

www.apostilastecnicas.com

Copyright 2008 – apostilastecnicas.com

Todos direitos reservados

Introdução

Visão Geral do curso	I
Objetivos do Curso.....	I
Descrição do Curso.....	I
Quem Deve Participar.....	II
Pré-requisitos.....	II
Resumo.....	II

Capítulos

Capítulo 1 – Redes TCP/IP

Introdução.....	1
As Pilhas de Protocolos.....	2
O modelo de pilha de 4 camadas do TCP/IP.....	3
Endereçamento de IP.....	6
Máscara de Sub-rede.....	12
Máscaras complexas.....	14
Máscaras de redes simples.....	16
Máscaras de sub-redes.....	18
Endereço de IP.....	18
Usando o DHCP.....	21
Default Gateway.....	23
Servidor DNS.....	24

Servidor WINS.....	25
Redes Virtuais Privadas.....	26
Comunicação.....	28
Como se processa a comunicação em uma Rede TCP/IP.....	28
Arquiteturas de Redes	30
Topologias Lógicas.....	30
Redes Ethernet.....	30
Pacotes.....	34
Como testar uma rede TCP/IP.....	36

Capítulo 2 – Hardware

Hardware.....	39
Placas de Rede.....	39
Cabeamento.....	42
Cabo Coaxial.....	42
Cabo Coaxial Fino (10 base 2).....	43
Cabo Coaxial Grosso (10 base 5).....	46
Cabo Par Trançado.....	47
Par Trançado X Coaxial.....	55
Fibra Ótica.....	57
Topologias.....	60
Topologia Linear.....	60
Topologia em Anel.....	62
Topologia em Estrela.....	63
Periféricos.....	65
Repetidor.....	65
Ponte (Bridge).....	66
Hub (Concentrador).....	68
Hub Inteligente.....	69

Visão geral do Curso

Objetivo do Curso : Concluindo o treinamento em *Rede Ethernet - Configuração*, o participante será capaz de colocar em operação uma rede Ethernet bem como realizar sua manutenção, possuindo os conhecimentos necessários para:

- Conectar-se à rede Ethernet
- Localizar falhas
- Configurar os controladores CLP-5, SLC-500 ou ControlLogix através de seus softwares de programação
- Configurar o software de comunicação RSLinx para rede Ethernet.

Descrição do curso : O treinamento em *Rede Ethernet - Configuração* foi desenvolvido para capacitar os participantes no processo de planejamento e configuração de uma rede Ethernet. Ao longo do curso, serão apresentados os principais dispositivos que compõe uma rede Ethernet como HUB's, roteadores, transceivers, repetidores, switches e gateways. Serão abordados também as classes de redes existentes, os tipos de cabeamentos e onde utilizar cada um.

A fim de capacitar o participante a integrar uma rede Ethernet ao nível produtivo, será abordada também a configuração do canal de comunicação Ethernet do controlador CLP-5, SLC-500 ou ControlLogix utilizando o software RSLogix5, RSLogix500 ou RSLogix5000 e sua comunicação com o microcomputador através do software RSLinx.

Quem deve participar ? Devem participar deste treinamento as pessoas que necessitam de capacitação para a implementação ou são responsáveis pela manutenção e localização de falhas em uma rede Ethernet.

Pré-requisitos : A fim de absorver ao máximo os conhecimentos demonstrados durante o treinamento, o participante deve possuir:

- Familiaridade na operação do ambiente Windows 95/98, Windows NT ou Windows 2000/XP.
- Conhecimentos básicos em CLP-5, SLC-500 ou ControlLogix
- Conhecimentos básicos do software RSLogix 5, RSLogix 500 ou RSLogix 5000

Resumo : Este curso consiste nos seguintes capítulos:

- Arquitetura de Redes TCP/IP
- Hardware
- Configurando a comunicação em Ethernet
- Exercícios

Redes TCP/IP

Introdução

No mundo de hoje, não se pode falar de redes sem falar do TCP/IP. O conjunto de protocolos originalmente desenvolvido pela Universidade da Califórnia em Berkeley, sob contrato para o Departamento de Defesa dos EUA, se tornou o conjunto de protocolos padrão das redes locais e remotas, suplantando conjuntos de protocolos bancados por pesos pesados da indústria, como a IBM (SNA), Microsoft (NetBIOS/NetBEUI) e Novell (IPX/SPX).

O grande motivo de todo este sucesso foi justamente o fato do TCP/IP não ter nenhuma grande empresa associada ao seu desenvolvimento. Isto possibilitou a sua implementação e utilização por diversas aplicações em praticamente todos os tipos de hardware e sistemas operacionais existentes.

Mesmo antes do boom da Internet o TCP/IP já era o protocolo obrigatório para grandes redes, formadas por produtos de muitos fornecedores diferentes, e havia sido escolhido pela Microsoft como o protocolo preferencial para o Windows NT, devido às limitações técnicas do seu próprio conjunto de protocolos, o NetBEUI.

Entretanto, ao contrário dos protocolos proprietários para redes locais da Microsoft e da Novell, que foram desenhados para serem praticamente "plug and play", as necessidades que orientaram o desenvolvimento do TCP/IP obrigaram ao estabelecimento de uma série de parametrizações e configurações que devem ser conhecidas pelo profissional envolvido com instalação, administração e suporte de redes.

As Pilhas de Protocolos

Quem já estudou mais a fundo a documentação de produtos de redes ou participou de cursos mais específicos certamente se deparou com o "Modelo OSI de 7 Camadas". Todos os softwares de redes são baseados em alguma arquitetura de camadas, e normalmente nos referimos a um grupo de protocolos criado para funcionar em conjunto como uma pilha de protocolos (em inglês, protocol stack, por exemplo the TCP/IP stack). O termo "pilha" é utilizado porque os protocolos de uma dada camada normalmente interagem somente com os protocolos das camadas imediatamente superior e inferior.

Entretanto, o Modelo OSI é uma modelo conceitual, e não a arquitetura de uma implementação real de protocolos de rede. Mesmo os protocolos definidos como padrão oficial pelo ISO - International Standards Organization - a entidade criadora do modelo OSI, não foram projetados e construídos segundo este modelo.

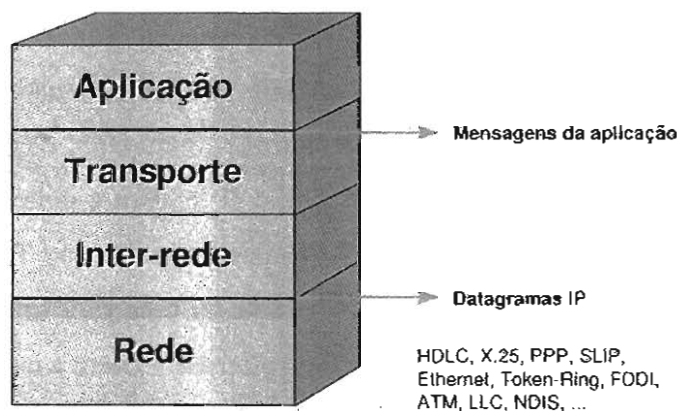
O modelo de pilha de 4 camadas do TCP/IP

O TCP/IP foi desenhado segundo uma arquitetura de pilha, onde diversas camadas de software interagem somente com as camadas acima e abaixo. Há diversas semelhanças com o modelo conceitual OSI da ISO, mas o TCP/IP é anterior à formalização deste modelo e portanto possui algumas diferenças.

O nome TCP/IP vem dos nomes dos protocolos mais utilizados desta pilha, o IP (Internet Protocol) e o TCP (Transmission Control Protocol). Mas a pilha TCP/IP possui ainda muitos outros protocolos, dos quais veremos apenas os mais importantes, vários deles necessários para que o TCP e o IP desempenhem corretamente as suas funções.

Visto superficialmente, o TCP/IP possui 4 camadas, desde as aplicações de rede até o meio físico que carrega os sinais elétricos até o seu destino:

4. Aplicação (Serviço)	FTP, TELNET, LPD, HTTP, SMTP/POP3, NFS, etc.
3. Transporte	TCP, UDP
2. Inter-Rede	IP
1. Rede	Ethernet, PPP, SLIP



Além das camadas propriamente ditas, temos uma série de componentes, que realizam a interface entre as camadas:

Aplicação / Transporte	DNS, Sockets
Rede / Enlace	ARP, DHCP

Vamos apresentar agora uma descrição da função de cada camada do TCP/IP:

1. O protocolo de rede tem a função de fazer com que informações sejam transmitidas de um computador para outro em uma mesma mídia de acesso compartilhado (também chamada de rede local) ou em uma ligação ponto-a-ponto (ex: modem). Nada mais do que isso. A preocupação destes protocolos é permitir o uso do meio físico que conecta os computadores na rede e fazer com que os bytes enviados por um computador cheguem a um outro computador diretamente desde que haja uma conexão direta entre eles.
2. Já o protocolo de Inter-Rede, o Internet Protocol (IP), é responsável por fazer com que as informações enviadas por um computador cheguem a outros computadores mesmo que eles estejam em redes fisicamente distintas, ou seja, não existe conexão direta entre eles. Como o próprio nome (Inter-net) diz, o IP realiza a conexão entre redes. É ele quem traz a capacidade da rede TCP/IP se "reconfigurar" quando uma parte da rede está fora do ar, procurando um caminho (rota) alternativo para a comunicação.

3. Os protocolos de transporte mudam o objetivo, que era conectar dois equipamentos, para conectar dois programas. Você pode ter em um mesmo computador vários programas trabalhando com a rede simultaneamente, por exemplo um browser da Web e um leitor de e-mail. Da mesma forma, um mesmo computador pode estar rodando ao mesmo tempo um servidor Web e um servidor POP3. Os protocolos de transporte (UDP e TCP) atribuem a cada programa um número de porta, que é anexado a cada pacote de modo que o TCP/IP saiba para qual programa entregar cada mensagem recebida pela rede.

4. Finalmente os protocolos de aplicação são específicos para cada programa que faz uso da rede. Desta forma existe um protocolo para a conversação entre um servidor web e um browser web (HTTP), um protocolo para a conversação entre um cliente Telnet e um servidor (daemon) Telnet, e assim em diante. Cada aplicação de rede tem o seu próprio protocolo de comunicação, que utiliza os protocolos das camadas mais baixas para poder atingir o seu destino.

Existem dois protocolos de transporte no TCP/IP. O primeiro é o UDP, um protocolo que trabalha com datagramas, que são mensagens com um comprimento máximo pré-fixado e cuja entrega não é garantida. Caso a rede esteja congestionada, um datagrama pode ser perdido e o UDP não informa as aplicações desta ocorrência. Outra possibilidade é que o congestionamento em uma rota da rede possa fazer com que os pacotes cheguem ao seu destino em uma ordem diferente daquela em que foram enviados. O UDP é um protocolo que trabalha sem estabelecer conexões entre os softwares que estão se comunicando.

Já o TCP é um protocolo orientado a conexão. Ele permite que sejam enviadas mensagens de qualquer tamanho e cuida de quebrar as mensagens em pacotes que possam ser enviados pela rede. Ele também cuida de rearrumar os pacotes no destino e de retransmitir qualquer pacote que seja perdido pela rede, de modo que o destino receba a mensagem original, da maneira como foi enviada.

Endereçamento IP

Dentro de uma rede TCP/IP, cada micro recebe um endereço IP único que o identifica na rede. Um endereço IP é composto de uma seqüência de 32 bits, divididos em 4 grupos de 8 bits cada. Cada grupo de 8 bits recebe o nome de octeto.

Veja que 8 bits permitem 256 combinações diferentes. Para facilitar a configuração dos endereços, usamos então números de 0 a 255 para representar cada octeto, formando endereços como 220.45.100.222, 131.175.34.7 etc. Muito mais fácil do que ficar decorando binários.

O endereço IP é dividido em duas partes. A primeira identifica a rede à qual o computador está conectado (necessário, pois numa rede TCP/IP podemos ter várias redes conectadas entre si, veja o caso da Internet) e a segunda identifica o computador (chamado de host) dentro da rede.

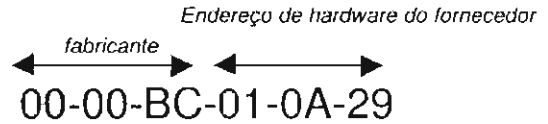
Obrigatoriamente, os primeiros octetos servirão para identificar a rede e os últimos servirão para identificar o computador em si. Como temos apenas 4 octetos, esta divisão limitaria bastante o número de endereços possíveis. Se fosse reservado apenas o primeiro octeto do endereço por exemplo, teríamos um grande número de hosts, mas em compensação poderíamos ter apenas 256 sub-redes. Mesmo se reservássemos dois octetos para a identificação da rede e dois para a identificação do host, os endereços possíveis seriam insuficientes.

Para permitir uma gama maior de endereços, os desenvolvedores do TPC/IP dividiram o endereçamento IP em cinco classes, denominadas A, B, C, D, e E, sendo que apenas as três primeiras são usadas para fins de endereçamento. Cada classe reserva um número diferente de octetos para o endereçamento da rede:

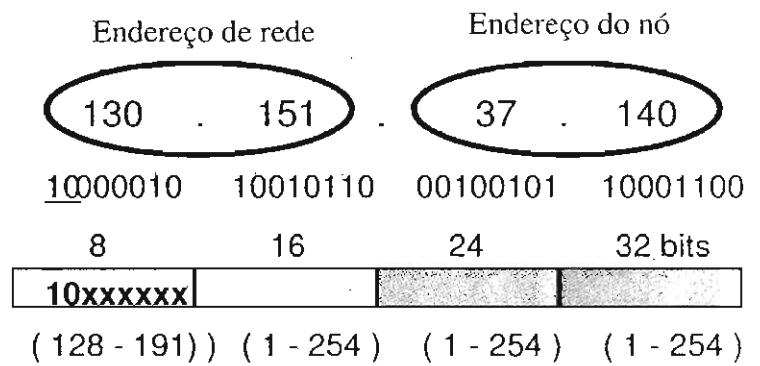
Na classe A, apenas o primeiro octeto identifica a rede, na classe B são usados os dois primeiros octetos e na classe C temos os três primeiros octetos reservados para a rede e apenas o último reservado para a identificação dos hosts.

O que diferencia uma classe de endereços da outra, é o valor do primeiro octeto. Se for um número entre 1 e 126 (como em 113.221.34.57) temos um endereço de classe A. Se o valor do primeiro octeto for um número entre 128 e 191, então temos um endereço de classe B (como em 167.27.135.203) e, finalmente, caso o primeiro octeto seja um número entre 192 e 223 teremos um endereço de classe C:

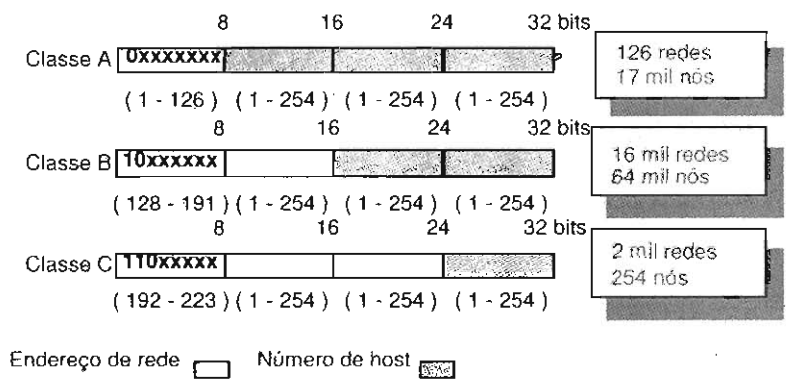
Todos os dispositivos capazes de se comunicar via Ethernet possuem um único **endereço de hardware**. Este pode ser encontrado em uma etiqueta no próprio dispositivo.

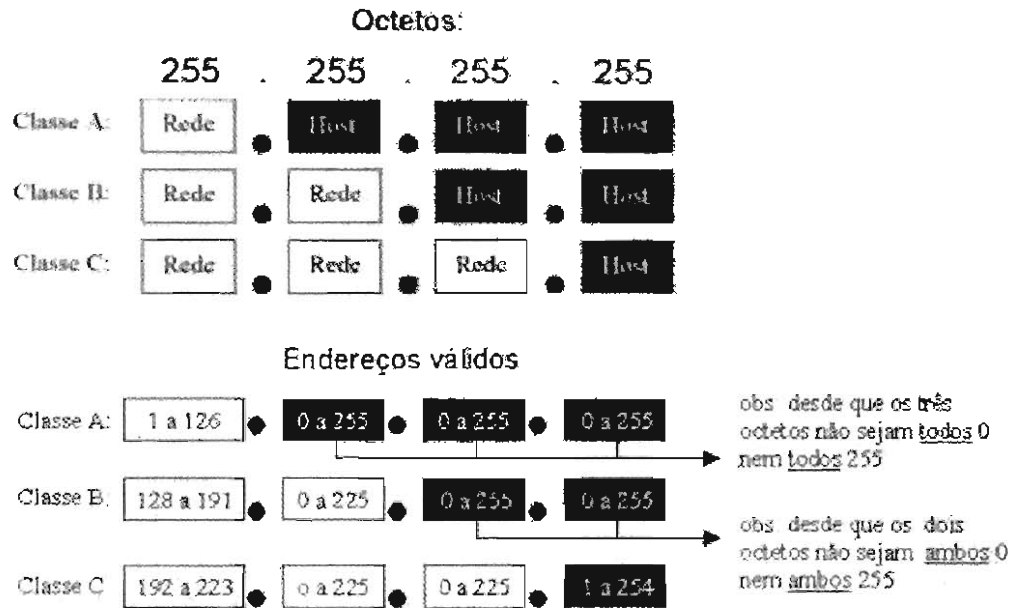


Um software ou endereço de IP (32 bits) é necessário para que um dispositivo pertença a rede.



Se dispositivos Ethernet vão comunicar através da Internet com outros dispositivos, é essencial para a configuração do endereço de IP, estar conforme o esquema abaixo:





Ao implantar uma rede TCP/IP você deverá analisar qual classe de endereços é a mais adequada, baseando-se no número de nós da rede. Veja que, com um endereço classe C, é possível endereçar apenas 254 nós de rede; com um endereço B já é possível endereçar até 65,534 nós, sendo permitidos até 16,777,214 nós usando endereços classe A. Claro que os endereços de classe C são muito mais comuns. Se você alugar um backbone para conectar a rede de sua empresa à Internet, muito provavelmente irá receber um endereço IP classe C, como 203.107.171.x, onde 203.107.171 é o endereço de sua rede dentro da Internet, e o "x" é a faixa de 254 endereços que você pode usar para identificar seus hosts. Veja alguns exemplos de endereços TCP/IP válidos:

Classe A:	105.206.56.185	45.210.173.98	124.186.45.190	89.42.140.202
Classe B:	134.65.108.207	189.218.34.100	156.23.219.45	167.45.208.99
Classe C:	222.45.198.205	196.45.32.145	218.23.108.45	212.23.187.98

Como você deve ter notado, nem todas as combinações de valores são permitidas. Alguns números são reservados e não podem ser usados em sua rede. Veja agora os endereços IPs inválidos:

Endereço inválido	Porque?
0.xxx.xxx.xxx	Nenhum endereço IP pode começar com zero, pois o identificador de rede 0 é utilizado para indicar que se está na mesma rede, a chamada rota padrão.
127.xxx.xxx.xxx	Nenhum endereço IP pode começar com o número 127, pois este número é reservado para testes internos, ou seja, são destinados à própria máquina que enviou o pacote. Se por exemplo você tiver um servidor de SMTP e configurar seu programa de e-mail para usar o servidor 127.0.0.1 ele acabará usando o próprio servidor instalado máquina
255.xxx.xxx.xxx xxx.255.255.255 xxx.xxx.255.255	Nenhum identificador de rede pode ser 255 e nenhum identificador de host pode ser composto apenas de endereços 255, seja qual for a classe do endereço. Outras combinações são permitidas, como em 65.34.255.197 (num endereço de classe A) ou em 165.32.255.78 (num endereço de classe B).
xxx.0.0.0 xxx.xxx.0.0	Nenhum identificador de host pode ser composto apenas de zeros, seja qual for a classe do endereço. Como no exemplo anterior, são permitidas outras combinações como 69.89.0.129 (classe A) ou 149.34.0.95 (classe B)
xxx.xxx.xxx.255 xxx.xxx.xxx.0	Nenhum endereço de classe C pode terminar com 0 ou com 255, pois como já vimos, um host não pode ser representado apenas por valores 0 ou 255. Os endereços xxx.255.255.255 , xxx.xxx.255.255 e xxx.xxx.xxx.255 são sinais de broadcast que são destinados simultaneamente à todos os computadores da rede. Estes endereços são usados por exemplo numa rede onde existe um servidor DHCP, para que as estações possam receber seus endereços IP cada vez que se conectam a rede.

Se você não pretender conectar sua rede à Internet, você pode utilizar qualquer faixa de endereços IP válidos e tudo irá funcionar sem problemas. Mas, a partir do momento em que você resolver conectá-los à Web os endereços da sua rede poderá entrar em conflito com endereços já usados na Web.

Para resolver este problema, basta utilizar uma das faixas de endereços reservados. Estas faixas são reservadas justamente ao uso em redes internas, por isso não são roteadas na Internet.

As faixas de endereços reservados mais comuns são 10.x.x.x e 192.168.x.x, onde respectivamente o 10 e o 192.168 são os endereços da rede e o endereço de host pode ser configurado da forma que desejar.

O ICS do Windows usa a faixa de endereços 192.168.0.x. Ao compartilhar a conexão com a Web utilizando este recurso, você simplesmente não terá escolha. O servidor de conexão passa a usar o endereço 192.168.0.1 e todos os demais micros que forem ter acesso à Web devem usar endereços de 192.168.0.2 a 192.168.0.254, já que o ICS permite compartilhar a conexão entre apenas 254 PCs.

O default em muitos sistemas é 192.168.1.x, mas você pode usar os endereços que quiser. Se você quiser uma faixa ainda maior de endereços para a sua rede interna, é só apelar para a faixa 10.x.x.x, onde você terá à sua disposição mais de 12 milhões de endereços diferentes.

Veja que usar uma destas faixas de endereços reservados não impede que os PCs da sua rede possam acessar a Internet, todos podem acessar através de um servidor proxy.

Máscara de sub-rede

Ao configurar o protocolo TPC/IP, seja qual for o sistema operacional usado, além do endereço IP é preciso informar também o parâmetro da máscara de sub-rede, ou “subnet mask”. Ao contrário do endereço IP, que é formado por valores entre 0 e 255, a máscara de sub-rede é formada por apenas dois valores: 0 e 255, como em 255.255.0.0 ou 255.0.0.0. onde um valor 255 indica a parte endereço IP referente à rede, e um valor 0 indica a parte endereço IP referente ao host.

A máscara de rede padrão acompanha a classe do endereço IP: num endereço de classe A, a máscara será 255.0.0.0, indicando que o primeiro octeto se refere à rede e os três últimos ao host. Num endereço classe B, a máscara padrão será 255.255.0.0, onde os dois primeiros octetos referem-se à rede e os dois últimos ao host, e num endereço classe C, a máscara padrão será 255.255.255.0 onde apenas o último octeto refere-se ao host

Ex. de endereço IP	Classe do Endereço	Parte referente à rede	Parte referente ao host	Mascara de sub-rede padrão
98.158.201.128	Classe A	98.	158.201.128	255.0.0.0 (rede.host.host.host)
158.208.189.45	Classe B	158.208.	189.45	255.255.0.0 (rede.rede.host.host)
208.183.34.89	Classe C	208.183.34.	89	255.255.255.0 (rede.rede.rede.host)

Para que servem as máscaras de sub-rede? Apesar das máscaras padrão acompanharem a classe do endereço IP, é possível “mascarar” um endereço IP, mudando as faixas do endereço que serão usadas para endereçar a rede e o host. O termo “máscara de sub-rede” é muito apropriado neste caso, pois a “máscara” é usada apenas dentro da sub-rede.

Por exemplo o endereço 208.137.106.103. Por ser um endereço de classe C, sua máscara padrão seria 255.255.255.0, indicando que o último octeto refere-se ao host, e os demais à rede. Porém, se mantivéssemos o mesmo endereço, mas alterássemos a máscara para 255.255.0.0 apenas os dois primeiros octetos (208.137) continuariam representando a rede, enquanto o host passaria a ser representado pelos dois últimos (e não apenas pelo último).

Ex. de endereço IP	Máscara de sub-rede	Parte referente à rede	Parte referente ao host
208.137.106.103	255.255.255.0 (padrão)	208.137.106.	103
208.137.106.103	255.255.0.0	208.137.	106.103
208.137.106.103	255.0.0.0	208.	137.106.103

Veja que 208.137.106.103 com máscara 255.255.255.0 é diferente de 208.137.106.103 com máscara 255.255.0.0: enquanto no primeiro caso temos o host 103 dentro da rede 208.137.106, no segundo caso temos o host 106.103 dentro da rede 208.137.

Dentro de uma mesma sub-rede, todos os hosts deverão ser configurados com a mesma máscara de sub-rede, caso contrário poderão não conseguir comunicar-se, pois pensarão estar conectados a redes diferentes. Se, por exemplo, houverem dois micros dentro de uma mesma sub-rede, configurados com os endereços 200.133.103.1 e 200.133.103.2 mas configurados com máscaras diferentes, 255.255.255.0 para o primeiro e 255.255.0.0 para o segundo, teremos um erro de configuração

Máscaras complexas

Até agora vimos apenas máscaras de sub-rede simples. Porém o recurso mais refinado das máscaras de sub-rede é quebrar um octeto do endereço IP em duas partes, fazendo com que dentro de um mesmo octeto, tenhamos uma parte que representa a rede e outra que representa o host.

Este conceito é um pouco complicado, mas em compensação, pouca gente sabe usar este recurso, por isso vele à pena fazer um certo esforço para aprender.

Configurando uma máscara complexa, precisaremos configurar o endereço IP usando números binários e não decimais. Para converter um número decimal em um número binário, você pode usar a calculadora do Windows. Configure a calculadora para o modo científico (exibir/científica) e verá que do lado esquerdo aparecerá um menu de seleção permitindo (entre outros) encolher entre decimal (dec) e binário (bin).