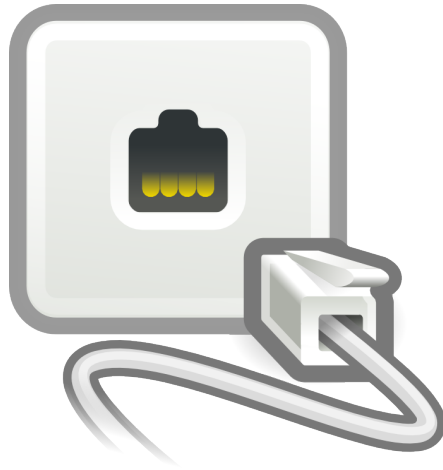




Curso 4451

Linux Security Administration in Cloud

Redes Avançado



4LINUX

2

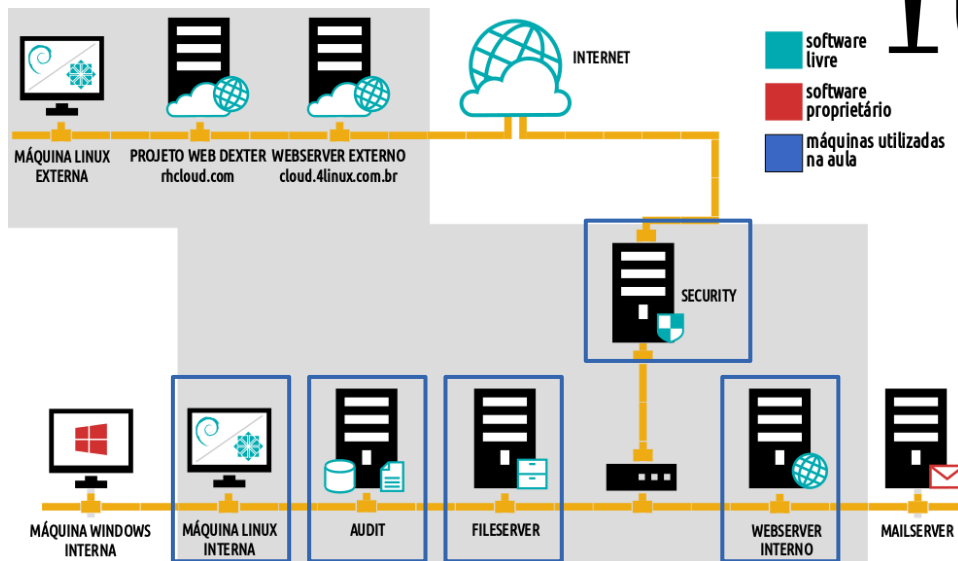
Fundamentação

O funcionamento da área de TI de uma empresa está totalmente associado a possibilidade dos computadores se comunicarem em Rede. E mesmo aqueles que não são familiarizados com redes, ou não atuam diretamente nestes setor devem possuir noções básicas sobre endereçamento IP e máscara de sub-rede.

Este capítulo objetiva demonstrar alguns conceitos relacionados a endereçamento IPV4 e IPV6 além de demonstrar o cálculo de máscara de rede em endereços IPV4, assunto amplamente abordado na LPI.

IT Experience

it
EXPERIENCE



Ligar as máquinas Circuladas!

4LINUX

3

Objetivos da Aula

Aula 07

- Trabalhar com endereços IP's:
 - Classes de Rede;
 - Cálculo de Máscara;
- Dividir a rede logicamente utilizando os cálculos de endereços IP;
- Adicionar rotas estáticas e permanentes;
- Compreender conceitos básicos sobre IPv6.



Redes Avançado

Servidor: Audit

Classes de Rede:

Classe	Range	Máscara Padrão	Reservado
A	0.0.0.0 a 127.255.255.255	255.0.0.0	10.0.0.0 a 10.255.255.255
B	128.0.0.0 a 191.255.255.255	255.255.0.0	172.16.0.0 a 172.31.255.255
C	192.0.0.0 a 192.255.255.255.0	255.255.255.0	192.168.0.0 a 192.168.255.255

4LINUX

5

IPV4

No IPV4, os endereço IP são compostos por 4 blocos de 8 bits (32 bits no total), que são representados através de números de 0 a 255, como "200.156.23.43" ou "192.168.1.1".

Endereços Reservados

As faixas de endereços começadas com "10", com "192.168" ou com o range que vai de "172.16" até "172.31" são reservadas para uso em redes locais e por isso não são usados na internet.

Redes Avançado

Servidor: Audit

Cálculo de Máscara:

Classe	Máscara Padrão	Binário	Octal
A	255.0.0.0	11111111.00000000.00000000.00000000	/8
B	255.255.0.0	11111111.11111111.00000000.00000000	/16
C	255.255.255.0	11111111.11111111.11111111.00000000	/24

4LINUX

6

Rede X Host

Embora aparentem ser uma coisa só, os endereços IP incluem duas informações. O endereço da rede e o endereço do host dentro dela. Em uma rede doméstica, por exemplo, você poderia utilizar os endereços "192.168.1.1", "192.168.1.2" e "192.168.1.3", onde o "192.168.1." é o endereço da rede (e por isso não muda) e o último número (1, 2 e 3) identifica os três micros que fazem parte dela.

Os micros da rede local podem acessar a internet através de um roteador, que pode ser tanto um servidor com duas placas de rede, quando um modem ADSL ou outro dispositivo que ofereça a opção de compartilhar a conexão. Neste caso, o roteador passa a ser o gateway da rede e utiliza seu endereço IP válido para encaminhar as requisições feitas pelos micros da rede interna. Este recurso é chamado de NAT (Network Address Translation).

Redes Avançado

Servidor: Audit

Qual o Endereço de Máscara para 192.168.200.0/27?

11111111.11111111.11111111.11100000
8 + 8 + 8 + 3 = 27

1# echo \$((2#11111111)) → 11111111 → 255

2# echo \$((2#11100000)) → 11100000 → 224

255.255.255.224

4LINUX

7

Máscara de Rede

A máscara de rede, juntamente com o endereço IP, define a rede o computador pertence, isto é, que outros endereços IP que o computador pode comunicar diretamente na mesma LAN.

Lembre-se sempre que os 4 bytes que definem tanto o endereço IP quanto a máscara de rede são representações de números binários.

A máscara de rede é, por definição, uma sequência de "1" a partir da esquerda para a direita, seguido por um certo número de "0" (a faixa de rede).

Redes Avançado

Servidor: Audit

Mas, como Saber sem Usar o Bash para Converter?

$$\begin{array}{ccccccc} 11111111 & . & 11111111 & . & 11111111 & . & 11100000 \\ \underbrace{}_8 & + & \underbrace{}_8 & + & \underbrace{}_8 & + & \underbrace{}_3 = 27 \end{array}$$

128	64	32	16	8	4	2	1	Soma-se os Bits 1
1	1	1	1	1	1	1	1	128+64+32+16+8+4+2+1 = 255
1	1	1	0	0	0	0	0	128+64+32 = 224

255.255.255.224

Redes Avançado

Servidor: Audit

Dividindo a Rede 192.168.200.0/24 em 2 Sub-Redes:

1ª Regra: $2^n \geq \text{Sub-Redes}$

2 elevado à N é igual ou maior ao número de Sub-Redes

Calculando: $2^n \geq 1 \rightarrow 2^1 \geq 2$

$N = 1$

4LINUX

9

“Para fazer a divisão de uma rede em sub-redes, é preciso aumentar o número de bits iguais a 1, alterando com isso a máscara de sub-rede.”

Agora, naturalmente, surge uma nova questão: "Quantos bits?". Ou de uma outra maneira (já procurando induzir o seu raciocínio): "O que define o número de bits a ser utilizados a mais?"

Esta é uma questão bem mais simples do que pode parecer. No exemplo proposto, precisamos dividir a rede em quatro sub-redes. Ou seja, o número de sub-redes deve ser, pelo menos, quatro.

Redes Avançado

Servidor: Audit

Dividindo a Rede 192.168.200.0/24 em 2 Sub-Redes:

2ª Regra: N = Número de Bits que se deve ligar

Máscara Padrão = 11111111.11111111.11111111.00000000

Nova Máscara = 11111111.11111111.11111111.10000000

Calculando:

$$2^1 \geq 2$$

128	64	32	16	8	4	2	1	Soma-se os Bits 1
1	0	0	0	0	0	0	0	= 128 → /25

4LINUX

10

Sabendo qual o número mínimo de sub-redes basta descobrirmos quantos bits são equivalentes a este número, aqui entra uma simplificação realmente providencial em relação ao cálculo:

$2^n \geq$ Número de Sub-redes

Onde o valor de “n” deverá ser definido para que a regra **$2^n \geq$ Número de Sub-redes** seja validada.

Em nosso modelo a condição **$2^2 \geq 4$** é verdadeira logo dois bits a mais alterados para “1” garantirão no mínimo 4 sub-redes conforme queremos em nossa divisão.

Redes Avançado

Servidor: Audit

Dividindo a Rede 192.168.200.0/24 em 2 Sub-Redes:

3ª Regra: $2^x - 2 = \text{Número de Hosts das SubRedes}$

X = Número de Bits Desligados!

Nova Máscara = 11111111.11111111.11111111.1**0000000**
x=7

Calculando: $2^x - 2 = \text{Hosts}$

$2^7 - 2 = 126$ Hosts Válidos em cada Sub-Rede

2 IPS Reservados ao Endereço de Rede e Endereço de Broadcast

4LINUX

11

Em relação ao número de hosts existentes em cada sub-rede temos outra regra, basta um conceito simples:

“O número de bits não setados, ou seja, com valor igual a “0” definirá quantos endereços caberão em cada sub-rede”.

Lembrando que o primeiro e o último endereço de cada sub-rede serão reservados para identificação da rede e broadcast respectivamente”

Clocando este raciocínio em fórmula temos o seguinte:

$2^x - 2 = \text{Número de Hosts válidos}$

Onde X é o número de bits com valor igual a “0”

Redes Avançado

Servidor: Audit

Dividindo a Rede 192.168.200.0/24 em 2 Sub-Redes:

Resumo: 2 Sub-Redes de Máscara /25 (255.255.255.128) com 128 IPs cada, onde 126 são Hosts Válidos.

REDE	Network	Range	Broadcast
1	192.168.200.0	192.168.200.1 a 192.168.200.126	192.168.200.127
2	192.168.200.128	192.168.200.129 a 192.168.200.254	192.168.200.255

4LINUX

12

No nosso exemplo foram disponibilizados 2 bits do último octeto para serem utilizados na máscara de sub-rede. Logo 6 bits estão disponíveis para identificação dos hosts, aplicando a fórmula do slide anterior temos:

$$2^6 - 2 = 62 \text{ hosts válidos por sub-rede.}$$

Redes Avançado

Servidor: Audit

Dividindo a Rede 192.168.200.0/24 em 2 Sub-Redes:



Dica: Podemos usar um utilitário para realizar todo o cálculo de Sub-Rede de forma automática. Valide seu cálculo anterior:

```
1# apt-get install ipcalc
2# ipcalc 192.168.200.0/24 /25
```

4LINUX

13

CIDR

A notação utilizada acima se chama CIDR (Classless Inter-Domain Routing), onde a máscara de sub-rede é indicada simplesmente pelo número de bits utilizados na máscara de sub-rede.

Subnets after transition from /24 to /25

```
Netmask: 255.255.255.128 = 25 11111111.11111111.11111111.1 00000000
Wildcard: 0.0.0.127           00000000.00000000.00000000.0 11111111
```

1.

```
Network: 192.168.200.0/25      11000000.10101000.11001000.0 00000000
HostMin: 192.168.200.1        11000000.10101000.11001000.0 00000001
HostMax: 192.168.200.126      11000000.10101000.11001000.0 11111110
Broadcast: 192.168.200.127    11000000.10101000.11001000.0 11111111
Hosts/Net: 126                Class C, Private Internet
```

2.

```
Network: 192.168.200.128/25   11000000.10101000.11001000.1 00000000
HostMin: 192.168.200.129      11000000.10101000.11001000.1 00000001
HostMax: 192.168.200.254      11000000.10101000.11001000.1 11111110
Broadcast: 192.168.200.255    11000000.10101000.11001000.1 11111111
Hosts/Net: 126                Class C, Private Internet
```

```
Subnets: 2
Hosts: 252
```

Redes Avançado

Servidor: Security

Configurando as Sub-Redes na máquina da empresa Dexter Courier:

```
1# vim /etc/network/interfaces

....
auto eth1                                auto eth2
iface eth1 inet static                  iface eth2 inet static
    address 192.168.200.1                address 192.168.200.129
    netmask 255.255.255.128             netmask 255.255.255.128
    network 192.168.200.0                network 192.168.200.128
    broadcast 192.168.200.127           broadcast 192.168.200.255

2# service networking restart
```

Redes Avançado

Servidor: WebServer Interno

Configurando as Sub-Redes na máquina da empresa Dexter Courier:

```
1# vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
IPADDR=192.168.200.130
```

```
NETMASK=255.255.255.128
```

```
GATEWAY=192.168.200.129
```

```
DNS1=8.8.8.8
```

```
2# systemctl restart network
```



NOTA: Altere no VirtualBox o Adaptador 1 da placa de rede para SubRede2.

Redes Avançado

Servidor: Audit

Adicionando rota entre as SubRedes:

Comando route:

Para adicionar uma rota até a SubRede 2 (192.168.200.128/25) utilizando como Gateway o IP 192.168.200.129 do servidor Security:

```
1# route add -net 192.168.200.128/25 gw 192.168.200.129
2# ping -c4 192.168.200.130
3# route del -net 192.168.200.128/25 gw 192.168.200.129
```


Redes Avançado

Servidores Debian

Adicionando rota permanente:

Arquivo interfaces:

Para adicionar uma rota permanente até a SubRede 2 (192.168.200.128/25) utilizando como Gateway o IP 192.168.200.129 do servidor Security:

```
1# vim /etc/network/interfaces
....

post-up route add -net 192.168.200.128/25 gw 192.168.200.129

2# service networking restart
```

Redes Avançado

Servidor Fileserver

Adicionando rota permanente:

Arquivo route-eth0:

Para adicionar uma rota permanente até a SubRede 2 (192.168.200.128/25) utilizando como Gateway o IP 192.168.200.129 do servidor Security:

```
1# vim /etc/sysconfig/network-scripts/route-eth0
```

```
GATEWAY0=192.168.200.129  
NETMASK0=255.255.255.128  
ADDRESS0=192.168.200.128
```

```
2# systemctl restart network
```

Redes Avançado

Servidor: Audit

Comandos Avançados de Rede:

Comando traceroute:

Mostra o caminho percorrido por um pacote para chegar ao seu destino. Este comando mostra, na tela, o caminho percorrido entre os Gateways da rede e o tempo gasto de retransmissão.

Este comando é útil para encontrar computadores defeituosos na rede caso o pacote não esteja chegando ao seu destino:

```
1# apt-get install traceroute
```

Redes Avançado

Servidor: Audit

Comandos Avançados de Rede:

Comando traceroute:

Sintaxe: traceroute <host/IP de destino>

-l	Mostra o tempo de vida do pacote (ttl)
-m	Ajusta a quantidade máximas de ttl dos pacotes. O padrão é 30.
-n	Mostra os endereços numericamente ao invés de usar resolução DNS.
-p	Ajusta a porta que será usada para o teste. A porta padrão é 33434.
-r	Pula as tabelas de roteamento e envia o pacote diretamente ao computador conectado a rede.

Redes Avançado

Servidor: Audit

Comandos Avançados de Rede:

Comando traceroute:

-v	Mostra mais detalhes sobre o resultado do traceroute.
-s [end]	Configura o tempo máximo que aguardará por uma resposta. O padrão é 3 segundos.
-w [num]	Usa o endereço IP/DNS [end] como endereço de origem para computadores com múltiplos endereços IPs ou nomes.

```
1# traceroute google.com
```

Comandos Avançados de Rede:

Comando mtr:

O MTR combina a funcionalidade dos testes de ping e traceroute em uma única ferramenta de diagnóstico.

Como ping, envia "echo" pacotes de sua máquina para a máquina alvo a fim de medir a latência e perda de pacotes ao longo do caminho de rede. Exibe continuamente, ainda, estatísticas atualizadas em tempo real como ele opera. Como traceroute, ele mostra os nomes ou endereços IP de cada máquina ao longo do caminho de rede e também atualiza as estatísticas para cada máquina.

Redes Avançado

Servidor: Audit

Comandos Avançados de Rede:

Comando mtr:

```
1# apt-get install mtr
```

```
2# mtr google.com
```



NOTA: Repare que ele também mostra se há perda de pacotes.

Limitando o ICMP

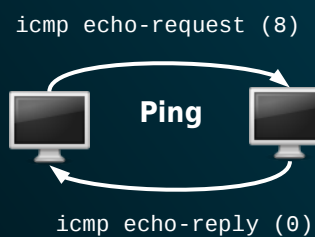


Servidor:
Webserver Interno

Bloqueando PING broadcast:

```
1# ping -b 192.168.200.255
2# cd /proc/sys/net/ipv4
3# echo 0 > icmp_echo_ignore_broadcasts
4# ping -b 192.168.200.255
5# ping 192.168.200.127
6# echo 1 > icmp_echo_ignore_all
7# ping 192.168.200.127
```

Ping é um utilitário que usa o protocolo **ICMP** (Internet Control Message Protocol) para testar a conectividade entre equipamentos:



Limitando o ICMP



*Servidor:
Webserver Interno*

Bloqueando PING definitivo:

```
1# vim /etc/sysctl.conf  
  
    net.ipv4.icmp_echo_ignore_all = 1  
2# sysctl -p (Aplica as Configurações)  
3# ping 127.0.0.1  
4# ping -b 192.168.200.255
```

O arquivo **sysctl.conf** é usado para definir parâmetros do kernel controlados pelo comando **sysctl**.

Os parâmetros disponíveis para serem alterados em tempo real pelo sysctl encontram-se em /proc/sys.

Pergunta LPI



Quantos hosts teremos para uma rede /25 que equivale a máscara 255.255.255.128?

Para um rede /29 temos o endereço de máscara sendo 255.255.255.____ ?

Pergunta LPI



Quantos hosts teremos para uma rede /25 que equivale a máscara 255.255.255.128?

Resposta: 126

Para um rede /29 temos o endereço de máscara sendo 255.255.255.____ ?

Resposta: 248

4LINUX

27

REPOSTA CORRETA: 126

Para chegar a quantidade de hosts devemos aplicar a seguinte regra:

$2^x - 2 = \text{Número de Hosts}$.

Onde X refere-se ao número de bits desligados, fazendo a conversão da máscara descrita para o padrão binário temos:

$255.255.255.128_{(\text{DEC.})} = 11111111.11111111.11111111.10000000_{(\text{BIN.})}$

Logo $2^7 - 2 = \text{Número de Hosts} \rightarrow 128 - 2 = \text{Número de Hosts} \rightarrow \underline{\underline{126 \text{ Hosts}}}$

REPOSTA CORRETA: 248

Para resolver este tipo de questão basta utilizar o valor da máscara para determinar como ficaria o quarto octeto em escala binária, ou seja, para uma máscara /29 temos 5 bits setados (valor igual a 1) logo nossa máscara em binário ficaria assim:

$11111111.11111111.11111111.11111000_{(\text{BIN.})}$

Obtendo esta informação basta converter o último octeto da máscara para a escala decimal, o valor obtido será 248.



Fundamentação

IPv6 é a “nova” versão do protocolo de redes de dados com especificações desenvolvidas pela IETF (Internet Engineering Task Force);

A principal motivação para seu desenvolvimento foi a expansão do espaço de endereços disponíveis na internet, uma preocupação que surgiu com o aumento da quantidade de dispositivos conectados, a chamada terceira onda da internet, a internet das coisas!

Redes Avançado

Possibilidades do IPv6:

- Sabemos que um endereço IPv4 é composto por 32 bits, gerando aproximadamente 4 bilhões de endereços possíveis:

```
1# echo "2 ^ 32" | bc
```

- Já um endereço IPv6 é formado por 128 bits:

```
2# echo "2 ^ 128" | bc
```

- O que gera cerca de 340 undecilhões de endereços possíveis!

Espaço de endereçamento

O espaço de endereçamento do IPv6 de 128 bits, contra os 32 bits do IPv4 é sem dúvidas a mudança mais visível do IPv6 em relação ao IPv4. Esse tamanho gerado pelo IPv6 comporta tanto profundas hierarquias de endereçamento por agregação como um grande número de nós por sub-rede o que permite:

a) Liberal distribuição de faixas de endereçamento a usuários finais, tornando desnecessários, por exemplo, os complexos roteadores NAT para compartilhamento de um IP por vários usuários.

b) Simplificação na configuração de servidores e dispositivos de rede, causada pelo desuso do NAT, o que contribui para o barateamento do acesso à Internet.

Redes Avançado

Constituição de um Endereço IPv6:

- Um endereço IPv6 é representado por 8 blocos de 16 bits, cada bloco separado pelo caractere dois pontos (:):

```
1# ifconfig eth0 | grep inet6 ou
```

```
2# ip -6 addr show dev eth0 | grep inet6
```

- Cada grupo de 16 bits (duocteto) possui 4 símbolos hexadecimais que podem variar de 0000 a FFFF.

Tipos de Endereços IPv6

O grande espaço de endereçamento visa a criação facilitada de classes de endereçamento. Tais classes, mais apropriadamente denominadas de faixas de endereçamento, são registradas junto à IETF. Segue uma lista das principais faixas e os respectivos prefixos IPv6.

Endereço	Descrição
0000::/8	Reservado
0000::/96	Endereços IPV6 compatíveis com IPV4
::FFFF:0:0/96	Endereços IPV4 mapeados em IPV6
0200::/8	NSAP (Obsoleto)
0400::/8	IPX (Obsoleto)
2000::/3	Endereços roteáveis na Internet (Prefixos 2xxx e 3xxx)
FE80::/10	Endereços de Rede local (Automáticos ou estáticos)
FEC0::/19	Endereços do sítio local
FF02::/8	Multicast

Redes Avançado

Servidor: Audit


Testando o IPv6:

1 – Verifique o endereço IPv6 da interface loopback na máquina Audit:

```
1# ifconfig lo | grep inet6
```

2 – Em seguida, verifique o endereço IPv6 da interface eth0:

```
2# ifconfig eth0 | grep inet6
```

 **NOTA:** Blocos vazios contínuos podem ser representados pelos caracteres :: (quatro pontos) **uma única vez dentro do endereço.**

Assim, o endereço de loopback: 0000:0000:0000:0000:0000:0000:0000:0001
Pode ser representado dessa forma: ::1

4LINUX

31

Segundo a RFC 2374, uma mesma interface, que utiliza o protocolo IPv6, pode utilizar mais de um endereço, diferentemente do IPv4, onde tal característica só era possível em roteadores.

Nas interfaces IPV6 existem 3 tipos de endereços:

Endereço de Unicast:

Esse tipo de endereço é comumente usado em IPv4, que identifica apenas uma única interface. Desta forma um pacote destinado a um endereço do tipo Unicast é enviado diretamente para a interface associada a esse endereço.

Redes Avançado

Servidor: FileServer

Testando o IPv6:

1 – Utilizando o FileServer, efetue um ping no endereço IPv6 do servidor Audit:



```
1# ping6 -I eth0 fe80:: ... .. < Endereço IPv6 obtido na  
Audit >
```

2 – Faça um segundo teste pingando o endereço de loopback da máquina FileServer:



```
2# ping6 -I lo ::1 ou  
3# ping6 -I lo 0000:0000:0000:0000:0000:0000:0000:0001
```

4LINUX

32

Endereços Anycast

Esse tipo de endereço é utilizado para identificar um grupo de interfaces pertencentes a hosts diferentes. Um pacote destinado a um endereço Anycast é enviado para um das interfaces identificadas pelo endereço. Especificamente, o pacote é enviado para a interface mais próxima, de acordo com o protocolo de roteamento.

Endereço Multicast

Da mesma forma que o endereço Anycast, este endereço identifica um grupo de interfaces pertencente a diferentes hosts mas um pacote destinado a um endereço Multicast é enviado para todas as interfaces que fazem parte deste grupo.

Testando o IPv6:

1 - Faça um ping6 em todos os hosts disponíveis:



```
1# ping6 -I eth0 ff02::1
```

- Diferente do **IPv4**, onde as respostas ao ping para endereços de broadcast podem ser desabilitadas; em **IPv6** este comportamento não pode ser desabilitado, exceto pela utilização de um firewall.



Existe uma série de endereços multicast reservados para funções específicas. Uma boa fonte é a lista disponível em:
<http://ipv6.br/entenda/enderecamento/#multicast>

Outra característica marcante do IPv6 é que não existem mais os endereços broadcast, que endereçavam todos os hosts de um mesmo domínio de colisão, isto é, uma pacote com endereço de destino do tipo broadcast era enviado para todos os hosts de seu domínio de colisão.

Com a abolição desse tipo endereço, outro protocolo muito comum no IPv4 também ficou em desuso, o ARP – Address Resolution Protocol, que usava endereços broadcast para descoberta do endereço MAC da interface referente ao endereço de destino do pacote.

Pergunta LPI



Na LPI conceitos sobre IPv6 ainda não são abordados a fundo, sendo requerido apenas conhecimento das principais diferenças em relação a IPv4.

Mas para os interessados no assunto uma boa opção é o curso gratuito disponibilizado pelo ceptro: <http://ipv6.br/curso/>

Quantos bits possui um endereço IPv6?

Pergunta LPI



Na LPI conceitos sobre IPv6 ainda não são abordados a fundo, sendo requerido apenas conhecimento das principais diferenças em relação a IPv4.

Mas para os interessados no assunto uma boa opção é o curso gratuito disponibilizado pelo ceptro: <http://ipv6.br/curso/>

Quantos bits possui um endereço IPv6?

Resposta: 128 bits

RESPOSTA CORRETA: 128

Um endereço de rede no padrão IPV6 possui exatamente 128 bits representados em 8 blocos de 16 bits.

Próximos Passos

Para que você tenha um melhor aproveitamento do curso, participe das seguintes atividades disponíveis no Netclass:

- Executar as tarefas do **Practice Lab**;
- Resolver o **Desafio Appliance Lab** e postar o resultado no Fórum Temático;
- Responder as questões do **Teste de Conhecimento** sobre o conteúdo visto em aula.

Mãos à obra!

4LINUX

OPEN SOFTWARE SPECIALISTS



ESPECIALISTA EM "JUNTAR AS PEÇAS" DO MUNDO OPEN SOURCE

WWW.4LINUX.COM.BR