hbase-master-info:
|_http-favicon: Unknown favicon MD5: E4888EE8491B4EB75501996E41AF6460
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:50:56:95:8B:EF (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 34.283 days (since Sat Nov 04 03:35:25 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE
HOP RTT       ADDRESS
1   120.58 ms 10.1.34.83

Nmap scan report for 10.1.34.85
Host is up (0.12s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.2.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 May 11  2016 pub
22/tcp   open  ssh        OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 96:54:ca:5a:e2:11:14:26:e1:08:2a:da:58:de:8f:cc (DSA)
|_  2048 ed:46:b7:1e:0a:6c:66:f6:c3:b6:a7:5c:5f:7a:55:1f (RSA)
111/tcp  open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|_  100000  2,3,4        111/udp  rpcbind
514/tcp  open  shell?
5432/tcp open  postgresql PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
```

```
6000/tcp open  X11        (access denied)
9090/tcp open  http       Jetty
|_hadoop-datanode-info:
|_hadoop-jobtracker-info:
|_hadoop-tasktracker-info:
|_hbase-master-info:
|_http-favicon: Unknown favicon MD5: E4888EE8491B4EB75501996E41AF6460
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:50:56:95:78:BA (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 29.804 days (since Wed Nov 08 15:06:00 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE
HOP RTT       ADDRESS
1   119.57 ms 10.1.34.85

Nmap scan report for 10.1.34.87
Host is up (0.12s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.2.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 May 11  2016 pub
22/tcp   open  ssh        OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 96:54:ca:5a:e2:11:14:26:e1:08:2a:da:58:de:8f:cc (DSA)
|_  2048 ed:46:b7:1e:0a:6c:66:f6:c3:b6:a7:5c:5f:7a:55:1f (RSA)
111/tcp  open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|_  100000  2,3,4       111/udp  rpcbind
514/tcp  open  shell?
5432/tcp open  postgresql PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
6000/tcp open  X11        (access denied)
9090/tcp open  http       Jetty
|_hadoop-datanode-info:
|_hadoop-jobtracker-info:
|_hadoop-tasktracker-info:
|_hbase-master-info:
|_http-favicon: Unknown favicon MD5: E4888EE8491B4EB75501996E41AF6460
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:50:56:95:4A:DA (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 29.772 days (since Wed Nov 08 15:51:58 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE
HOP RTT       ADDRESS
1   121.46 ms 10.1.34.87

Nmap scan report for 10.1.34.89
Host is up (0.12s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.2.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Jul 24  2015 pub
22/tcp   open  ssh        OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
```

```
|   1024 c1:86:7f:56:63:4c:ef:f0:14:d2:6b:da:1f:6b:63:7a (DSA)
|_  2048 a5:63:c8:59:c4:0f:9e:d4:32:dc:0e:52:f7:96:8e:b3 (RSA)
23/tcp   open  telnet     Linux telnetd
111/tcp  open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100024  1         47478/tcp  status
|_  100024  1         52485/udp  status
514/tcp  open  shell?
5432/tcp open  postgresql PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
5989/tcp open  ssl/http   Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd
| http-methods:
|_  Supported Methods: POST
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=srv1/organizationName=The Open
Group/stateOrProvinceName=Berkshire/countryName=UK
| Issuer: commonName=srv1/organizationName=The Open Group/stateOrProvinceName=Berkshire/countryName=UK
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-04-11T15:33:32
| Not valid after:  2026-04-09T15:33:32
| MD5:   5deb a02b 9ee9 7717 d0e3 605f 4c0a f029
|_SHA-1: 68dc ebe0 a514 bc55 13e6 23bb fe63 8167 4375 f9fc
|_ssl-date: 2017-12-08T12:15:01+00:00; -1s from scanner time.
9090/tcp open  http       Jetty
|_hadoop-datanode-info:
|_hadoop-jobtracker-info:
|_hadoop-tasktracker-info:
|_hbase-master-info:
| http-cookie-flags:
|   /:
|     JSESSIONID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: E4888EE8491B4EB75501996E41AF6460
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:50:56:95:05:72 (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 7.320 days (since Fri Dec 01 02:42:53 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT       ADDRESS
1   124.50 ms 10.1.34.89

Nmap scan report for 10.1.34.97
Host is up (0.12s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 3d:74:a9:7b:be:37:55:d1:6f:87:05:92:a1:07:a4:6a (DSA)
|_  2048 66:47:67:a3:78:4d:5b:9f:21:6c:d0:fa:98:78:9e:32 (RSA)
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100003  2,3,4      2049/tcp  nfs
|   100003  2,3,4      2049/udp  nfs
|   100005  1,2,3     38765/udp  mountd
|   100005  1,2,3     43799/tcp  mountd
|   100011  1,2         875/tcp  rquotad
|   100011  1,2         875/udp  rquotad
```

```
|   100021  1,3,4      47085/udp  nlockmgr
|   100021  1,3,4      53068/tcp  nlockmgr
|   100024  1          33796/tcp  status
|   100024  1          48523/udp  status
|   100227  2,3         2049/tcp  nfs_acl
|_  100227  2,3         2049/udp  nfs_acl
2049/tcp open  nfs     2-4 (RPC #100003)
MAC Address: 00:50:56:95:20:FC (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 2.498 days (since Tue Dec 05 22:25:38 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT       ADDRESS
1   122.82 ms 10.1.34.97

Nmap scan report for 10.1.34.99
Host is up (0.13s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ed:f1:cf:49:a5:f3:7f:ac:f0:81:e8:24:8d:9b:0c:a1 (DSA)
|_  2048 a7:58:2f:c9:23:15:fb:41:ba:05:41:e8:15:51:32:bc (RSA)
37/tcp   open  time    (32 bits)
|_rfc868-time: 2017-12-08T12:15:08
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100003  2,3,4      2049/tcp  nfs
|   100003  2,3,4      2049/udp  nfs
|   100005  1,2,3     55189/udp  mountd
|   100005  1,2,3     57474/tcp  mountd
|   100011  1,2         875/tcp  rquotad
|   100011  1,2         875/udp  rquotad
|   100021  1,3,4     35958/udp  nlockmgr
|   100021  1,3,4     49278/tcp  nlockmgr
|   100024  1         46389/udp  status
|   100024  1         54235/tcp  status
|   100227  2,3        2049/tcp  nfs_acl
|_  100227  2,3        2049/udp  nfs_acl
2049/tcp open  nfs     2-4 (RPC #100003)
MAC Address: 00:50:56:95:FD:C3 (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 1.645 days (since Wed Dec 06 18:53:40 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT       ADDRESS
1   129.18 ms 10.1.34.99

Nmap scan report for 10.1.34.100
Host is up (0.13s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 22:9b:22:00:7f:13:59:2d:4b:90:12:19:cb:9f:b4:61 (DSA)
|_  2048 bf:49:72:45:86:2c:0a:93:2d:06:fc:d5:7c:ed:b7:bc (RSA)
80/tcp   open  http     Apache httpd 2.2.15 ((CentOS))
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
```

```
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.15 (CentOS)
|_http-title: Apache HTTP Server Test Page powered by CentOS
111/tcp  open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100003  2,3,4      2049/tcp  nfs
|   100003  2,3,4      2049/udp  nfs
|   100005  1,2,3     41291/tcp  mountd
|   100005  1,2,3     51434/udp  mountd
|   100011  1,2         875/tcp  rquotad
|   100011  1,2         875/udp  rquotad
|   100021  1,3,4     36397/udp  nlockmgr
|   100021  1,3,4     54811/tcp  nlockmgr
|   100024  1         45265/tcp  status
|   100024  1         47497/udp  status
|   100227  2,3        2049/tcp  nfs_acl
|_  100227  2,3        2049/udp  nfs_acl
443/tcp  open  ssl/http Apache httpd 2.2.15 ((CentOS))
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.15 (CentOS)
|_http-title: Apache HTTP Server Test Page powered by CentOS
| ssl-cert: Subject:
commonName=webscada/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Issuer: commonName=webscada/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-04-15T18:20:54
| Not valid after:  2017-04-15T18:20:54
| MD5:   a91a cf5d 738a d35d b847 20ea fb41 6960
|_SHA-1: ecff ecc6 f059 de0b ae39 5379 3ce2 ba40 6931 d6e6
|_ssl-date: 2017-12-08T12:12:57+00:00; 0s from scanner time.
2049/tcp open  nfs      2-4 (RPC #100003)
MAC Address: 00:50:56:95:73:16 (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 43.617 days (since Wed Oct 25 19:34:06 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT       ADDRESS
1   128.09 ms 10.1.34.100

Nmap scan report for 10.1.34.101
Host is up (0.13s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 cf:76:00:fe:90:a8:65:a0:a9:11:7d:9f:55:0f:75:ef (DSA)
|_  2048 84:de:55:a9:a9:a4:79:d2:7f:7c:c8:d5:bd:1c:17:42 (RSA)
37/tcp   open  time       (32 bits)
|_rfc868-time: 2017-12-08T12:12:57
111/tcp  open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|_  100000  2,3,4       111/udp  rpcbind
514/tcp  open  shell?
5432/tcp open  postgresql PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
6000/tcp open  X11        (access denied)
MAC Address: 00:50:56:95:47:CE (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 1.763 days (since Wed Dec 06 16:05:02 2017)
Network Distance: 1 hop
```

```
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT      ADDRESS
1   125.22 ms 10.1.34.101

Nmap scan report for 10.1.34.102
Host is up (0.13s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.2.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Jul 24  2015 pub
22/tcp   open  ssh        OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 93:3b:64:66:b2:37:39:04:3c:4c:90:63:d4:1c:5e:44 (DSA)
|_  2048 77:d1:68:bd:d9:d2:67:4a:52:2a:13:24:3c:e4:b1:35 (RSA)
23/tcp   open  telnet     Linux telnetd
111/tcp  open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|   100000  2,3,4       111/udp  rpcbind
|   100024  1         47654/tcp  status
|_  100024  1         48735/udp  status
514/tcp  open  shell?
5432/tcp open  postgresql PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
5989/tcp open  ssl/http   Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd
| http-methods:
|_  Supported Methods: POST
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=srv1/organizationName=The Open
Group/stateOrProvinceName=Berkshire/countryName=UK
| Issuer: commonName=srv1/organizationName=The Open Group/stateOrProvinceName=Berkshire/countryName=UK
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-04-12T20:48:04
| Not valid after:  2026-04-10T20:48:04
| MD5:   c156 ba51 d6f9 d86e d912 471b 38a0 f9d6
|_SHA-1: 9ce8 773e 8cbb 59f4 b8c6 9153 6744 3a32 5d79 d592
|_ssl-date: 2017-12-08T12:14:08+00:00; -1s from scanner time.
9090/tcp open  http       Jetty
|_hadoop-datanode-info:
|_hadoop-jobtracker-info:
|_hadoop-tasktracker-info:
|_hbase-master-info:
| http-cookie-flags:
|   /:
|     JSESSIONID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: E4888EE8491B4EB75501996E41AF6460
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:50:56:95:1A:C9 (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 7.187 days (since Fri Dec 01 05:54:17 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT      ADDRESS
1   132.74 ms 10.1.34.102
```

```
Nmap scan report for 10.1.34.111
Host is up (0.12s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 2.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 May 24  2008 pub
22/tcp   open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 7b:e4:55:06:31:19:71:e3:d5:99:0c:1e:eb:e9:df:95 (DSA)
|_  2048 93:d1:fb:09:23:d6:f4:21:86:5b:88:3e:86:57:29:af (RSA)
37/tcp   open  time       (32 bits)
|_rfc868-time: 2017-12-08T12:14:53
111/tcp  open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|_  100000  2           111/udp  rpcbind
514/tcp  open  shell?
5432/tcp open  postgresql PostgreSQL DB 8.2.5 - 8.2.19
6000/tcp open  X11        X.Org (open)
MAC Address: 00:15:17:CD:EE:9A (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Uptime guess: 9.599 days (since Tue Nov 28 20:00:47 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=205 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

Host script results:
|_clock-skew: mean: 2s, deviation: 0s, median: 2s

TRACEROUTE
HOP RTT       ADDRESS
1   121.31 ms 10.1.34.111

Nmap scan report for 10.1.34.126
Host is up (0.048s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE    VERSION
443/tcp open  ssl/https?
|_ssl-date: 2017-12-08T12:15:12+00:00; -1s from scanner time.
MAC Address: 00:09:8E:FA:10:9A (ipcas GmbH)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: router|switch|general purpose
Running: Juniper embedded, Nortel embedded, Wind River VxWorks
OS CPE: cpe:/h:juniper:j4350 cpe:/h:nortel:ethernet_routing_switch_4550t-pwr cpe:/o:windriver:vxworks
OS details: Juniper J4350 router, Nortel Ethernet Routing Switch 4550T-PWR, VxWorks
Uptime guess: 51.472 days (since Tue Oct 17 23:02:56 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT      ADDRESS
1   48.23 ms 10.1.34.126

Nmap scan report for 10.1.34.127
Host is up (0.055s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE    VERSION
443/tcp open  ssl/https?
|_ssl-date: 2017-12-08T12:14:04+00:00; -1s from scanner time.
MAC Address: 00:09:8E:FA:05:F5 (ipcas GmbH)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|general purpose
Running: Nortel embedded, Wind River VxWorks
OS CPE: cpe:/h:nortel:ethernet_routing_switch_4550t-pwr cpe:/o:windriver:vxworks
OS details: Nortel Ethernet Routing Switch 4550T-PWR, VxWorks
Uptime guess: 51.473 days (since Tue Oct 17 23:02:36 2017)
```

```
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT      ADDRESS
1   54.65 ms 10.1.34.127

Nmap scan report for 10.1.34.128
Host is up (0.056s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE    VERSION
443/tcp open  ssl/https?
|_ssl-date: 2017-12-08T12:14:03+00:00; -1s from scanner time.
MAC Address: 00:09:8E:FA:10:97 (ipcas GmbH)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|general purpose
Running: Nortel embedded, Wind River VxWorks
OS CPE: cpe:/h:nortel:ethernet_routing_switch_4550t-pwr cpe:/o:windriver:vxworks
OS details: Nortel Ethernet Routing Switch 4550T-PWR, VxWorks
Uptime guess: 51.466 days (since Tue Oct 17 23:12:21 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT      ADDRESS
1   55.99 ms 10.1.34.128

Nmap scan report for 10.1.34.151
Host is up (0.11s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Tornado vxWorks ftpd 5.5.1
23/tcp   open  telnet  VxWorks telnetd
80/tcp   open  http    WindWeb 4.00
|_http-favicon: Unknown favicon MD5: E5A839BF2CADB92C294E4D04E69DA7FA
| http-methods:
|_  Supported Methods: GET
|_http-server-header: WindWeb/4.00
|_http-title: webCAT-Login
111/tcp  open  rpcbind 2 (RPC #100000)
|_rpcinfo:
1100/tcp open  mctp?
MAC Address: 00:50:C2:28:20:6F (Ieee Registration Authority)
Device type: general purpose
Running: Wind River VxWorks
OS CPE: cpe:/o:windriver:vxworks
OS details: VxWorks
Uptime guess: 14.895 days (since Thu Nov 23 12:54:11 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=155 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: VxWorks; CPE: cpe:/o:windriver:vxworks

TRACEROUTE
HOP RTT      ADDRESS
1   111.46 ms 10.1.34.151

Nmap scan report for 10.1.34.152
Host is up (0.11s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Tornado vxWorks ftpd 5.5.1
23/tcp   open  telnet  VxWorks telnetd
80/tcp   open  http    WindWeb 4.00
|_http-favicon: Unknown favicon MD5: E5A839BF2CADB92C294E4D04E69DA7FA
| http-methods:
|_  Supported Methods: GET
|_http-server-header: WindWeb/4.00
|_http-title: webCAT-Login
```

```
111/tcp  open  rpcbind 2 (RPC #100000)
|_rpcinfo:
1100/tcp open  mctp?
MAC Address: 00:50:C2:28:21:82 (Ieee Registration Authority)
Device type: general purpose
Running: Wind River VxWorks
OS CPE: cpe:/o:windriver:vxworks
OS details: VxWorks
Uptime guess: 14.895 days (since Thu Nov 23 12:54:04 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=154 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: VxWorks; CPE: cpe:/o:windriver:vxworks

TRACEROUTE
HOP RTT      ADDRESS
1   111.15 ms 10.1.34.152

Nmap scan report for 10.1.34.153
Host is up (0.051s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:5E:D3:21 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:professional
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::-
cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft
Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server
2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 93.975 days (since Tue Sep 05 09:59:29 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: WIN-G4CIU2H5JMM; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 23s, deviation: 0s, median: 23s
| nbstat: NetBIOS name: WIN-G4CIU2H5JMM, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:5e:d3:21 (VMware)
| Names:
|   WIN-G4CIU2H5JMM<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WIN-G4CIU2H5JMM<20>  Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-G4CIU2H5JMM
|   NetBIOS computer name: WIN-G4CIU2H5JMM\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2017-12-08T10:15:23-02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT      ADDRESS
1   51.27 ms 10.1.34.153

Nmap scan report for 10.1.34.195
Host is up (0.11s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE        VERSION
22/tcp   open  ssh            OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 06:fc:58:2e:b9:5c:2d:1a:0c:1d:9d:26:fd:84:d8:80 (DSA)
|_  2048 d5:83:4a:c3:92:79:9a:28:e1:56:b1:74:41:af:6b:d8 (RSA)
```

```
37/tcp   open  time          (32 bits)
|_rfc868-time: 2017-12-08T12:14:41
111/tcp  open  rpcbind       2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|_  100000  2,3,4       111/udp  rpcbind
514/tcp  open  shell?
5432/tcp open  postgresql    PostgreSQL DB 8.0.5 or 8.2.20 - 8.2.23
8000/tcp open  http-alt?
8100/tcp open  xprint-server?
MAC Address: A0:36:9F:88:8A:2C (Intel Corporate)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 45.240 days (since Tue Oct 24 04:37:59 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=253 (Good luck!)
IP ID Sequence Generation: All zeros

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT      ADDRESS
1   112.89 ms 10.1.34.195

Nmap scan report for 10.1.34.201
Host is up (0.13s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 6.6.1 (protocol 2.0)
| ssh-hostkey:
|   2048 66:05:2a:70:3b:07:42:2c:c3:11:c8:a6:46:f4:1c:0f (RSA)
|   256 a9:b9:01:d6:a0:47:11:53:5e:f2:1a:b4:3a:af:92:26 (ECDSA)
|_  256 4d:93:9e:b6:f5:35:e0:d3:4d:40:87:36:7e:6a:e7:f3 (EdDSA)
80/tcp   open  http       nginx 1.10.2
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.10.2
|_http-title: Test Page for the Nginx HTTP Server on Fedora
111/tcp  open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4       111/tcp  rpcbind
|_  100000  2,3,4       111/udp  rpcbind
5432/tcp open  postgresql PostgreSQL DB 9.6.2
6000/tcp open  X11        (access denied)
MAC Address: 00:50:56:95:BA:48 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Uptime guess: 2.972 days (since Tue Dec 05 11:02:46 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE
HOP RTT      ADDRESS
1   126.36 ms 10.1.34.201

Nmap scan report for 10.1.34.225
Host is up (0.12s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
```

```
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:C2:F1:4A (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1
Update 1
Uptime guess: 2.008 days (since Wed Dec 06 10:11:33 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: WIN-5JTJUC6QMMO; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2s, deviation: 0s, median: 2s
| nbstat: NetBIOS name: WIN-5JTJUC6QMMO, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:c2:f1:4a (VMware)
| Names:
|   WIN-5JTJUC6QMMO<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WIN-5JTJUC6QMMO<20>  Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: WIN-5JTJUC6QMMO
|   NetBIOS computer name: WIN-5JTJUC6QMMO\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2017-12-08T10:13:27-02:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT       ADDRESS
1   118.57 ms 10.1.34.225

Nmap scan report for 10.1.34.230
Host is up (0.12s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE    VERSION
9/tcp    open  discard?
21/tcp   open  ftp        QNX ftpd 20081216
23/tcp   open  telnet     Openwall GNU/*/Linux telnetd
7777/tcp open  tcpwrapped
MAC Address: 00:1B:EB:02:3F:E3 (DMP Electronics)
Device type: WAP|storage-misc|general purpose
Running: Apple NetBSD 4.X, QNX 6.X
OS CPE: cpe:/h:apple:airport_extreme cpe:/o:apple:netbsd:4.99 cpe:/o:qnx:qnx:6.5.0
OS details: Apple AirPort Extreme WAP or Time Capsule NAS device (NetBSD 4.99), or QNX 6.5.0
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=218 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: utr; OSs: QNX, Linux; CPE: cpe:/o:qnx:qnx, cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT       ADDRESS
1   121.64 ms 10.1.34.230

Nmap scan report for 10.1.34.233
Host is up (0.12s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds (workgroup: WORKGROUP)
| fingerprint-strings:
|   SMBProgNeg:
|_    SMBr
MAC Address: 00:0C:29:EA:C5:06 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp3
```

```
OS details: Microsoft Windows XP SP3
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: JULIO-E1F3355D1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2m11s, deviation: 0s, median: 2m11s
| nbstat: NetBIOS name: JULIO-E1F3355D1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:ea:c5:06 (VMware)
| Names:
|   JULIO-E1F3355D1<00>  Flags: <unique><active>
|   JULIO-E1F3355D1<20>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: julio-e1f3355d1
|   NetBIOS computer name: JULIO-E1F3355D1\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2017-12-08T10:15:39-02:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

TRACEROUTE
HOP RTT       ADDRESS
1   123.32 ms 10.1.34.233

Nmap scan report for 10.1.34.243
Host is up (0.13s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Cisco router telnetd
80/tcp open  http    Cisco IOS http config
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=level_15_access
| http-methods:
|_  Supported Methods: POST
|_http-server-header: cisco-IOS
|_http-title: Site doesn't have a title.
MAC Address: 00:1E:79:28:D7:44 (Cisco Systems)
Device type: switch
Running: Cisco IOS 12.X
OS CPE: cpe:/h:cisco:catalyst_2960 cpe:/h:cisco:catalyst_3560 cpe:/h:cisco:catalyst_3750 cpe:/o:cisco:ios:12.2
OS details: Cisco Catalyst 2960, 3560, or 3750 switch (IOS 12.2)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT       ADDRESS
1   132.32 ms 10.1.34.243

Nmap scan report for 10.1.34.244
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Cisco router telnetd
80/tcp open  http    Cisco IOS http config
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=level_15_access
| http-methods:
|_  Supported Methods: POST
|_http-server-header: cisco-IOS
|_http-title: Site doesn't have a title.
MAC Address: 00:1E:79:88:DE:C4 (Cisco Systems)
Device type: switch
Running: Cisco IOS 12.X
OS CPE: cpe:/h:cisco:catalyst_2960 cpe:/h:cisco:catalyst_3560 cpe:/h:cisco:catalyst_3750 cpe:/o:cisco:ios:12.2
OS details: Cisco Catalyst 2960, 3560, or 3750 switch (IOS 12.2)
```

```
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT       ADDRESS
1   124.26 ms 10.1.34.244

Nmap scan report for 10.1.34.247
Host is up (0.12s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   Cisco router telnetd
80/tcp  open  http     Cisco IOS http config
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=level_15_or_view_access
| http-methods:
|_  Supported Methods: POST
|_http-server-header: cisco-IOS
|_http-title: Site doesn't have a title.
443/tcp open  ssl/http Cisco IOS http config
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=level_15_or_view_access
| http-methods:
|_  Supported Methods: POST
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=IOS-Self-Signed-Certificate-590500352
| Subject Alternative Name: DNS:FTBO-A03P.
| Issuer: commonName=IOS-Self-Signed-Certificate-590500352
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 1993-03-01T00:02:39
| Not valid after:  2020-01-01T00:00:00
| MD5:   4351 b3a4 fa2b c90a 6785 6425 cd08 ae4a
|_SHA-1: 2e8c dd2b 9e7a 57ac afb0 28d3 d791 66a8 3ed4 87b1
|_ssl-date: 2017-12-08T12:15:14+00:00; -1s from scanner time.
MAC Address: 3C:0E:23:32:52:44 (Cisco Systems)
Device type: switch|router|firewall
Running: Cisco IOS 12.X|15.X, Cisco embedded
OS CPE: cpe:/h:cisco:catalyst_2950 cpe:/h:cisco:catalyst_2960 cpe:/h:cisco:catalyst_3550 cpe:/h:cisco:catalyst_3560
cpe:/h:cisco:catalyst_3750 cpe:/h:cisco:catalyst_4500 cpe:/o:cisco:ios:12 cpe:/o:cisco:ios:15
OS details: Cisco 2950, 2960, 3550, 3560, 3750, or 4500 switch or 6500 router (IOS 12.1 - 15.0); or Adaptive Security Appliance
firewall
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT       ADDRESS
1   115.22 ms 10.1.34.247

Nmap scan report for 10.1.34.248
Host is up (0.053s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
23/tcp  open  telnet   Cisco router telnetd
80/tcp  open  http     Cisco IOS http config
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=level_15_or_view_access
| http-methods:
|_  Supported Methods: POST
|_http-server-header: cisco-IOS
|_http-title: Site doesn't have a title.
443/tcp open  ssl/http Cisco IOS http config
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=level_15_or_view_access
|_http-server-header: cisco-IOS
```

```
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=IOS-Self-Signed-Certificate-590502016
| Subject Alternative Name: DNS:FTBO-A03S.
| Issuer: commonName=IOS-Self-Signed-Certificate-590502016
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 1993-03-01T00:02:35
| Not valid after:  2020-01-01T00:00:00
| MD5:   6677 cf2c d907 a9cf 1ed9 e32a ffb3 0685
|_SHA-1: ed06 6cad 15c8 1cd3 4c69 833d 0e18 a6da d25d c005
|_ssl-date: 2017-12-08T12:13:37+00:00; -1s from scanner time.
MAC Address: 3C:0E:23:32:58:C4 (Cisco Systems)
Device type: switch|router|firewall
Running: Cisco IOS 12.X|15.X, Cisco embedded
OS CPE: cpe:/h:cisco:catalyst_2950 cpe:/h:cisco:catalyst_2960 cpe:/h:cisco:catalyst_3550 cpe:/h:cisco:catalyst_3560
cpe:/h:cisco:catalyst_3750 cpe:/h:cisco:catalyst_4500 cpe:/o:cisco:ios:12 cpe:/o:cisco:ios:15
OS details: Cisco 2950, 2960, 3550, 3560, 3750, or 4500 switch or 6500 router (IOS 12.1 - 15.0); or Adaptive Security Appliance
firewall
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT      ADDRESS
1   53.27 ms 10.1.34.248

Nmap scan report for 10.1.34.250
Host is up (0.13s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 f6:de:d8:ba:71:71:85:e0:07:41:0a:1d:3d:6f:04:2d (DSA)
|_  2048 fa:7d:89:b9:5e:df:3b:9b:13:cf:3d:b2:8a:5d:4a:61 (RSA)
80/tcp   open  http    Apache httpd 2.2.15 ((CentOS))
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.15 (CentOS)
|_http-title: Apache HTTP Server Test Page powered by CentOS
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:50:56:95:B9:36 (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 2.572 days (since Tue Dec 05 20:39:19 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT      ADDRESS
1   125.47 ms 10.1.34.250

Nmap scan report for 10.1.34.253
Host is up (0.025s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Cisco router telnetd
MAC Address: 00:1E:49:1C:5B:C6 (Cisco Systems)
Aggressive OS guesses: Cisco 836, 890, 1751, 1841, 2800, or 2900 router (IOS 12.4 - 15.1) (96%), Cisco Aironet 1141N (IOS
12.4) or 3602I (IOS 15.3) WAP (96%), Cisco Catalyst 2960 switch (IOS 15.2) (96%), Cisco Aironet 2600-series WAP (IOS
15.2(2)) (96%), Cisco 1841 router (IOS 12.4) (95%), Cisco 877 router (IOS 12.4) (95%), Cisco 1841 router (IOS 12) (95%),
Cisco IOS 12.4 or IOS-XE 15.3 (94%), Cisco 10000 router (IOS 12.3) (94%), Cisco 7600 router (IOS 12.2) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT      ADDRESS
1   25.40 ms 10.1.34.253
```

```
Nmap scan report for 10.1.34.254
Host is up (0.13s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Cisco router telnetd
80/tcp open  http    Cisco IOS http config
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=level_15_access
| http-methods:
|_  Supported Methods: POST
|_http-server-header: cisco-IOS
|_http-title: Site doesn't have a title.
MAC Address: 00:1E:79:64:39:46 (Cisco Systems)
Device type: switch|router|firewall
Running: Cisco IOS 12.X|15.X, Cisco embedded
OS CPE: cpe:/h:cisco:catalyst_2950 cpe:/h:cisco:catalyst_2960 cpe:/h:cisco:catalyst_3550 cpe:/h:cisco:catalyst_3560
cpe:/h:cisco:catalyst_3750 cpe:/h:cisco:catalyst_4500 cpe:/o:cisco:ios:12 cpe:/o:cisco:ios:15
OS details: Cisco 2950, 2960, 3550, 3560, 3750, or 4500 switch or 6500 router (IOS 12.1 - 15.0); or Adaptive Security Appliance
firewall
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT       ADDRESS
1   127.46 ms 10.1.34.254

Skipping SYN Stealth Scan against 10.1.34.129 because Windows does not support scanning your own machine (localhost) this
way.
Initiating Service scan at 10:23
Skipping OS Scan against 10.1.34.129 because it doesn't work against your own machine (localhost)
NSE: Script scanning 10.1.34.129.
Initiating NSE at 10:23
Completed NSE at 10:23, 0.00s elapsed
Initiating NSE at 10:23
Completed NSE at 10:23, 0.00s elapsed
Nmap scan report for 10.1.34.129
Host is up.

PORT     STATE   SERVICE            VERSION
1/tcp    unknown tcpmux
3/tcp    unknown compressnet
4/tcp    unknown unknown
6/tcp    unknown unknown
7/tcp    unknown echo
9/tcp    unknown discard
13/tcp   unknown daytime
17/tcp   unknown qotd
19/tcp   unknown chargen
20/tcp   unknown ftp-data
21/tcp   unknown ftp
22/tcp   unknown ssh
23/tcp   unknown telnet
24/tcp   unknown priv-mail
25/tcp   unknown smtp
26/tcp   unknown rsftp
30/tcp   unknown unknown
32/tcp   unknown unknown
33/tcp   unknown dsp
37/tcp   unknown time
42/tcp   unknown nameserver
43/tcp   unknown whois
49/tcp   unknown tacacs
53/tcp   unknown domain
70/tcp   unknown gopher
79/tcp   unknown finger
80/tcp   unknown http
81/tcp   unknown hosts2-ns
82/tcp   unknown xfer
83/tcp   unknown mit-ml-dev
84/tcp   unknown ctf
85/tcp   unknown mit-ml-dev
88/tcp   unknown kerberos-sec
89/tcp   unknown su-mit-tg
```

90/tcp unknown dnsix
99/tcp unknown metagram
100/tcp unknown newacct
106/tcp unknown pop3pw
109/tcp unknown pop2
110/tcp unknown pop3
111/tcp unknown rpcbind
113/tcp unknown ident
119/tcp unknown nntp
125/tcp unknown locus-map
135/tcp unknown msrpc
139/tcp unknown netbios-ssn
143/tcp unknown imap
144/tcp unknown news
146/tcp unknown iso-tp0
161/tcp unknown snmp
163/tcp unknown cmip-man
179/tcp unknown bgp
199/tcp unknown smux
211/tcp unknown 914c-g
212/tcp unknown anet
222/tcp unknown rsh-spx
254/tcp unknown unknown
255/tcp unknown unknown
256/tcp unknown fw1-secureremote
259/tcp unknown esro-gen
264/tcp unknown bgmp
280/tcp unknown http-mgmt
301/tcp unknown unknown
306/tcp unknown unknown
311/tcp unknown asip-webadmin
340/tcp unknown unknown
366/tcp unknown odmr
389/tcp unknown ldap
406/tcp unknown imsp
407/tcp unknown timbuktu
416/tcp unknown silverplatter
417/tcp unknown onmux
425/tcp unknown icad-el
427/tcp unknown svrloc
443/tcp unknown https
444/tcp unknown snpp
445/tcp unknown microsoft-ds
458/tcp unknown appleqtc
464/tcp unknown kpasswd5
465/tcp unknown smtps
481/tcp unknown dvs
497/tcp unknown retrospect
500/tcp unknown isakmp
512/tcp unknown exec
513/tcp unknown login
514/tcp unknown shell
515/tcp unknown printer
524/tcp unknown ncp
541/tcp unknown uucp-rlogin
543/tcp unknown klogin
544/tcp unknown kshell
545/tcp unknown ekshell
548/tcp unknown afp
554/tcp unknown rtsp
555/tcp unknown dsf
563/tcp unknown snews
587/tcp unknown submission
593/tcp unknown http-rpc-epmap
616/tcp unknown sco-sysmgr
617/tcp unknown sco-dtmgr
625/tcp unknown apple-xsrvr-admin
631/tcp unknown ipp
636/tcp unknown ldapssl
646/tcp unknown ldp
648/tcp unknown rrp
666/tcp unknown doom
667/tcp unknown disclose
668/tcp unknown mecomm
683/tcp unknown corba-iiop
687/tcp unknown asipregistry
691/tcp unknown resvc

700/tcp unknown epp
705/tcp unknown agentx
711/tcp unknown cisco-tdp
714/tcp unknown iris-xpcs
720/tcp unknown unknown
722/tcp unknown unknown
726/tcp unknown unknown
749/tcp unknown kerberos-adm
765/tcp unknown webster
777/tcp unknown multiling-http
783/tcp unknown spamassassin
787/tcp unknown qsc
800/tcp unknown mdbs_daemon
801/tcp unknown device
808/tcp unknown ccproxy-http
843/tcp unknown unknown
873/tcp unknown rsync
880/tcp unknown unknown
888/tcp unknown accessbuilder
898/tcp unknown sun-manageconsole
900/tcp unknown omginitialrefs
901/tcp unknown samba-swat
902/tcp unknown iss-realsecure
903/tcp unknown iss-console-mgr
911/tcp unknown xact-backup
912/tcp unknown apex-mesh
981/tcp unknown unknown
987/tcp unknown unknown
990/tcp unknown ftps
992/tcp unknown telnets
993/tcp unknown imaps
995/tcp unknown pop3s
999/tcp unknown garcon
1000/tcp unknown cadlock
1001/tcp unknown webpush
1002/tcp unknown windows-icfw
1007/tcp unknown unknown
1009/tcp unknown unknown
1010/tcp unknown surf
1011/tcp unknown unknown
1021/tcp unknown exp1
1022/tcp unknown exp2
1023/tcp unknown netvenuechat
1024/tcp unknown kdm
1025/tcp unknown NFS-or-IIS
1026/tcp unknown LSA-or-nterm
1027/tcp unknown IIS
1028/tcp unknown unknown
1029/tcp unknown ms-lsa
1030/tcp unknown iad1
1031/tcp unknown iad2
1032/tcp unknown iad3
1033/tcp unknown netinfo
1034/tcp unknown zincite-a
1035/tcp unknown multidropper
1036/tcp unknown nsstp
1037/tcp unknown ams
1038/tcp unknown mtqp
1039/tcp unknown sbl
1040/tcp unknown netsaint
1041/tcp unknown danf-ak2
1042/tcp unknown afrog
1043/tcp unknown boinc
1044/tcp unknown dcutility
1045/tcp unknown fpitp
1046/tcp unknown wfremotertm
1047/tcp unknown neod1
1048/tcp unknown neod2
1049/tcp unknown td-postman
1050/tcp unknown java-or-OTGfileshare
1051/tcp unknown optima-vnet
1052/tcp unknown ddt
1053/tcp unknown remote-as
1054/tcp unknown brvread
1055/tcp unknown ansyslmd
1056/tcp unknown vfo
1057/tcp unknown startron

1058/tcp unknown nim
1059/tcp unknown nimreg
1060/tcp unknown polestar
1061/tcp unknown kiosk
1062/tcp unknown veracity
1063/tcp unknown kyoceranetdev
1064/tcp unknown jstel
1065/tcp unknown syscomlan
1066/tcp unknown fpo-fns
1067/tcp unknown instl_boots
1068/tcp unknown instl_bootc
1069/tcp unknown cognex-insight
1070/tcp unknown gmrupdateserv
1071/tcp unknown bsquare-voip
1072/tcp unknown cardax
1073/tcp unknown bridgecontrol
1074/tcp unknown warmspotMgmt
1075/tcp unknown rdrmshc
1076/tcp unknown sns_credit
1077/tcp unknown imgames
1078/tcp unknown avocent-proxy
1079/tcp unknown asprovatalk
1080/tcp unknown socks
1081/tcp unknown pvuniwien
1082/tcp unknown amt-esd-prot
1083/tcp unknown ansoft-lm-1
1084/tcp unknown ansoft-lm-2
1085/tcp unknown webobjects
1086/tcp unknown cplscrambler-lg
1087/tcp unknown cplscrambler-in
1088/tcp unknown cplscrambler-al
1089/tcp unknown ff-annunc
1090/tcp unknown ff-fms
1091/tcp unknown ff-sm
1092/tcp unknown obrpd
1093/tcp unknown proofd
1094/tcp unknown rootd
1095/tcp unknown nicelink
1096/tcp unknown cnrprotocol
1097/tcp unknown sunclustermgr
1098/tcp unknown rmiactivation
1099/tcp unknown rmiregistry
1100/tcp unknown mctp
1102/tcp unknown adobeserver-1
1104/tcp unknown xrl
1105/tcp unknown ftranhc
1106/tcp unknown isoipsigport-1
1107/tcp unknown isoipsigport-2
1108/tcp unknown ratio-adp
1110/tcp unknown nfsd-status
1111/tcp unknown lmsocialserver
1112/tcp unknown msql
1113/tcp unknown ltp-deepspace
1114/tcp unknown mini-sql
1117/tcp unknown ardus-mtrns
1119/tcp unknown bnetgame
1121/tcp unknown rmpp
1122/tcp unknown availant-mgr
1123/tcp unknown murray
1124/tcp unknown hpvmmcontrol
1126/tcp unknown hpvmmdata
1130/tcp unknown casp
1131/tcp unknown caspssl
1132/tcp unknown kvm-via-ip
1137/tcp unknown trim
1138/tcp unknown encrypted_admin
1141/tcp unknown mxomss
1145/tcp unknown x9-icue
1147/tcp unknown capioverlan
1148/tcp unknown elfiq-repl
1149/tcp unknown bvtsonar
1151/tcp unknown unizensus
1152/tcp unknown winpoplanmess
1154/tcp unknown resacommunity
1163/tcp unknown sddp
1164/tcp unknown qsm-proxy
1165/tcp unknown qsm-gui

1166/tcp unknown qsm-remote
1169/tcp unknown tripwire
1174/tcp unknown fnet-remote-ui
1175/tcp unknown dossier
1183/tcp unknown llsurfup-http
1185/tcp unknown catchpole
1186/tcp unknown mysql-cluster
1187/tcp unknown alias
1192/tcp unknown caids-sensor
1198/tcp unknown cajo-discovery
1199/tcp unknown dmidi
1201/tcp unknown nucleus-sand
1213/tcp unknown mpc-lifenet
1216/tcp unknown etebac5
1217/tcp unknown hpss-ndapi
1218/tcp unknown aeroflight-ads
1233/tcp unknown univ-appserver
1234/tcp unknown hotline
1236/tcp unknown bvcontrol
1244/tcp unknown isbconference1
1247/tcp unknown visionpyramid
1248/tcp unknown hermes
1259/tcp unknown opennl-voice
1271/tcp unknown excw
1272/tcp unknown cspmlockmgr
1277/tcp unknown miva-mqs
1287/tcp unknown routematch
1296/tcp unknown dproxy
1300/tcp unknown h323hostcallsc
1301/tcp unknown ci3-software-1
1309/tcp unknown jtag-server
1310/tcp unknown husky
1311/tcp unknown rxmon
1322/tcp unknown novation
1328/tcp unknown ewall
1334/tcp unknown writesrv
1352/tcp unknown lotusnotes
1417/tcp unknown timbuktu-srv1
1433/tcp unknown ms-sql-s
1434/tcp unknown ms-sql-m
1443/tcp unknown ies-lm
1455/tcp unknown esl-lm
1461/tcp unknown ibm_wrless_lan
1494/tcp unknown citrix-ica
1500/tcp unknown vlsi-lm
1501/tcp unknown sas-3
1503/tcp unknown imtc-mcs
1521/tcp unknown oracle
1524/tcp unknown ingreslock
1533/tcp unknown virtual-places
1556/tcp unknown veritas_pbx
1580/tcp unknown tn-tl-r1
1583/tcp unknown simbaexpress
1594/tcp unknown sixtrak
1600/tcp unknown issd
1641/tcp unknown invision
1658/tcp unknown sixnetudr
1666/tcp unknown netview-aix-6
1687/tcp unknown nsjtp-ctrl
1688/tcp unknown nsjtp-data
1700/tcp unknown mps-raft
1717/tcp unknown fj-hdnet
1718/tcp unknown h323gatedisc
1719/tcp unknown h323gatestat
1720/tcp unknown h323q931
1721/tcp unknown caicci
1723/tcp unknown pptp
1755/tcp unknown wms
1761/tcp unknown landesk-rc
1782/tcp unknown hp-hcip
1783/tcp unknown unknown
1801/tcp unknown msmq
1805/tcp unknown enl-name
1812/tcp unknown radius
1839/tcp unknown netopia-vo1
1840/tcp unknown netopia-vo2
1862/tcp unknown mysql-cm-agent

1863/tcp unknown msnp
1864/tcp unknown paradym-31
1875/tcp unknown westell-stats
1900/tcp unknown upnp
1914/tcp unknown elm-momentum
1935/tcp unknown rtmp
1947/tcp unknown sentinelsrm
1971/tcp unknown netop-school
1972/tcp unknown intersys-cache
1974/tcp unknown drp
1984/tcp unknown bigbrother
1998/tcp unknown x25-svc-port
1999/tcp unknown tcp-id-port
2000/tcp unknown cisco-sccp
2001/tcp unknown dc
2002/tcp unknown globe
2003/tcp unknown finger
2004/tcp unknown mailbox
2005/tcp unknown deslogin
2006/tcp unknown invokator
2007/tcp unknown dectalk
2008/tcp unknown conf
2009/tcp unknown news
2010/tcp unknown search
2013/tcp unknown raid-am
2020/tcp unknown xinupageserver
2021/tcp unknown servexec
2022/tcp unknown down
2030/tcp unknown device2
2033/tcp unknown glogger
2034/tcp unknown scoremgr
2035/tcp unknown imsldoc
2038/tcp unknown objectmanager
2040/tcp unknown lam
2041/tcp unknown interbase
2042/tcp unknown isis
2043/tcp unknown isis-bcast
2045/tcp unknown cdfunc
2046/tcp unknown sdfunc
2047/tcp unknown dls
2048/tcp unknown dls-monitor
2049/tcp unknown nfs
2065/tcp unknown dlsrpn
2068/tcp unknown avocentkvm
2099/tcp unknown h2250-annex-g
2100/tcp unknown amiganetfs
2103/tcp unknown zephyr-clt
2105/tcp unknown eklogin
2106/tcp unknown ekshell
2107/tcp unknown msmq-mgmt
2111/tcp unknown kx
2119/tcp unknown gsigatekeeper
2121/tcp unknown ccproxy-ftp
2126/tcp unknown pktcable-cops
2135/tcp unknown gris
2144/tcp unknown lv-ffx
2160/tcp unknown apc-2160
2161/tcp unknown apc-agent
2170/tcp unknown eyetv
2179/tcp unknown vmrdp
2190/tcp unknown tivoconnect
2191/tcp unknown tvbus
2196/tcp unknown unknown
2200/tcp unknown ici
2222/tcp unknown EtherNetIP-1
2251/tcp unknown dif-port
2260/tcp unknown apc-2260
2288/tcp unknown netml
2301/tcp unknown compaqdiag
2323/tcp unknown 3d-nfsd
2366/tcp unknown qip-login
2381/tcp unknown compaq-https
2382/tcp unknown ms-olap3
2383/tcp unknown ms-olap4
2393/tcp unknown ms-olap1
2394/tcp unknown ms-olap2
2399/tcp unknown fmpro-fdal

2401/tcp unknown cvspserver
2492/tcp unknown groove
2500/tcp unknown rtsserv
2522/tcp unknown windb
2525/tcp unknown ms-v-worlds
2557/tcp unknown nicetec-mgmt
2601/tcp unknown zebra
2602/tcp unknown ripd
2604/tcp unknown ospfd
2605/tcp unknown bgpd
2607/tcp unknown connection
2608/tcp unknown wag-service
2638/tcp unknown sybase
2701/tcp unknown sms-rcinfo
2702/tcp unknown sms-xfer
2710/tcp unknown sso-service
2717/tcp unknown pn-requester
2718/tcp unknown pn-requester2
2725/tcp unknown msolap-ptp2
2800/tcp unknown acc-raid
2809/tcp unknown corbaloc
2811/tcp unknown gsiftp
2869/tcp unknown icslap
2875/tcp unknown dxmessagebase2
2909/tcp unknown funk-dialout
2910/tcp unknown tdaccess
2920/tcp unknown roboeda
2967/tcp unknown symantec-av
2968/tcp unknown enpp
2998/tcp unknown iss-realsec
3000/tcp unknown ppp
3001/tcp unknown nessus
3003/tcp unknown cgms
3005/tcp unknown deslogin
3006/tcp unknown deslogind
3007/tcp unknown lotusmtap
3011/tcp unknown trusted-web
3013/tcp unknown gilatskysurfer
3017/tcp unknown event_listener
3030/tcp unknown arepa-cas
3031/tcp unknown eppc
3052/tcp unknown powerchute
3071/tcp unknown csd-mgmt-port
3077/tcp unknown orbix-loc-ssl
3128/tcp unknown squid-http
3168/tcp unknown poweronnud
3211/tcp unknown avsecuremgmt
3221/tcp unknown xnm-clear-text
3260/tcp unknown iscsi
3261/tcp unknown winshadow
3268/tcp unknown globalcatLDAP
3269/tcp unknown globalcatLDAPssl
3283/tcp unknown netassistant
3300/tcp unknown ceph
3301/tcp unknown unknown
3306/tcp unknown mysql
3322/tcp unknown active-net
3323/tcp unknown active-net
3324/tcp unknown active-net
3325/tcp unknown active-net
3333/tcp unknown dec-notes
3351/tcp unknown btrieve
3367/tcp unknown satvid-datalnk
3369/tcp unknown satvid-datalnk
3370/tcp unknown satvid-datalnk
3371/tcp unknown satvid-datalnk
3372/tcp unknown msdtc
3389/tcp unknown ms-wbt-server
3390/tcp unknown dsc
3404/tcp unknown unknown
3476/tcp unknown nppmp
3493/tcp unknown nut
3517/tcp unknown 802-11-iapp
3527/tcp unknown beserver-msg-q
3546/tcp unknown unknown
3551/tcp unknown apcupsd
3580/tcp unknown nati-svrloc

3659/tcp unknown apple-sasl
3689/tcp unknown rendezvous
3690/tcp unknown svn
3703/tcp unknown adobeserver-3
3737/tcp unknown xpanel
3766/tcp unknown sitewatch-s
3784/tcp unknown bfd-control
3800/tcp unknown pwgpsi
3801/tcp unknown ibm-mgr
3809/tcp unknown apocd
3814/tcp unknown neto-dcs
3826/tcp unknown wormux
3827/tcp unknown netmpi
3828/tcp unknown neteh
3851/tcp unknown spectraport
3869/tcp unknown ovsam-mgmt
3871/tcp unknown avocent-adsap
3878/tcp unknown fotogcad
3880/tcp unknown igrs
3889/tcp unknown dandv-tester
3905/tcp unknown mupdate
3914/tcp unknown listcrt-port-2
3918/tcp unknown pktcablemmcops
3920/tcp unknown exasoftport1
3945/tcp unknown emcads
3971/tcp unknown lanrevserver
3986/tcp unknown mapper-ws_ethd
3995/tcp unknown iss-mgmt-ssl
3998/tcp unknown dnx
4000/tcp unknown remoteanything
4001/tcp unknown newoak
4002/tcp unknown mlchat-proxy
4003/tcp unknown pxc-splr-ft
4004/tcp unknown pxc-roid
4005/tcp unknown pxc-pin
4006/tcp unknown pxc-spvr
4045/tcp unknown lockd
4111/tcp unknown xgrid
4125/tcp unknown rww
4126/tcp unknown ddrepl
4129/tcp unknown nuauth
4224/tcp unknown xtell
4242/tcp unknown vrml-multi-use
4279/tcp unknown vrml-multi-use
4321/tcp unknown rwhois
4343/tcp unknown unicall
4443/tcp unknown pharos
4444/tcp unknown krb524
4445/tcp unknown upnotifyp
4446/tcp unknown n1-fwp
4449/tcp unknown privatewire
4550/tcp unknown gds-adppiw-db
4567/tcp unknown tram
4662/tcp unknown edonkey
4848/tcp unknown appserv-http
4899/tcp unknown radmin
4900/tcp unknown hfcs
4998/tcp unknown maybe-veritas
5000/tcp unknown upnp
5001/tcp unknown commplex-link
5002/tcp unknown rfe
5003/tcp unknown filemaker
5004/tcp unknown avt-profile-1
5009/tcp unknown airport-admin
5030/tcp unknown surfpass
5033/tcp unknown jtnetd-server
5050/tcp unknown mmcc
5051/tcp unknown ida-agent
5054/tcp unknown rlm-admin
5060/tcp unknown sip
5061/tcp unknown sip-tls
5080/tcp unknown onscreen
5087/tcp unknown biotic
5100/tcp unknown admd
5101/tcp unknown admdog
5102/tcp unknown admeng
5120/tcp unknown barracuda-bbs

5190/tcp unknown aol
5200/tcp unknown targus-getdata
5214/tcp unknown unknown
5221/tcp unknown 3exmp
5222/tcp unknown xmpp-client
5225/tcp unknown hp-server
5226/tcp unknown hp-status
5269/tcp unknown xmpp-server
5280/tcp unknown xmpp-bosh
5298/tcp unknown presence
5357/tcp unknown wsdapi
5405/tcp unknown pcduo
5414/tcp unknown statusd
5431/tcp unknown park-agent
5432/tcp unknown postgresql
5440/tcp unknown unknown
5500/tcp unknown hotline
5510/tcp unknown secureidprop
5544/tcp unknown unknown
5550/tcp unknown sdadmind
5555/tcp unknown freeciv
5560/tcp unknown isqlplus
5566/tcp unknown westec-connect
5631/tcp unknown pcanywheredata
5633/tcp unknown beorl
5666/tcp unknown nrpe
5678/tcp unknown rrac
5679/tcp unknown activesync
5718/tcp unknown dpm
5730/tcp unknown unieng
5800/tcp unknown vnc-http
5801/tcp unknown vnc-http-1
5802/tcp unknown vnc-http-2
5810/tcp unknown unknown
5811/tcp unknown unknown
5815/tcp unknown unknown
5822/tcp unknown unknown
5825/tcp unknown unknown
5850/tcp unknown unknown
5859/tcp unknown wherehoo
5862/tcp unknown unknown
5877/tcp unknown unknown
5900/tcp unknown vnc
5901/tcp unknown vnc-1
5902/tcp unknown vnc-2
5903/tcp unknown vnc-3
5904/tcp unknown unknown
5906/tcp unknown unknown
5907/tcp unknown unknown
5910/tcp unknown cm
5911/tcp unknown cpdlc
5915/tcp unknown unknown
5922/tcp unknown unknown
5925/tcp unknown unknown
5950/tcp unknown unknown
5952/tcp unknown unknown
5959/tcp unknown unknown
5960/tcp unknown unknown
5961/tcp unknown unknown
5962/tcp unknown unknown
5963/tcp unknown indy
5987/tcp unknown wbem-rmi
5988/tcp unknown wbem-http
5989/tcp unknown wbem-https
5998/tcp unknown ncd-diag
5999/tcp unknown ncd-conf
6000/tcp unknown X11
6001/tcp unknown X11:1
6002/tcp unknown X11:2
6003/tcp unknown X11:3
6004/tcp unknown X11:4
6005/tcp unknown X11:5
6006/tcp unknown X11:6
6007/tcp unknown X11:7
6009/tcp unknown X11:9
6025/tcp unknown x11
6059/tcp unknown X11:59

6100/tcp unknown synchronet-db
6101/tcp unknown backupexec
6106/tcp unknown isdninfo
6112/tcp unknown dtspc
6123/tcp unknown backup-express
6129/tcp unknown unknown
6156/tcp unknown unknown
6346/tcp unknown gnutella
6389/tcp unknown clariion-evr01
6502/tcp unknown netop-rc
6510/tcp unknown mcer-port
6543/tcp unknown mythtv
6547/tcp unknown powerchuteplus
6565/tcp unknown unknown
6566/tcp unknown sane-port
6567/tcp unknown esp
6580/tcp unknown parsec-master
6646/tcp unknown unknown
6666/tcp unknown irc
6667/tcp unknown irc
6668/tcp unknown irc
6669/tcp unknown irc
6689/tcp unknown tsa
6692/tcp unknown unknown
6699/tcp unknown napster
6779/tcp unknown unknown
6788/tcp unknown smc-http
6789/tcp unknown ibm-db2-admin
6792/tcp unknown unknown
6839/tcp unknown unknown
6881/tcp unknown bittorrent-tracker
6901/tcp unknown jetstream
6969/tcp unknown acmsoda
7000/tcp unknown afs3-fileserver
7001/tcp unknown afs3-callback
7002/tcp unknown afs3-prserver
7004/tcp unknown afs3-kaserver
7007/tcp unknown afs3-bos
7019/tcp unknown doceri-ctl
7025/tcp unknown vmsvc-2
7070/tcp unknown realserver
7100/tcp unknown font-service
7103/tcp unknown unknown
7106/tcp unknown unknown
7200/tcp unknown fodms
7201/tcp unknown dlip
7402/tcp unknown rtps-dd-mt
7435/tcp unknown unknown
7443/tcp unknown oracleas-https
7496/tcp unknown unknown
7512/tcp unknown unknown
7625/tcp unknown unknown
7627/tcp unknown soap-http
7676/tcp unknown imqbrokerd
7741/tcp unknown scriptview
7777/tcp unknown cbt
7778/tcp unknown interwise
7800/tcp unknown asr
7911/tcp unknown unknown
7920/tcp unknown unknown
7921/tcp unknown unknown
7937/tcp unknown nsrexecd
7938/tcp unknown lgtomapper
7999/tcp unknown irdmi2
8000/tcp unknown http-alt
8001/tcp unknown vcom-tunnel
8002/tcp unknown teradataordbms
8007/tcp unknown ajp12
8008/tcp unknown http
8009/tcp unknown ajp13
8010/tcp unknown xmpp
8011/tcp unknown unknown
8021/tcp unknown ftp-proxy
8022/tcp unknown oa-system
8031/tcp unknown unknown
8042/tcp unknown fs-agent
8045/tcp unknown unknown

8080/tcp unknown http-proxy
8081/tcp unknown blackice-icecap
8082/tcp unknown blackice-alerts
8083/tcp unknown us-srv
8084/tcp unknown unknown
8085/tcp unknown unknown
8086/tcp unknown d-s-n
8087/tcp unknown simplifymedia
8088/tcp unknown radan-http
8089/tcp unknown unknown
8090/tcp unknown opsmessaging
8093/tcp unknown unknown
8099/tcp unknown unknown
8100/tcp unknown xprint-server
8180/tcp unknown unknown
8181/tcp unknown intermapper
8192/tcp unknown sophos
8193/tcp unknown sophos
8194/tcp unknown sophos
8200/tcp unknown trivnet1
8222/tcp unknown unknown
8254/tcp unknown unknown
8290/tcp unknown unknown
8291/tcp unknown unknown
8292/tcp unknown blp3
8300/tcp unknown tmi
8333/tcp unknown bitcoin
8383/tcp unknown m2mservices
8400/tcp unknown cvd
8402/tcp unknown abarsd
8443/tcp unknown https-alt
8500/tcp unknown fmtp
8600/tcp unknown asterix
8649/tcp unknown unknown
8651/tcp unknown unknown
8652/tcp unknown unknown
8654/tcp unknown unknown
8701/tcp unknown unknown
8800/tcp unknown sunwebadmin
8873/tcp unknown dxspider
8888/tcp unknown sun-answerbook
8899/tcp unknown ospf-lite
8994/tcp unknown unknown
9000/tcp unknown cslistener
9001/tcp unknown tor-orport
9002/tcp unknown dynamid
9003/tcp unknown unknown
9009/tcp unknown pichat
9010/tcp unknown sdr
9011/tcp unknown unknown
9040/tcp unknown tor-trans
9050/tcp unknown tor-socks
9071/tcp unknown unknown
9080/tcp unknown glrpc
9081/tcp unknown unknown
9090/tcp unknown zeus-admin
9091/tcp unknown xmltec-xmlmail
9099/tcp unknown unknown
9100/tcp unknown jetdirect
9101/tcp unknown jetdirect
9102/tcp unknown jetdirect
9103/tcp unknown jetdirect
9110/tcp unknown unknown
9111/tcp unknown DragonIDSConsole
9200/tcp unknown wap-wsp
9207/tcp unknown wap-vcal-s
9220/tcp unknown unknown
9290/tcp unknown unknown
9415/tcp unknown unknown
9418/tcp unknown git
9485/tcp unknown unknown
9500/tcp unknown ismserver
9502/tcp unknown unknown
9503/tcp unknown unknown
9535/tcp unknown man
9575/tcp unknown unknown
9593/tcp unknown cba8

9594/tcp unknown msgsys
9595/tcp unknown pds
9618/tcp unknown condor
9666/tcp unknown zoomcp
9876/tcp unknown sd
9877/tcp unknown unknown
9878/tcp unknown kca-service
9898/tcp unknown monkeycom
9900/tcp unknown iua
9917/tcp unknown unknown
9929/tcp unknown nping-echo
9943/tcp unknown unknown
9944/tcp unknown unknown
9968/tcp unknown unknown
9998/tcp unknown distinct32
9999/tcp unknown abyss
10000/tcp unknown snet-sensor-mgmt
10001/tcp unknown scp-config
10002/tcp unknown documentum
10003/tcp unknown documentum_s
10004/tcp unknown emcrmirccd
10009/tcp unknown swdtp-sv
10010/tcp unknown rxapi
10012/tcp unknown unknown
10024/tcp unknown unknown
10025/tcp unknown unknown
10082/tcp unknown amandaidx
10180/tcp unknown unknown
10215/tcp unknown unknown
10243/tcp unknown unknown
10566/tcp unknown unknown
10616/tcp unknown unknown
10617/tcp unknown unknown
10621/tcp unknown unknown
10626/tcp unknown unknown
10628/tcp unknown unknown
10629/tcp unknown unknown
10778/tcp unknown unknown
11110/tcp unknown sgi-soap
11111/tcp unknown vce
11967/tcp unknown sysinfo-sp
12000/tcp unknown cce4x
12174/tcp unknown unknown
12265/tcp unknown unknown
12345/tcp unknown netbus
13456/tcp unknown unknown
13722/tcp unknown netbackup
13782/tcp unknown netbackup
13783/tcp unknown netbackup
14000/tcp unknown scotty-ft
14238/tcp unknown unknown
14441/tcp unknown unknown
14442/tcp unknown unknown
15000/tcp unknown hydap
15002/tcp unknown onep-tls
15003/tcp unknown unknown
15004/tcp unknown unknown
15660/tcp unknown bex-xr
15742/tcp unknown unknown
16000/tcp unknown fmsas
16001/tcp unknown fmsascon
16012/tcp unknown unknown
16016/tcp unknown unknown
16018/tcp unknown unknown
16080/tcp unknown osxwebadmin
16113/tcp unknown unknown
16992/tcp unknown amt-soap-http
16993/tcp unknown amt-soap-https
17877/tcp unknown unknown
17988/tcp unknown unknown
18040/tcp unknown unknown
18101/tcp unknown unknown
18988/tcp unknown unknown
19101/tcp unknown unknown
19283/tcp unknown keysrvr
19315/tcp unknown keyshadow
19350/tcp unknown unknown

19780/tcp unknown unknown
19801/tcp unknown unknown
19842/tcp unknown unknown
20000/tcp unknown dnp
20005/tcp unknown btx
20031/tcp unknown unknown
20221/tcp unknown unknown
20222/tcp unknown ipulse-ics
20828/tcp unknown unknown
21571/tcp unknown unknown
22939/tcp unknown unknown
23502/tcp unknown unknown
24444/tcp unknown unknown
24800/tcp unknown unknown
25734/tcp unknown unknown
25735/tcp unknown unknown
26214/tcp unknown unknown
27000/tcp unknown flexlm0
27352/tcp unknown unknown
27353/tcp unknown unknown
27355/tcp unknown unknown
27356/tcp unknown unknown
27715/tcp unknown unknown
28201/tcp unknown unknown
30000/tcp unknown ndmps
30718/tcp unknown unknown
30951/tcp unknown unknown
31038/tcp unknown unknown
31337/tcp unknown Elite
32768/tcp unknown filenet-tms
32769/tcp unknown filenet-rpc
32770/tcp unknown sometimes-rpc3
32771/tcp unknown sometimes-rpc5
32772/tcp unknown sometimes-rpc7
32773/tcp unknown sometimes-rpc9
32774/tcp unknown sometimes-rpc11
32775/tcp unknown sometimes-rpc13
32776/tcp unknown sometimes-rpc15
32777/tcp unknown sometimes-rpc17
32778/tcp unknown sometimes-rpc19
32779/tcp unknown sometimes-rpc21
32780/tcp unknown sometimes-rpc23
32781/tcp unknown unknown
32782/tcp unknown unknown
32783/tcp unknown unknown
32784/tcp unknown unknown
32785/tcp unknown unknown
33354/tcp unknown unknown
33899/tcp unknown unknown
34571/tcp unknown unknown
34572/tcp unknown unknown
34573/tcp unknown unknown
35500/tcp unknown unknown
38292/tcp unknown landesk-cba
40193/tcp unknown unknown
40911/tcp unknown unknown
41511/tcp unknown unknown
42510/tcp unknown caerpc
44176/tcp unknown unknown
44442/tcp unknown coldfusion-auth
44443/tcp unknown coldfusion-auth
44501/tcp unknown unknown
45100/tcp unknown unknown
48080/tcp unknown unknown
49152/tcp unknown unknown
49153/tcp unknown unknown
49154/tcp unknown unknown
49155/tcp unknown unknown
49156/tcp unknown unknown
49157/tcp unknown unknown
49158/tcp unknown unknown
49159/tcp unknown unknown
49160/tcp unknown unknown
49161/tcp unknown unknown
49163/tcp unknown unknown
49165/tcp unknown unknown
49167/tcp unknown unknown

```
49175/tcp unknown unknown
49176/tcp unknown unknown
49400/tcp unknown compaqdiag
49999/tcp unknown unknown
50000/tcp unknown ibm-db2
50001/tcp unknown unknown
50002/tcp unknown iiimsf
50003/tcp unknown unknown
50006/tcp unknown unknown
50300/tcp unknown unknown
50389/tcp unknown unknown
50500/tcp unknown unknown
50636/tcp unknown unknown
50800/tcp unknown unknown
51103/tcp unknown unknown
51493/tcp unknown unknown
52673/tcp unknown unknown
52822/tcp unknown unknown
52848/tcp unknown unknown
52869/tcp unknown unknown
54045/tcp unknown unknown
54328/tcp unknown unknown
55055/tcp unknown unknown
55056/tcp unknown unknown
55555/tcp unknown unknown
55600/tcp unknown unknown
56737/tcp unknown unknown
56738/tcp unknown unknown
57294/tcp unknown unknown
57797/tcp unknown unknown
58080/tcp unknown unknown
60020/tcp unknown unknown
60443/tcp unknown unknown
61532/tcp unknown unknown
61900/tcp unknown unknown
62078/tcp unknown iphone-sync
63331/tcp unknown unknown
64623/tcp unknown unknown
64680/tcp unknown unknown
65000/tcp unknown unknown
65129/tcp unknown unknown
65389/tcp unknown unknown

NSE: Script Post-scanning.
Initiating NSE at 10:23
Completed NSE at 10:23, 0.00s elapsed
Initiating NSE at 10:23
Completed NSE at 10:23, 0.00s elapsed
Post-scan script results:
| clock-skew:
|   -1s:
|     10.1.34.127
|     10.1.34.101
|     10.1.34.248
|     10.1.34.89
|     10.1.34.77
|     10.1.34.99
|     10.1.34.20
|     10.1.34.102
|     10.1.34.73
|     10.1.34.128
|     10.1.34.195
|     10.1.34.247
|     10.1.34.75
|     10.1.34.126
|     10.1.34.18
|   2s:
|     10.1.34.225
|     10.1.34.111
|_    10.1.34.71
| ssh-hostkey: Possible duplicate hosts
| Key 2048 93:d1:fb:09:23:d6:f4:21:86:5b:88:3e:86:57:29:af (RSA) used by:
|   10.1.34.71
|   10.1.34.111
| Key 1024 7e:12:c0:39:3b:8a:81:b7:05:6a:16:8c:ba:b8:05:b3 (DSA) used by:
|   10.1.34.75
|   10.1.34.77
```

```
| Key 2048 ed:46:b7:1e:0a:6c:66:f6:c3:b6:a7:5c:5f:7a:55:1f (RSA) used by:
|   10.1.34.81
|   10.1.34.83
|   10.1.34.85
|   10.1.34.87
| Key 2048 b1:4d:6a:62:13:60:75:66:3d:00:db:26:42:5c:07:b5 (RSA) used by:
|   10.1.34.75
|   10.1.34.77
| Key 1024 7b:e4:55:06:31:19:71:e3:d5:99:0c:1e:eb:e9:df:95 (DSA) used by:
|   10.1.34.71
|   10.1.34.111
| Key 1024 96:54:ca:5a:e2:11:14:26:e1:08:2a:da:58:de:8f:cc (DSA) used by:
|   10.1.34.81
|   10.1.34.83
|   10.1.34.85
|_  10.1.34.87
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (45 hosts up) scanned in 981.50 seconds
        Raw packets sent: 49736 (2.232MB) | Rcvd: 43057 (1.771MB)
```

ANEXO 3 - EXEMPLO DE RELATÓRIO, CONTEÚDO DE *DATASET* (PARCIAL)

SEL_451MET/METMMXU1MXA1$phsA$cValmagf
SEL_451ANN/AMVGGIO6MXAnIn01
SEL_451PRO/BK1XCBR1STPos
SEL_451ANN/ASVGGIO4STInd001
SEL_451ANN/PSVGGIO1STInd01
SEL_451ANN/IN1GGIO14STInd01
SEL_451MET/METMMXU1MXTotW
SEL_451ANN/AMVGGIO6MXAnIn01
SEL_451PRO/BK1XCBR1STPos
SEL_451ANN/ASVGGIO4STInd001
SEL_451ANN/PSVGGIO1STInd01
SEL_451ANN/IN1GGIO14STInd01
SEL_451ANN/CCOUTGGIO21STInd01$stVal
SEL_451PRO/TRIPPTRC1STTr$general
SEL_451MET/METMMXU1MXPhV$phsA$instCValmagf
SEL_451ANN/AMVGGIO6MXAnIn02
SEL_451PRO/BK2XCBR2STPos
SEL_451ANN/ASVGGIO4STInd002
SEL_451ANN/PSVGGIO1STInd02
SEL_451ANN/IN1GGIO14STInd02
SEL_451MET/METMMXU1MXTotVAr
SEL_451ANN/AMVGGIO6MXAnIn02
SEL_451PRO/BK2XCBR2STPos
SEL_451ANN/ASVGGIO4STInd002
SEL_451ANN/PSVGGIO1STInd02
SEL_451ANN/IN1GGIO14STInd02
SEL_451ANN/CCOUTGGIO21STInd02$stVal
SEL_451PRO/BK1XCBR1STPos$stVal
SEL_451ANN/PLTGGIO2STInd03$stVal
SEL_451ANN/AMVGGIO6MXAnIn03
SEL_451PRO/BKR1CSWI1STPos
SEL_451ANN/ASVGGIO4STInd003
SEL_451ANN/PSVGGIO1STInd03
SEL_451ANN/IN1GGIO14STInd03
SEL_451MET/METMMXU1MXTotVA
SEL_451ANN/AMVGGIO6MXAnIn03
SEL_451PRO/BKR1CSWI1STPos
SEL_451ANN/ASVGGIO4STInd003
SEL_451ANN/PSVGGIO1STInd03
SEL_451ANN/IN1GGIO14STInd03
SEL_451ANN/CCOUTGGIO21STInd03$stVal
SEL_451PRO/BK2XCBR2STPos$stVal
SEL_451ANN/PLTGGIO2STInd01$stVal
SEL_451ANN/AMVGGIO6MXAnIn04
SEL_451PRO/BKR2CSWI2STPos
SEL_451ANN/ASVGGIO4STInd004
SEL_451ANN/PSVGGIO1STInd04
SEL_451ANN/IN1GGIO14STInd04
SEL_451MET/METMMXU1MXTotPF

ANEXO 4 - EXEMPLO DE RELATÓRIO, ARQUIVOS GERADOS PELO SISTEMA

192.168.1.10_ProtAnsiDisponiveis_08_11_2017_17_03_28.txt

192.168.1.10_dataset contents_08_11_2017_17_03_28.txt

192.168.1.10_DatasetAddress_08_11_2017_17_03_28.txt

192.168.1.10_LogicalDevices_08_11_2017_17_03_28.txt

192.168.1.10_LogicalNodes_08_11_2017_17_03_28.txt

ANEXO 5 - CÓDIGO DO NETSCANNER

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
from xml.dom.minidom import parse
import xml.dom.minidom
import sys
import os
import subprocess
from collections import Counter #para contar as ocorrencias de ieds por fabricante
import time
import matplotlib.pyplot as plt
from PyQt4 import QtGui, QtCore, QtXml

import NetScannerInterface
import ComparaRelatorio
import ComparaPastas

class ComparaPastas (QtGui.QDialog, ComparaPastas.Ui_Dialog_Pastas):
  def __init__(self, parent=None):
    super(ComparaPastas, self).__init__(parent)
    self.setupUi(self)
    self.pushButton_comparar_pastas.clicked.connect(self.comparar)

  def abre_pasta_01(self):
    pasta01 = unicode(QtGui.QFileDialog.getExistingDirectory(self, 'Abrir Pasta 01',
      'C:\\NetScanner'))
    nome_pasta01 = unicode(pasta01)
    self.label_relatorio_01.setText((nome_pasta01))
    return pasta01

  def abre_pasta_02(self):
    pasta02 = unicode(QtGui.QFileDialog.getExistingDirectory(self, 'Abrir Pasta 02',
```

```
        'C:\\ NetScanner'))
    nome_pasta02 = unicode(pasta02)
    self.label_relatorio_02.setText((nome_pasta02))
    return pasta02

  def comparar(self):
    nomepasta1 = self.abre_pasta_01()
    nomepasta2 = self.abre_pasta_02()
    arqs1 = os.listdir(nomepasta1)
    arqs2 = os.listdir(nomepasta2)

    de1pra2 = list(set(arqs1) - set(arqs2))
    de2pra1 = list(set(arqs2) - set(arqs1))
    self.textEdit_pasta01.clear()
    self.textEdit_pasta02.clear()
    if (len(de2pra1) == 0) and (len(de1pra2) == 0):
      self.textEdit_pasta01.append("Os arquivos são os mesmos")
      self.textEdit_pasta02.append("Os arquivos são os mesmos")

    for linha in de1pra2:
      self.textEdit_pasta01.append(linha)

    for linha in de2pra1:
      self.textEdit_pasta02.append(linha)


class ComparaRelatorio (QtGui.QDialog, ComparaRelatorio.Ui_DialogCompara):
  def __init__(self, parent=None):
    super(ComparaRelatorio, self).__init__(parent)
    self.setupUi(self)
    self.pushButton_comparar.clicked.connect(self.comparar)

  def abre_arq_01(self):
    relatorio01 = unicode(QtGui.QFileDialog.getOpenFileName(self, 'Abrir Relatorio 01',
```

```
        'C:\\Users \\NetScanner', "Todos os Arquivos (*.*)"))
    nome_relatorio01 = unicode(relatorio01)
    self.label_relatorio_01.setText(os.path.basename(nome_relatorio01))
    return relatorio01

def abre_arq_02(self):
    relatorio02 = unicode(QtGui.QFileDialog.getOpenFileName(self, 'Abrir Relatorio 02',
        'C:\\ NetScanner', "Todos os Arquivos (*.*)"))
    nome_relatorio02 = unicode(relatorio02)
    self.label_relatorio_02.setText(os.path.basename(nome_relatorio02))
    return relatorio02

def comparar(self):
    nomearq1 = self.abre_arq_01()
    nomearq2 = self.abre_arq_02()
    arq1 = open(nomearq1)
    arq2 = open(nomearq2)
    relatorio_1 = arq1.readlines()
    relatorio_2 = arq2.readlines()
    #relatorio_1 = ["oi", "tem","ip"]
    #relatorio_2 = ["oi", "nao tem","ip"]

    de1pra2 = list(set(relatorio_1) - set(relatorio_2))
    de2pra1 = list(set(relatorio_2) - set(relatorio_1))
    self.textEdit_arq01.clear()
    self.textEdit_arq02.clear()
    if (len(de2pra1) == 0) and (len(de1pra2) == 0):
        self.textEdit_arq01.append("Os relatorios sao identicos")
        self.textEdit_arq02.append("Os relatorios sao identicos")

    for linha in de1pra2:
        self.textEdit_arq01.append(linha)

    for linha in de2pra1:
```

```
        self.textEdit_arq02.append(linha)


#

# for i in range(limite):
#       if relatorio_1[i] == relatorio_2[i]:



class Aplicacao(QtGui.QMainWindow, NetScannerInterface.Ui_MainWindow):
  def __init__(self, parent=None):
    super(Aplicacao,self).__init__(parent)
    self.setupUi(self)
    self.formCompara=ComparaRelatorio(self) #instancia da classe
    self.formComparaPasta = ComparaPastas(self)
    self.pushButton_ok.clicked.connect(self.chamaNmap)
    self.pushButton_comparar.clicked.connect(self.chamaComparar)
    self.pushButton_comparar_pastas.clicked.connect(self.chamaCompararPastas)
    self.pushButton_testa_61850.clicked.connect(self.testa61850)

    os.popen("netsh interface ipv4 show address > interfaces.txt")
    arq = open("interfaces.txt","r")
    interfaces = arq.read()
    arq.close()
    listaInterfaces= interfaces.split("Configuration for interface ")
    listaInterfaces.pop(0)
    interfacesValendo = []
    for i in range (len(listaInterfaces)):
      try:
        nome = listaInterfaces[i].split("\n")[0].strip("\"")
      except:
        nome = ""
      try:
```

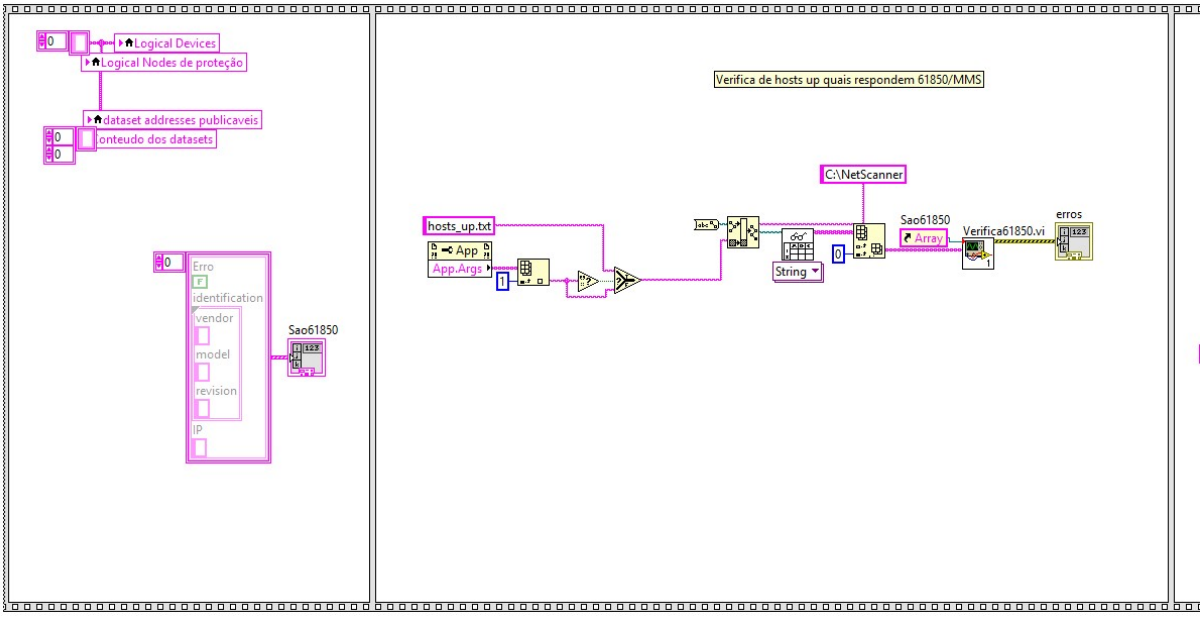
```
            endereco = listaInterfaces[i].split("\n")[2].split(":")[1].strip(" ")
          except:
            endereco = ""
          try:
            mascara =
listaInterfaces[i].split("\n")[3].split(":")[1].split("/")[1].split("(")[0].strip(" ")
          except:
            mascara = ""

          if (nome != "") and (endereco != "") and (mascara != ""):
            #listaInterfaces[i] = nome+", "+endereco+", /"+mascara
            interfacesValendo.append(nome+", "+endereco+" /"+mascara)

        self.comboBox_interfaces.addItems(interfacesValendo)



    def lista_hosts_down(self, lista):
        arqLog=lista.split("host down")
        for i in range(len(arqLog)-1):
            arqLog[i] = arqLog[i].split("Nmap scan report for ")[1]
            arqLog[i] = arqLog[i].split(" [")[0]
        arqLog[-1] = arqLog[-1].split("]")[0]
        arqLog.pop(-1)
        return arqLog

    def lista_hosts_up(self, lista):
        arqLog = lista.split("Completed SYN Stealth Scan against ")
        for i in range(len(arqLog)):
            arqLog[i] = arqLog[i].split(" in")[0]
        arqLog.pop(0)
        return arqLog

    def lista_relatorio(self, lista):
        arqLog = lista.split("Nmap scan report for ")
```

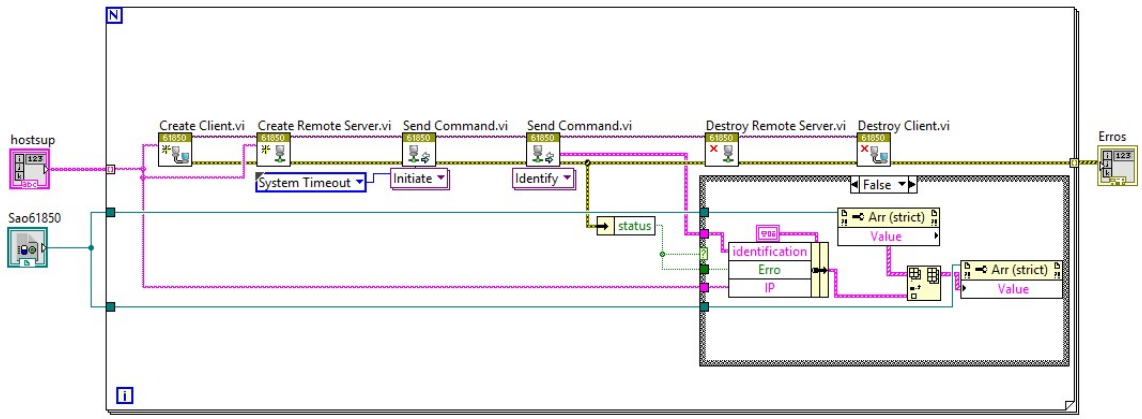
```
    arqLog.pop(0)
    arqLog[-1] = arqLog[-1].split("NSE: Script Post-scanning.")[0] #texto se utilizar -sN no comando nmap = "Initiating ARP Ping Scan at "
    return arqLog

  def analise_resultados(self, lista):
    relatorio = []
    for elemento in lista:
      if (elemento.find("host down")) == -1:
        relatorio.append("_____")
        relatorio.append(elemento.split("\n")[0])
        try:
          mac = elemento.split("MAC Address: ")[1]
        except:
          mac = "\n"
        mac = mac.split("\n")[0]
        relatorio.append(mac)
        try:
          osdetails = elemento.split("OS details: ")[1]
        except:
          osdetails = "\n"
        osdetails = osdetails.split("\n")[0]
        if (osdetails.find("Windows")) != -1:
          osdetails = "Windows"
        relatorio.append(osdetails)

    return relatorio

  def chamaComparar(self):
    self.formCompara.show()

  def chamaCompararPastas(self):
    self.formComparaPasta.show()
```

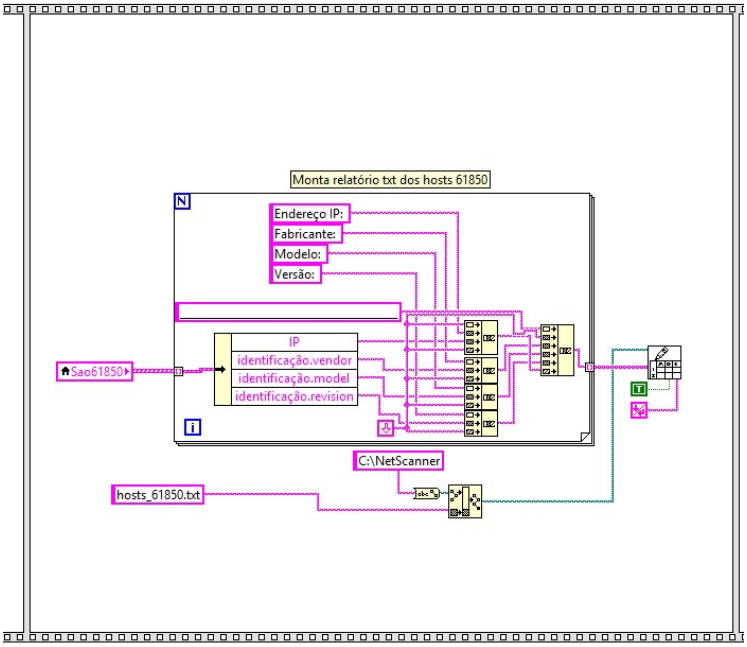
```
def chamaNmap(self):
  endereco = str(self.comboBox_interfaces.currentText()).split(",")[1].replace(" ","")
  QtGui.QApplication.setOverrideCursor(QtGui.QCursor(QtCore.Qt.WaitCursor))
  self.statusbar.showMessage("Buscando na rede. Aguarde...",0)
  os.popen("nmap -T4 -A -v " + endereco + " > resultadoNmapTeste.txt")
  self.statusbar.showMessage("OK", 0)
  arq = open("resultadoNmapTeste.txt", "r")
  arqLog = arq.read()
  arq.close()
  QtGui.QApplication.restoreOverrideCursor()
  self.statusbar.clearMessage()
  hosts_down = self.lista_hosts_down(arqLog)
  hosts_up = self.lista_hosts_up(arqLog)

  self.textEdit_relatorio.clear()
  arq = open("hosts_up.txt","w")
  for linha in hosts_up:
    arq.write(linha+"\n")
  arq.close()

  resultados = self.lista_relatorio(arqLog)

  relatorio = self.analise_resultados(resultados)
  for linha in relatorio:
    self.textEdit_relatorio.append(linha.strip())
  self.textEdit_relatorio.verticalScrollBar().setValue(0)

  self.testa61850()

def testa61850(self):
  QtGui.QApplication.setOverrideCursor(QtGui.QCursor(QtCore.Qt.WaitCursor))
  self.statusbar.showMessage("Buscando hosts 61850. Aguarde...",0)
  linha_executavel = "\"C:\LabVIEW 2013\LabVIEW.exe\" "
  linha_vi = "\"C:\\Main.vi\" "
```

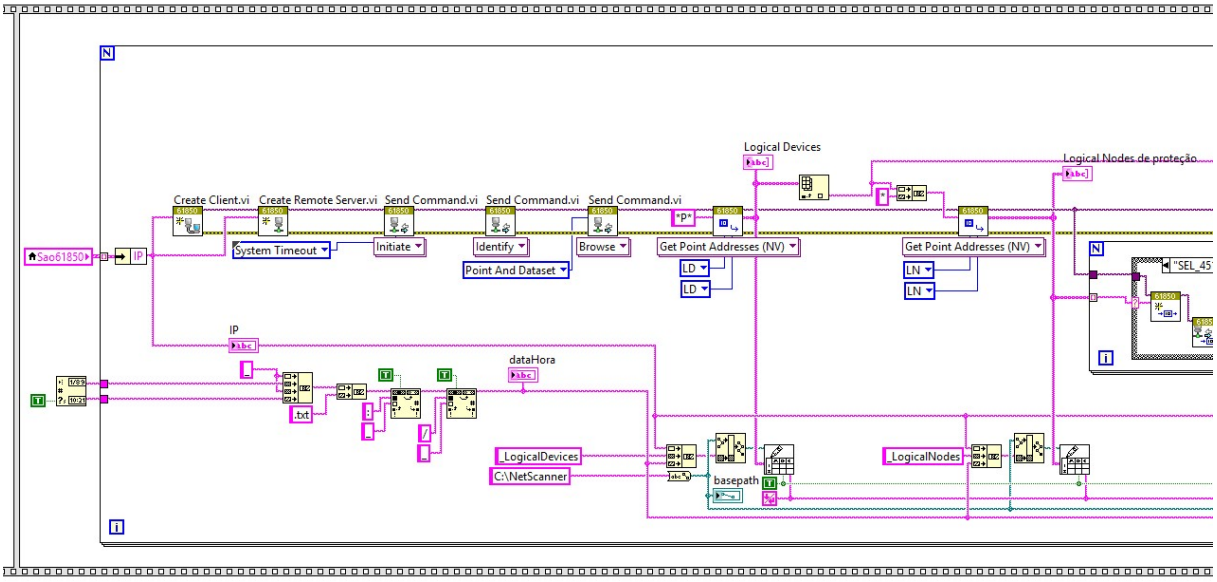
```
        linha_parametro = "-- hosts_up.txt"
        LV = subprocess.Popen(linha_executavel + linha_vi + linha_parametro)
        LV.wait()

        arq = open("hosts_61850.txt")
        hosts_61850 = arq.readlines(0)
        self.textEdit_61850.clear()
        for linha in hosts_61850:
          self.textEdit_61850.append(linha)

        self.textEdit_61850.verticalScrollBar().setValue(0)
        QtGui.QApplication.restoreOverrideCursor()
        self.statusbar.clearMessage()


def main():
  app=QtGui.QApplication(sys.argv)
  form=Aplicacao()
  form.show()
  app.exec_()
  return 0

if __name__ == '__main__':
  main()
```

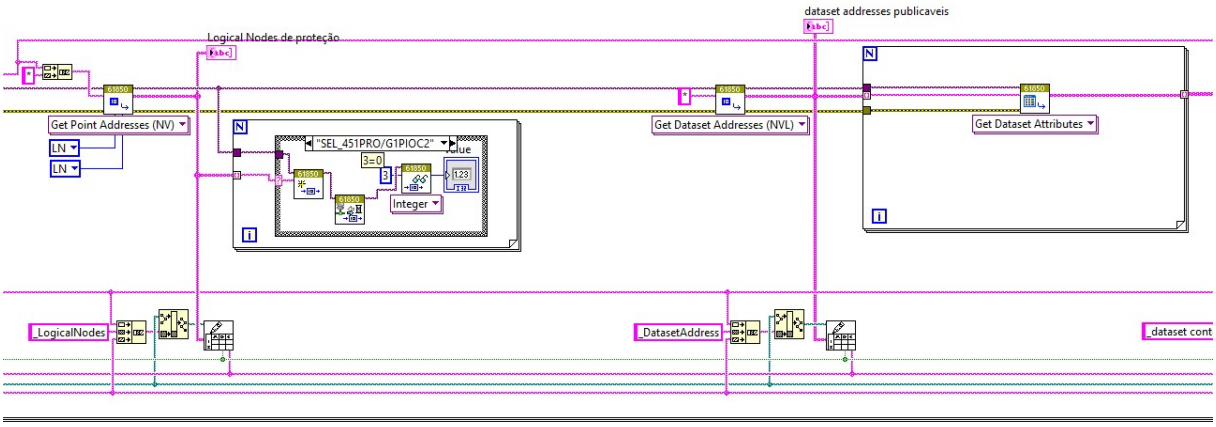
ANEXO 6 - CÓDIGO DO GET61850NODES

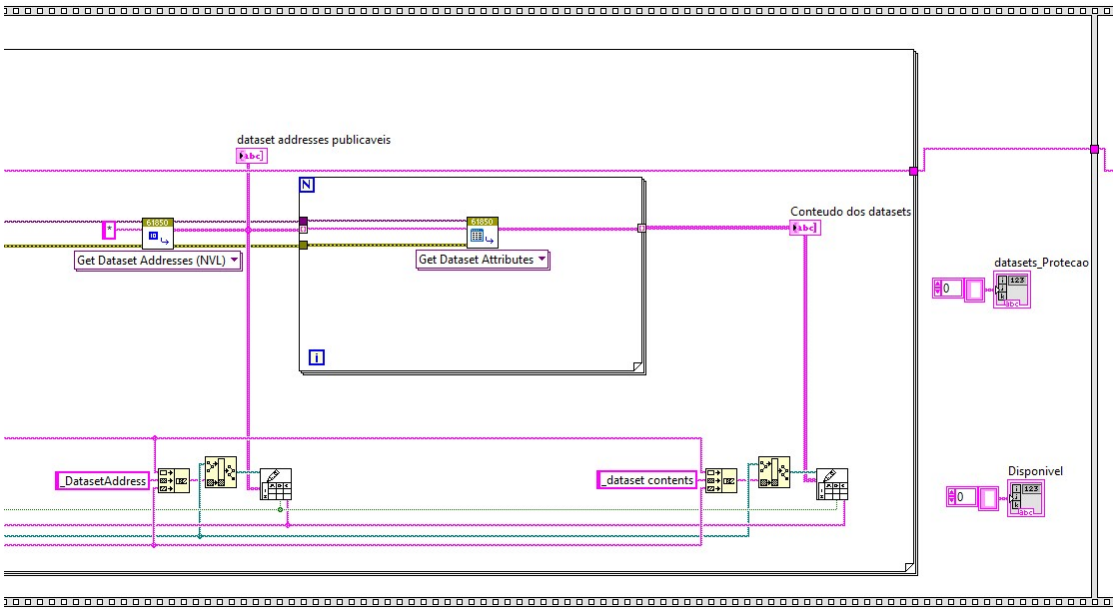


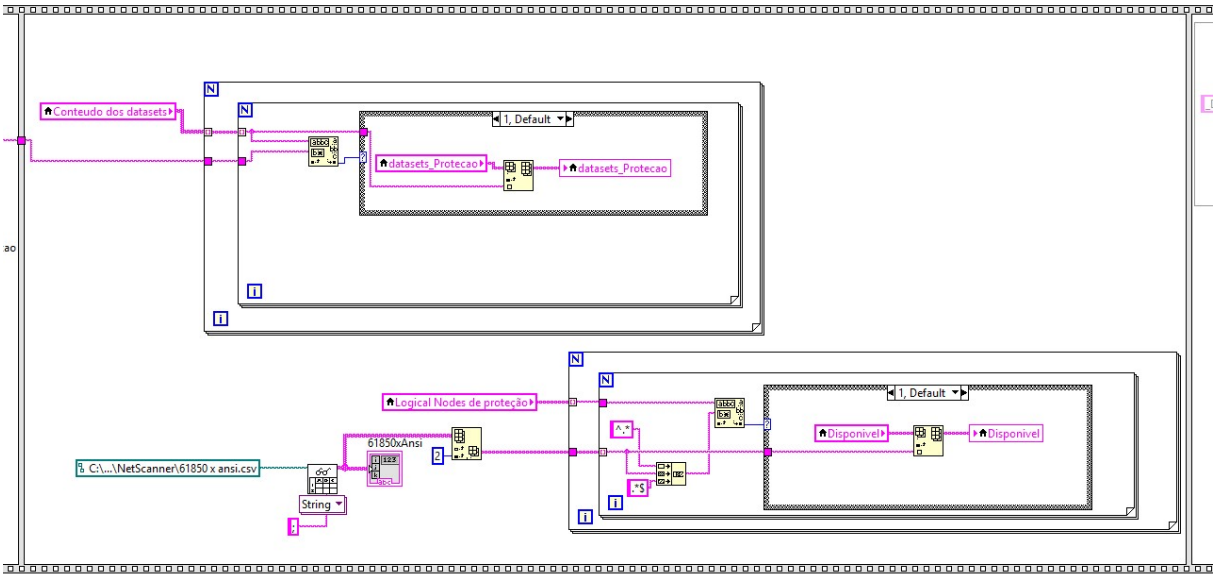


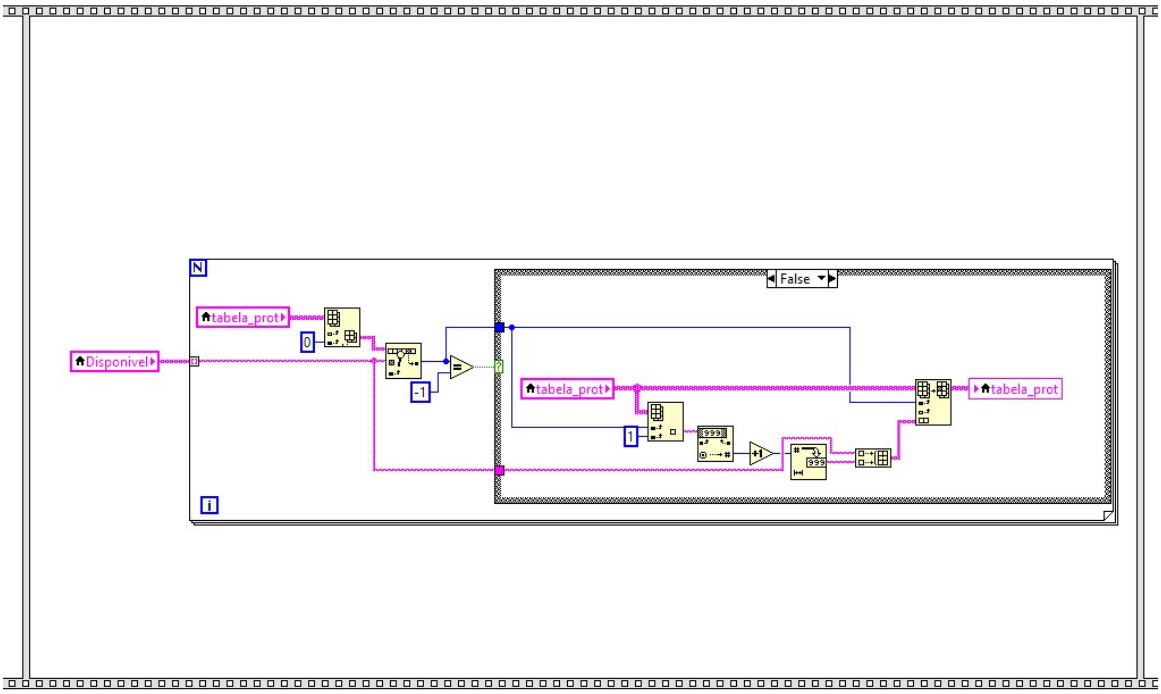

Monta relatório txt dos hosts 61850
Endereço IP:
Fabricante:
Modelo:
Versão:
IP
identificação.vendor
identificação.model
identificação.revision
Sao61850
C:\NetScanner
hosts_61850.txt

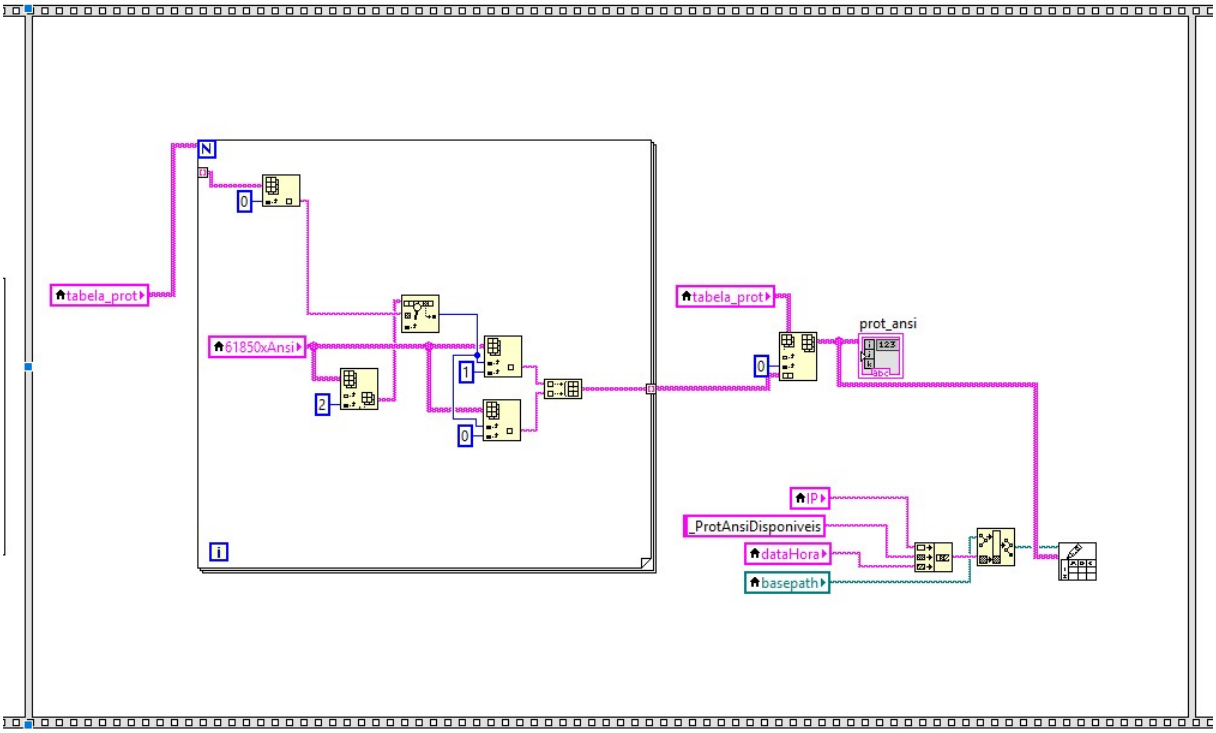

Logical Devices
Logical Nodes de proteção
Create Client.vi
Create Remote Server.vi
Send Command.vi
Send Command.vi
Send Command.vi
Sao61850
IP
System Timeout
Initiate
Identify
Point And Dataset
Browse
"P*"
Get Point Addresses (NV)
LD
LD
Get Point Addresses (NV)
LN
LN
IP
.txt
dataHora
_LogicalDevices
C:\NetScanner
basepath
_LogicalNodes

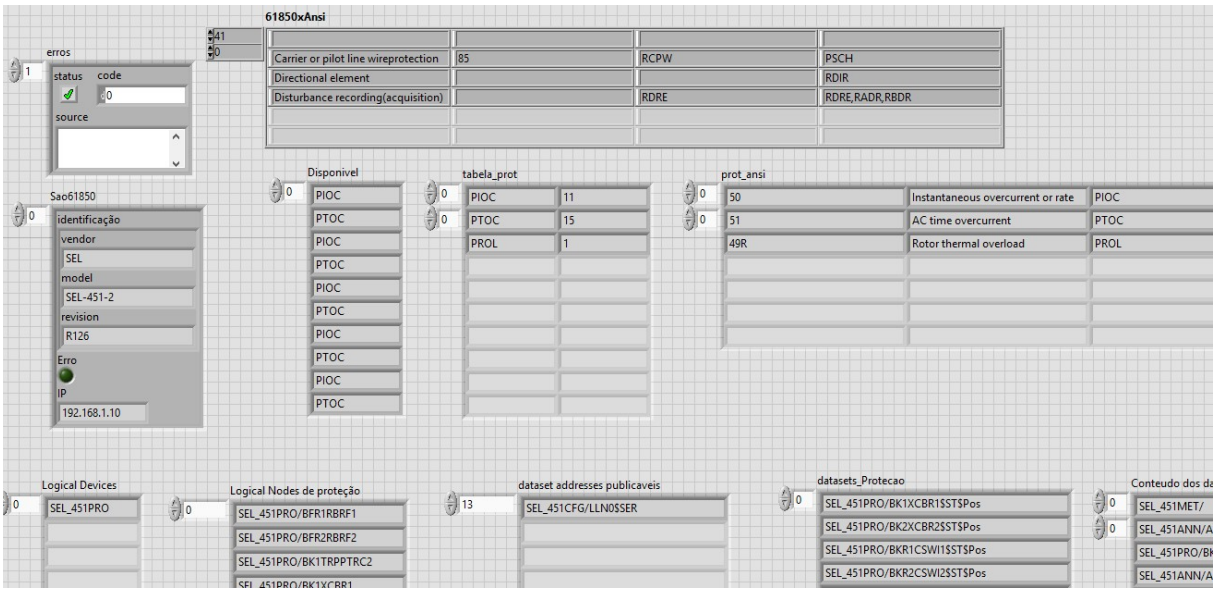

dataset addresses publicaveis
Logical Nodes de proteção
Get Point Addresses (NV)
LN
LN
"SEL_451PRO/G1PIOC2"
Integer
Get Dataset Addresses (NVL)
Get Dataset Attributes
_LogicalNodes
_DatasetAddress
_dataset cont


dataset addresses publicaveis
Get Dataset Addresses (NVL)
Get Dataset Attributes
Conteudo dos datasets
datasets_Protecao
_DatasetAddress
_dataset contents
Disponivel


Conteudo dos datasets
1, Default
datasets_Protecao
datasets_Protecao
Logical Nodes de proteção
61850xAnsi
C:\...\NetScanner\61850 x ansi.csv
String
1, Default
Disponivel
Disponivel
^.*
.*$


Disponivel
tabela_prot
0
-1
False
tabela_prot
1
tabela_prot


tabela_prot
61850xAnsi
tabela_prot
prot_ansi
IP
_ProtAnsiDisponiveis
dataHora
basepath


61850xAnsi
erros
status
code
source
Carrier or pilot line wireprotection
85
RCPW
PSCH
Directional element
RDIR
Disturbance recording(acquisition)
RDRE
RDRE,RADR,RBDR
Sao61850
identificação
vendor
SEL
model
SEL-451-2
revision
R126
Erro
IP
192.168.1.10
Disponivel
PIOC
PTOC
tabela_prot
11
15
1
prot_ansi
50
Instantaneous overcurrent or rate
51
AC time overcurrent
49R
Rotor thermal overload
Logical Devices
SEL_451PRO
Logical Nodes de proteção
SEL_451PRO/BFR1RBRF1
SEL_451PRO/BFR2RBRF2
SEL_451PRO/BK1TRPPTRC2
dataset addresses publicaveis
SEL_451CFG/LLN0$SER
datasets_Protecao
SEL_451PRO/BK1XCBR1STPos
SEL_451PRO/BK2XCBR2STPos
SEL_451PRO/BKR1CSWI1STPos
SEL_451PRO/BKR2CSWI2STPos
SEL_451MET/
SEL_451ANN/