BGP Statistics
Engenharia de Segurança Cibernética

Bruna Zamith
Lucas Queiroz
Vitor Gallera

Sumário

Introdução

- Identificação de redundância de IPs em rotas entre IXs
- **IX**: *Internet exchange point*
  - Hubs: Provedores podem conectar seus servidores
  - Facilita o tráfego das informações
  - Brasil: Nic.br
- Diferentes representações de endereços de IP iguais
  - 37.142.191.0/15
  - 37.142.191.32/16
  - Subnet = 37.142.0.0

Tabelas BGP

- **ASes**: *Autonomous Systems*
  - Conjunto de prefixos de IPs sob gestão de um grupo ou instituição comum;
  - Possuem características e políticas de roteamento comuns.
- **BGP**: *Border Gateway Protocol*
  - Protocolo de roteamento entre ASes;
  - Troca de informações de roteamento entre os roteadores = determinar os caminhos ideais para o fluxo de tráfego.
- 3 Tipos de tabelas:
  - *BGP Neighbor*
  - *BGP Table*
  - Tabela de Roteamento BGP

Desenvolvimento: Extração dos Dados

- Protocolo Telnet
- Expect Script
- Tabelas IPv4 e IPv6

Tabela: Relação dos IXs cujas tabelas foram extraídas

Salvador, BA (ba)	Belém, PA (bel)	Campinas, SP (cas)
Fortaleza, CE (ce)	Cuiabá, MT (cgb)	Campina Grande, PB (cpv)
Caxias do Sul, RS (cxj)	Brasília, DF (df)	Goiânia, GO (gyn)
Foz do Iguaçu, PR (igu)	João Pessoa, PB (jpa)	Lajeado, RS (laj)
Londrina, PR (lda)	Manaus, AM (mao)	Maringá, PR (mgf)
Belo Horizonte, MG (mg)	Natal, RN (nat)	Recife, PE (pe)
Curitiba, PR (pr)	Santa Maria, RS (ria)	Rio de Janeiro, RJ (rj)
Porto Alegre, RS (rs)	Florianópolis, SC (sc)	Aracajú, SE (se)
São José dos Campos, SP (sjc)	São José do Rio Preto, SP (sjp)	São Paulo, SP (sp)
Teresina, PI (the)	Vitória, ES (vix)	

Desenvolvimento: Extração dos Dados

- Apenas uma tabela de cada IX (29 tabelas)
- Apenas IPv4
- 812.513 diferentes endereços IP

```
spawn telnet lg.gyn.ptt.br
terminal length 0
show ip bgp
Trying 187.17.156.130...
Connected to lg.gyn.ptt.br.
Escape character is '^]'.
lg.gyn.ptt.br> terminal length 0
lg.gyn.ptt.br>
lg.gyn.ptt.br> show ip bgp
BGP table version is 0, local router ID is 200.192.111.252
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  1.18.129.0/24    200.192.111.15                         0 14026 16735 22548 23596 i
*                   200.192.111.15          30             0 16735 22548 23596 i
*                   200.192.111.15          30             0 16735 22548 23596 i
*>                  200.192.111.15          30             0 16735 22548 23596 i
*  2.16.188.0/23    200.192.111.15          30             0 16735 20940 20940 i
*                   200.192.111.15                         0 14026 16735 20940 20940 i
*                   200.192.111.15          30             0 16735 20940 20940 i
*>                  200.192.111.15          30             0 16735 20940 20940 i
*  2.20.68.0/23     200.192.111.15          30             0 16735 20940 20940 16625 i
*                   200.192.111.15                         0 14026 16735 20940 20940 16625 i
*                   200.192.111.15          30             0 16735 20940 20940 16625 i
*>                  200.192.111.15          30             0 16735 20940 20940 16625 i
*  2.21.176.0/22    200.192.111.15                         0 14026 16735 28663 61813 20940 20940 i
*                   200.192.111.15                         0 16735 28663 61813 20940 20940 i
*                   200.192.111.15                         0 16735 28663 61813 20940 20940 i
*>                  200.192.111.15                         0 16735 28663 61813 20940 20940 i
```

Desenvolvimento: Banco de Dados

- Banco de Dados Completo SQL: *Looking Glass*
- Inclusão das tabelas: **Routes** e **BGP_Path**
- Tabelas utilizadas:
  - File: Armazena o nome do arquivo;
  - Files_Description: Chave estrangeira para a tabela "File", amarzena o "*local router id*" e a versão da tabela BGP;
  - IP: Armazena o número IP em decimal e sua respectiva máscara;
  - Routes: Armazena as informações de cada rota da Tabela de Roteamento BGP;
  - BGP_Path: Armazena os *paths* de cada rota (uma rota pode ter um ou mais *paths*).

Desenvolvimento: Banco de Dados

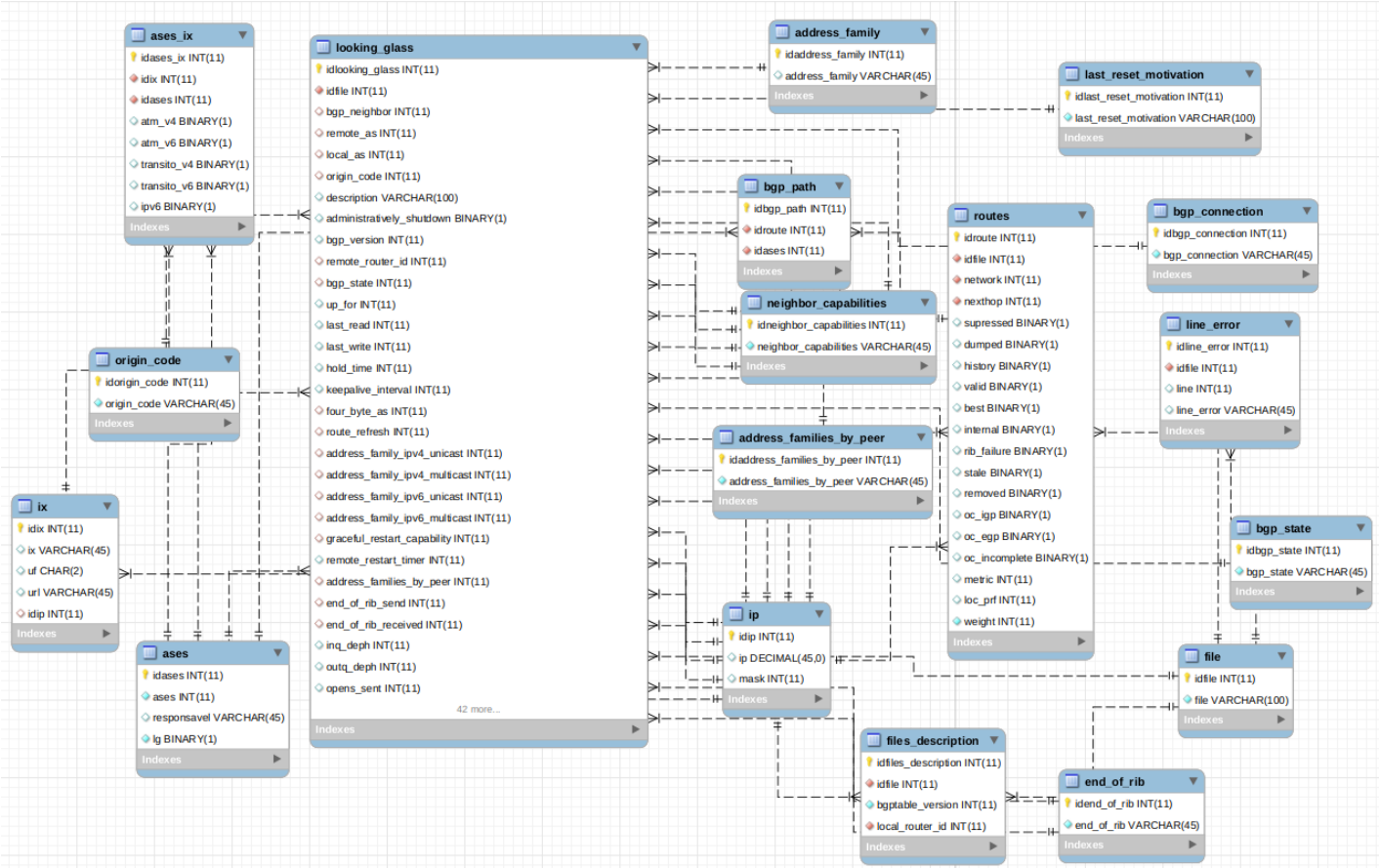


Figura: Modelo esquemático do banco de dados

Desenvolvimento: Parsing

- Python
- Parsing + Inserção
- Valores:
  - *Local Router Id*;
  - Versão da tabela;
  - Para cada rota:
    - *Status codes*;
    - *Network*;
    - *Next hop*;
    - *Metric*;
    - *Local preference*;
    - *Weight*;
    - *Path*;
    - *Origin codes*.

Desenvolvimento: Parsing

- Dificuldades:
  - Espaçamento indeterminado > Indíces com base no cabeçalho;
  - Valores ausentes;
  - Tabelas corrompidas ou vazias > Tratamento especial;
  - Repetição de valores > Consulta ao banco antes de cada inserção;
  - Grande volume de dados > Otimização (Dicionário, tabela *hash* + acesso a memória);
  - Formatação e quebra de linhas diferentes pro IPv4 e pro IPv6;

Desenvolvimento: Análise

- R
- Extração dos IPs da tabela IP;
- Conversão String $->$ Decimal e depois, Decimal $->$ String;
- Função para obtenção das *subnets*;
- Construção de blocos;
- Classes A, B, C, D e E. Conversão do primeiro octeto para binário:
  - Classe A: Começa com 0;
  - Classe B: Começa com 10;
  - Classe C: Começa com 110;
  - Classe D: Começa com 1110;
  - Classe E: Resto.

Desenvolvimento: Análise

- Perguntas:
  - Qual a porcentagem de redundância de IPs em rotas da Tabela de Roteamento BGP?
  - Em quais classes elas mais ocorrem (Classes A, B, C e D)?
  - Qual a frequência desses blocos de endereços IPs?
  - Esses blocos com maior frequência estão bem distribuídos ou concentrados em uma determinada região e/ou estado?

Resultados

- 752.148 blocos de IP, 60.365 endereços redundantes: **7.43% de redundância**

Tamanho do Bloco	Quantidade de Blocos
1	700.478
2	44.449
3	6.018
4	970
5	199
6	30
7	4

Resultados

Tabela: Frequência das classes de endereço IP

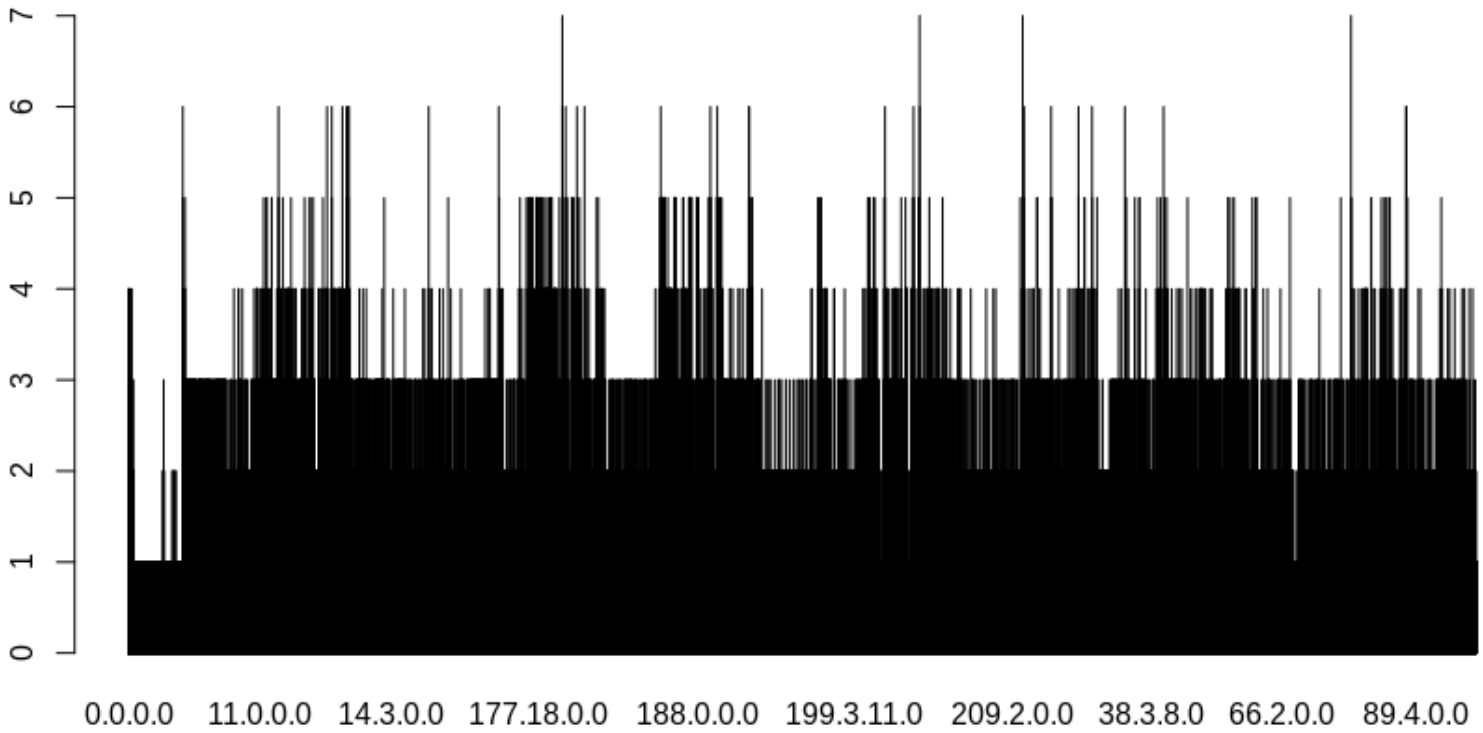
Classe	Frequência
A	4.234
B	406.307
C	27.6393
D	32.210
E	33.004

Resultados

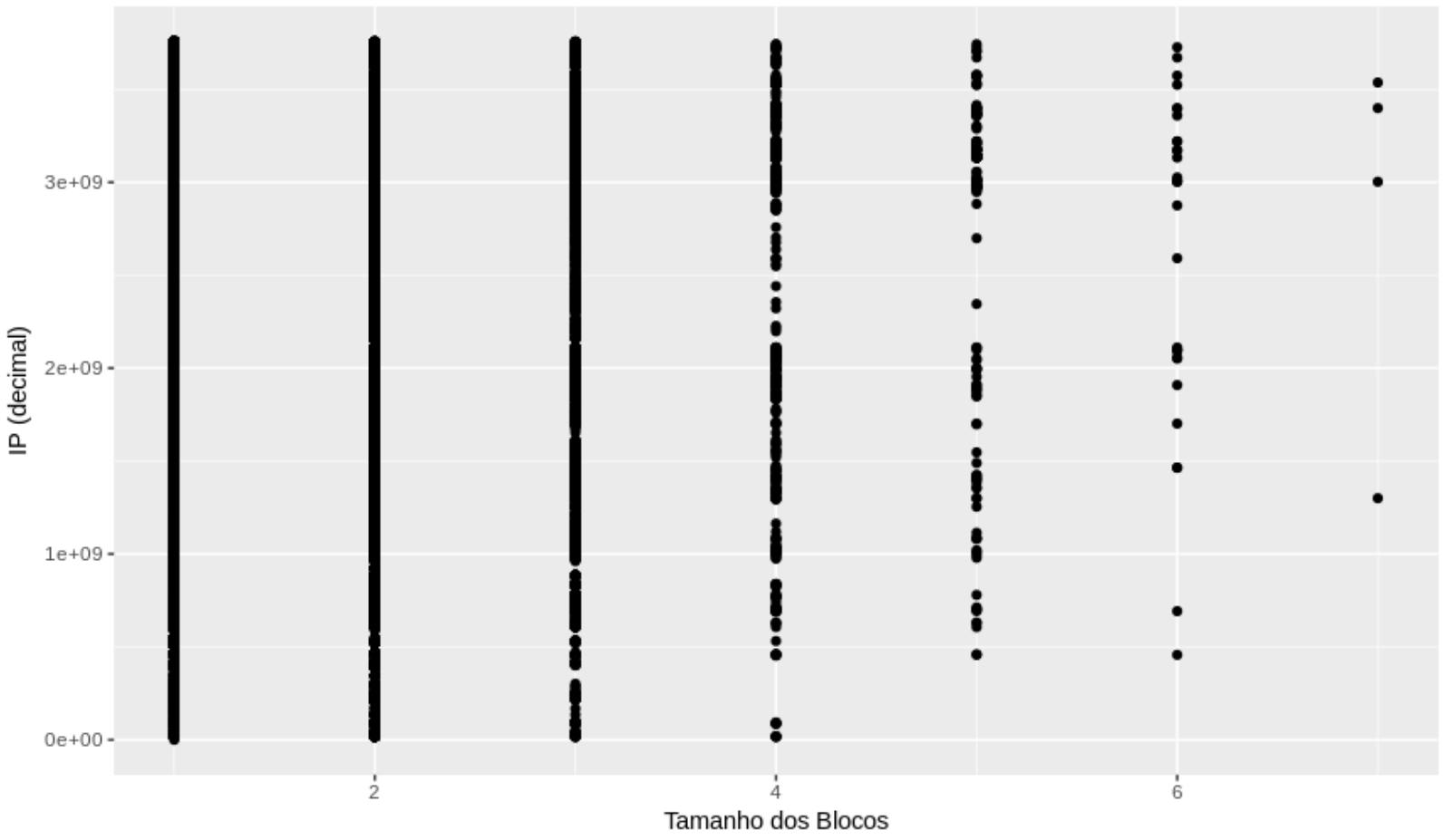
Tabela: Tamanho dos blocos por Classes

Tamanho do Bloco	A (%)	B (%)	C (%)	D (%)	E (%)
1	0.57	53.77	37.14	4.17	4.34
2	0.51	56.32	32.42	5.73	5.00
3	0.33	63.40	25.75	5.61	4.88
4	0.51	65.46	22.37	4.94	6.70
5	69.34	21.10	6.03	3.51	0
6	46.66	30.00	3.33	20.00	0
7	0	50	50	0	0

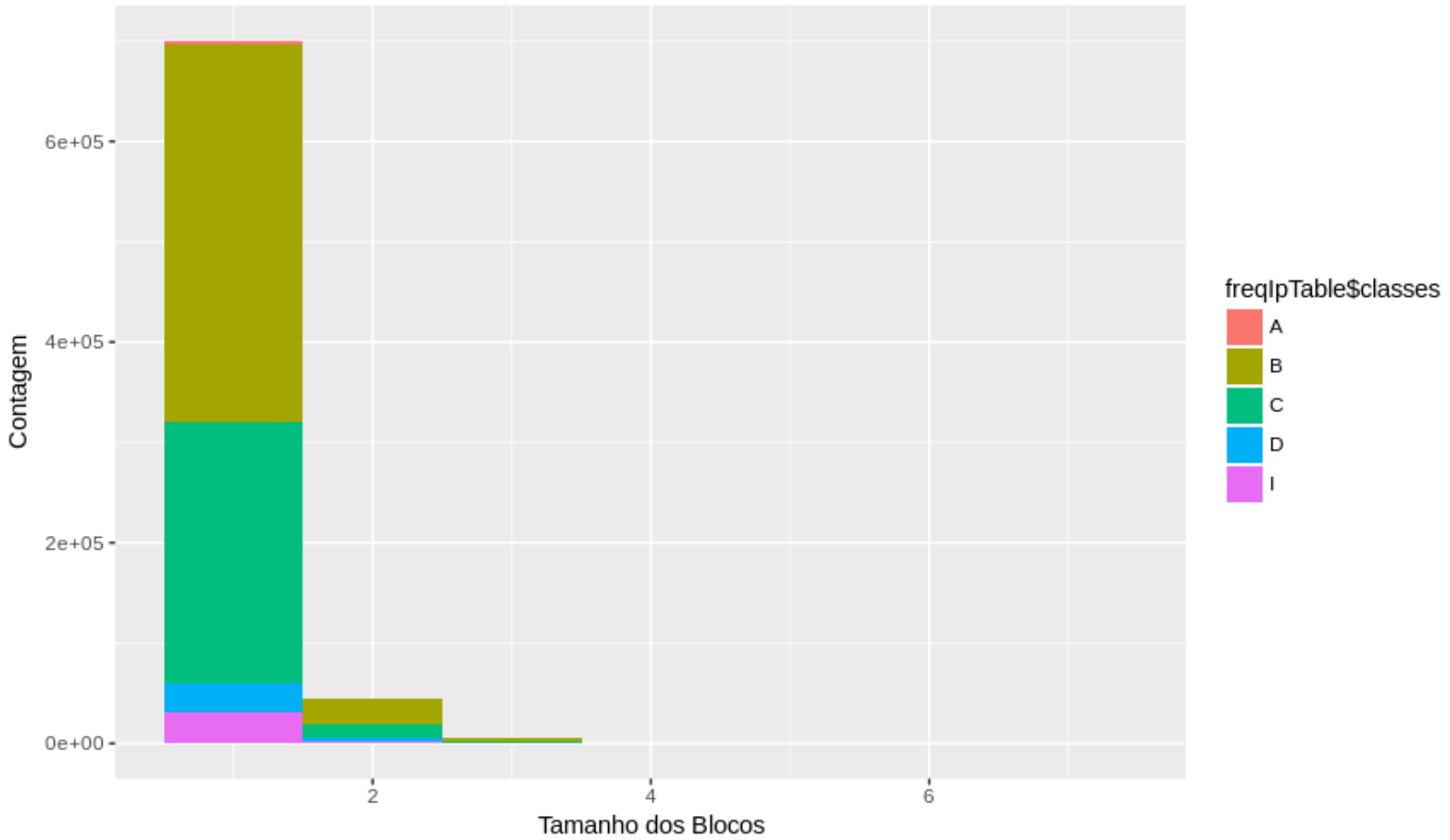
Resultados


0
1
2
3
4
5
6
7
0.0.0.0
11.0.0.0
14.3.0.0
177.18.0.0
188.0.0.0
199.3.11.0
209.2.0.0
38.3.8.0
66.2.0.0
89.4.0.0

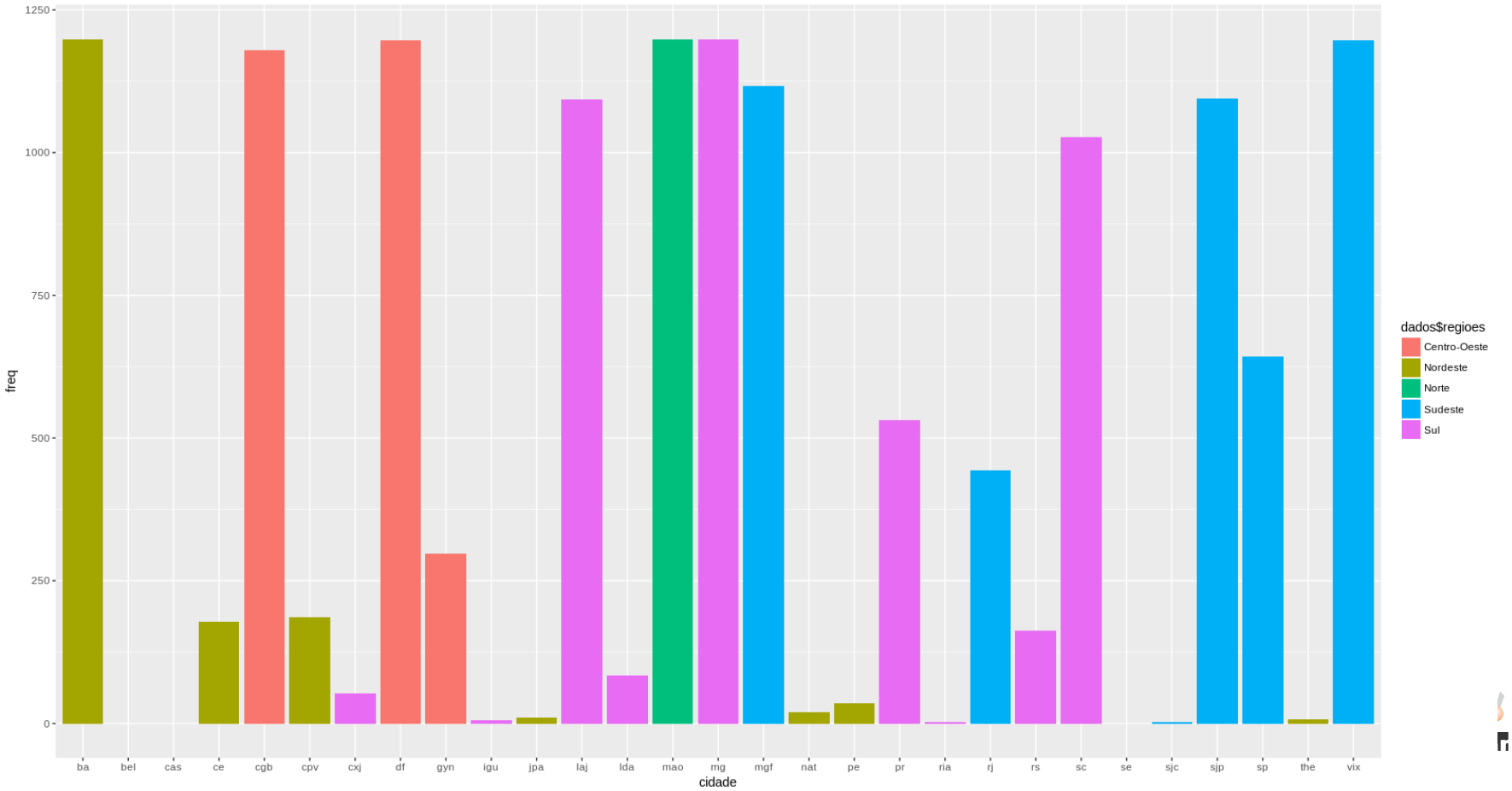
Resultados



Resultados


6e+05
4e+05
2e+05
0e+00
Contagem
2
4
6
Tamanho dos Blocos
freqIpTable$classes
A
B
C
D
I

Resultados


1250
1000
750
500
250
0
freq
ba
bel
cas
ce
cgb
cpv
cxj
df
gyn
igu
jpa
laj
lda
mao
mg
mgf
nat
pe
pr
ria
rj
rs
sc
se
sjc
sjp
sp
the
vix
cidade
dados$regioes
Centro-Oeste
Nordeste
Norte
Sudeste
Sul

Conclusões

- Conseguimos chegar a uma porcentagem de redundância em endereços de IP das rotas BGP: 7.43%;
  - Informação relevante em casos de busca por padronização ou generalização das tabelas, como no caso da criação de uma tabela única.
- Gostaríamos de ter expandido a pesquisa para tabelas de roteamento BGP obtidas dos mais diversos Looking Glass;
  - Dificuldades: Contato, SQL injection...

Conclusões

- Qual a porcentagem de redundância de IPs em rotas da Tabela de Roteamento BGP? 7.43%.
- Em quais classes elas mais ocorrem (Classes A, B, C e D)? Classes A e B.
- Qual a frequência desses blocos de endereços IPs? Exposto na Tabela do slide 14.
- Esses blocos com maior frequência estão bem distribuídos ou concentrados em uma determinada região e/ou estado? Não existe nenhuma relação óbvia entre os tamanhos dos blocos e determinada região e/ou estado.