



**HEXA**  
NETWORKS

Routing and Internet **Experts.**

Palestra **Lições de Casa** que  
**Todos os Sistemas**  
**Autônomos Deveriam Fazer**



# André Dias

- **Fundador e CEO** da **Hexa Networks** e **NetConfig**;
- **Mais de 12** anos atuando na área de **redes**;
- **Mais de 20** anos atuando na área de **tecnologia** (iniciando aos 8 anos de idade);
- **Aos 16** anos iniciou em um provedor de VoIP (Telefonia sobre IP);
- **Aos 17** ingressou em um ISP (Provedor de Acesso a Internet);
- Certificações **Mikrotik MTCNA** , **MTCRE**, **MTCINE**, **MTCIPv6E**, **Juniper JNCIA**, **JNCIS-SP**, **Nokia NRS-I** ;
- Autor de artigos para o "**Brasil Peering Fórum**";
- Fanático assíduo por **IPv6**;
- Já fez parte da maior orquestra do planeta;
- Sou chato e teimoso;
- Colaborador para a maior obra coletiva da humanidade, a Internet.



## O Que **A Hexa Networks** faz

Fundada em 2017, a Hexa Networks nasceu com escopo a prestar serviços para provedores de acesso e operadoras de trânsito que buscavam direcionamento para alcançar estabilidade, excelência, escalabilidade e estruturação em suas operações de redes para crescerem de forma saudável.

Para prover toda a demanda deste mercado, a Hexa Networks agregou especialidades como protocolos de roteamento, serviços de MPLS, entre outros. O que nos permitiu atuar em cenários que vão desde os mais simples, até os mais complexos e críticos.

## O Que é **O NetConfig**

O NetConfig é uma plataforma completa de automação e gestão de redes, projetada para provedores de internet e empresas de consultoria.

Acesso aos equipamentos com um SSH Web com auditoria, automação de RPKI, IRR, Backup e configurações de equipamentos de rede via interface gráfica são algumas funções que o NetConfig provê.



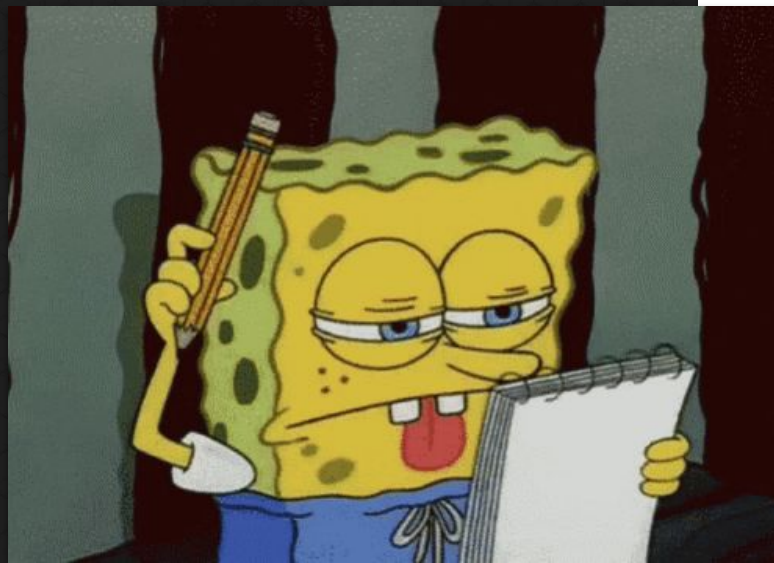
# Agenda:

- Motivação;
- uRPF;
- Portas Sensíveis;
- ARP Flooding no IX;
- RPKI;
- IRR;
- PeeringDB;
- Radar Qrator;
- NETBOX / PHPIPAM;
- MANRS;
- Looking Glass;
- IPv6.



# Motivações Para a **Palestra**

- Vemos muitos provedores que não fazem o mínimo das boas práticas;
- Fornecer um guia para que possam se adequar;
- Fazer meu papel ajudando a comunidade.



# Calma Pequeno **Gafanhoto!**

- Devido ao tempo limitado da apresentação, esta lista inclui apenas algumas das principais boas práticas!
- Use esta apresentação como um guia inicial e aprofunde-se nos artigos que mencionei ao longo dela!



# Anti-Spoofing - uRPF



- Unicast Reverse Path Forward;
- Anti-Spoofing baseado em roteamento;
- Verificando se existe uma rota de retorno válida para o endereço IP de origem na tabela de roteamento;
- Modo Strict (mais restrito) e Loose (menos restrito);
- Se todos tivessem implementado, seria muito mais fácil rastrear origem de DDoS!
- Mandatório para participar do MANRS!

# Anti-Spoofing - **uRPF**

Exemplo de loose em Huawei:

```
interface GigabitEthernet0/0/0
```

```
ip urpf loose
```

```
ipv6 urpf loose
```





# Drop/Controle Portas **Sensíveis**

Drop e Controle de portas que são vetores de amplificação de DDoS!

Drop:

- 19 - TCP/UDP - Chargen;
- 25 - TCP/UDP - SMTP;
- 1900 - TCP/UDP - SSDP;

PS: Antes de fazer algo, leia sobre os protocolos para não fazer caquinha!

# Drop/Controle Portas **Sensíveis**

Drop e Controle de portas que são vetores de amplificação de DDoS!

Controlar:

- 53 - UDP - DNS;
- 161 - UDP - SNMP;
- 11211 - TCP/UDP - Memcached.

PS: Antes de fazer algo, leia sobre os protocolos para não fazer caquinha!

# Arp Flooding - IX.br



- É mandatorio que participantes do IX.br façam essa boa pratica!
- Um dos principais problemas atualmente em ambientes de IX;
- Alguns equipamentos ~~nojentos~~ mandam ARP Request por padrão a cada 30 segundos;
- ARP é broadcast, logo, todos participantes recebem. Se seu equipamento não tem Alzheimer, siga o artigo do QR CODE e corrija isso!

# RPKI





- Ajuda a prevenir sequestro de prefixos;
- Resource Public Key Infrastructure;
- Atua como se fosse um “certificado” para as rotas;
- RoA - Route Origin Authorization;
- 3 estados: **valid**, **invalid** e not found;
- Dropem os **invalid**, e por enquanto aceitem **valid** e not found;
- Krill - Gera os RoA;
- Routinator - Plataforma que o roteador de borda consegue consultar se a rota tem RoA;
- 2 Artigos no BPF sobre o assunto, Diorges e Thiago Setti.



# Certificate Authority **AS26**

[ROAs](#) [Parents](#) [Repository](#)

Search for ASN, prefix, state...

ASN	Prefix	Comment	State
> 267	::/32-128		SEEN 3 
> 267	6.0/22-32		SEEN 3 

25 / page

< 1 >

Add ROA

Analyse my ROAs



Welcome to Routinator 3000.

Origin ASN

Prefix

Validate

Validation run done at 2021-07-21T20:40:45Z UTC (3 minutes ago)



LACNIC

Valid ROAs  
8352

Final VRPs  
14960

Unsafe VRPs  
0

VRPs Filtered Locally  
0

Duplicate VRPs  
1341



AFRNIC

Valid ROAs  
1936

Final VRPs  
2641

Unsafe VRPs  
0

VRPs Filtered Locally  
0

Duplicate VRPs  
48



ARIN

Valid ROAs  
42396

Final VRPs  
40043

Unsafe VRPs  
0

VRPs Filtered Locally  
0

Duplicate VRPs  
9154



RIPE

Valid ROAs  
24768

Final VRPs  
132925

Unsafe VRPs  
0

VRPs Filtered Locally  
0

Duplicate VRPs  
2



APNIC

Valid ROAs  
15842

Final VRPs  
75786

Unsafe VRPs  
0

VRPs Filtered Locally  
0

Duplicate VRPs  
243

# IRR



- Internet Route Registry;
- Publica suas políticas de roteamento de forma pública;
- MNTR, Route/Route6, AUT-NUM, AS-SET;
- BGPQ3 e BGPQ4 já integra perfeitamente;
- RPSL;
- Facilita automação e acelera liberação de prefixos;
- Facilita compartilhamento de políticas de roteamento entre AS's.
- Obrigatório para o MANRS;
- Artigos sobre IRR nos QR CODE acima;

## WIZARD - ASSISTENTE PARA INCLUSÃO DE NOVOS ASES

---

Política de uso: ao incluir seus objetos na base está automaticamente concordando com a política sumarizada na seguinte [apresentação](#), em especial o slide 42.

ATENÇÃO: este assistente é uma ferramenta experimental e foi testado apenas com ASN's provenientes de registros efetuados no Registro.br. Qualquer ação não esperada resultará numa resposta com um código HTTP 403 (Acesso Negado), nestes casos entre em contato com [db-admin@bgp.net.br](mailto:db-admin@bgp.net.br) informando em qual parte do assistente o erro ocorreu, data/horário e o ASN.

Através deste assistente é possível publicar os objetos de um AS (listados a seguir) apenas informando o ASN (a validação é efetuada através das informações que já constam no NIR, portanto é necessário ter acesso ao registro, ou seja, ser o "dono" do AS).

Serão criados automaticamente os seguintes objetos:

- \* mntner (registro necessário para habilitar o AS a utilizar a base)
- \* route e route6 (a ferramenta analisará automaticamente os prefixos que estão sendo anunciados pelo AS, através das informações provenientes dos coletores do RIS e criará, também automaticamente, os objetos correspondentes para cada prefixo)
- \* aut-num (sem a política, detalhe: o as-name, baseado no ASN, deve ser editado posteriormente se necessário). Caso tenha sido registrado a política na interface do NIR, a mesma será importada/convertida (e publicada).

Para continuar preencha o ASN e clique em "Submeter".





Seu ASN: \*  Selecione ▾

 Senha não criptografada do mntner:  👁

Limpar formulário
Exibir relatório de IRR
Criar novo AS-SET

AS-SETS Cadastrados
Lista de Downstreams
 resultados por página

AS-SET ▲	Descrição do AS-SET ⚙	Membros ⚙	Última alteração ⚙
<span style="color: #007bff;">+</span> AS-BRITIS	Britis Telecom Ltda	AS28306,AS266260,AS53224,AS53095,AS53113...	2024-10-08T11:18:42Z
<span style="color: #007bff;">+</span> AS-BRITIS-CUSTOMERS	AS266260,AS53224,AS264876,AS53095,AS52762,		2024-01-10T22:50:57Z
<span style="color: #007bff;">+</span> AS-BRITIS-MIT	Britis Telecom Ltda	AS28306,AS263159,AS52528,AS262779,AS270473...	2024-05-22T20:16:29Z
<span style="color: #007bff;">+</span> AS270562:AS-CONE	Voluy Telecom LTDA		2023-11-13T16:09:33Z
<span style="color: #007bff;">+</span> AS28306:AS-CONE	Voluy Telecom LTDA		2023-11-13T16:09:45Z
<span style="color: #007bff;">+</span> AS53113:AS-CONE	Voluy Telecom LTDA		2023-11-13T16:09:45Z

# Base de Dados BGP - **PeeringDB**



- Plataforma aberta;
- Documentação pública dos peerings daquele AS;
- Documentação pública dos IXPs que o AS participa;
- Capacidade e fluxo de tráfego;
- Informações de URL para LG e RS;
- Contatos importantes do AS (abuse, por exemplo);
- Diversas operações utilizam o PeeringDB como principal meio para coletar informações para peerings;
- Suporte a API.





## N4 Telecomunicacoes LTDA ME

[EXPORT](#)

Organization	N4 Telecomunicacoes LTDA ME
Also Known As	N4 TELECOM
Long Name	N4 Telecomunicacoes LTDA
Company Website	<a href="http://www.n4telecom.com.br/">http://www.n4telecom.com.br/</a>
ASN	262505
IRR as-set/route-set ?	AS262505:AS-CLIENTES
Route Server URL	
Looking Glass URL	<a href="http://lg.n4telecom.com.br">http://lg.n4telecom.com.br</a>
Network Types	NSP
IPv4 Prefixes ?	700
IPv6 Prefixes ?	700
Traffic Levels ?	100-200Gbps
Traffic Ratios	Balanced
Geographic Scope	Regional
Protocols Supported	<input checked="" type="radio"/> Unicast IPv4 <input type="radio"/> Multicast <input checked="" type="radio"/> IPv6 <input type="radio"/> Never via route servers ?
Last Updated	2023-12-19T20:06:31Z
Public Peering Info Updated	2023-12-19T19:51:55Z
Peering Facility Info Updated	2018-09-14T11:01:19Z
Contact Info Updated	2020-08-06T18:59:23Z
Notes ?	
RIR Status	ok

### Public Peering Exchange Points

Exchange Åž ∨ IPv4	ASN IPv6	Speed Port Location	RS Peer	BFD Support
<a href="#">Equinix São Paulo</a> 64.191.232.79	262505 2001:504:0:7:0:26:2505:1	10G	<input type="radio"/>	<input type="radio"/>
<a href="#">IX.br (PTT.br) São José do Rio Preto</a> 187.16.199.7	262505 2001:12f8:0:22::7	10G	<input type="radio"/>	<input type="radio"/>
<a href="#">IX.br (PTT.br) São Paulo</a> 187.16.217.69	262505 2001:12f8::217:69	40G	<input type="radio"/>	<input type="radio"/>

### Interconnection Facilities

Facility Åž ∨ ASN	Country City
<a href="#">Equinix SP2 - São Paulo</a> 262505	Brazil Barueri

# Documentação - **PHPIPAM/NETBOX**

- Se trabalha com Tecnologia da Informação, precisa ter informação sobre o que está fazendo;
- Ambos os softwares são Open Source;
- Documentação de:
  - IPv4 e IPv6;
  - VLAN;
  - VRF;
  - NAT;
  - POP, etc
- PHPIPAM mais simples de usar, porém NETBOX muito mais completo!

## Statistics

Number of Sections	3
Number of Subnets	551
Number of VLANs	170
Number of VRFs	7
Number of IPv4 addresses	214
Number of IPv6 addresses	44
Number of Devices	1
Number of Locations	19
Number of Racks	0
Number of users	4

## Favourite subnets

No favourite subnets selected

— You can add subnets to favourites by clicking star icon in subnet details!

## Last 5 change log entries

User	Type	Object	Date	Change
phpIPAM Admin	Subnet / delete success	Deleted	2024-09-04 14:25:05	<a href="#">View</a>
phpIPAM Admin	Subnet / add success	[REDACTED]	2024-09-04 14:23:41	<a href="#">View</a>
phpIPAM Admin	IP address / add success	10.26.10.38	2024-09-03 18:03:53	<a href="#">View</a>
phpIPAM Admin	Subnet / add success	[REDACTED]/48	2024-09-03 17:45:01	<a href="#">View</a>
phpIPAM Admin	Subnet / add success	[REDACTED]/64	2024-09-03 17:44:37	<a href="#">View</a>

## Last 5 informational logs

Severity	Command	Date	Username
Info	User login	2024-09-12 17:44:11	admin
Info	User login	2024-09-11 17:53:05	sos telecom
Info	Address create	2024-09-04 15:00:13	
Info	User login	2024-09-04 14:43:02	admin
Info	User logged out	2024-09-04 14:42:59	Admin

## Last 5 warning / error logs

Severity	Command	Date	Username
Err	User login	2024-08-20 13:12:22	afiskc
Err	User login	2024-08-18 13:13:55	afiskc
Err	User login	2024-08-16 22:20:52	afiskc
Err	User login	2024-08-12 12:24:14	8hYTSUFK
Err	User login	2024-07-26 06:00:59	afiskc

### 🔔 New Release Available

NetBox v4.1.1 is available. [Upgrade Instructions](#)

#### ⚙️ Bookmarks ✕

🔔 No bookmarks have been added yet.

#### ⚙️ Organization ✕

Sites	0
Tenants	0
Contacts	0

#### ⚙️ IPAM ✕

VRFs	0
Aggregates	0
Prefixes	0
IP Ranges	0
IP Addresses	0
VLANs	0

#### ⚙️ Circuits ✕

Providers	0
Circuits	0

#### ⚙️ DCIM ✕

Sites	0
Packs	0

#### ⚙️ Welcome!

This is your personal dashboard. Feel free to customize it by rearranging, resizing, or adding widgets. You can also add new widgets using the "add widget" button below. Any changes only *your* dashboard, so feel free to experiment!

#### ⚙️ NetBox News

**How Equipment Refreshes and Platform Upgrades Got a lot easier with NetBox Branching**  
Network infrastructure is constantly evolving. Teams frequently tasked with performing upgrades, replacing outdated equipment, and updating device platforms to maintain performance and security. The challenge with these operations is not just the execution of the work, but also the planning, communication, and synchronization between teams. Upgrades often involve multiple stakeholders—from network engineers and architects...

**How Audits Just Got a Lot Easier with NetBox Branching**  
Audits like SOC 2, ISO 27001, and PCI DSS require meticulous attention to detail, especially when it comes to configuration management...

- Organization
- Devices
- Connections
- Wireless
- IPAM
- VPN
- Virtualization
- Circuits
- Power
- Provisioning
- Customization
- Operations
- Admin

# Radar - QRATOR



- Plataforma de monitoramento e análise de redes;
- Envie seu full route para o QRATOR;
- Análise de Route Leaks;
- Análise de Hijacks;
- Análise de portas que são abertas para exploit (TCP/179 por exemplo);
- Recebe relatórios periódicos sobre as informações da rede.

Overview

Graph

IP Connectivity

BGP Neighbors 5

Providers 2

Customers 1

Peerings 1

Unspecified 1

Prefixes 35

Internet Exchanges 0

Security issues

Route Leaks 610

Hijacks 8

Bogons 68

Routing Loops 0

Vulnerable Ports 6

DDoS amplifiers 0

Whois

AS [REDACTED] ([REDACTED])

9 584th place in IPv4 score rating 2 848th place in IPv6 score rating

[REDACTED] Telecom • [REDACTED] telecom.com.br

Prefixes

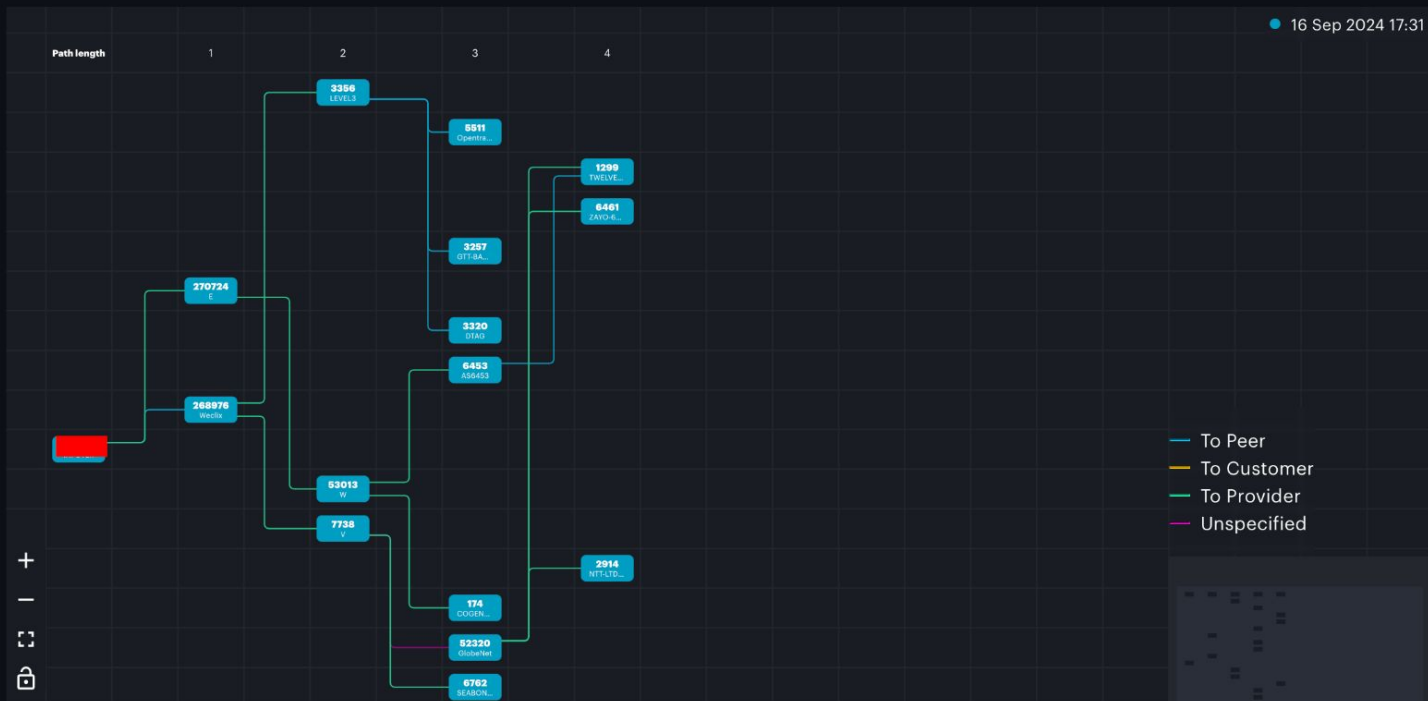
Targets

Extended graph

[REDACTED].0/22

1299, 1668, 7018, 33...

Extended







## Certificado - **MANRS**

- Fiz a lição de casa, quero um biscoito!
- Mutually Agreed Norms for Routing Security;
- Normas de Acordo Mútuo para Segurança de Roteamento;
- Após seguir alguns passos de boa prática, conseguirá o certificado de que faz parte do MANRS, sendo um dos poucos que fizeram a lição de casa;
- Artigo completasso do Marcelo Gondim no BPF sobre o assunto no QR Code.



Bora fazer a lição de casa?

**NETCONFIG**



**MANRS**

# Looking Glass



- Acessado via WEB ou CLI (SSH ou TELNET);
- Executa comandos de “show”, ping e traceroute dentro de um router do provedor;
- Essa execução de comandos costuma ser via SSH;
- A resposta desses comandos são apresentados na tela do usuário;
- Instalação extremamente simples;
- Tutorial de instalação no BPF e também pelo Remontti;
- Minha apresentação no GTER52 foi sobre esse assunto.



[Home](#)[Sobre nós](#)[Blog](#)[Central do Cliente](#)[Contato](#)[Indique & Ganhe!](#)

## Router to use

ARAUJOSAT-RT-NE40M2KB-BGP01-CRATO  
ARAUJOSAT-RT-NE8KM8-BGP02-AURORA

## Command to issue

show route IP\_ADDRESS  
show route as-path-regex AS\_PATH\_REGEX  
show route ^AS  
ping IP\_ADDRESS|HOSTNAME  
traceroute IP\_ADDRESS|HOSTNAME

## Parameter

[? HELP](#)

ENTER

RESET

Your IP address: 2804:1

**Crato-CE**

R. Monsenhor Esmeraldo, 559, 63100-310,

**E-Mail**

contato@araujosat.com.br

**Ligue**

0800 280 7227 8hs-22hs



28

[Home](#)[Sobre nós](#)[Blog](#)[Central do Cliente](#) [Contato](#)[Indique & Ganhe!](#)

```
Command: display bgp routing-table 8.8.8.8 | no-more | exclude nexthop: | exclude From:
```

```
Info: The max number of VTY users is 21, the number of current VTY users online is 1, and total number of terminal users online is 1.
```

```
The current login time is 2023-11-26 21:29:30-03:00.
```

```
The last login time is 2023-11-25 20:53:31-03:00 from 186.249.81.5 through SSH.
```

```
Info: It will take a long time if the content you search is too much or the string you input is too long, you can press CTRL_C to break.
```

```
BGP local router ID : 172.21.12.1
```

```
Local AS number : 263024
```

```
Paths: 4 available, 1 best, 1 select, 0 best-external, 0 add-path
```

```
BGP routing table entry information of 8.8.8.0/24:
```

```
Route Duration: 12d03h32m49s
```

```
Direct Out-interface: GigabitEthernet0/3/12.1928
```

```
Relay Tunnel Out-Interface:
```

```
Qos information : 0x0
```

```
Community: <0:28598>
```

```
Ext-Community: RT <263024 : 41000>, RT <263024 : 51000>, RT <263024 : 51200>
```

```
AS-path 28598 15169, origin igp, pref-val 0, valid, external, best, select, active, pre 20
```

```
Advertised to such 3 peers:
```

```
10.51.20.2
```

```
172.21.50.186
```



# Cadê teu IPv6?



- Tópico mais do que batido, mas comum de ver.
- Só implemente seu IPv6.
- BPF possui um monte de artigos sobre IPv6. Sério.



## Nossos **Contatos e links:**

E-mail: [andredias@hexanetworks.com.br](mailto:andredias@hexanetworks.com.br)

Linkedin: <https://www.linkedin.com/in/andreIrdias/>

WhatsApp: (17) 99670-0482

Brasil Peering Fórum:

<https://wiki.brasilpeeringforum.org>



**Implemente IPv6!**

**>Aberto para perguntas e contribuições!<**