

2010

Guia do TCP/IP

Entendendo o IPv4 e IPv6

3ª Edição

Daniel Donda
Mcsolution.com
01/10/2010



Sumário

O IPv4	2
Sobre este documento	2
Um pouco da história do IP	2
O Endereçamento IP	3
Controle dos IPs na Internet	5
Entendendo números binários.....	7
De binário para decimal:	7
Conversão de decimal para binário.....	8
Classes de Endereços	8
Classe A	9
Classe B.....	9
Classe C.....	10
Endereços de rede privados.....	11
Identificando o endereço de rede através do operador lógico “AND”	11
Classless Inter-Domain Routing.....	12
Compreendendo o CIDR.....	13
O IPv6	17
Tipo de endereço IPv6.....	18
Unicast.....	18
Multicast.....	19
Anycast	19
Format Prefix (FP).....	19
Global Unicast	20
Link-Local ou Site-Local	20
Unique-Local	21
Endereço Privado da rede local.....	21
Ambiente misto IPv4 e IPv6	22
IPv4-compatible address.....	22
IPv4-mapped address.....	22
6to4	22
ISATAP	22

TEREDO.....	22
Endereços especiais	22
Endereço não especificado	22
Endereço de auto retorno (LoopBack)	23
O sistema Hexadecimal	23
Conversão de Hexadecimal para Decimal.....	23
Configurando o Windows Server 2008 e o Windows 7 para utilizar o IPv6.....	24
Configurando o Servidor Windows Server 2008 R2	24
Configurando o Windows 7.....	26

O IPv4

Sobre este documento

A ideia de criar esse documento surgiu da dificuldade de encontrar informações precisas na Internet. Comecei juntando alguns materiais e em 2000 eu publiquei a primeira versão sobre IPv4. Hoje com as novas tecnologias e lançamentos de sistemas operacionais de rede totalmente compatíveis e prontos para o Ipv6 eu me senti na obrigação de reformular este documento.

Depois de algum tempo tive ainda que alterar pois o IPv6 precisava de uma nova abordagem.

No mundo tecnológico as coisas acontecem muito rápidas e precisamos ter em mão informações de maneira rápida e concisa e este é o propósito desde documento.

Espero que possa ser de grande valia.

Um pouco da história do IP

O “**Department of defense advanced Research Projects Agency – DARPA**” iniciou em 1969 o projeto **ARPANET** autorizado pelo **DOD (Department of Defense)**.

Um projeto destinado a interligar os computadores do governo americano que possuíam diferentes hardwares e sistemas.

O TCP/IP é um conjunto (pilha) de protocolos padrão em redes com Windows 2000 e na Internet.

O TCP/IP é dividido em quatro camadas e em cada camada existem diferentes protocolos exercendo diversas funções

Como no início o modelo de referência OSI de 7 camadas ainda não tinha sido criado o pelo **ISO (International Standards Organization)**. Foi adotado o modelo de 4 camadas conhecido também pelo modelo DARPA.

Camada OSI	Camada TCP/IP	Protocolos
Aplicação	Aplicação	FTP, Telnet, POP3, http...
Apresentação		
Sessão		
Transporte	Transporte	TCP, UDP...
Rede	Internet	IP, ICMP, IGMP, ARP...
Link de dados	Rede	Ethernet, Token Ring, Wi-fi...
Física		

★ **LINK** - Você pode conferir a tabela da **camada OSI** na íntegra, através do link:

<http://www.mcsesolution.com/Grupo-Mcsesolution/posters-tecnicosv10-windows-2008-r2-exchange-2010-e-redes.html>

O Endereçamento IP

RFCs 791, 1122 e 1812

Em uma rede de computadores interligadas fisicamente, cada computador é identificado como **host**.

As placas de rede recebem uma numeração única de fábrica. Essa numeração é o endereço físico chamado MAC (**Media Access Control**). E é composto por seis bytes exibidos na notação hexadecimal.

Exemplo: **00-10-B5-E5-33-11**

Em redes cada host além de possuir um endereço físico possui também um endereço lógico que o identifica em uma rede.

Esse endereço lógico é o endereço IP que por sua vez é dividido em duas partes.

Endereço da rede (**Network ID**) - Identifica a rede no qual o computador faz parte

Endereço do host (**Host ID**) - identifica o endereço do computador nessa rede.

Quando dois computadores estiverem no mesmo **Network ID**, podemos dizer que eles estão no mesmo **segmento** e que são **hosts locais**.
Quando não forem do mesmo segmento serão designados **hosts remotos**.



Na figura 1 podemos notar que existe uma máquina que está com o endereço IP diferente. Esta máquina é um **host remoto**, mesmo estando fisicamente conectada a rede.

Para que essa máquina possa comunicar com as demais (segmento 192.168.2.0)

É necessário um roteador, assim como mostra a seguir:



A maneira mais fácil de entender como funciona a comunicação através do TCP/IP é fazendo uma analogia ao mapa de uma cidade.

Imagine a sua rua e o carteiro deve entregar-lhe uma carta.

Para encontrar a sua casa, os correios usam um sistema de numeração, que é o código de endereçamento postal (CEP) e o número de sua casa.

Assim fica fácil entender, a entrega da carta será no CEP 04578000 e no número 12901.

Da mesma maneira ocorre com os computadores, a entrega de um pacote de dados é entregue em uma rede e em um determinado numero.

Vamos tomar como exemplo o endereço **192.168.2.204**.

192.168.2 seria o CEP e **204** seria o numero da casa.

192.168.2 é o **Network ID** e deve ser completo (ter 32 bits) para identificar a rede, assim ele deve ser completado com zero **192.168.2.0**.

204 é o **Host ID**, ele identifica um computador em uma rede, neste caso na rede 192.168.2.0.

Sem a ajuda de um “**roteador**”, os computadores podem apenas fazer comunicação como os computadores que estão na mesma rede.

Como essas informações já podemos entender de maneira resumida o que é:

- **Unicast** - Quando um computador envia um pacote de dados diretamente para outro computador, basta saber qual é a rede e o numero do host.
- **Multicast** – Quando um grupo selecionado de computadores recebe a mesma informação simultaneamente. (usando um endereço de multicast)
- **Broadcast** – Quando **todos** os computadores em uma rede recebem a mesma informação.
- **Anycast** – Quando os dados são encaminhados para o mais próximo ou o melhor destino na topologia (roteamento)

Mais adiante iremos discutir sobre as classes de endereçamento e então poderemos compreender melhor com quais computadores, determinado host pode se comunicar e como é feita a divisão lógica da rede IP, veremos também que em determinados intervalos de endereço IP, pode haver um numero muito grande de redes e em cada uma dessas redes poucos hosts e vice versa.

Controle dos IPs na Internet

Na internet A **IANA** (*Internet Assigned Numbers Authority*) é responsável pelo controle de todos os números IPs, e atualmente, ela realiza suas operações através da ICANN (Internet Corporation for Assigned Names and Numbers).

Entendendo números binários

Normalmente usamos a notação decimal para representar um endereço de Ipv4.

Exemplo: **192.168.2.200**

Porém um computador ou um ativo de rede (roteador) enxerga o endereço Ipv4 como número binário (32 bits)

32 bits = 4 bytes e esses são separados por pontos.

Um endereço Ipv4 pode ser representado da seguinte forma:

Decimal: 192.168.4.2

Binário: 11000000101010000000010000000010

Para entendermos melhor vamos utilizar a notação binária.

O número IP consiste em um valor de 32 bits, nos quais podem receber dois valores 0 ou 1.

00000000.00000000.00000000.00000000 = 32 bits = 4 bytes = 4 octetos

11111111.11111111.11111111.11111111 = 32 bits = 4 bytes = 4 octetos

Cada oito bits, ou seja, cada octeto pode ir de 0 a 255 em decimal.

(Oito bits podem conter 256 combinações).

A maneira mais prática de calcular números binários para decimal e vice-versa é criar uma tabela de cálculo.

De binário para decimal:

Byte de 8 bits	1	1	1	1	1	1	1	1
Calcule	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valor equivalente	128	64	32	16	8	4	2	1
Valor binário	1	1	1	1	1	1	1	1
Multiplique pelo bit	$128*1$	$64*1$	$32*1$	$16*1$	$8*1$	$4*1$	$2*1$	$1*1$
Some o resultado	$128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 =$							255



Oito bits equivalem a um octeto, que é o mesmo que um byte. Nossa tabela serve apenas para um octeto, o endereço IP possui 4 octetos (32 bits)

Como exemplo, tomaremos um octeto de valor em binário igual 11000000 e somaremos apenas os resultados onde o bit for igual a um (1).

Acompanhe no exemplo a seguir:

Byte de 8 bits	1	1	1	1	1	1	1	1
Calcule	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valor equivalente	128	64	32	16	8	4	2	1
Valor binário	1	1	0	0	0	0	0	0
Multiplique pelo bit	$128 * 1$	$64 * 1$	$32 * 0$	$16 * 0$	$8 * 0$	$4 * 0$	$2 * 0$	$1 * 0$
Some o resultado	128 + 64 =						192	

Conversão de decimal para binário

Para conseguir o valor em binário do número 200, somaremos o valor em decimal equivalente de cada dígito binário da **esquerda para a direita** até encontrar o valor desejado.

Exemplo:

$128 + 64 = 192$ (ainda não deu o valor)

$128 + 64 + 32 = 224$ (passou, então não somaremos o 32, vamos para o próximo).

$128 + 64 + 16 = 208$ (também passou, não somaremos o 16, vamos para o próximo).

$128 + 64 + 8 = 200$ encontramos o valor exato. Agora é só preencher a tabela.

Byte de 8 bits	1	1	1	1	1	1	1	1
Calcule	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valor equivalente	128	64	32	16	8	4	2	1
Some até achar o valor decimal e marque com um X	x	x			x			
Coloque "1" onde existir X e "0" nas demais casas	1	1	0	0	1	0	0	0
O valor binário de 224 é	11001000							

Classes de Endereços

Os endereços IP's são divididos em cinco classes, A, B, C, D e E. iremos estudar apenas as classes A, B e C, pois a classe D é reservada para Broadcast e a classe E para futuras utilizações.

O que define a classe é o primeiro octeto (ou seja, os oito primeiros bits).

Classe	Início binário	Fim binário	1º Octeto (início e fim em decimal)	Bits mais significantes
A	00000001	01111111	1~127	0
B	10000000	10111111	128~191	10
C	11000000	11011111	192~223	110
D	11100000	11101111	224~239	1110
E	11110000	11110111	240~247	11110

👉 127 é um valor reservado para loopback (auto teste). Mas nem por isso deixa de ser classe A.

Determinando a quantidade de redes por classe.

- **Classe A** – Usa apenas o primeiro octeto para identificar a rede e os seguintes 3 octetos (24 bits) para identificar hosts.
- **Classe B** – Usa os dois primeiros octetos para rede e os últimos dois octetos (16 bits) para hosts.
- **Classe C** – Usa os três primeiros octetos para a rede e o último octeto (8 bits) para hosts.

	1º octeto	2º octeto	3º octeto	4º octeto
Classe A	Rede	Host	Host	Host
Classe B	Rede	Rede	Host	Host
Classe C	Rede	Rede	Rede	Host

		Rede	Hosts
Classe A	01111111.00000000.00000000.00000000	8 bits	24 bits (zeros)
Classe B	10111111.11111111.00000000.00000000	16 bits	16 bits (zeros)
Classe C	11011111.11111111.11111111.00000000	24 bits	8 bits (zeros)

Classe A

Usa o primeiro bit para sua identificação (veja tabela 5)

Como na classe A são 8 bits para identificar a rede, e 1 bit é reservado para identificar a classe
 $8-1=7$

Então $2^7 - 2 = 126$ redes

Porque -2 ?

Porque não se usa o 0.x.y.z. e o endereço 127.x.y.z é para auto teste (loopback)

Classe B

Usa os dois primeiros bits para sua identificação

Na classe B são 16 bits para identificar a rede, então 16 bits de rede – 2 bits de identificação da classe = 14

$2^{14} = 16.384$ redes

Porque não – 2 ?

Como o primeiro octeto inicia em 10, não existe a possibilidade de ser tudo 0 ou 1

Classe C

Usa os três primeiros bits para identificar a classe, e 24 bits para identificar a rede.

$3 - 24 = 21$

$2^{21} = 2.097.152$ redes

Como o primeiro octeto inicia em 110, não existe a possibilidade de ser tudo 0 ou 1

A mascara de sub-rede

A Mascara de subrede é um mecanismo usado para distinguir qual parte do endereço IP é destinado a host e qual parte é destinada rede (network).

A mascara de subrede é constituída de uns seguidos de zeros.

- Classe A - define a mascara de subrede é o primeiro octeto
- Classe B - define a mascara de subrede é o primeiro e o segundo octeto
- Classe C - define a mascara de subrede é o primeiro, o segundo e o terceiro octeto.

Exemplo:

Classe	Mascara de subrede	Mascara de subrede em binário.
Classe A	255.0.0.0	11111111.00000000.00000000.00000000
Classe B	255.255.0.0	11111111.11111111.00000000.00000000
Classe C	255.255.255.0	11111111.11111111.11111111.00000000

Tendo essa informação um roteador, por exemplo, não precisa analisar cada bit do endereço IP, basta analisar a mascara de subrede e ele identificara os bits mais significantes.

Com base nessas informações podemos entender a seguinte tabela:

Classe A	1 a 126	255.0.0.0	11111111.00000000.00000000.00000000
Classe B	128 a 191	255.255.0.0	11111111.11111111.00000000.00000000
Classe C	192 a 221	255.255.255.0	11111111.11111111.11111111.00000000

Na mascara de subrede temos a porção que identifica a rede (que sempre será 1) e porção que identifica o host (que sempre será 0).

Classe A = 24 bits.

$$2^{24}-2 = 16.777.214$$

Classe B = 16 bits

$$2^{16}-2 = 65.534$$

Classe C = 8 bits

$$2^8-2 = 254$$

Por que -2?

Porque na mascara de subrede tudo zero é igual ao endereço da rede e tudo um é igual a broadcast.

Endereços de rede privados

- Classe A 10.0.0.0 até 10.255.255.255
- Classe B 172.16.0.0 até 172.31.255.255
- Classe C 192.168.0.0 até 192.168.255.255

Esses endereços acima definidos no RFC 1627 devem ser usados exclusivamente em redes privadas e não devem ser roteados para a Internet. Mesmo que ocorra o roteamento esses endereços serão descartados pelos roteadores da Internet.

Identificando o endereço de rede através do operador lógico “AND”.

Para identificar o endereço de rede é necessário o uso do operador “AND” da álgebra **BOOLEANA** (matemático George Boole 1815-1864) Existem outros operadores "OR", "XOR" e "NOT", mas iremos usar apenas o operador “AND”

Segundo o operador “AND” ou também conhecido como tabela verdade, temos os seguintes valores:



George **Boole** nasceu em
2 de Novembro de 1814

A	B	AB
0	0	0
0	1	0
1	0	0
1	1	1

Para identificar o endereço de rede devemos converter os valores em decimais do endereço IP e da máscara de subrede.

Endereço IP	192.168.2.200	A	11000000.10101000.00000010.11001000
subrede	255.255.255.0	B	11111111.11111111.11111111.00000000
AND		AB	11000000.10101000.00000010.00000000
O resultado da operação "AND" é a identificação da rede = 192.168.2.0			

👉 A comunicação entre redes só é possível quando a identificação de rede de origem for exatamente igual a rede de destino

Classless Inter-Domain Routing

RFCs 1518 e 1519

No início, aproximadamente duas dezenas de redes classe B foram obtidas pelo Brasil, Essas rede foram solicitadas por instituições de ensino e pesquisa diretamente ao Internic. Da USP ao Observatório Nacional, o uso dos endereços de classe B vai de próximo a 10% a menos de 0,1% do número possível de endereços.

A partir de 1993 a Internic passou a distribuir endereços de Classe C, pois seria mais aproveitado que os endereços de classe B.

Com a distribuição de endereços de classe C onde temos mais redes do que hosts, surgiu outro problema. O grande crescimento nas tabelas de roteamento da internet.

Como solução o uso do "**Classless Inter-Domain Routing**".

O Internic respondeu repassando ao Brasil metade do espaço latino-americano, que corresponde hoje a faixa que vai de 200.128.0.0 até 200.255.0.0

Mas o que é esse tal de "Classless Inter-Domain Routing"?

O **Classless Inter-Domain Routing** é a maneira de dividir o endereço IP em endereço de rede e host.

Sendo assim a definição de endereços não é mais determinada pela classe e sim pelos bits que compõe a máscara de sub-rede.

Fornecendo maior flexibilidade e melhor aproveitamento do endereçamento IP, além de diminuir a complexidade nas tabelas de roteamento.

Resumindo o **CIDR** aperfeiçoa a alocação de endereços IP através da divisão em subrede e a combinação de redes.

A combinação de redes é o procedimento de alocar vários endereços em uma única identificação de rede.

Em CIDR não existe mais classe definida e a identificação é feita usando a notação **CIDR** que consiste nos bits uns contínuos da máscara de subrede.

👉 O IPv4 permite 4.294.967.296 endereços IPs

Notação CIDR	Máscara de subrede	Números de Os.	Números de hosts (2 ⁿ -2)
/1	128.0.0.0	31	2.147.486.646
/2	192.0.0.0	30	1.073.741.822
/3	224.0.0.0	29	536.870.910
/4	240.0.0.0	28	268.435.454
/5	248.0.0.0	27	134.217.726
/6	252.0.0.0	26	67.108.862
/7	254.0.0.0	25	33.554.430
/8	255.0.0.0	24	16.777.214
/9	255.128.0.0	23	8.388.606
/10	255.192.0.0	22	4.194.302
/11	255.224.0.0	21	2.097.150
/12	255.240.0.0	20	1.048.574
/13	255.248.0.0	19	524.286
/14	255.252.0.0	18	262.142
/15	255.254.0.0	17	131.070
/16	255.255.0.0	16	65.534
/17	255.255.128.0	15	32.766
/18	255.255.192.0	14	16.382
/19	255.255.224.0	13	8.190
/20	255.255.240.0	12	4.094
/21	255.255.248.0	11	2.046
/22	255.255.252.0	10	1.022
/23	255.255.254.0	9	510
/24	255.255.255.0	8	254
/25	255.255.255.128	7	126
/26	255.255.255.192	6	62
/27	255.255.255.224	5	30
/28	255.255.255.240	4	14
/29	255.255.255.248	3	6
/30	255.255.255.252	2	2
/31	255.255.255.254	1	Não disponível
/32	255.255.255.255	1	Não disponível

Compreendendo o CIDR

Primeira situação:

1) Determinada empresa recebe o endereço IP 132.7.0.0 (classe B) e precisa segmentar a rede em 5 subrede com pelo menos 1.500 hosts por rede.

A empresa não deseja investir em ativos de rede como roteadores.

O que pode ser feito?

Através do CIDR podemos dividir (segmentar) essa rede.

Para isso devemos seguir os seguintes passos.

1. Encontrar a quantidade desejada de subrede
2. Encontrar a quantidade de hosts por subrede.
3. Encontrar o valor incremental.

4. Montar a tabela.

O endereço em questão é um endereço de classe B, portanto tem os dois primeiros octetos (16 bits) para identificação (1s) e esses são “bloqueados” temos os dois octetos (16 bits) restantes para trabalhar (0s).

Para encontrar a quantidade de subrede desejada devemos elevar 2 a quantidade de bits adicionados a mascara de rede padrão.

Trabalhando na mascara de rede temos:

11111111	11111111	00000000	00000000
255.255.0.0			

Dos 0s restantes podemos da esquerda para a direita adicionar bits de redes a fim de encontrar a **quantidade desejada de subrede**.

Vejamos o que acontece:

Binário	11111111	11111111	10000000	00000000
Decimal	255.255.128.0			
$2^1 = 2$	Não é o suficiente.			

Binário	11111111	11111111	11000000	00000000
Decimal	255.255.192.0			
$2^2 = 4$	Não é subrede suficiente precisamos de pelo menos cinco.			

Binário	11111111	11111111	11100000	00000000
Decimal	255.255.224.0			
$2^3 = 8$	Encontramos a quantidade de subrede e ainda sobram três subrede para futura expansão.			

Usando esses três bits encontramos oito possíveis valores. Cada um desses valores representa uma subrede.

0 = 000	RRRRRRR.RRRRRRR.SSSHHHH.HHHHHHHH R = REDE S = SUBREDE H = HOST
1 = 001	
2 = 010	
3 = 011	
4 = 100	
5 = 101	
6 = 110	Em decimal a mascara de subrede ficaria 255.255.224.0. Na notação CIDR seria representada por /19
7 = 111	

b) Ainda falta encontrar a quantidade de hosts por subrede.

O Calculo de hosts por subrede não muda. dois elevados a quantidade de zeros menos dois.
11111111. 11111111. 11100000. 00000000

$2^{13} - 2 = 8.190$ Excelente. Poderíamos adicionar mais bits de rede pra expansão futura ou parar aqui.

c) Devemos agora encontrar o valor incremental para calcular o intervalo de rede.

Pelo nosso calculo a mascara de subrede ficaria 255.255.224.0.

Pegaremos então o valor em decimal do octeto que sofreu alteração e subtrairemos pelos valores possíveis em um octeto que é igual a 256.

```
256
- 224
---
 32
```

32 é o valor incremental usado pelos intervalos de subrede iniciando do 1 até 32, do 32 até 64 até alcançar o valor encontrado de quantidade de redes (6).

Poderíamos também ter feito o seguinte:

Quantidade de subrede	Valor em binário completado com zeros à direita.	Valor em decimal
0	000 00000	0
1	001 00000	32
2	010 00000	64
3	011 00000	96
4	100 00000	128
5	101 00000	160
6	110 00000	192
7	111 00000	224

d) Vejamos na tabela como ficaria:

Sub-redes: 8

Hosts por rede.8190

Rede: 132.7.0.0

Broadcast 132.31.255

Rede	Intervalo		Broadcast
132.7.0.0	132.7.0.1	132.7.31.254	132.7.31.255
132.7.32.0	132.7.32.1	132.7.63.254	132.7.63.255
132.7.64.0	132.7.64.1	132.7.95.254	132.7.95.255
132.7.96.0	132.7.96.1	132.7.127.254	132.7.127.255
132.7.128.0	132.7.128.1	132.7.159.254	132.7.159.255
132.7.160.0	132.7.160.1	132.7.191.254	132.7.191.255
132.7.192.0	132.7.192.1	132.7.223.254	132.7.223.255
132.7.224.0	132.7.224.1	132.7.255.254	132.7.255.255

() O RFC 1878 (Variable Length Subnet Table For IPv4) descreve que podemos usar todas as sub-redes incluindo todos os um's e zero's Segundo o RFC 1879 a pratica de excluir esses valores é obsoleto já que a maioria dos softwares são capazes de utilizar todas as redes definidas.*

Segunda situação:

2) Determinada empresa usa um endereço de rede IP 192.168.1.0 para acomodar seus 250 computadores. A empresa acaba de adquirir mais 1.000 computadores e não deseja investir em equipamentos para comunicação dos 1250 computadores. O que pode ser feito?

Podemos usar uma mascara de rede que acomode todos.

Vejamos:

A rede 192.168.1.0 usa mascara de subrede de classe "C" 255.255.255.0

Em binário 11111111.11111111.11111111.**00000000**
 $2^8 - 2 = 254$

Se roubarmos um bit de rede da classe "C" quantos hosts poderiam existir?
11111111.11111111.11111111.**00000000**
 $2^9 - 2 = 510$ Precisamos alocar 1.250 hosts. Ainda não dá.

Vamos pegar mais um bit de rede. 11111111.11111111.11111111.**00000000**
 $2^{10} - 2 = 1022$

Precisamos alocar 1.250 hosts. Ainda não dá.

Vamos ter que roubar mais um. 11111111.11111111.11111111.**00000000**
 $2^{11} - 2 = 2046$

Precisamos alocar 1.250 hosts. Dá e sobra.

Agora é só pegar esse valor em binário e transformar em decimal.

11111111.11111111.11111111.**00000000**

👉 **255.255.248.0** assim fica é mascara de sub-rede capaz de alocar 2046 hosts.

Mas qual os endereços de redes IPs que podem ser usados ?

Do Octeto que foi alterado somam-se apenas 3 bits, portanto.

$2^3 = 8$ é a quantidade de variações que podem ocorrer no IP.

Veja a tabela:

192.168.0.0	11000000.10101000.00000000.00000000	
255.255.248.0	11111111.11111111.11111000.00000000	
AND	11000000.10101000.00000000.00000000	192.168.0.0 Pode ser usado
192.168.1.0	11000000.10101000.00000001.00000000	
255.255.248.0	11111111.11111111.11111000.00000000	
AND	11000000.10101000.00000000.00000000	192.168.0.0 Pode ser usado
192.168.2.0	11000000.10101000.00000010.00000000	
255.255.248.0	11111111.11111111.11111000.00000000	
AND	11000000.10101000.00000000.00000000	192.168.0.0 Pode ser usado
192.168.3.0	11000000.10101000.00000011.00000000	
255.255.248.0	11111111.11111111.11111000.00000000	
AND	11000000.10101000.00000000.00000000	192.168.0.0 Pode ser usado
192.168.4.0	11000000.10101000.00000100.00000000	
255.255.248.0	11111111.11111111.11111000.00000000	
AND	11000000.10101000.00000000.00000000	192.168.0.0 Pode ser usado
192.168.5.0	11000000.10101000.00000101.00000000	
255.255.248.0	11111111.11111111.11111000.00000000	
AND	11000000.10101000.00000000.00000000	192.168.0.0 Pode ser usado
192.168.6.0	11000000.10101000.00000110.00000000	
255.255.248.0	11111111.11111111.11111000.00000000	
AND	11000000.10101000.00000000.00000000	192.168.0.0 Pode ser usado
192.168.7.0	11000000.10101000.00000111.00000000	
255.255.248.0	11111111.11111111.11111000.00000000	
AND	11000000.10101000.00000000.00000000	192.168.0.0 Pode ser usado
192.168.8.0	11000000.10101000.00001000.00000000	
255.255.248.0	11111111.11111111.11111000.00000000	
AND	11000000.10101000.00001000.00000000	192.168.8.0 Não pode!

O IPv6

Até agora vimos como funciona o endereçamento Ipv4 com seus 32 bits, agora vamos entender o endereçamento do Ipv6 com 128 bits.

O IPv4 pode acomodar $2^{32} = 4.294.967.296$ endereços

O IPv6 pode acomodar $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$ (3,4 x 10^{38}) endereços



Curiosidade: O IPv6 oferece **655.570.793.348.866.943.898.599** (6,5 x 10^{23}) endereços por metro quadrado de superfície terrestre. (será que vai faltar?)

Outra curiosidade- Cada pessoa em 100 bilhões de mundos com 100 bilhões de pessoas tenham 34 quadrilhões de endereços IP e ainda restam 2.8236×10^{33} endereços de IP (Fonte desconhecida)

Um endereço IPV6 é representado pelo sistema numérico HEXADECIMAL. O sistema numérico Hexadecimal possui a base 16.

DEC	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
HEX	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Um endereço IPV6 é constituído de 8 grupos de 16 bits separados por ":"

16bits:16bits:16bits:16bits:16bits:16bits:16bits:16bits

Veja os exemplos de endereço Ipv6.

Endereço completo.

fe80:0000:0000:0000:260:97ff:fefe:9ced

Endereço compactado (os zeros foram compactados)

fe80:0:0:0:260:97ff:fefe:9ced

Onde há uma seqüência de zeros este poderá ser representado por "::", exemplo:

fe80::260:97ff:fefe:9ced No entanto, esta substituição só pode ser feita uma única vez em cada endereço.



Estes são exemplos de um mesmo Ipv6.

Outra notação importante é a divisão dos bits que são de rede e os bits que representam a interface.

Exemplo: 2001:DB8:0:DC00::/54

Neste caso os 54 primeiros bits são de rede e os outros 74 bits são de interface

Tipo de endereço IPv6

No IPv6 foram definidos 3 tipos de endereços:

- Unicast
- Multicast
- Anycast

Unicast

Os endereços Unicast identificam uma única Interface. Assim um pacote que é enviado para um endereço Unicast é entregue em uma única interface.

Ainda existem nos endereços Unicasts os seguintes tipos:

- **Global Unicast** – Igual aos endereços Públicos IPv4
- **Link-Local** – Atribuído Automaticamente – Igual ao APIPA
- **Unique-Local** – Endereço Único similar aos endereços IPv4 privados

- **IPv4 Mapeado em IPv6** – É utilizado para representar um IPv4 como um IPv6 no formato 0:0:0:0:FFFF:wxyz (wxyz=ipv4 em hexa)
- **LoopBack** – Equivalente ao 127.0.0.1 (em IPv6 ::1)
- **Unspecified** – Equivalente ao 0 (em IPv6 ::0)– Indica ausencia de endereço.

Estes serão estudados mais adiante.

Multicast

Os endereços **Multicast** são semelhantes aos endereços **Anycast**, pois identificam um grupo de interfaces pertencentes a diferentes nós.

Os endereços Multicast substituem os endereços de Broadcast

👉 **Não existe broadcast no IPv6**

👉 **Diferente do IPv4 onde multicast é opcional, no IPv6 todos os nós devem ter suporte a Multicast.**

Anycast

Utilizado para identificar um grupo de interfaces pertencentes a nós diferentes.

Este tipo é útil para detectar rapidamente determinados servidores ou serviços como por exemplo o DNS.

Format Prefix (FP)

Esses prefixos identificam os diferentes usos de endereços (sub-rede a qual o endereço pertence).

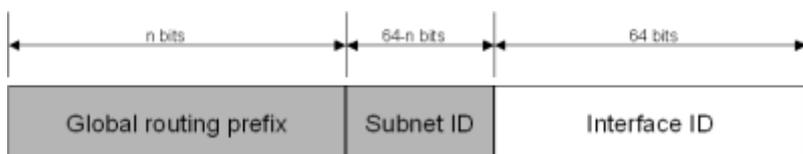
Esse prefixo definido pelos primeiros bits do endereço indica cada tipo de endereço IPv6. O campo variável que compreende esses bits é denominado Format Prefix (FP).

Alocação	Prefixo (binário)	Fração do Espaço de Endereçamento
Reservado	0000 0000	1/256
Reservado para Alocação NSAP	0000 001	1/128
Aggregatable Global Unicast Address *(Endereços globais de difusão ponto a ponto agregáveis)	001	1/8
Site-local Unicast Address (Difusão ponto a ponto de conexões locais)	1111 1110 10	1/1024
Link-local Unicast Address (Difusão ponto a ponto de sites locais)	1111 1110 11	1/1024
Difusão seletiva (Multicast)	1111 1111	1/256

Global Unicast

Endereço público na Internet.

Os endereços globais de difusão ponto a ponto agregáveis, identificados pelo prefixo de formato (FP) 001, são equivalentes aos endereços IPv4 públicos. Eles podem ser roteados e encontrados globalmente na Internet IPv6. Os endereços globais de difusão ponto a ponto agregáveis também são conhecidos como endereços globais.



Link-Local ou Site-Local

Endereço automático (APIPA).

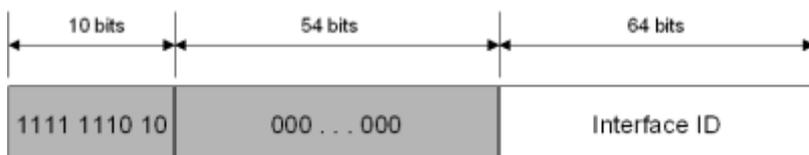
Os endereços de conexões locais são identificados pelo FP 1111 1110 10.

Em uma rede IPv6 de conexão única que não tenha roteador, os endereços de conexões locais são usados para estabelecer a comunicação entres os hosts.

Os endereços de conexões locais equivalem a endereços IPv4 com endereçamento IP particular automático (APIPA) (usando o prefixo 169.254.0.0/16).

Os endereços de conexões locais sempre começam com FE80. Com o identificador de interface de 64 bits, o prefixo dos endereços de conexões locais sempre é FE80::/64.

Um roteador IPv6 nunca encaminha o tráfego de conexão local para fora dos limites da conexão.

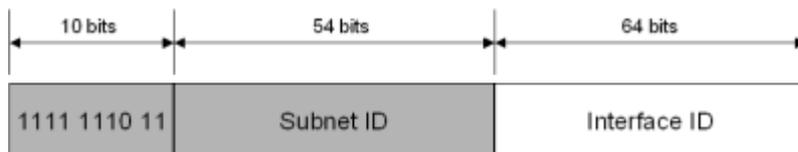


Unique-Local

Endereço Privado da rede local.

Os endereços de sites locais são identificados pelo FP 1111 1110 11 e equivalem ao espaço de endereço particular IPv4 (10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16). Diferente dos endereços de conexões locais, os endereços de sites locais não são configurados automaticamente.

Os primeiros 48 bits são sempre fixos nos endereços de sites locais, começando com FEC0::/48. Depois dos 48 bits fixos a um identificador de subrede de 16 bits (campo Subnet ID) que fornece os 16 bits com os quais você poderá criar subrede em sua organização. Com 16 bits, você pode ter até 65.536 subredes em uma estrutura de subrede simples ou pode subdividir os bits superiores do campo Subnet ID para criar uma infraestrutura de roteamento hierárquica e agregável. Depois do campo Subnet ID, está o campo Interface ID de 64 bits que identifica uma interface específica em uma subrede.



RFC 3879 formalmente reprovava o uso de endereços de sites locais para futuras implementações IPv6.

Portanto:

Para substituir os endereços de sites locais com um novo tipo de endereço privado em uma organização, mas único em todos os sites da organização, a RFC 4193 define os únicos endereços IPv6 unicast locais.

Prefixo FC00::/7

Prefixo globalmente único (com alta probabilidade de ser único);

Utilizado apenas na comunicação dentro de um enlace ou entre um conjunto limitado de enlaces;

Flag Local (L): se o valor for 1 (FD) o prefixo é atribuído localmente. Se o valor for 0 (FC), o prefixo deve ser atribuído por uma organização central (ainda a definir).

Identificador global: identificador de 40 bits usado para criar um prefixo globalmente único. Identificador da Interface: identificador da interface de 64 bits.

Ambiente misto IPv4 e IPv6

IPv4-compatible address

0:0:0:0:0:w.x.y.z – Onde w.x.y.z representa endereços públicos IPv4

Quando o endereço IPv4 compatível é usado como um destino IPv6, o tráfego IPv6 é automaticamente encapsulado com um cabeçalho IPv4 e enviado para o destino, utilizando a infra-estrutura IPv4

IPv4-mapped address

0:0:0:0:FFFF:w.x.y.z o ::FFFF:w.x.y.z - Onde w.x.y.z representa endereços IPv4

O endereço IPv4-mapped nunca é usado como um endereço de origem ou do destino de um pacote IPv6.

6to4

O endereço 6to4 é usado para comunicação entre dois nós IPv4 e IPv6 através da Internet. Você forma o endereço 6to4, combinando o prefixo global 2002:: / 16 com os 32 bits de um endereço IPv4 público, formando um prefixo de 48 bits. 6to4 é uma tecnologia de transição IPv6 descrito na RFC 3056.

ISATAP

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) define endereços ISATAP usados entre dois nós IPv4 e IPv6 em uma intranet privada.

Você pode combinar o ID de interface ISATAP com qualquer prefixo de 64 bits que é válido para endereços IPv6 unicast, incluindo o prefixo de endereço link-local (FE80:: / 64), os prefixos de sites locais e prefixos globais. ISATAP é uma tecnologia de transição IPv6 descrito na RFC 4214.

TEREDO

O endereço Teredo é usado para comunicação entre dois nós execução IPv4 e IPv6 através da Internet, quando um ou ambos os terminais estão localizados atrás de uma rede NAT IPv4. Você forma o endereço Teredo, combinando o prefixo Teredo 2001:: / 32 com o endereço IPv4 público de um servidor Teredo e outros elementos. Teredo é uma tecnologia de transição IPv6 descrito na RFC 4380

Endereços especiais

Endereço não especificado

O endereço não especificado (**0:0:0:0:0:0:0 ou ::**) é usado somente para indicar a ausência de um endereço.

Ele equivale ao endereço IPv4 não especificado 0.0.0.0. O endereço não especificado costuma ser usado como endereço de origem dos pacotes que estão tentando verificar a exclusividade de um endereço de tentativa. O endereço não especificado nunca é atribuído a uma interface ou usado como endereço de destino.

Endereço de auto retorno (LoopBack)

O endereço de auto retorno (**0:0:0:0:0:0:1 ou ::1**) é usado para identificar uma interface de auto retorno. Ele equivale ao endereço de auto-retorno IPv4 127.0.0.1.

No Windows Server 2008 utilize o comando **ping ::1**

O sistema Hexadecimal

Já vimos o sistema binário (base 2) e já sabemos como funciona a base 10 (0-9).

Agora vamos entender como funciona a conversão de hexadecimal para decimal.

Conversão de Hexadecimal para Decimal

O sistema hexadecimal (base 16) é muito simples, vai de 0-9 dígitos mais seis.

DEC	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
HEX	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Assim como a base 10 utiliza a posição para unidades, dezena, centena, etc. o sistema hexadecimal também utiliza "casas".

exemplo:

16^0	16^1	16^2	16^3	16^4	16^n
1	16	256	4096	65536	$16 \times 16 \times 16 \times 16 \times \dots \times 16$

Para entender melhor vamos escolher um numero hexadecimal:

FE80

Escrevendo da direita para a esquerda:

hexa	decimal	casa			
0	0	Primeira	$16^0 \times 0$	= 1×0	=0
8	8	Segunda	$16^1 \times 8$	= 16×8	=128
E	14	Terceira	$16^2 \times 14$	= 256×14	=3584
F	15	quarta	$16^2 \times 15$	= 4096×15	=64440
					=65152

Portanto, o valor hexadecimal FE80 equivale a 65.152 em decimal.

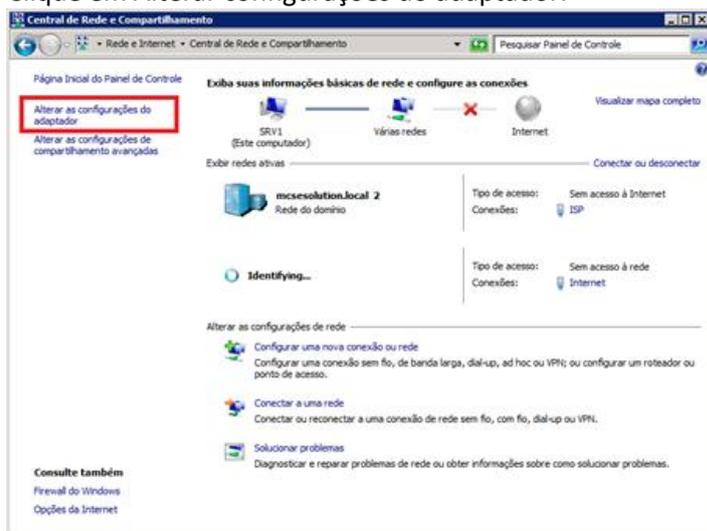
Configurando o Windows Server 2008 e o Windows 7 para utilizar o IPv6

Neste tutorial um servidor Servidor com Windows Server 2008 R2 será configurado com o endereço do tipo Unique-Local FC00::1/7

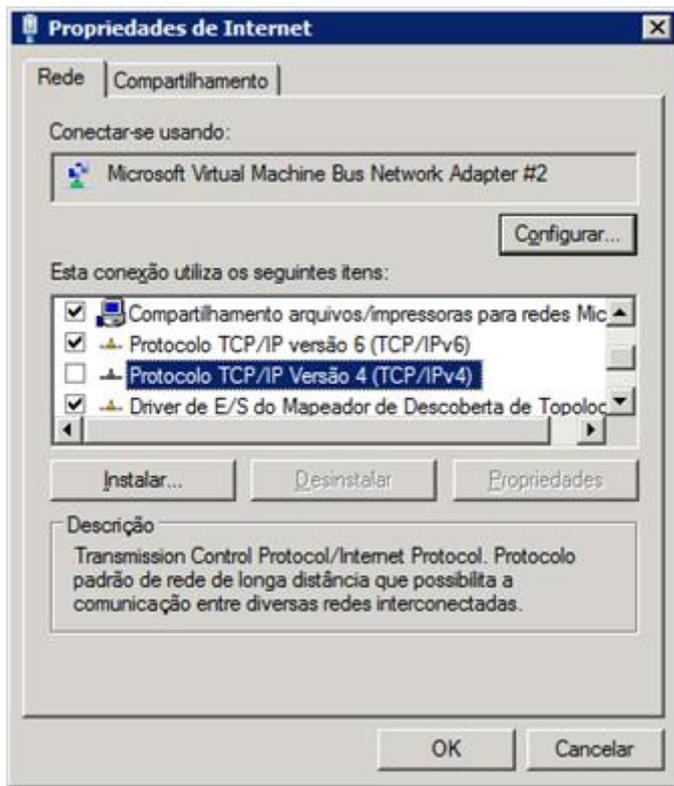
E neste mesmo servidor que possui a Role DNS Server instalado será configurado um registro de recurso AAAA para o cliente que também será configurado com endereço IPv6 FC00::2/7

Configurando o Servidor Windows Server 2008 R2

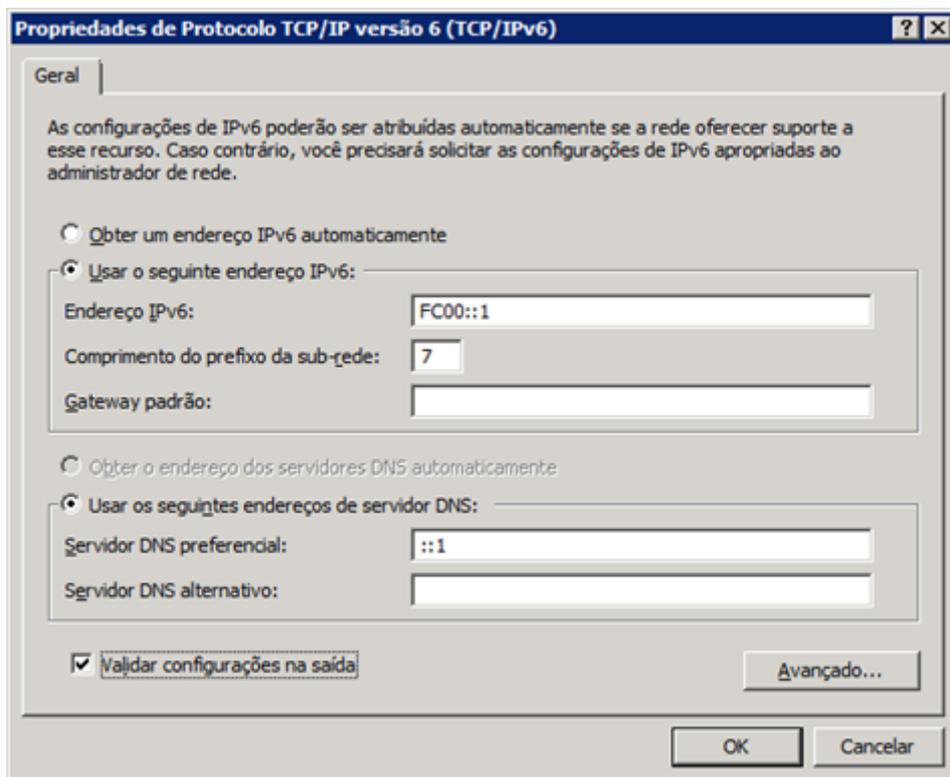
Clique Iniciar\Painel de Controle\Rede e Internet\Central de Rede e Compartilhamento
Clique em Alterar configurações do adaptador.



Clique sobre a placa de rede que deseja configurar e selecione Propriedades:



Desmarque o protocolo TCP/IP Versão 4 e selecione o protocolo TCP/IP versão 6. Clique em propriedades.



Nas propriedades digite o endereço IP **FC00::1**
Em comprimento do prefixo de sub-rede digite **7**.

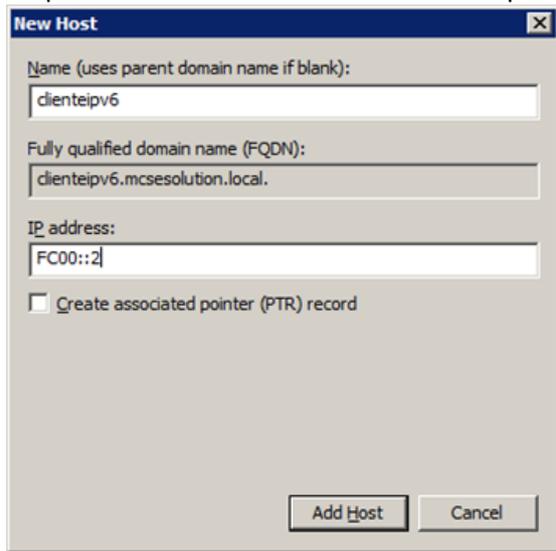
Em servidor DNS digite:

::1 Se a maquina for um servidor DNS para sua rede local.

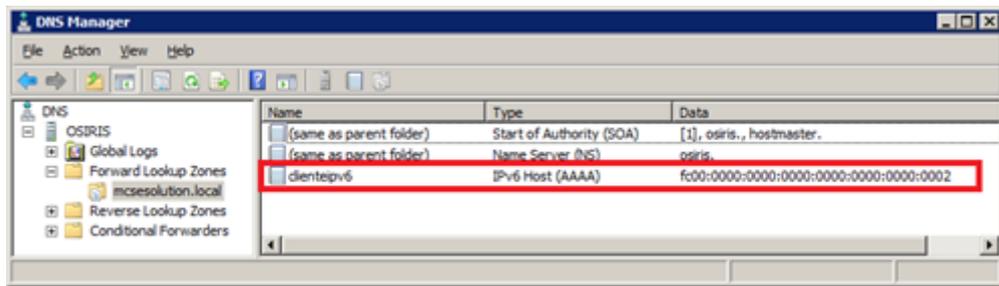
Abra o console do DNS.

Start \Administrative Tools\DNS

Clique com o lado direito em sua zona de pesquisa e selecione criar um HOST A ou AAAA



Clique em ADD HOST



Feche o DNS

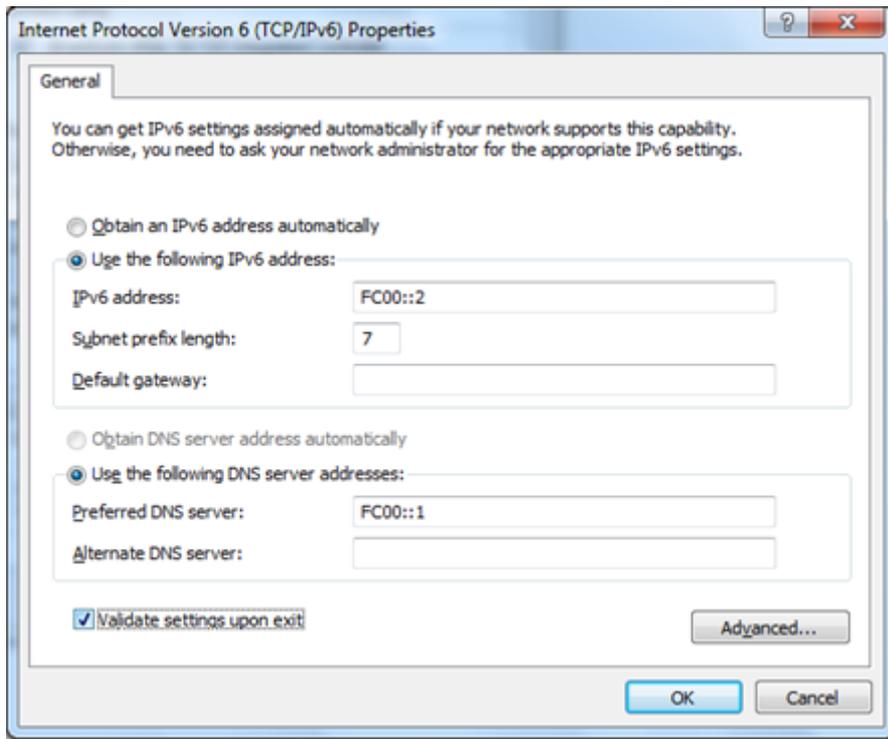
Configurando o Windows 7

Clique em Iniciar\Painel de Controle\Rede e Internet\Central de Rede e Compartilhamento e clique em “Alterar configurações do adaptador”

Nas propriedades da placa de rede do computador cliente repita a operação adicionando o endereço IPv6 **FC00:2**

Em comprimento do prefixo de sub-rede digite **7**.

Em servidor DNS digite **FC00::1** se a maquina anteriormente configurada for um servidor DNS para sua rede local.



Testando o seu ambiente:

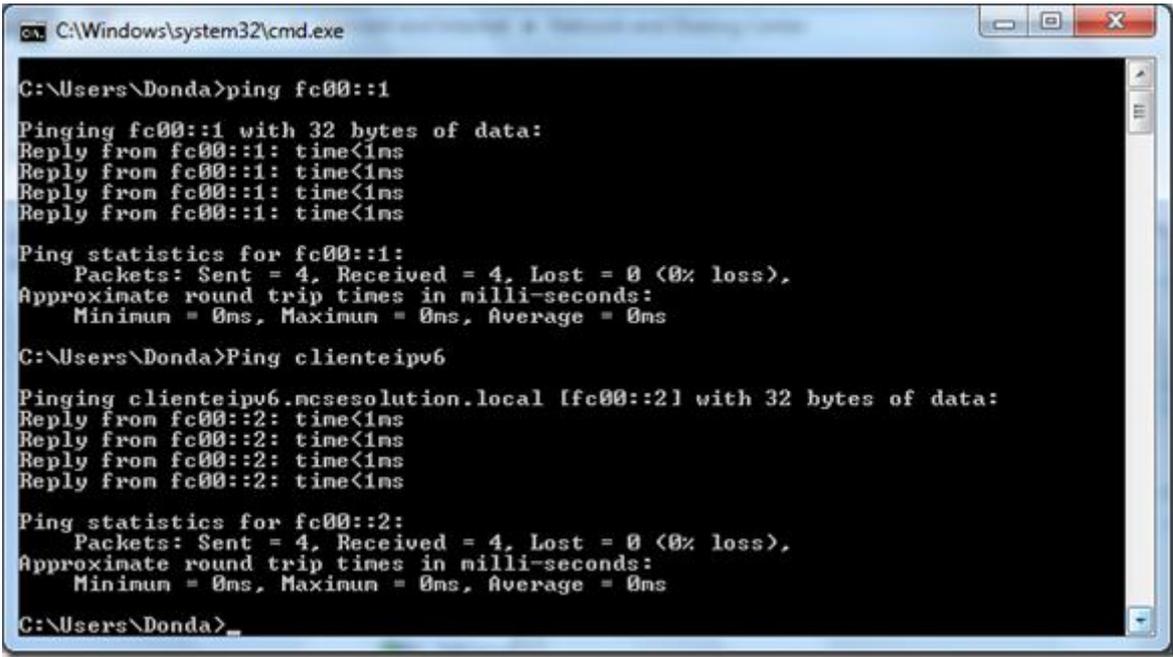
No prompt de comando digite:

Ping fc00::1

Para testar o IPv6 do Servidor

Ping clienteipv6

Para testar o registro AAAA do servidor DNS

A screenshot of a Windows command prompt window. The title bar shows the path 'C:\Windows\system32\cmd.exe'. The command prompt is in the directory 'C:\Users\Donda'. The user has entered 'ping fc00::1', and the output shows four successful replies with times less than 1ms. The statistics for 'fc00::1' show 4 packets sent, 4 received, 0% loss, and 0ms round trip times. The user then enters 'Ping clienteipv6', and the output shows four successful replies with times less than 1ms. The statistics for 'clienteipv6.ncsesolution.local [fc00::2]' show 4 packets sent, 4 received, 0% loss, and 0ms round trip times. The prompt ends with 'C:\Users\Donda>_'.

```
C:\Windows\system32\cmd.exe
C:\Users\Donda>ping fc00::1
Pinging fc00::1 with 32 bytes of data:
Reply from fc00::1: time<1ms
Reply from fc00::1: time<1ms
Reply from fc00::1: time<1ms
Reply from fc00::1: time<1ms

Ping statistics for fc00::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Donda>Ping clienteipv6
Pinging clienteipv6.ncsesolution.local [fc00::2] with 32 bytes of data:
Reply from fc00::2: time<1ms
Reply from fc00::2: time<1ms
Reply from fc00::2: time<1ms
Reply from fc00::2: time<1ms

Ping statistics for fc00::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Donda>_
```

Os principais problemas que podem ocorrer são os de digitação e o firewall que pode bloquear o PING.

Bibliografia

TCP/IP Fundamentals for Microsoft Windows

<http://technet.microsoft.com/en-us/library/bb726983.aspx>

Data do acesso 25 de outubro de 2010

Comitê gestor da Internet no Brasil

<http://www.cg.org.br/publicacoes/documentacao/regrasip.htm>

Data do acesso 25 de outubro de 2010

RFC editor

<http://www.rfc-editor.org/>

Data do acesso 25 de outubro de 2010

Fundação de Amparo à Pesquisa do Estado de São Paulo

<http://www.fapesp.br/>

Data do acesso 6 de janeiro de 2008

Wikipédia, a enciclopédia livre.

http://pt.wikipedia.org/wiki/George_Boole

Data do acesso 6 de janeiro de 2008

Ipv6 do Brasil

http://www.ipv6dobrasil.com.br/index.php?id_pagina=39

Data do acesso 25 de outubro de 2010

Microsoft TechNet

<http://technet2.microsoft.com/WindowsServer/pt-BR/Library/01f5811d-589e-4c11-9161-0ce24a6f8a181046.mspx?mfr=true>

Data do acesso 25 de outubro de 2010

Rede Nacional de Ensino e Pesquisa (RNP)

http://www.rnp.br/newsgen/0103/end_ipv6.html

Data do acesso 23 de janeiro de 2008

Links

Department of defense advanced Research Projects Agency

<http://www.darpa.mil/>

Department of Defense

www.defenselink.mil

International Standards Organization

www.iso.org