Questões Relacionadas com Aplicação de Rede Ethernet em Subestações

Darold Woodward
Schweitzer Engineering Laboratories, Inc.

Apresentado na
3rd Annual Western Power Delivery Automation Conference
Spokane, Washington
10–12 de abril de 2001

Traduzido para o português em julho de 2017

QUESTÕES RELACIONADAS COM APLICAÇÃO DE REDE ETHERNET EM SUBESTAÇÕES

Darold Woodward, PE
Schweitzer Engineering Laboratories
Pullman, WA USA

Este artigo fornece uma introdução à utilização de rede Ethernet nas subestações de energia elétrica. Além dos termos e conceitos básicos das redes Ethernet, ele trata de assuntos específicos relativos às redes Ethernet em subestações.

ETHERNET

Robert Metcalf e vários outros parceiros de pesquisa inventaram a Rede Ethernet no Centro de Pesquisas da Xerox, em Palo Alto (Xerox PARC) [1]. Em 1972, eles construíram a Alto Aloha network, conectando diversos computadores Xerox Alto. Metcalf, David Boggs, Charles Thacker e Butler Lampson protocolaram um pedido de patente para rede Ethernet em 1975. O desenho mostrado na Figura 1 é similar ao que Metcalf usou em uma apresentação explicando o conceito da rede Ethernet.

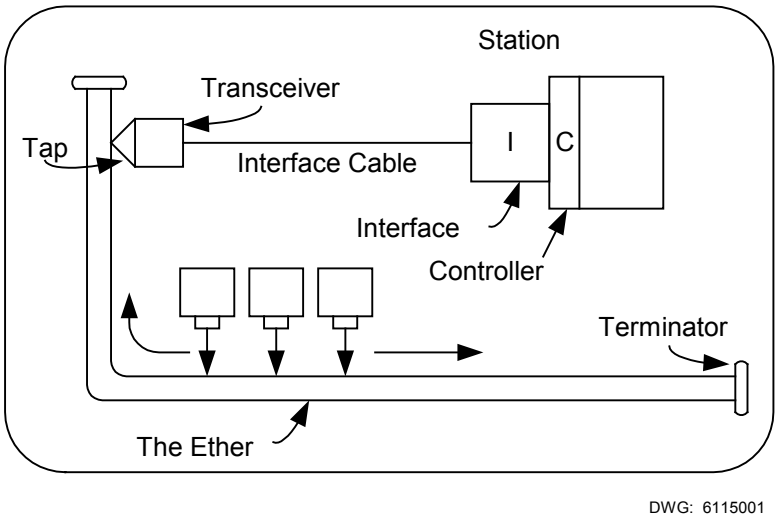

Figura 1 Ilustração de Rede Ethernet

Similar ao éter luminoso usado pelos antigos pesquisadores para explicar como a luz e outras ondas magnéticas viajam através do vácuo, a rede atua como o éter permitindo a transmissão de mensagens entre computadores.

Atualmente, a Ethernet é a tecnologia de rede dominante utilizada em escritórios e residências. Tendo em vista que as redes Ethernet são baratas e razoavelmente bem compreendidas, a sua utilização está rapidamente se popularizando para aplicações industriais e em concessionárias, incluindo redes de automação de subestações.

As redes Ethernet não foram desenvolvidas especificamente para operação em subestações e outros ambientes desfavoráveis. Por quê há tanto interesse na aplicação de redes Ethernet nesses locais? A resposta é similar à pergunta de por quê os computadores pessoais são agora utilizados em muitas aplicações de sistemas industriais e de potência. A Ethernet é tão popular em outras aplicações que é mais simples empregar e reforçar a Ethernet, do que de criar alguma coisa nova.

Há apenas 15 anos atrás, a maioria das Interfaces Homem-Máquina (IHMs) operavam em computadores mainframe dedicados com terminais, ao invés da legião de computadores pessoais que é utilizada atualmente. As antigas IHMs de computadores pessoais utilizavam sistemas de operação customizados dedicados à operação da IHM. Embora os sistemas dedicados sejam mais estáveis e confiáveis, os sistemas atuais freqüentemente custam de 1 a 10 por cento do valor dos sistemas dedicados de finalidade única.

Os especialistas em redes tanto industriais como para concessionárias estão caminhando no sentido de conviver com as limitações das redes Ethernet e resolver os problemas associados às redes Ethernet. Avanços na tecnologia de computação e de redes nos permitem tirar partido da popularidade e disponibilidade dos equipamentos e soluções de redes Ethernet.

Há dois excelentes recursos na Internet [1], [2] onde você pode receber uma introdução sobre as redes Ethernet.

MODELO OSI DE SETE CAMADAS

Nenhuma discussão da tecnologia de redes seria completa sem uma introdução ao modelo de sete camadas Open Systems Interconnect (OSI) da International Standards Organization (ISO). O modelo representa a ligação em rede (tanto software como hardware), em um nó de rede individual, dividindo as tarefas em camadas que executam funções específicas. O modelo OSI proporciona uma boa maneira de se organizar a discussão sobre a Rede Ethernet. O modelo OSI para operação da rede em dois nós de rede é mostrado na Figura 2.

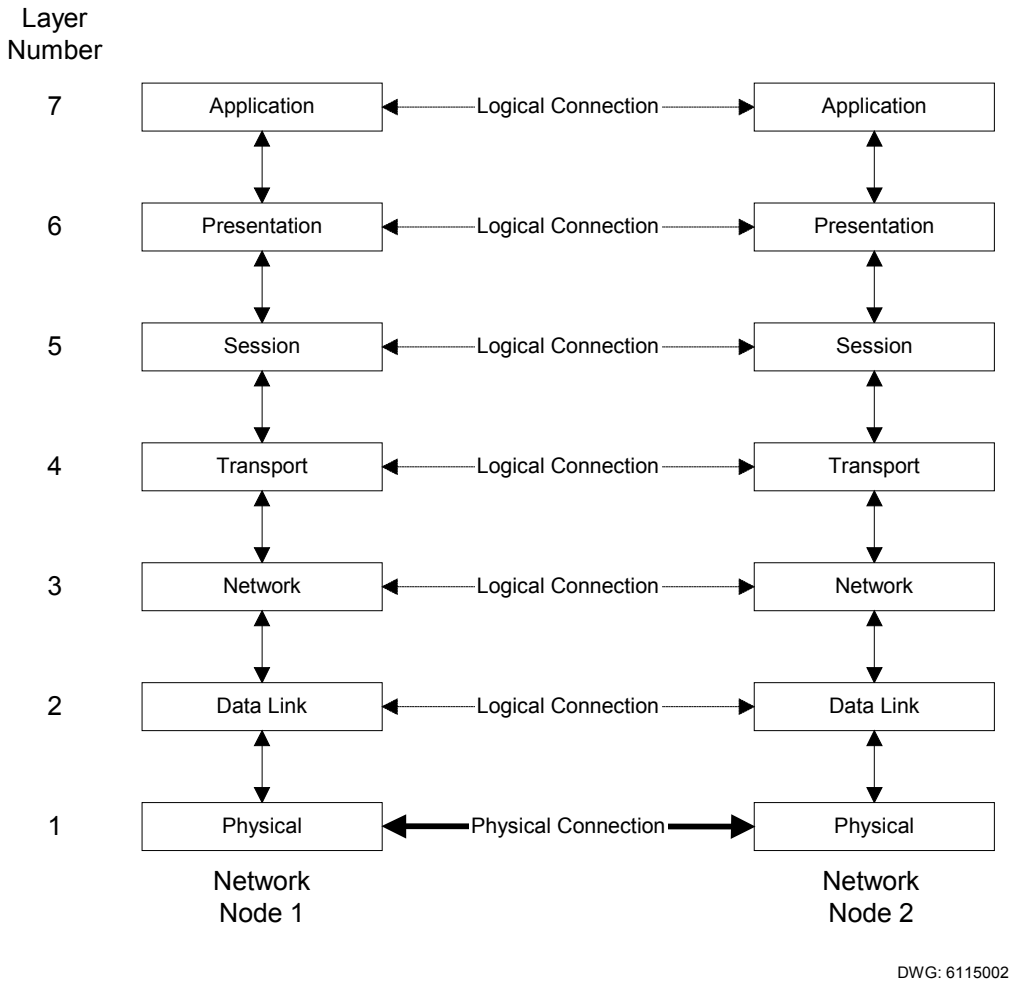

Figura 2 O Modelo OSI de Sete Camadas

No modelo OSI, cada camada (por exemplo, a camada de enlace de dados) comunica via uma comunicação lógica com a mesma camada no outro dispositivo. A operação em rede é mais complexa. Dados de aplicação, tais como os caracteres em uma sessão no terminal Telnet ou dados de modelo UCA2 GOMSFE, passam para baixo através das camadas e depois atravessam o meio físico. Cada camada adiciona alguma informação à mensagem e a remete à camada seguinte

Finalmente, a mensagem chega à camada mais inferior (física), e é enviada através da conexão física para o segundo nó da rede. Aqui, o processo opera no sentido inverso. Cada camada remove e usa informação específica da camada, passando o restante da informação pela cadeia acima, até que o dado original se torne disponível para o usuário da aplicação.

Enquanto houver uma interface definida entre as camadas, uma camada pode ser substituída por outra que atenda à especificação da interface. Por exemplo, as redes Ethernet podem operar através de muitos meios diferentes, desde cabos de condutores, a cabos de fibra ótica e conexões via rádio. A camada física pode ser substituída desde que a interface permaneça inalterada.

Inicialmente codificado no padrão Dec-Intel-Xerox (DIX), os padrões de rede Ethernet são agora definidos pela norma 802/3 do Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE). As redes Ethernet são definidas pelas duas camadas mais inferiores do modelo OSI, física e enlace de dados. A Ethernet por si mesma não é capaz de mover dados entre os dispositivos sem as camadas superiores.

CAMADAS FÍSICA E DE ENLACE DE DADOS DA ETHERNET

Cada camada física standard e a correspondente camada de enlace de dados possuem um designador (por exemplo, 10BASE-T), que identifica as especificações da camada. As combinações mais populares de camada física e de enlace de dados para Redes de Área Local (LANs) dentro de um único prédio são a fibra ótica (10BASE-FL e 100BASE-FX) e par trançado metálico (10BASE-T e 100BASE-TX). Para redes de uso geral, 10 Mbps e 100 Mbps são as velocidades de transmissão de dados mais populares.

Na medida que aumentaram as demandas sobre as redes, as redes de 100 Mbps se tornaram mais populares. O carregamento efetivo da rede para uma determinada carga oferecida é cerca de 10 vezes mais baixa nas redes de 100 Mbps do que nas redes de 10 Mbps, reduzindo as colisões e a latência da rede.

Cabo Coaxial

A rede Ethernet original desenvolvida no Xerox PARC foi uma rede de 2.94 Mbps, que utilizava pesado cabo coaxial (coax), comumente chamado de Thicknet. O desenvolvimento posterior de uma fiação coaxial mais leve e menos onerosa foi chamado de Thinnet. As redes Coax são as verdadeiras redes multiponto. O cabo tronco principal conecta cada nó com o seguinte. Um dispositivo de derivação em cada nó proporciona um local para o nó acessar o cabo tronco. Embora as redes multiponto sejam simples de imaginar, elas apresentam duas desvantagens principais.

Primeiro, os sistemas de cabos multiponto podem falhar se uma única seção do cabo for danificada ou cortada. Segundo, é difícil e caro acrescentar novos nós. A extensão da derivação, por exemplo, é limitada. Se você desejar acrescentar um novo nó a 30 metros de distância do cabo tronco existente, você talvez terá de colocar 30 m de cabo tronco indo para o novo nó e mais 30 m de cabo tronco voltando para o cabo tronco existente. A configuração resultante é mostrada na Figura 3.

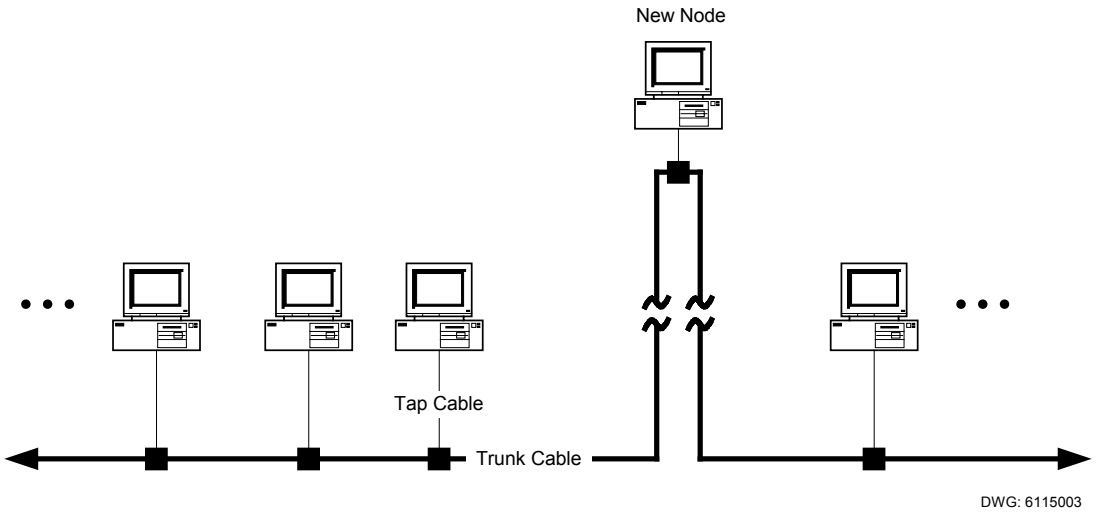

Figura 3 Adicionando um nó a uma Rede Multiponto

Cabo coaxial é caro e não está disponível, a não ser que você o acrescente ao prédio (um esforço que produz desarrumação e despesas), ou seja, instalado já durante a construção. Conforme mencionado acima, a adição de um nó a uma rede coaxial multiponto já existente é onerosa se você se esquecer de um nó e tiver de instalar mais tarde.

Cabo de Par Trançado

Os telefones e a fiação de telefones eram coisas comuns antes da utilização indiscriminada de computadores. A fiação de telefone utiliza cabos de par trançado de baixo preço, que são conectados em uma configuração de rede em estrela. Cada nó é conectado via cabo a uma localização central. Esta configuração é barata e simples de expandir. Uma segunda geração de normas Ethernet utiliza fiação de par trançado, incluindo a fiação existente em alguns locais.

As redes Ethernet de par trançado utilizam uma topologia de rede em estrela. Uma topologia de rede em estrela requer um nó central para conectar os segmentos de redes individuais. Este nó central (hub) atua como uma seção de cabo tronco, com muitas linhas em um local. O hub, ou núcleo, conecta os nós das extremidades dos cabos internos, para formar uma rede única. Os aperfeiçoamentos do hub incluem chaves e roteadores reforçam o desempenho da rede.

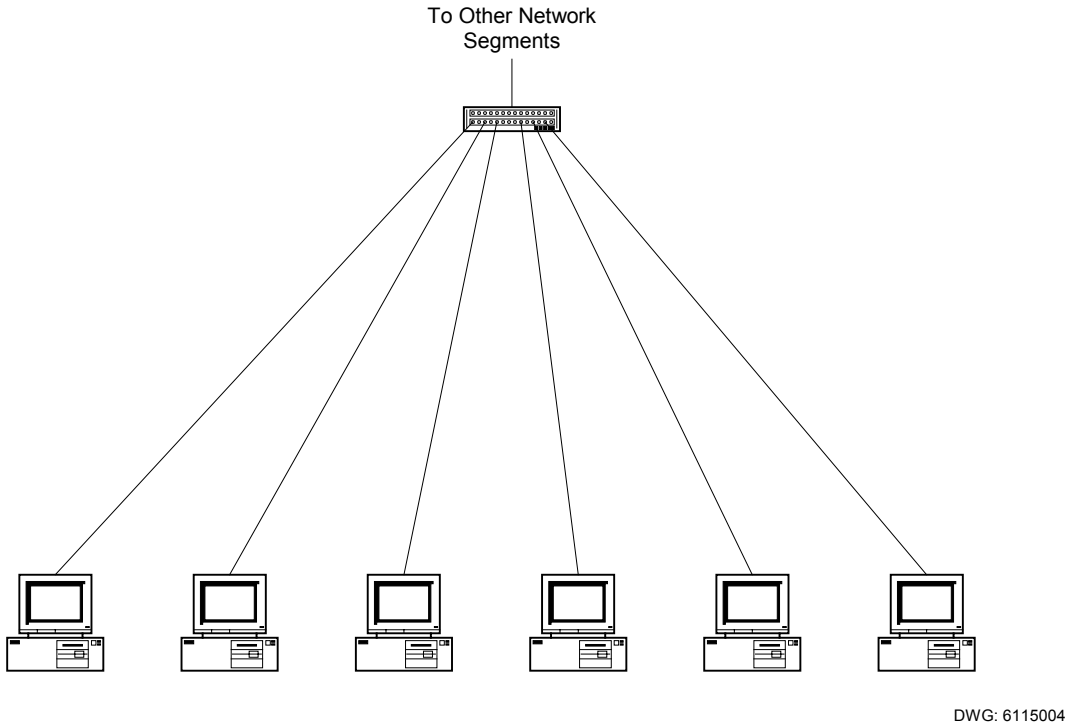

Figura 4 Topologia da Rede Ethernet Estrela

As normas de redes de par trançado permitem a fiação com par trançado não blindado (UTP), similar à exigida para telefones. Você pode pré-cabear os locais utilizando cabos múltiplos do mesmo tipo para cada local previsto de nó. Os cabos podem então ser utilizados para operação de telefones ou rede, conforme exigido, aumentando a flexibilidade e diminuindo o custo das redes de par trançado.

Duas normas para redes Ethernet sobre cabos de par trançado dominam a cena das redes atualmente. A primeira, 10BASE-T, é um padrão de 10 Mbps que pode operar através de muitos tipos de fiações telefônicas existentes, A segunda, 100BASE-X (também comumente chamada de 100BASE-T), é um padrão de 100 Mbps que requer um sistema de fiação de par trançado de qualidade mais alta. No entanto, os sistemas de telefones digitais também requerem uma fiação de par trançado de qualidade mais alta chamada Categoria 5. Agora é comum instalar os mesmos cabos tanto para redes telefônicas, como para redes Ethernet.

Os cabos são classificados em divisões utilizando um sistema de “categorias”. As categorias são classificadas pelas suas características de perda e outros fatores nas freqüências capazes de serem exigidas pelas redes digitais de alta velocidade. Categoria 3 é a categoria mais baixa que suporta 10BASE-T. Categoria 5 é exigida para as velocidades de dados de 100 Mbps e é também aceitável para as redes telefônicas digitais típicas. Os padrões para Categoria 6 e acima encontram-se sob desenvolvimento e se destinam a suportar futuras aplicações de redes a velocidades de 1 Gbps ou mais.

Infelizmente, embora os cabos UTP sejam baratos e simples de aplicar em um ambiente de escritório, os mesmos podem se constituir num problema em outros ambientes. Por exemplo, os escritórios tipicamente não contém fortes fontes de interferência de rádio freqüência (RFI), por causa da blindagem proporcionada pelos prédios de escritórios e a falta de fortes fontes de RFI dentro do prédio.

No entanto, as instalações das concessionárias e as instalações industriais, muitas vezes contém fortes fontes internas (rádios portáteis, drives de freqüência variável, máquinas de solda, etc.), e podem não estar bem blindadas em relação a fontes externas, incluindo torres de

rádio transmissores. As subestações também incluem fiação de controle que tipicamente não é blindada e pode induzir tensões elétricas na fiação adjacente.

Pode-se minimizar muitos dos problemas associados aos cabos UTP, encerrando-os dentro de um conduite ou outros dutos ferrosos totalmente fechados. Os conduites, no entanto, alteram as características de impedância dos cabos, aumentando o retardo e a perda do sinal [3]. Outra estratégia, algumas vezes empregadas nas instalações industriais, é utilizar cabos de par trançado blindados (STP).

Os cabos STP incluem uma blindagem geral que reduz RFI e ajuda a proteger o equipamento conectado ao cabo de descargas eletrostáticas (ESD). Embora a cablagem STP da rede Ethernet seja considerada rara em geral, ela é relativamente comum nos ambientes industriais e em outros de ruído elevado, onde cabos UTP não são aceitáveis.

Nunca deve-se passar qualquer cabo de comunicações metálico entre a sala de controle da subestação e os equipamentos no pátio da subestação. As diferenças de potencial de terra na subestação, experimentadas durante uma falta, podem submeter o seu equipamento a perigosas tensões e correntes, especialmente em cabos com blindagens que são aterradas em ambas as extremidades.

Em uma sala de controle de subestação, muitos desses riscos são reduzidos, porém o ruído proveniente dos circuitos de controle e instrumentação, e dos disjuntores dentro de conjuntos de manobra blindados, pode perturbar as redes. Mesmo com a blindagem e a separação física dos outros cabos e da fiação, cabos metálicos com blindagens fornecem trajetos para que a corrente circule a partir das diferenças de potencial de terra, falhas de CC e outras eletricidades parasitas. A única proteção certa em relação a esses problemas é um sistema de cabo que não seja afetado pela interferência elétrica e eletromagnética.

Cabo de Fibra Ótica

Os sistemas de cabos de fibra ótica proporcionam dois benefícios principais. Primeiro, os sinais dentro dos cabos de fibra ótica ficam imunes à interferência de RFI e eletrostática capaz de perturbar a comunicação nos cabos metálicos. Segundo, os cabos de fibra ótica podem apresentar uma construção totalmente dielétrica (não condutora). Isso significa que você pode passar cabos de fibra ótica fora da casa de controle para proporcionar uma comunicação robusta e confiável, sem ameaça de danificar equipamentos críticos nas extremidades do circuito de comunicação.

Onde a fiação de par trançado utiliza dois pares, um para transmitir e um para receber, os sistemas de cabos de fibra ótica utilizam um par de fibras, sendo um para transmitir e um para receber. Os sistemas de cabo de fibra ótica também requerem um nó central ou hub, que combina os segmentos de cabos de fibra ótica ponto a ponto para formar uma rede lógica. Os padrões das redes Ethernet de fibra ótica mais populares são 10BASE-FL e 100BASE-FX, 10 Mbps e 100 Mbps, respectivamente.

Os cabos de fibra ótica são mais caros do que cabos metálicos. No entanto, as medidas de blindagem para cabos de par trançado e a mão de obra de instalação constituem custos significativos de construção. Deve-se considerar o custo instalado da rede para se poder avaliar corretamente o impacto da sua opção de meio físico para rede.

Hubs, adaptadores de rede e outros equipamentos para redes de fibra ótica são mais caros do que os equipamentos utilizados para redes de par trançado. Nas aplicações onde alta confiabilidade é exigida e a proteção dos equipamentos críticos para a missão é essencial, os sistemas de cabo de fibra ótica freqüentemente compensam a despesa adicional.

Comparação de Custo dos Componentes de Sistemas de Cabos

Tabela 1 compara o custo de cabos de fibra ótica e acessórios que seriam necessários em uma rede Ethernet de uma subestação típica.

Tabela 1 Comparação de Custos de Componentes de Rede de Par trançado e Fibra Ótica

Componente	Par trançado	Fibra-Ótica
1 metro de cabo de conexão	$7,00 UTP	$35,00
5 metros de cabo de conexão	$12,00 UTP	$45,00
Cabo interno a granel	$0,12 per foot	$0,60 por pé (par simples)
Conector de terminação de cabo	$1,60	$12,00
Adaptador Ethernet reforçado para subestação para relé de proteção	$1100,00	$1500,00
Adaptador Ethernet PC	$73,00	$340,00
Hub industrialmente reforçado (8 portas)	$800,00	$3400,00

Frames da Ethernet

Todos os dados trocados nas redes Ethernet viajam dentro de Frames (quadros ou molduras) da Ethernet. O quadro Ethernet é o envoltório externo para todas as informações da camada superior e dados de aplicação enviados através da rede. Todo o tráfego da Ethernet se desloca dentro de quadros Ethernet que incluem um endereço da fonte, endereço do destino, carga de dados (até 1500 bytes) e uma soma de verificação.

Há uma ligeira diferença entre os quadros definidos na Ethernet II (evoluída do padrão DIX) e os quadros IEEE 802.3. Os quadros podem coexistir na mesma rede, porém todos os dispositivos precisam incluir compatibilidade com quadros da Ethernet II e devem ser compatíveis com os quadros IEEE 802.3.

Acesso à mídia

Com as redes Ethernet, o tempo exigido para que o dado se desloque através da rede não é garantido. A interface da rede Ethernet em um dispositivo pode perder pacotes de dados se o tráfego da rede for muito alto. Este desempenho de tempo não determinístico precisa ser considerado para as aplicações críticas em termos de tempo, tais como proteção peer-to-peer e mensagens de controle. Em um sistema determinístico, todos os eventos ocorrem com tempo e seqüência completamente previsíveis. Um entendimento básico das regras de acesso à mídia Ethernet é importante para entender por que as redes Ethernet são não determinísticas.

As redes de barramentos de alta velocidade e multiponto podem operar através de muitas conexões ou mídias físicas diferentes (por exemplo, cabo de fibra ótica ou cabo de par trançado). A operação da rede requer que todos os dispositivos sejam conectados a um meio comum. Todos os nós da rede utilizam o mesmo método de sinalização.

Tendo em vista que apenas um nó de cada vez pode enviar dados satisfatoriamente, as redes multiponto e de barramento precisam ter regras de acesso à mídia para poderem movimentar dados eficazmente através das mesmas. Em redes similares ao Modbus®, há um único dispositivo mestre. Todo o tráfego da rede é tanto do mestre solicitando informação, quanto de uma resposta enviada para o mestre.

Um segundo método de controle de acesso à mídia é a rotação da ficha (token). Uma mensagem especial, ou token, é controlada por um mestre ou despachada de cada dispositivo para o próximo. Cada nó apanha a ficha, age como um mestre da rede e envia mensagens a outros dispositivos. Para redes com baixa carga, a rotação da ficha é ineficiente, porque os nós que não estão com qualquer operação de rede pendente ainda recebem a ficha. Um erro da rede também pode corromper ou destruir a mensagem da rede, fazendo com que a mesma tenha de gerar uma nova ficha. A geração de fichas é muito lenta, comparada às operações normais da rede.

Para poder superar as desvantagens do controle de acesso à mídia baseado em mestre e em rotação de ficha, as redes Ethernet utilizam um sistema chamado de Carrier Sense Multiple Access/Collision Detection (CSMA/CD) (protocolo de rede de comunicação que impede duas fontes de transmitirem ao mesmo tempo). Neste sistema, qualquer nó pode enviar dados a qualquer momento. Para um nó poder transmitir dados, ele precisa primeiro ouvir a portadora para determinar se nenhum outro nó está transmitindo. As colisões ocorrem quando dois nós encontram a rede disponível e transmitem dados ao mesmo tempo. Os nós da rede Ethernet possuem mecanismos para detectar colisões e tomar medidas adicionais para resolver a colisão e transmitir mensagens.

Quando ocorre uma colisão em uma Rede Ethernet, os nós emissores param de transmitir e introduzem um retardo antes de ouvir e começar a seqüência de transmissão novamente. Este processo é chamado de back off. Se as colisões persistirem (mais de 16 vezes), o nó eventualmente irá abandonar a mensagem enviada e as camadas de protocolo superiores terão de lidar com a perda de dados.

Por causa da operação CSMA/CD, os tempos de transmissão de comunicação em uma rede Ethernet não são determinísticos. As redes Ethernet não têm tempos de entrega garantidos ou desempenho garantido. Para redes pequenas e de baixa carga, CSMA/CD é eficiente e rápido. Para redes grandes ou durante períodos de tráfego elevado sustentado na rede, os tempos de transporte de dados podem ficar mais longos, altamente variáveis e pode haver perda de pacotes de dados.

Se se examinar de perto a operação do CSMA/CD, também se constatará que ela não dá prioridade para a informação mais antiga ou mais atrasada. Se diversos nós estão brigando para ter acesso à rede e um novo nó tenta enviar dados, as chances são de que a mensagem proveniente do novo nó irá sair primeiro. Isso tem sido chamado de “captura de canal” e, em casos extremos, leva ao “efeito de fome de pacotes” (PSE) [4].

Nas redes pesadamente carregadas, quando o canal é capturado, as mensagens mais antigas eventualmente serão abandonadas quando o máximo de 16 antigas for consumido. Isso leva a mais mensagens da camada de aplicação na medida que os dados perdidos forem repetidos. As colisões e retransmissões levam a maior carga na rede. O alto carregamento e PSE levam a excessivas latências na rede ou a total queda da mesma.

Um estudo [4] constatou que os atrasos de mensagens para redes altamente carregadas tornam-se inaceitáveis para dados que requerem entrega determinística, de baixa latência. Por exemplo, uma rede com 40 nós e uma carga oferecida (carregamento solicitado da rede entre nós) de 71,9 por cento (muito mais alta do que a operação normal da rede) teve uma latência média de 3,4 ms. A média é aceitável para proteção das mensagens de controle, porém a variação em latência é inaceitável. O desvio padrão foi 12,6 ms, com muitos retardos observados de mais de 100 ms e um máximo se aproximando de 1000 ms.

Embora esses testes tenham sido executados sob o que alguns denominariam de níveis de carregamento irrealisticamente elevados, é importante observar que a Ethernet não inclui mecanismos para limitar o carregamento. As condições de teste incluem três canais de “streaming vídeo” (65,4 por cento de carga oferecida) e tráfego de dados entre os nós (6,5 por cento de carga oferecida). O caso em teste poderia facilmente representar o que

acontece quando você (a título de experiência) tenta usar a rede Ethernet para enviar vídeo de câmeras de segurança através da mesma para o centro de controle SCADA, além de dados de supervisão em tempo real.

Para a maior parte das coletas de medições e dados de status, o desempenho não determinístico da rede Ethernet não constitui causa de preocupação. Para dados sensíveis ao tempo, tal como proteção peer-to-peer e controle, o desempenho da rede Ethernet, carregamento e arquitetura são considerações importantes no projeto da rede. Uma chave Ethernet, por exemplo, pode grandemente melhorar o determinismo e o desempenho da Ethernet para redes pesadamente carregadas. Ver o tópico ***Componentes da Rede Ethernet*** para mais discussão sobre os componentes das redes Ethernet.

Taxa de Transferência de Dados da Rede vs. Desempenho

Também é muito importante reconhecer que a taxa de transferência de dados de uma rede não corresponde diretamente a um aumento do desempenho ou taxa de rendimento. Se se está acostumado com uma conexão discada de 9600 bps, pode-se esperar que a rede Ethernet de 10 Mbpz seja capaz de transferir dados mais de 1000 vezes mais rápido. Na realidade, a transmissão de dados em alta velocidade também inclui um aumento no overhead de mensagens, sendo a taxa de rendimento limitada pela capacidade de processamento de mensagens dos nós da rede.

Os testes executados para um artigo apresentado durante a 2000 Western Power Delivery Automation Conference [5], compararam uma rede Modbus multiponto de 9600 bps com uma rede UCA2 de 10 Mbps. O comando de abertura manual proveniente de um operador em uma IHM chegou nos contatos de saída de um IED em 1,446 segundos através da rede Modbus e 0,021 segundos, através da rede UCA2, menos de 70 vezes mais rápido na Ethernet. O tempo para ida e volta a partir do comando do operador para exibir na tela da IHM foi de 3,106 segundos, e na rede Ethernet UCA2 foi de 0,389 segundos, menos de 8 vezes mais rápido na Ethernet.

PILHAS DE PROTOCOLO

As funções de camada superior são reunidas e recebem o nome de pilha de protocolo. A maior parte dos serviços da pilha de protocolo está nas Camadas 3 e 4, porém as pilhas de protocolo, na maioria das vezes, são parte de um conjunto de protocolos que inclui serviços para as camadas mais altas. O conjunto de protocolos mais popular é TCP/IP e UDP/IP (freqüentemente chamado somente de TCP/IP).

TCP/IP e UDP/IP

TCP/IP e UDP/IP são as pilhas da rede que ganharam fama como a base da Internet. Figura 5 é um diagrama do conjunto de protocolos Internet e componentes. TCP/IP, UDP/IP, e protocolos da camada de aplicação (FTP, SMTP, Telnet, etc.) são coletivamente conhecidos como conjunto de protocolos da Internet.

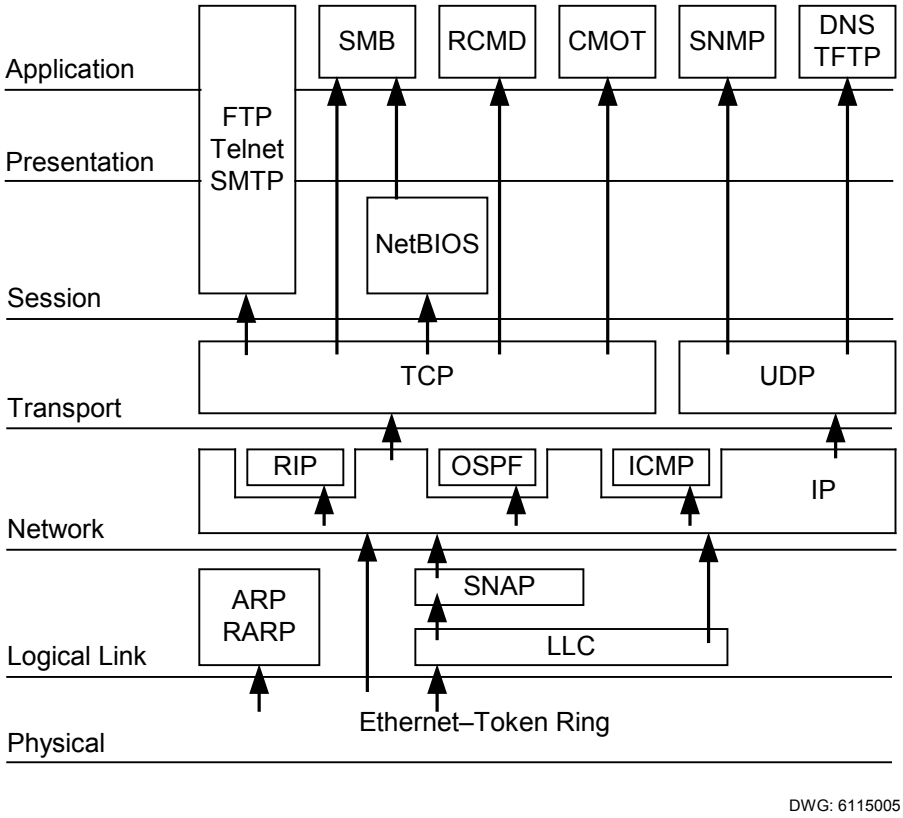

Figura 5 Diagrama de TCP/IP e UDP/IP [6]

TCP/IP e UDP/IP são pilhas separadas, porém a fundação IP comum tende a mantê-las juntas. A maior parte dos softwares que suportam TCP ou UDP, suporta ambos. O Protocolo Internet (IP) é uma camada que proporciona transmissão de pacotes básicos através de endereçamento, fragmentação de pacotes, time-outs de pacotes e diversas outras funções.

O Protocolo de Datagrama do Usuário (UDP) consiste de camadas acima de IP e completa um protocolo simples para troca de pacotes de informação entre os nós da rede. UDP aciona números das portas e somas de verificação ao IP. Ao contrário do TCP, o UDP não usa conexões, o que evita o handshake exigido para verifique se o nó receptor está disponível ou a mensagem chegou ao seu destino.

O Protocolo de Controle de Transmissão (TCP) adiciona streams, entrega confiável, adaptação da rede e controle de fluxo ao IP para criar um protocolo orientado para conexão razoavelmente robusto para intercâmbio de pacotes na rede. Uma vez que TCP inclui roteamento e conexões, ele é utilizado para a maioria das tarefas de troca de dados ponto a ponto.

OSI

Além do modelo OSI, há também uma pilha OSI, que segue o modelo de sete camadas OSI. Similar ao conjunto de protocolos TCP/IP e UDP/IP, a pilha OSI tipicamente é associada com diversos protocolos ISO para proporcionar um conjunto completo para algumas aplicações. A pilha OSI é primeiramente utilizada na infra-estrutura de rede e telecomunicações. A pilha OSI também é uma parte importante do protocolo UCA2.

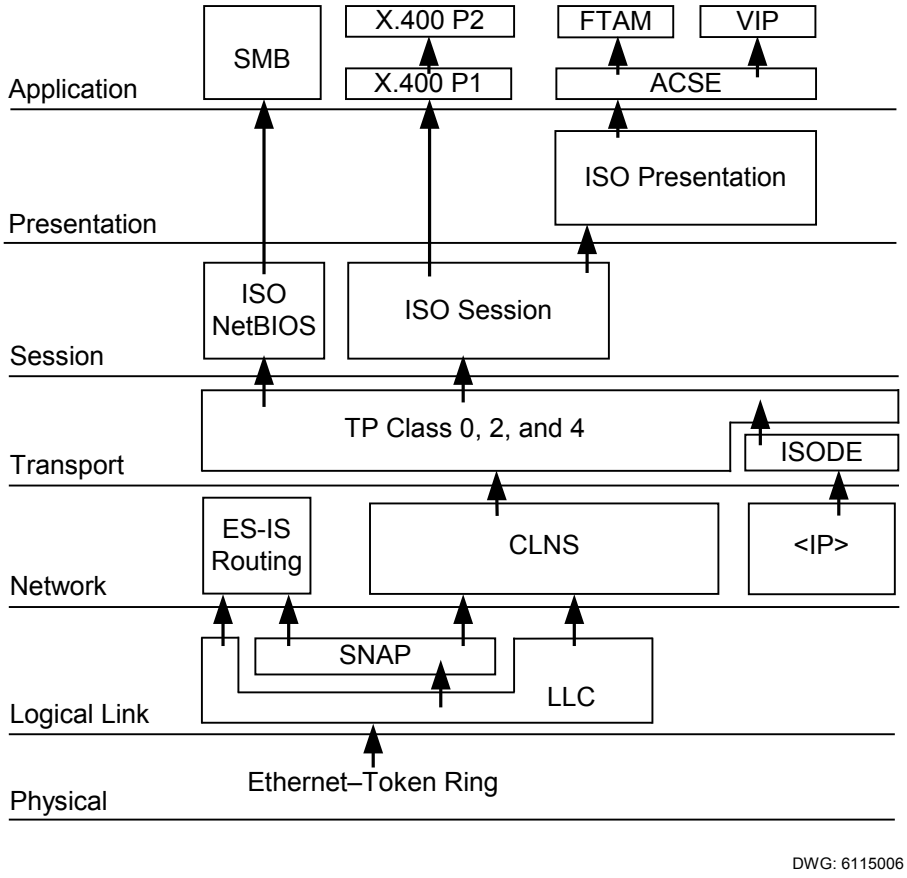

Figura 6 Conjunto de Protocolos OSI [6]

PROTOCOLOS DE TROCA DE DADOS

Na camada de aplicação (Camada 7), um protocolo de troca de dados permite que os nós troquem informação. Por exemplo, arquivos são trocados com o protocolo FTP ou dados do sistema de potência em tempo real podem ser coletados utilizando UCA2.

UCA2

UCA2 é parte do conjunto de protocolos da Utility Communications Architecture. O UCA para Protocolo de Dispositivos de Campo, agora conhecido como UCA2, é o resultado de um esforço de desenvolvimento conjunto do Electric Power Research Institute (EPRI), iniciado no final da década de 80. Os componentes primários do UCA são UCA2 e TASE.2 (Telecontrol Application Service Element 2). UCA2 é projetado para comunicação com IEDs da subestação. O TASE.2, também conhecido como ICCP (Inter-Control Center Communication Protocol), é projetado para transportar dados entre bases de dados em tempo real.

Todos os protocolos UCA são projetados na forma de uma solução em camadas, como independência completa da rede na camada de modelagem mais alta. Para agilizar a implementação e auxiliar na interoperabilidade, os projetos de demonstração e especificações incorporam camadas específicas de pilha e rede.

Tanto o TASE.2 como o UCA2 são baseados no protocolo de comunicações subjacente, Manufacturing Messaging Specification (MMS). O MMS é um protocolo de automação industrial desenvolvido em grande parte pela General Motors, que tem servido como um centro de pesquisa e desenvolvimento para tecnologias avançadas em automação industrial. Embora o MMS não esteja mais sendo largamente utilizado no ambiente de automação industrial, o mesmo constitui um protocolo capaz que serve como base tanto para o UCA2, como para o TASE.2.

O UCA2 é um perfil para comunicação orientada para objeto com IEDs de subestação, utilizando MMS. O Common Application Service Models (CASM) define como os objetos interagem com os serviços da rede (MMS). O GOMSFE é a especificação de modelo objeto para UCA2. A Figura 7 ilustra como os componentes do UCA2 trabalham e como a pilha da rede e as camadas da rede física combinam para formar um protocolo UCA2 completo.

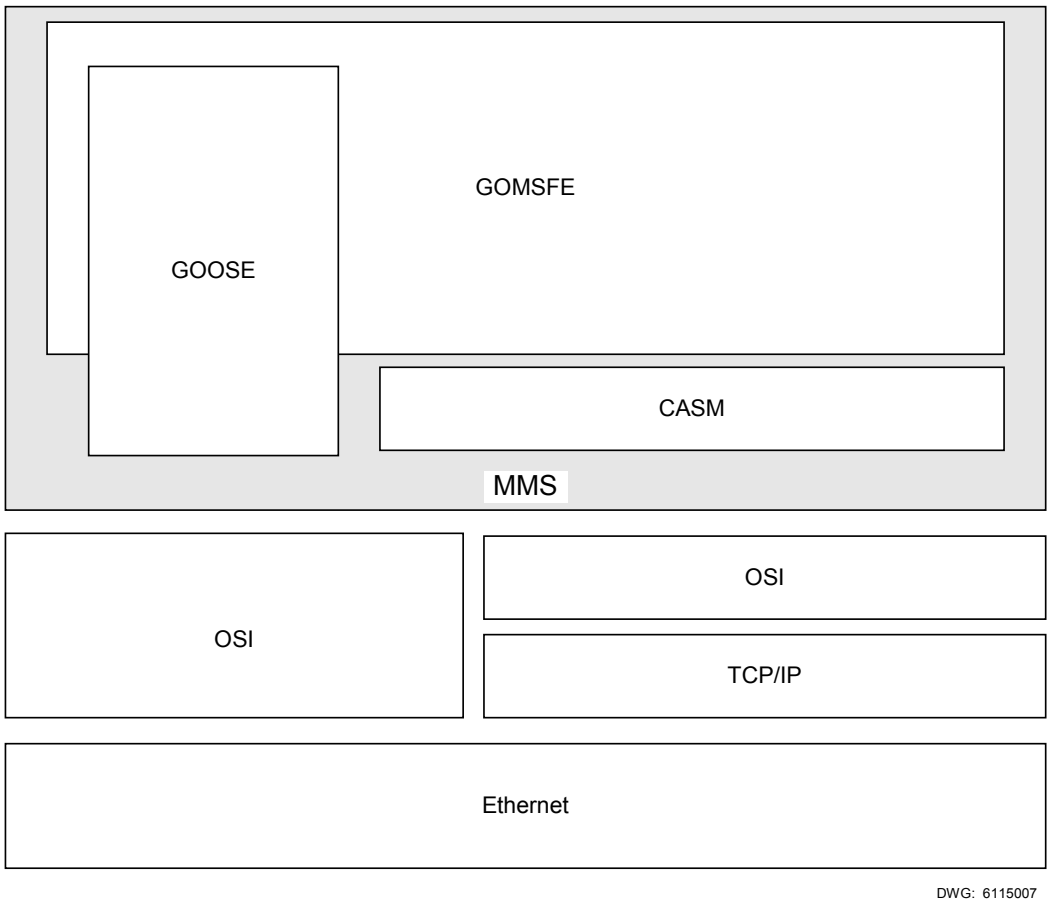

Figura 7 Componentes UCA2

A camada da pilha de protocolo de implementações do UCA2 que está sendo utilizada atualmente é uma combinação de OSI e TCP/IP. Pode-se utilizar puramente a pilha OSI ou camadas inferiores da pilha TCP/IP combinadas com as camadas superiores da pilha OSI. A maior parte das implementações inclui os componentes necessários para operar em qualquer configuração de pilha.

As especificações e padrões para UCA2 são completas do ponto de vista do documento funcional, porém não são parte de uma norma ratificada. Os documentos de trabalho foram

desenvolvidos através de uma série de projetos de demonstração e reuniões técnicas do EPRI. A especificação GOMSFE completa mais recente é a 0,91. Diversos outros documentos descrevem CASM e outras facetas da UCA2. O EPRI não atua como uma organização normativa, e no momento não existe qualquer grupo de especificação e nenhuma maneira de solicitar um jogo de documentos do UCA2 em vigor. Dois esforços paralelos nas comissões de normas estão em andamento para desenvolver e ratificar normas funcionais.

A International Electrotechnical Comission (IEC) está trabalhando em uma norma sob o rótulo de IEC 61850 para modelos GOMSFE. Não está claro se o projeto da IEC irá incluir o CASM, MMS e componentes de redes Ethernet como a única implementação, e se o mapeamento para outras camadas inferiores, incluindo os protocolos IEC 61870, será incluído.

P1525 é um esforço de normas para redes de subestação dentro da IEEE. Não está claro neste momento se o trabalho com P1525 irá complementar o trabalho da IEC ou tomar um rumo diferente. Muitos dos antigos proponentes da UCA2 estão pedindo esforços do EPRI, IEEE e IEC para culminar em uma "harmonização", onde todas as especificações serão compatibilizadas e tornadas interoperáveis. Atualmente, não há qualquer cronograma para a harmonização ou coordenação de esforços entre esses dois grupos. Embora não exista um movimento conjugado para padronizar a UCA2, os fabricantes estão implementando a UCA2 utilizando os documentos do trabalho do EPRI.

GOMSFE

O GOMSFE é um modelo objeto para coletar dados de medição e status a partir de IEDs. O GOMSFE utiliza um resumo orientado para objeto para criar definições standard para representar medidores, relés de proteção e outros dispositivos nas redes UCA2. Ao contrário das gerações anteriores de protocolos, o UCA2 não depende dos conceitos de índices ou registros. O GOMSFE organiza dados em modelos objeto chamados modelos ou tijolos.

O GOMSFE descreve dispositivos multifuncionais com diversos modelos, cada um descrevendo uma função. Um exemplo disto é um relé de proteção. Um relé pode conter dados de medição que preenchem um modelo de medição multifásico. O relé de proteção também pode funcionar como uma interface de disjuntor, com um modelo para um controlador de disjuntor.

Os modelos GOMSFE consistem de pedaços standard de dados com nomes standard formados a partir de um conjunto de tipos de dados standard. Por exemplo, o tijolo de medição polifásico (MMXU) inclui corrente da fase A. Tabela 2 relaciona os objetos do componente funcional MX do modelo MMXU. A corrente da fase A é parte do objeto MMXUMXA, que é indicada como sendo da classe WYE.

Tabela 2 Componente Funcional MX do Modelo MMXU [7]

FC	Nome do Objeto	Classe	rwec	mo	Descrição
MX	V	WYE	r	o	Tensão na fase A, B, C a G
	PPV	DELTA	r	o	Tensão AB, BC, CA
	A	WYE	r	o	Corrente na fase A, B, C e N
	W	WYE	r	o	Watts na fase A, B e C
	TotW	AI	r	o	Total de Watts em todas as 3 fases
	VAr	WYE	r	o	VArs na fase A, B, C
	TotVAr	AI	r	o	Total de VArs em todas as 3 fases
	VA	WYE	r	o	VA na fase A, B, C
	TotVA	AI	r	o	Total de VA em todas as 3 fases
	PF	WYE	r	o	Fator de Potência para fase A, B, C
	AvgPF	AI	r	o	Fator de potência médio de todas as 3 fases
	Ang	WYE	r	o	Ângulo entre tensão e corrente de fase
	Hz	AI	r	o	Freqüência do sistema de potência
	FltMagA	WYE	r	o	Magnitude da falta na fase A, B, C

Na coluna “rwec” da Tabela 2, vemos que as correntes de fase são apenas para leitura. As medições também são mostradas como opcional na coluna “m/o”. Isso significa que os dispositivos que não têm este dado não irão incluir o objeto corrente de fase. O tipo WYE é definido em uma tabela separada, conforme mostrado nas Tabela 3.

Tabela 3 Classe Comum Tipo WYE [7]

Nome	Tipo de Dado	m/o
PhsAi	INT16S	o
PhsAf	FLT32	o
PhsBi	INT16S	o
PhsBf	FLT32	o
PhsCi	INT16S	o
PhsCf	FLT32	o
Neuti	INT16S	o
Neutf	FLT32	o
q	BSTR16	o
t	BTIME6	o

Verificando a medição para fase A, vemos PhsAi e PhsAf dos tipos INT16S e FLT32, respectivamente, que são opcionais. Se o dispositivo tem uma medição de inteiros assinada, de 16 bits, PhsAi estará disponível, e se a medição é um ponto flutuante de 32 bits, PhsAf estará disponível. Na parte inferior da tabela, q é uma seqüência de valores de 16 bits, que é

utilizada para flags de qualidade de dados, enquanto t é uma chancela de tempo representando quando a medição foi coletada. Se o dispositivo do exemplo tem a medição de ponto flutuante da corrente da fase A, poderíamos anotar a referência "achatada" para o valor como MMXUMXA$PhsAf.

Embora isso seja um processo simples, o mesmo é demorado. Uma função chamada "autodescrição" agiliza o processo significativamente. Um browser MMS standard pode solicitar uma descrição dos dados contidos num dispositivo UCA2 e apresentar essa descrição na tela de um computador. Pode-se, em seguida, apontar e clicar no valor de interesse.

Modelos objeto standard isoladamente não permitem que os fabricantes individuais inovem e adicionem novas funções. Por causa desta limitação potencial, GOMSFE permite a extensão de modelos e a criação de modelos customizados. Os modelos customizados também são incluídos no processo de auto-descrição, para que se possa utilizar um browser para descobrir o que está disponível, na base nó por nó.

O GOMSFE também utiliza uma estrutura organizacional de alto nível, chamada domínio. Todos os dispositivos UCA2 têm pelo menos um domínio, chamado dispositivo lógico, e podem incluir mais dispositivos lógicos ou mais domínios. Os modelos são agrupados nos domínios.

Embora não universalmente implementado, um mecanismo para reportar mudanças de dados e dados com chancela de tempo é incluído no UCA2. Um objeto genérico para mover grandes itens, chamado Objeto Binário Grande (BLOB) é disponível para transferência de arquivos e outros dados não utilizados pelo UCA2, porém coletados para outros fins.

GOOSE

O GOOSE é parte do modelo GLOBE do GOMSFE e também se constitui num sistema de mensagens independente. IEDs UCA2 utilizam mensagens GOOSE para comunicação e controle peer-to-peer geradas por eventos. Cada dispositivo UCA2 envia uma mensagem GOOSE quando ocorre um evento interno de mudança de dados. Um evento de mudança de dados ocorre quando um ponto monitorado muda de estado, por exemplo, de um para zero ou de zero para um. As mensagens geradas por eventos limitam o tráfego da rede e melhoram a velocidade de resposta, enviando mensagens somente quando ocorrem eventos de mudança de dados. Isso é uma melhoria significativa em relação aos mecanismos de interrogação, que sobrecarregam a rede mesmo quando nenhum valor de dados está disponível.

Além das mensagens geradas por eventos, os dispositivos UCA2 enviam mensagens GOOSE a uma taxa default de uma vez por minuto. Os dispositivos que recebem mensagens GOOSE utilizam as mensagens de taxa de default para rastrear o status dos emissores GOOSE e coletar valores iniciais quando entram na rede.

Cada mensagem GOOSE contém um nome de identificação de texto do emissor GOOSE e um endereço de destinação multicasting da Ethernet. Os dispositivos UCA2 utilizam os endereços de destinação multicast da Ethernet para filtrar as mensagens GOOSE entrantes. Cada dispositivo aceita e processa apenas as mensagens contendo informação que ele esteja preparado para utilizar.

Cada mensagem GOOSE inclui um valor Hold Time, que define por quanto tempo deve o dado da mensagem ser considerado como válido. Quando o hold time expira, o recipiente da mensagem GOOSE pode executar ações apropriadas com base na informação de que as mensagens provenientes do emissor GOOSE não estão mais chegando ao recipiente.

DNP 3.00

Em 1998, um artigo apresentado ao Grupo do Usuário do Distributed Network Protocol (DNP) [8] resumia os trabalhos anteriores com DNP através das redes Ethernet e propunha diversas soluções. Embora o documento não tivesse sido ratificado oficialmente como parte das normas DNP, ele segue sendo utilizado como a especificação funcional para muitas implementações de DNP 3.00 através de redes Ethernet.

Os documentos contém diversas recomendações chaves sobre operação DNP 3.00 com enlaces LAN e WAN. As recomendações mais significativas para o usuário final médio são listadas abaixo:

- DNP utilizará o conjunto de protocolos TCP/IP e UDP/IP também chamado "The Internet Protocol Suite".
- A Ethernet é a camada física recomendada, porém a implementação recomendada irá funcionar através de qualquer enlace onde o conjunto de protocolos TCP/IP e UDP/IP estiver presente.
- Todos os dispositivos têm que suportar mensagens tanto através de mecanismos TCP (orientada a conexão), como UDP (sem conexões).
- As camadas DNP são retidas e suplementam camadas de protocolo da rede de modo que uma grande restruturação da DNP não seja necessária.

O DNP 3.00 utiliza um sistema orientado a objeto que não é tão completo quanto aquele utilizado pelo UCA2. Os tipos de dados e solicitações são especificados como objetos DNP. Os objetos de dados especificam tipos ao invés de dados específicos, de modo que não há qualquer modo padronizado de solicitar a corrente da fase A, como no exemplo UCA2 acima. Se puder haver mais de um caso de objeto, há um índice que torna cada caso singular. Os objetos são utilizados para solicitação de dados abreviados, tipos de dados específicos e operações tais como coleção de buffer de controle e eventos.

Protocolos Industriais

Vários dos protocolos de integração industrial mais populares estão rodando através de redes Ethernet ou estão sendo preparados para serem operados através das redes Ethernet. Por exemplo, Modbus TCP é Modbus para uso nas redes TCP/IP [9]. Outros protocolos industriais, incluindo ControlNet®, Profibus e o Foundation Fieldbus estão migrando para as redes Ethernet.

É importante considerar este trabalho quando se planeja utilizar a Ethernet em aplicações para sistemas de potência. O ambiente do escritório tem tornado as tecnologias baratas e disponíveis para aplicações industriais e em casos onde o equipamento projetado para escritórios não é adequadamente robusto ou resistente. O equipamento destinado a escritórios proporciona uma base para o entendimento e desenvolvimento de componentes apropriados para redes Ethernet industriais. Da mesma forma, as redes Ethernet industriais servem como excelente base e campo de experiências para produtos e tecnologias que irão ser utilizados em redes Ethernet para subestações.

Uma das melhores fontes de informação a respeito das redes Ethernet industriais é a página na Web http://ethernet.industrial-networking.com/. Baseada no Reino Unido, o site é a versão on-line do "The Industrial Ethernet Book", uma publicação tipo revista trimestral que inclui artigos informativos, listas de fornecedores e fontes para informação a respeito das redes Ethernet industriais.

Uma vez que poucos protocolos de rede Ethernet têm sido utilizados em aplicações Ethernet para subestações, os mesmos não serão considerados em discussões subseqüentes das tecnologias que se deve considerar ao se projetar uma rede Ethernet para subestações.

COMPONETES DA REDE ETHERNET

Há diversos componentes que são necessários para se construir uma rede Ethernet. Os parágrafos abaixo relacionam o equipamento essencial e proporcionam algumas informações sobre cada um. Figura 8 mostra uma rede Ethernet com cada um dos dispositivos listados indicado.

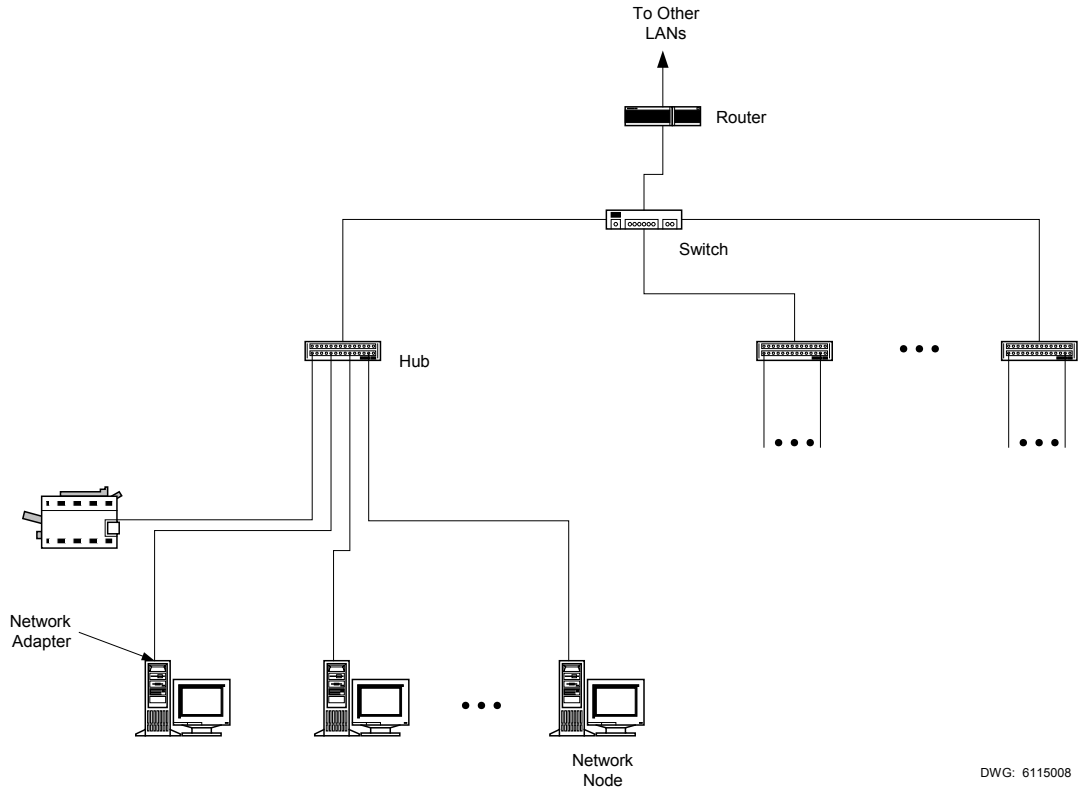

Figura 8 Componentes da Rede Ethernet

Nó da Rede

Um nó da rede é um dispositivo da rede que realiza processamento inteligente de dados ou geração de dados. Os nós da rede podem ser classificados como mestres ou escravos, clientes ou servidores e peers (dispositivos) para sedescrever o fluxo de dados entre os nós.

Adaptador da Rede

Cada dispositivo de uma rede Ethernet deve incluir uma interface física para a rede Ethernet standard. Esta interface freqüentemente é chamada de adaptador, um cartão da rede ou um cartão de interface da rede (NIC). Mesmo se o NIC for uma parte integrante do dispositivo, o mesmo precisa estar lá para que possa ser parte da rede Ethernet.

Cada interface Ethernet tem um endereço de camada de controle de acesso de mídia (MAC) da Ethernet, que é designado na fábrica. Cada fabricante registra uma faixa de endereços e, durante a fabricação, programa a interface para usar um endereço. Isso significa que cada

dispositivo da rede Ethernet tem um endereço exclusivo que é usado nos *frames* (molduras) da Ethernet.

Hubs

Um hub é um dispositivo que atua como um cabo tronco, com segmentos muitos curtos que conecta cada cabo de nó à rede. Um hub repete todo o tráfego vindo da rede para todos os nós. Uma conexão uplink permite que o hub envie dados para outros Hubs, chaves ou roteadores. Os Hubs são uma maneira fácil e barata de conectar muitos dispositivos a uma rede Ethernet.

Os hubs são basicamente dispositivos passivos. Se um nó falhar e enviar um fluxo contínuo de dados errados para a rede, o hub repete os dados errados para todos os nós da rede. Uma vantagem dos hubs é que eles são menos complexos e, portanto, bastante confiáveis, em comparação com chaves e roteadores [10].

Chaves

Uma chave atua como um hub, conectando nós para formar uma rede que opera logicamente como uma rede multipontos. Além de repetir dados, no entanto, a chave decodifica algumas partes das mensagens Ethernet e dirige o tráfego em uma rede Ethernet.

Um método de evitar colisões de mensagens em uma rede Ethernet é limitar o número de nós na rede. Um grupo de nós que compartilha um meio comum é chamado de domínio de colisão. Quando há menos nós em um domínio de colisão, menos colisões ocorrem e a rede Ethernet opera mais deterministicamente e eficientemente.

Uma chave reduz o domínio de colisão de cada nó para o mínimo final – dois nós. Uma chave decodifica o tráfego entrante proveniente de cada nó da rede e direciona tráfego da rede. A chave reduz drasticamente o número de colisões de mensagens, aumentando grandemente o desempenho da rede.

Embora as chaves sejam menos confiáveis do que os hubs, o maior desempenho da rede Ethernet compensa a menor confiabilidade da rede. As chaves operam nas camadas mais inferiores (camadas físicas e de enlace de dados) das redes Ethernet e são independentes da pilha da rede ou protocolo de aplicação.

Roteadores

Um roteador opera de maneira similar a uma chave. A diferença é que os roteadores mantém as mensagens em uma rede local e enviam apenas as mensagens que precisam deixar a rede local. O roteador contém tabelas sobre como rotear mensagens e decodifica algumas das informações da Camada 3 ou pilha para direcionar mensagens. Tendo em vista que os roteadores operam em camadas de protocolo mais altas do que as chaves e hubs, tem-se que selecionar roteadores que sejam compatíveis com os stacks de protocolo da rede.

Os roteadores não despacham mensagens de difusão Ethernet, mensagens GOOSE, por exemplo. As mensagens de difusão Ethernet não são destinadas para nós situados fora da rede local. Alguns roteadores mais avançados atuam como pontes de rede que permitem rotear protocolos não roteáveis, como GOOSE. Deve-se ter bastante cuidado ao se rotear mensagens de difusão, porque pode-se aumentar drasticamente o tráfego através de enlaces de baixa largura de banda entre as redes. Tráfego alto pode significativamente diminuir o rendimento das conexões inter-rede e significativamente aumentar as despesas para serviços medidos de acesso à rede.

Os roteadores também podem atuar como uma firewall (parede corta-fogo). Uma parede corta-fogo opera como uma barreira de segurança entre a rede e o mundo externo. Utilizadas corretamente, as firewalls e proteção de senha de dispositivo podem prevenir acesso não autorizado aos sistemas críticos.

TOPOLOGIA DA REDE ETHERNET

É muito popular caracterizar as redes Ethernet (e outras redes de automação de subestações) como um barramento mágico que conecta todos os dispositivos e resolve todos os problemas. Os diagramas são usualmente similares à Figura 9.

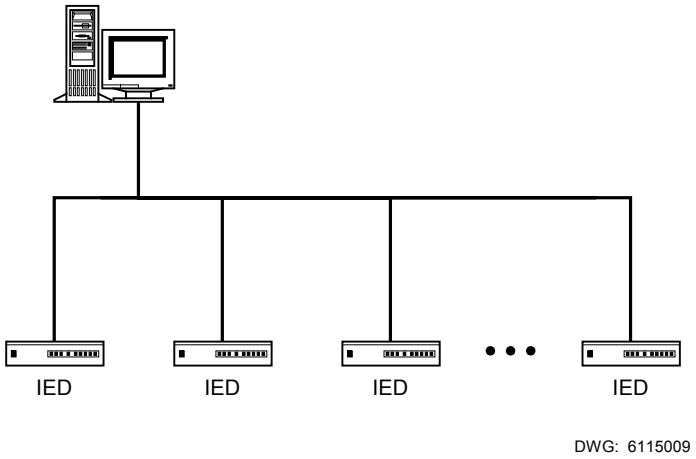

Figura 9 Rede Barramento Mágico

O conceito do barramento mágico é correto apenas parcialmente, mesmo em um sentido lógico. Com uma rede Ethernet que contenha um hub, a rede é na realidade conectada como uma estrela que funciona logicamente como um barramento. Se o nó central for uma chave, cada segmento entre uma chave e um nó opera independentemente, com a chave fazendo buffer e direcionando tráfego para reduzir as colisões e diminuir os atrasos na transmissão de mensagens.

Se você está projetando uma rede pequena com um nó central simples, você pode usar uma topologia similar a aquela mostrada na Figura 4. Se a sua rede é mais complexa, e inclui links para outras redes, você poderá ter uma topologia mais complexa similar a da Figura 8. A rede da Figura 8 utiliza chaves para reduzir o número de nós em cada domínio de colisão e fazer o tráfego fluir para o roteador mais eficientemente. O roteador permite que apenas o tráfego destinado a outras redes saia da rede. O roteador também permite que apenas as mensagens que são destinadas para os nós dentro da rede entrem na rede.

REDES DE SUBESTAÇÃO

Esta seção descreve os requisitos principais das redes para subestações e examina como os protocolos e as tecnologias já descritas atendem a tais requisitos.

Robustez Ambiental

As salas de controle das subestações tipicamente não são espaços ambientalmente controlados. Freqüentemente há um mínimo de aquecimento (talvez para 50ºF) e nenhuma refrigeração. Há também a possibilidade de que a sala de controle possa ficar sem energia. Durante ess e tempo, a bateria da subestação mantém a operação da proteção de outras funções essenciais, porém não proporciona uma fonte de energia de reserva para aquecimento e refrigeração. Os equipamentos de redes para escritórios, incluindo transceptores, hubs e chaves muitas vezes não são apropriados para ambientes sem aquecimento ou refrigeração adequados.

A natureza crítica dos relés de proteção tem levado a diversos requisitos ambientais, incluindo RFI, ESD, temperatura de operação e vibração. Deve-se avaliar cuidadosamente se a Ethernet é um componente crítico da subestação e selecionar os equipamentos de acordo.

Topologia da Rede

Você talvez deseja conectar a sua rede em topologia estrela simples com uma chave ou hub, porém há diversas considerações adicionais. O acesso externo a partir de uma rede de engenharia requer um ponto de entrada na LAN da subestação, tipicamente através de um roteador. Você deve considerar se o acesso de engenharia e dados potencialmente críticos devem viajar através do mesmo segmento da rede.

As redes de engenharia também freqüentemente são conectadas a redes corporativas e finalmente à Internet. Se você conectar uma LAN crítica à rede de engenharia, você terá provido um trajeto (se um hacker vencer as barreiras de segurança) entre a Internet e a sua LAN crítica da subestação. Um simples ataque do tipo recusa de serviço dentro de sua LAN corporativa poderia prejudicar a LAN da subestação.

Há diversas soluções para mitigar os problemas de acesso de engenharia e estabelecimento de uma rede crítica. A mais fácil é utilizar dois adaptadores de rede em cada IED conforme mostrado na Figura 10.

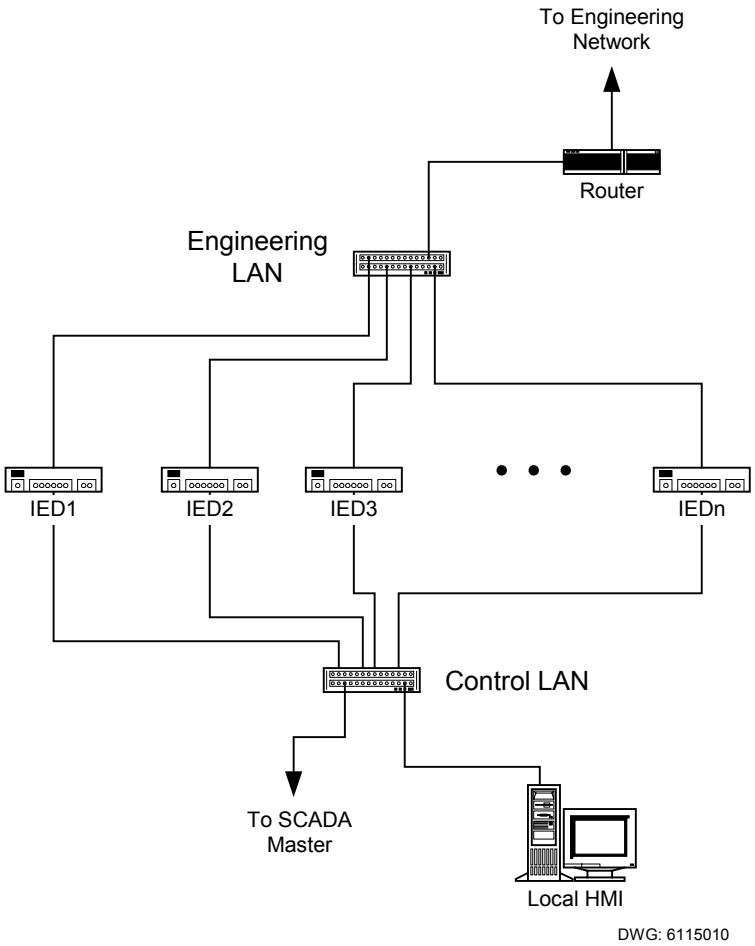

Figura 10 Topologia de Rede de Subestação LAN Dupla

A topologia de rede de subestação LAN dupla protege a LAN de Controle eliminando o tráfego que não se destina a mensagens de controle peer-to-peer or as funções de IHM e do SCADA. Embora essa topologia aborde diversas considerações importantes, ela não proporciona sincronismo de tempo de alta precisão. Também, muitos IEDs de subestação são disponíveis com interfaces físicas redundantes, porém não com interfaces de rede dupla que operam simultaneamente. As interfaces Ethernet também custam quase $1500 em IEDs da subestação, tornando essa arquitetura mais cara do que algumas alternativas.

Você deve considerar o reforço de sua topologia com outros dispositivos que podem proporcionar capacitações adicionais, além de reduzir o custo da implementação. Os processadores de comunicações utilizados na topologia mostrada na Figura 11 proporcionam diversas funções.

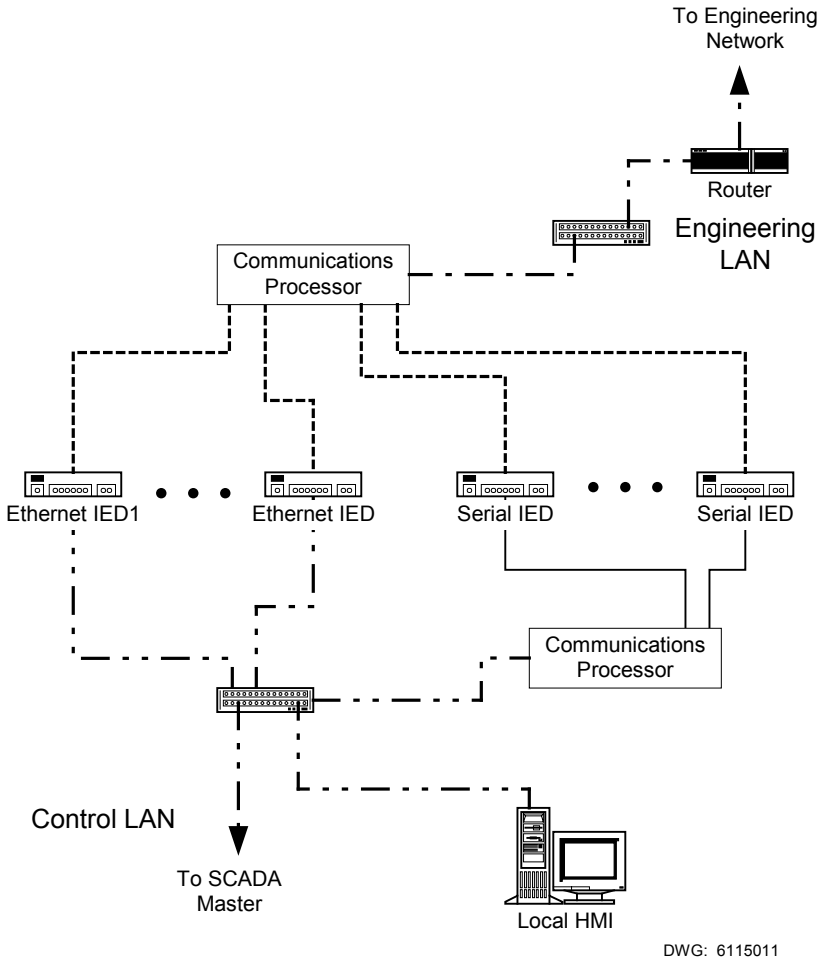

Figura 11 Rede de Subestação Ethernet com Processador de Comunicações

Primeiro, os processadores de comunicação proporcionam sincronismo de tempo IRIG-B a todos os IEDs da Subestação. Segundo, o processador de comunicação permite a você usar IEDs existentes ou novos que não têm interfaces Ethernet diretas. Isso significa que você pode proteger os seus investimentos em equipamento já existente, usando-o ao invés de trocá-lo mediante consideráveis despesas. Por último, o processador de comunicação proporciona uma interface serial para acesso de engenharia discada em backup e acesso à base de dados centralizada da subestação no processador de comunicação.

Sincronismo de Tempo

Para poder coletar dados do Registrador de Eventos Seqüencial (SER) e de oscilografia de eventos que podem ser coordenados entre dois dispositivos, é importante que todos os dispositivos da subestação estejam coordenados no tempo correto. Atualmente, isso é conseguido através de um sinal IRIG-B através de conexão direta a um clock GPS, ou através de um dispositivo que eletricamente distribua o sinal de sincronismo de tempo. O referido dispositivo é um processador de comunicações.

Não há padrão de sincronismo de tempo UCA2 que seja largamente implementado ou suportado por clocks GPS. O padrão de sincronismo de tempo proposto para DNP 3.00 operando na Ethernet irá inclui as imprecisões na medida que aumenta a carga na Rede Ethernet.

Há dois padrões de sincronismo de tempo que são largamente utilizados nas redes Ethernet: Network Time Protocol (NTP-RFC-1305) e o Simple Network Time Protocol (SNTP – RFCs 1361, 1769, 2030), ambos padronizados pela Internet Engineering Task Force (IETF). Com esses protocolos, a exatidão típica de sincronismo é de 1–5 ms. Exatidões mais altas são possíveis sob condições controladas.

A exatidão de 1–5 ms não é suficiente para amostragem de dados oscilográficos e dados sincronizado no tempo do sistema de potência. Para poder obter sincronismo de tempo adequado, você precisa diretamente conectar a sua fonte IRIG-B aos IEDs ou utilizar um dispositivo que distribua IRIG-B para os IEDs.

Proteção para Mensagens de Controle Peer-to-peer

Apenas o protocolo GOOSE UCA2 proporciona um sistema de mensagens de controle peer-to-peer padronizado para as redes Ethernet. O DNP 3.00, através da Ethernet, não proporciona um mecanismo de mensagens peer-to-peer. Se você vai usar GOOSE para aplicações críticas, considere cuidadosamente se os mecanismos e temporização das mensagens GOOSE são adequados para a sua aplicação. Para uma comparação completa de GOOSE com os requisitos da IEC 834 [10], veja [11] para uma discussão detalhada de GOOSE e das normas da IEC 834.

Se você tiver determinado que o timing de mensagens GOOSE e a probabilidade de entrega de mensagens são adequados para a sua aplicação específica, então considere a confiabilidade da topologia da rede que você está utilizando [12]. A indisponibilidade da melhor (e mais cara) configuração de Rede Ethernet é 100 vezes pior do que a de uma conexão serial direta.

Você pode utilizar conexões seriais diretas além das redes Ethernet em esquemas de proteção de subestações e comunicação. A comunicação com conexões seriais diretas proporciona um sistema completamente fechado que não está exposto aos riscos potenciais de segurança e confiabilidade de uma conexão de rede. Se a sua rede Ethernet não é utilizada para mensagens críticas, você pode montá-la como equipamentos muito menos onerosos.

Acesso da Engenharia

Um dos locais onde as redes Ethernet podem ser mais úteis é para acesso da engenharia aos IEDs da subestação. Há três razões primárias para os engenheiros se comunicarem com relés:

1) Comunicar diretamente para informação de diagnóstico e status

2) Recuperar dados baseados em arquivos, incluindo relatórios de oscilografia e SER

3) Gerenciar e manipular configurações de relés

É possível conectar redes Ethernet de modo que os relés da subestação se tornem acessíveis a partir dos terminais da engenharia localizados no escritório central. Este tipo de arquitetura precisa ser implementado com cuidado, já que numerosas questões de administração e segurança que precisam ser atendidas.

Nenhum dos protocolos discutidos até agora (suíte de protocolos TCP/IP, UCA2 ou DNP 3.00) inclui funções de segurança para proteger os IEDs da subestação contra acesso não autorizado. É vital que se aborde as questões de segurança da rede ao projetar qualquer sistema que permita acesso a dispositivos IED da subestação a partir de um ponto fora da SE; caso contrário isso poderia se transformar num caminho que forneceria acesso interno (um empregado) ou externo (pela Internet) diretamente aos dispositivos de proteção críticos.

Comunicar Diretamente com o IED

O conjunto de protocolos de rede TCP/IP inclui um protocolo chamado Telnet que foi usado para comunicações entre terminal e o computador central. Atualmente, Telnet proporciona uma excelente maneira de acessar relés com uma interface de terminal simples e de baixo preço. A maioria dos sistemas de operação de computador, incluindo a família Microsoft® Windows® de sistemas de operação, inclui uma aplicação Telnet grátis.

O UCA2 não inclui um objeto GOMSFE que proporciona acesso terminal direto aos IEDs da subestação. O DNP 3.00 através da Ethernet inclui um objeto terminal virtual, porém esse objeto é razoavelmente novo e não há qualquer master DNP para suporta-lo. O IED individual pode possuir proteção de senha, porém a simples proteção de senha isoladamente não é uma defesa adequada contra todas as fontes de invasão.

Recuperação de Dados Baseados em Arquivo

A maioria dos engenheiros deseja recuperar arquivos de base de dados, incluindo oscilografia, relatórios SER e outros diagnósticos de IED que são apresentados em formatos de arquivo. O FTP, dentro do conjunto de protocolos TCP/IP, proporciona um mecanismo para troca de arquivos. Como acontece com Telnet, a maioria dos sistemas de operação de computadores inclui aplicações FTP grátis.

As redes UCA2 permitem transferência de arquivos através do objeto GOMSFE BLOB mencionado anteriormente, ou serviços de transferência de arquivo MMS. O objeto GOMSFE BLOB não é universalmente implementado. Tanto o BLOB quanto os serviços de transferência de arquivos MMS, requerem que se tenha software MMS para recuperar os dados. Isso significa que cada terminal de trabalho tem que incluir um browser MMS (aproximadamente $1500 - $2000) instalado, para acessar os dados.

O NDP 3.00 inclui um mecanismo de transferência de arquivos, porém como acontece com a comunicação de terminal virtual DNP, há muito pouco suporte entre os fornecedores de master DNP 3.00 para esta função. Na medida que as redes DNP 3.00 se tornam mais comuns, o suporte para esta função poderá se tornar mais ampliado.

O FTP inclui um sistema de senha simples para segurança. Como acontece com a comunicação direta com um IED, a simples proteção de senha isoladamente não é uma defesa adequada contra todas as fontes de invasão. O UCA2 e o DNP 3.00 não incluem segurança para operações de transferência de arquivos. No entanto, eles requerem software especializado que atue como uma barreira contra alguns intrusos.

Modificação de Configurações

Embora a manipulação dos ajustes em um IED remoto pareça uma coisa atraente, deve-se considerar as ramificações antes de implementar uma rede que permita manipulação dos ajustes. A Ethernet proporciona um bom meio de comunicação para ajuste de IEDs localmente (dentro da subestação).

Embora o UCA2 tenha uma interface de ajustes limitado incorporado em alguns modelos GOMSFE standard, ele é inadequado para configurar e gerenciar corretamente um relé de proteção multifuncional. O modelo GOMSFE procura dividir o relé em várias funções orientadas para proteção e não trata dos relacionamentos entre as funções de proteção ou outros tipos de configurações que são exigidos. O UCA2 também não tem qualquer segurança para configurações; qualquer um com um browser MMS pode manipular os ajustes que são parte dos modelos GOMSFE.

O DNP 3.00 não inclui qualquer interface definida para ajustes. Como acontece com UCA2, não há quaisquer funções dentro do DNP 3.00 que sejam adequadas para configurar e gerenciar ajustes no caso de um dispositivo multifuncional complexo. Também, o DNP 3.00 não inclui segurança para ajustes, permitindo que qualquer pessoa com acesso ao mestre ou rede de comunicações possa manipular os ajustes.

Você pode desejar usar a Ethernet como uma interface para configurar os IEDs remotamente. Primeiro, você deve decidir se é bom mudar ajustes a partir de um local remoto sem testes locais e a observação dos resultados. No passado, tendo em vista que as tradicionais redes SCADA não proporcionavam qualquer segurança para os ajustes, as interfaces de configuração dentro de protocolos SCADA eram raras. Alguns engenheiros têm insistido que a natureza de rede fechada da comunicação SCADA elimina a necessidade de segurança adicional, porém isso significa que qualquer pessoa que possa acessar o mestre ficaria em condições de alterar ajustes.

Nos locais onde o acesso local é impraticável ou tão difícil, que os riscos de modificação dos ajustes remotamente compensam os custos de viajar para o IED, você pode usar uma rede Ethernet para proporcionar conexão com os IEDs para gerenciamento das configurações. Interfaces de ajuste podem ser providas usando FTP ou outros mecanismos de transferência de arquivo, terminal virtual ou diretamente dentro do protocolo de troca de dados.

Dados em Tempo Real

Se você deixar todos os dados da subestação nos IEDs, você está usando uma arquitetura de base de dados distribuída. Em uma arquitetura distribuída, você não terá oportunidade de coletar os dados e proporcionar uma interface otimizada para cada consumidor de dados (IHM local e outros).

As estruturas de base de dados distribuída requerem que quaisquer cálculos ou decisões tomadas a respeito dos dados sejam tomadas em cada dispositivo que está recuperando dados. Por exemplo, você pode comparar as medições feitas por dois IEDs em cada consumidor de dados, porém você não pode comparar os dados em um dispositivo e fornecer os resultados a todos os outros dispositivos interessados.

As bases de dados distribuídas também requerem que você acesse a rede para poder acessar dados. É difícil criar um pequeno subconjunto de dados que esteja disponível para acesso de dados por discagem ou envio discado automático, sem inclusão de um dispositivo ou processo dedicado para essa função.

A sua rede também terá significativamente mais tráfego se você usar uma base de dados distribuída. Cada consumidor de dados tem de coletar dados de cada dispositivo. O overhead de mensagens envolvido nas conversações pode facilmente ficar maior do que a quantidade de dados servida.

IHM Local

Os protocolos simples de troca de dados do conjunto TCP/IP não são adequados para coleta de dados da IHM. Você pode usar o UCA2 ou o DNP 3.00 como o protocolo de troca de dados entre a sua IHM e os IEDs da subestação. Com o UCA2 ou o DNP 3.00, você precisa de um “driver” ou software especial de comunicações para coletar dados dos IEDs e disponibilizá-los para o software da IHM. Você está usando um sistema operacional Windows, este link é tipicamente Troca de Dados Dinâmica (DDE) ou Ole for Process Control (OPC).

Quando você usa um browser MMS com IED UCA2, você pode pesquisar o IED para determinar os dados que estão disponíveis e em alguns casos copiar e colar uma referência no

software de sua IHM. Este processo é rápido e simples para alguns pontos, porém para uma base dados típica de subestação de 500 a 1000 pontos, você deve considerar o uso de técnicas automatizadas para criar a base de dados da IHM, incluindo referências a dados de IED.

SCADA

A Ethernet para coleta de dados SCADA em tempo real não é prática em larga escala se você está usando comunicações diretas com cada IED. Por exemplo, uma concessionária com 50 subestações com 50 IEDs em cada subestação tem um total de 2500 IEDs. Projetando uma estrutura de WAN e adquirindo um master suficientemente poderoso para conduzir 2500 conversações simultâneas (ao invés das 50 exigidas pelas tradicionais instalações SCADA) fica muito caro. Como ocorre com os dados IHM, o overhead da comunicação da solução de base de dados distribuída rapidamente se torna maior do que a quantidade de dados que você gostaria de transmitir.

O UCA2 tem uma solução potencial para este dilema. O protocolo ICCP utilizado com uma robusta base de dados de subestação centralizada pode proporcionar uma maneira prática de se utilizar as redes Ethernet para coleta de dados SCADA. Atualmente, há muito pouco suporte para ICCP nas estações mestras.

O DNP 3.00 foi projetado para telecontrole e, semelhantemente ao GOMSFE, não é prático para aplicações de base de dados distribuída, porém é razoável para arquiteturas que utilizam bases de dados de subestação centralizada.

CONCLUSÕES

1. A Ethernet não foi projetada para redes de subestações, porém será aplicada em muitas subestações. A popularidade e a familiaridade das redes Ethernet impulsionarão as pessoas para achar soluções para problemas através da utilização das redes Ethernet em subestações.

2. As técnicas de instalação e equipamentos dimensionados para escritórios não são adequados para uso em subestações. Você pode usar equipamento Ethernet que seja mais robusto, porém mediante custo adicional.

3. A mídia física de fibra ótica é mais cara, porém pode ser utilizada sem as restrições impostas pelo cabo metálico. Os cabos de fibra ótica proporciona melhoria da segurança do pessoal, melhor proteção ao equipamento e maior imunidade à ruídos.

4. Uma topologia de barramento simples não aborda todos os requisitos para redes de subestações e não reflete a construção efetiva da rede. Criar diagramas de topologia que mostrem todos os componentes vitais na sua topologia de modo que possa entender quais equipamentos são críticos para a operação da rede.

5. As redes Ethernet não proporcionam sincronismo de tempo adequado para os IEDs das subestações. Componentes adicionais podem fornecer essa função.

6. Considere se a sua solução utiliza uma arquitetura de base de dados distribuída ou centralizada e desenhe os caminhos de dados da maneira apropriada.

7. Mensagens peer-to-peer através das redes Ethernet podem não proporcionar segurança e velocidade adequadas para a sua aplicação. Considere as questões de carga e confiabilidade da rede e administre o carregamento da rede ao longo da vida da mesma.

8. As conexões para as redes que são conectadas à rede da sua subestação podem proporcionar um trajeto para invasão da rede da SE.

9. Mensagens peer-to-peer para coordenação da proteção para um ponto situado fora do local são mais seguras, mais confiáveis e menos onerosas se forem implementadas utilizando comunicação serial direta.

10. As redes Ethernet proporcionam uma boa conexão para coleta de dados da engenharia dos IEDs para os terminais da engenharia em locais remotos.

REFERÊNCIAS

[1] C. Spurgeon, *Ethernet: The Definitive Guide*, O'Reilly and Associates, 2000.

[2] B. Baccala, editor, *Connected: An Internet Encyclopedia*, Third Edition http://www.freesoft.org/CIE/index.htm, April 1997.

[3] B. Lounsbury, et al., "Surviving the Industrial Environment." Proceedings of the ISA Technical Conference on Industrial Ethernet, Cleveland, OH, May 25, 2000.

[4] B. Whetten, S. Steinberg, D. Ferrari, "The Packet Starvation Effect in CSMA/CD LANs and a Solution," University of California at Berkeley.

[5] D. Woodward and D. Tao, "Comparing Throughput of Substation Networks." Proceedings of the Second Annual Western Power Delivery and Automation Conference, Spokane, WA, April 3–6, 2000.

[6] "Web Site Reference Library," http://www.lex-con.com/refer.htm, Lexicon Consulting.

[7] KC Associates, "UCA2: Generic Object Models for Substation & Feeder Equipment," Version 0.91, EPRI, February 5, 2000.

[8] M. Thesing, "Transporting DNP V3.00 Over Local And Wide Area Networks," Version 1.0, DNP User's Group, December 1998.

[9] R. Gwizdak and J. Moyne, "Object Messaging Specification for the Modbus/TCP Protocol," Version 1.0, Groupe Schneider, April 7, 1999.

[10] CEI IEC 834 International Standard, Performance and Testing of Teleprotection Equipment of Power Systems, International Electrotechnical Commission, 1988.

[11] G. W. Scheer and D. A. Woodward, "Speed and Reliability of Ethernet Networks for Teleprotection and Control." Proceedings of the 3rd Annual Western Power Delivery Automation Conference, April 10–12, 2001.

[12] G. W. Scheer and D. J. Dolezilek, "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks." Proceedings of the Second Annual Western Power Delivery and Automation Conference, Spokane, WA, April 3–6, 2000.

BIOGRAFIA

Darold Woodward recebeu um B.S. em Engenharia Elétrica da *Washington State University*. Ele é membro da *Instrument Society of America* (ISA). Ingressou na Schweitzer Engineering Laboratories em 1998 na posição de Engenheiro de Integração de Sistemas. Trabalhou na empresa de consultoria HDR Inc. durante seis anos, onde participou do desenvolvimento e comissionamento de projetos de sistemas elétricos, automação e instrumentação de instalações de abastecimento de água, tratamento de águas residuais e hidroelétricas. Antes de ingressar na HDR Inc., ele trabalhou na *R. W. Beck and Associates*, colaborando com o projeto de sistemas elétricos e instrumentação para instalações de subestações, tratamento de águas residuais e hidroelétricas.