

nic.br cgi.br

ceptro.br

Rodrigo Regis dos Santos
Tiago Jun Nakamura
São Paulo, SP
16 de julho de 2015

Introdução ao Gerenciamento de Redes

O que é a Internet?

O que é a Internet?

Equipamentos que compõe a Internet:



Switch



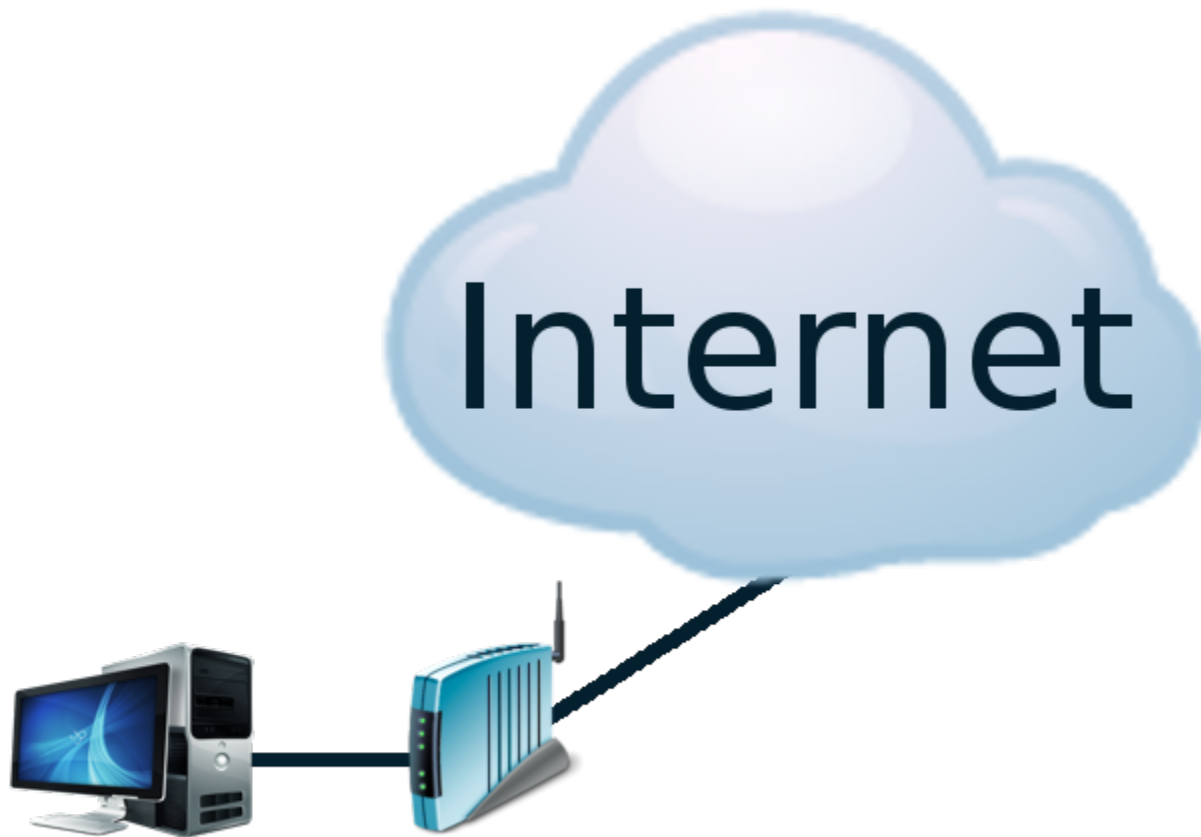
Roteador



Nuvem

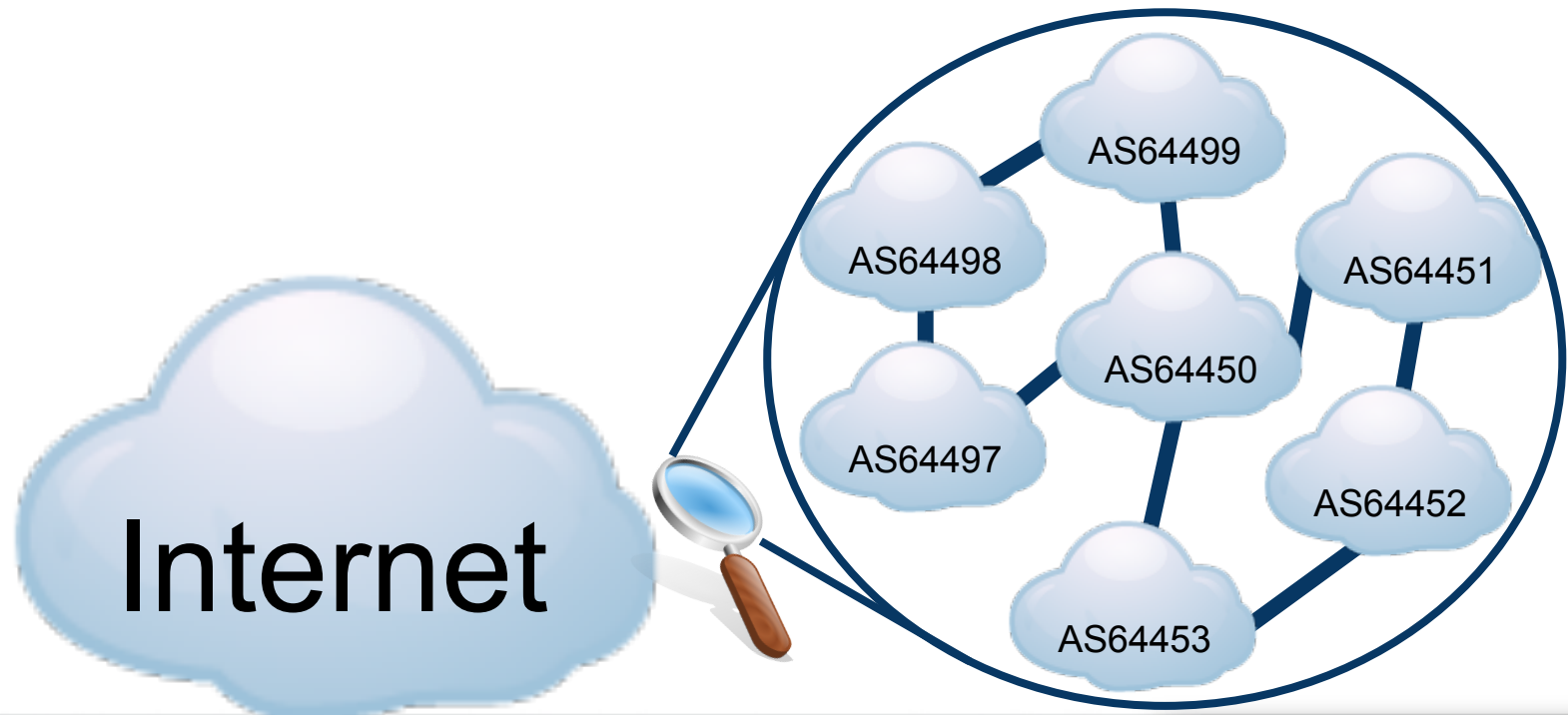
O que é a Internet?

Do ponto de vista do usuário



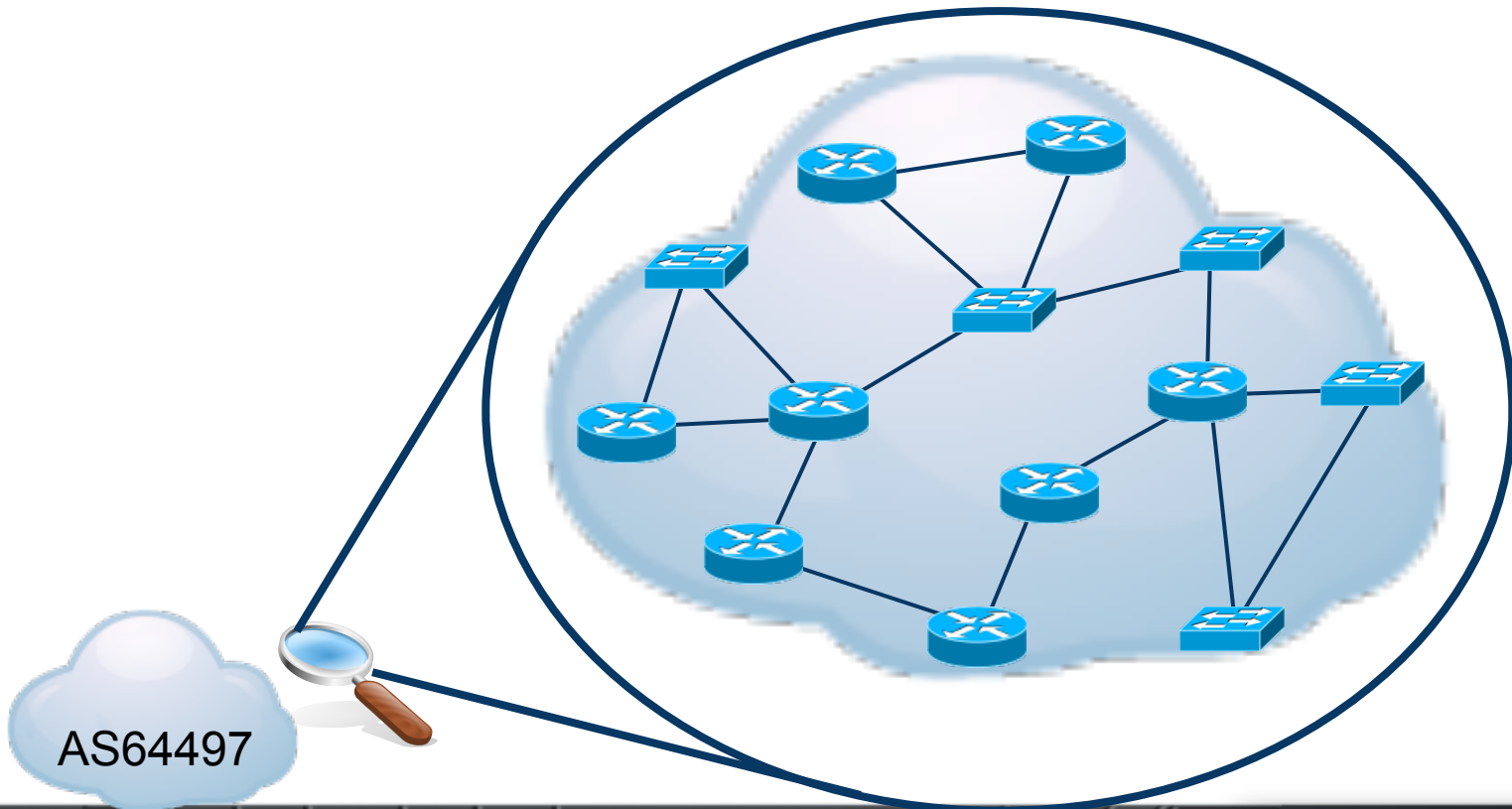
O que é a Internet?

A Internet é um aglomerado de "nuvens", conhecidas como Sistemas Autônomos (AS)



O que é a Internet?

Cada Sistema Autônomo possui sua própria rede interna



O que é um ISP?

O que é um ISP?

ISP = Internet Service Provider

Também conhecido como IAP (Internet Access Provider), é o AS que leva a Internet ao usuário final

O que é um ISP?

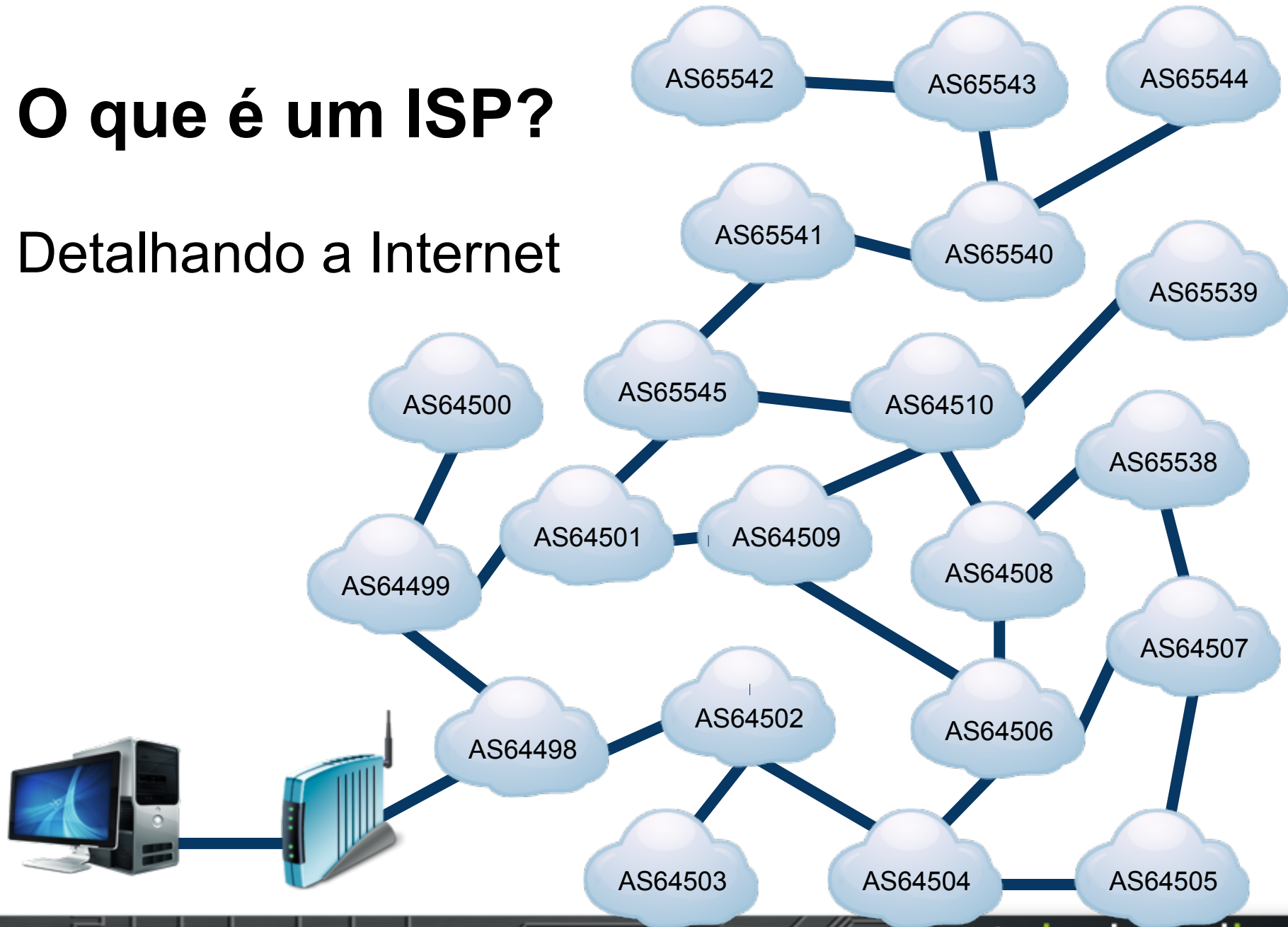
Do ponto de vista do usuário



Internet

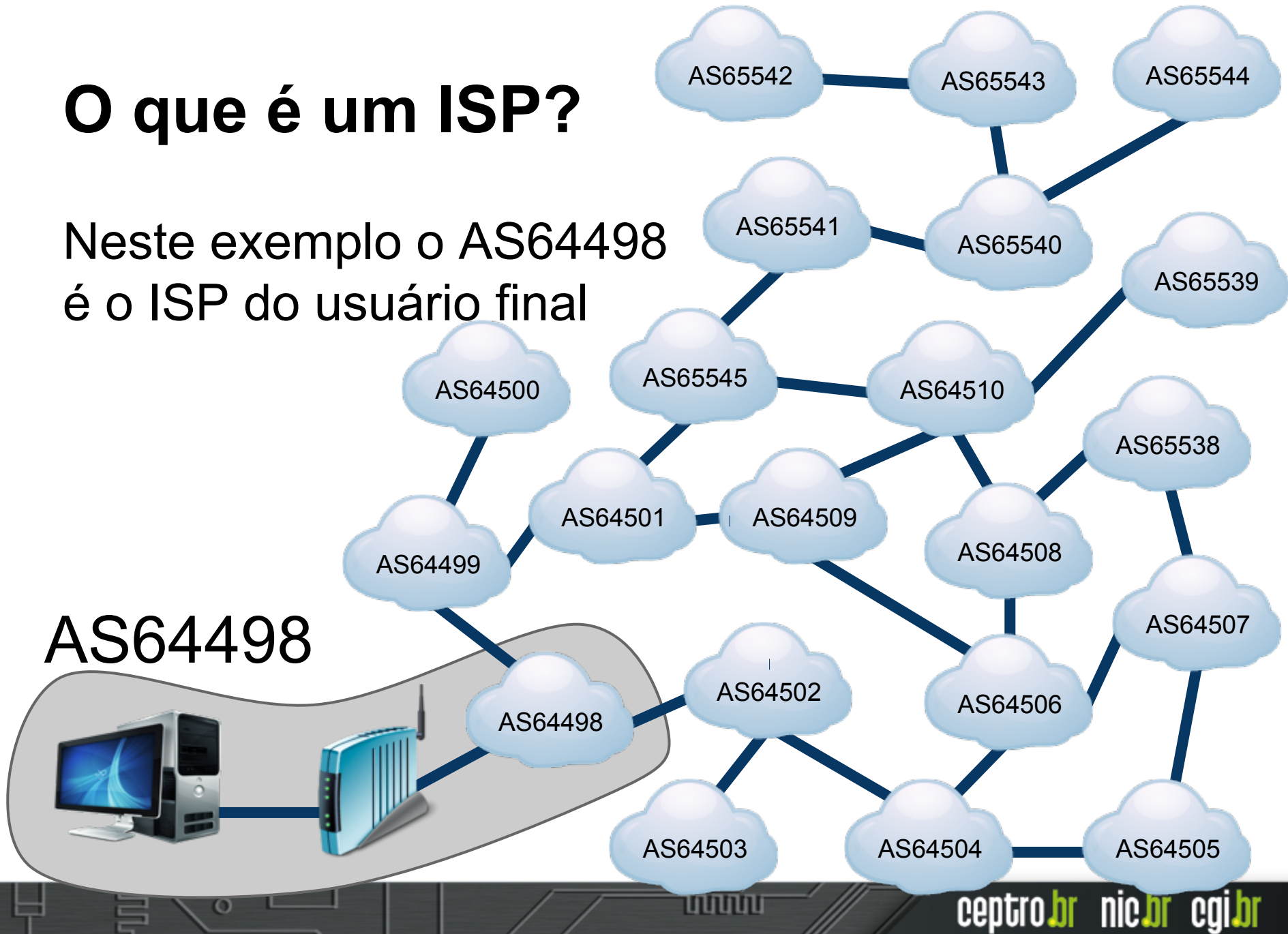
O que é um ISP?

Detalhando a Internet



O que é um ISP?

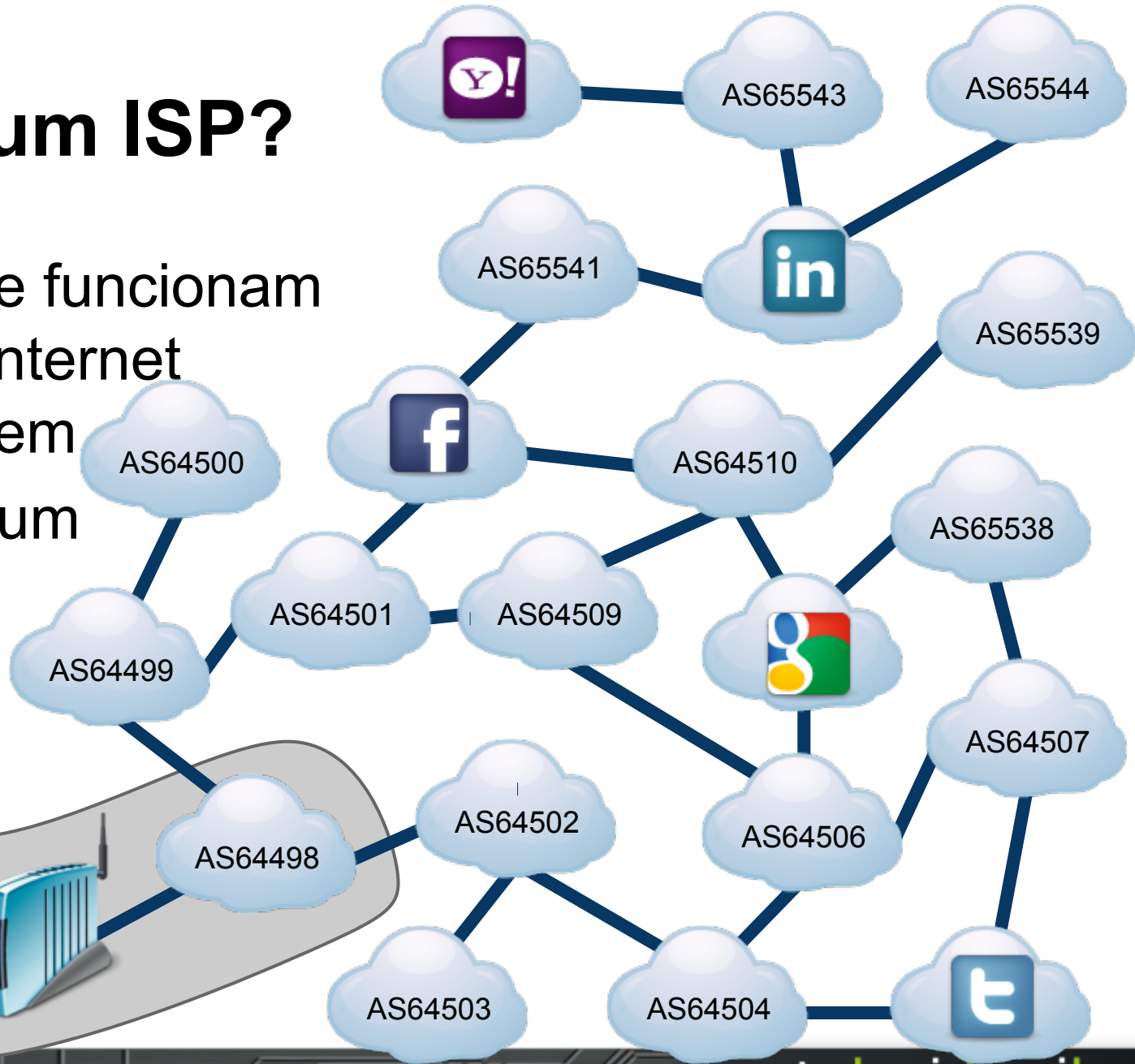
Neste exemplo o AS64498 é o ISP do usuário final



O que é um ISP?

Serviços que funcionam através da Internet também fazem parte de algum AS

AS64498



O que é BGP?

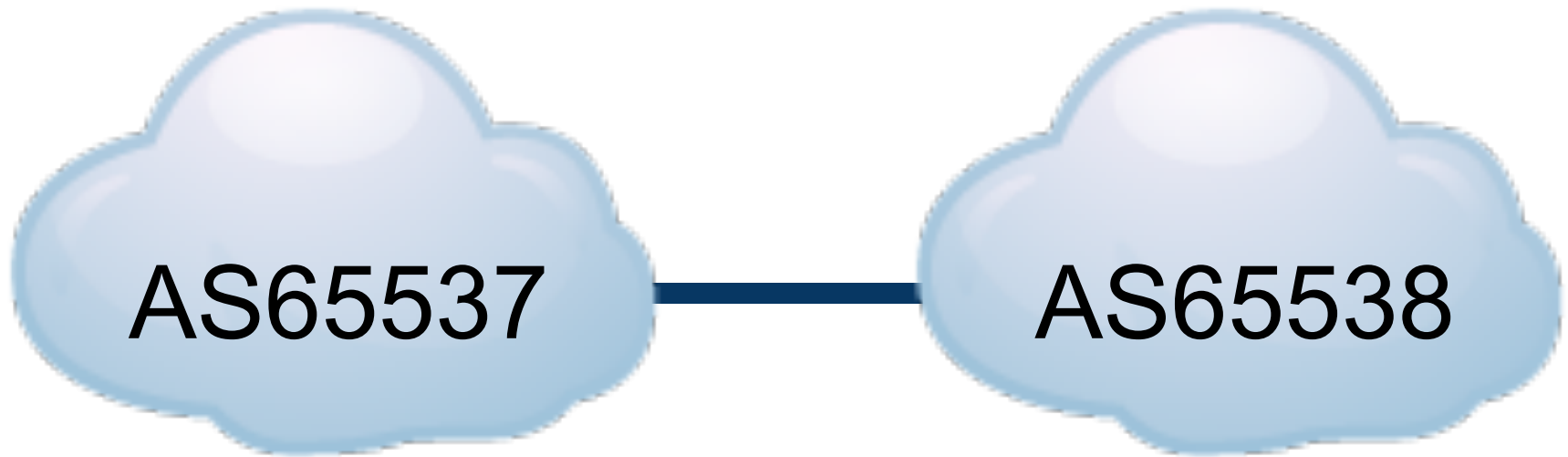
O que é BGP?

BGP = Border Gateway Protocol

Protocolo que os AS usam para comunicar entre si

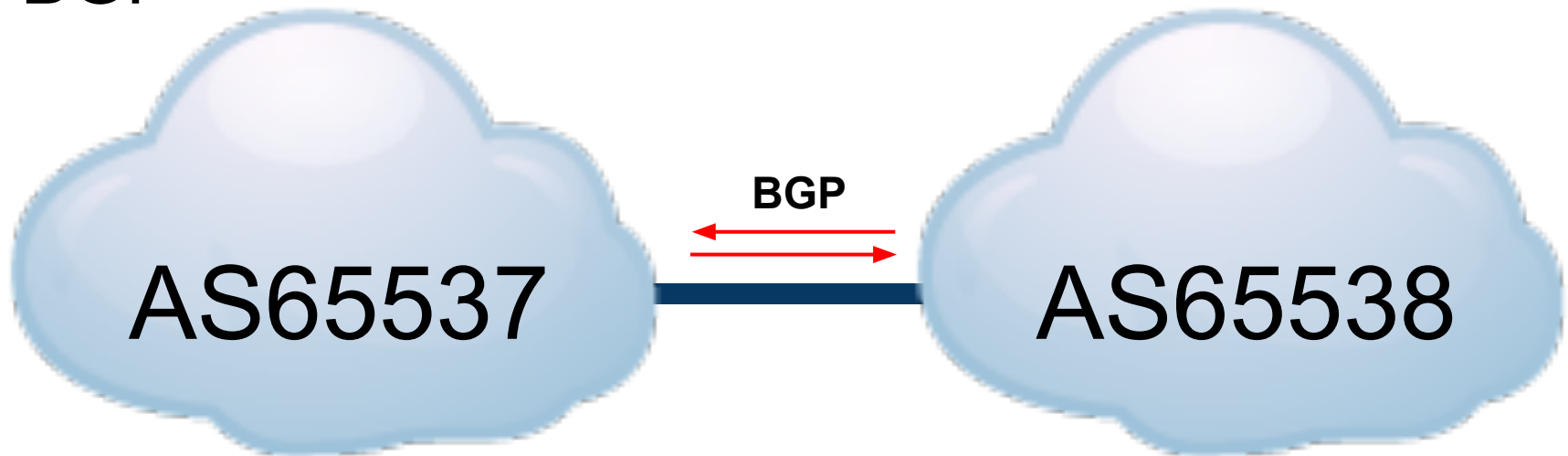
O que é BGP?

Exemplo: 2 AS conectados entre si



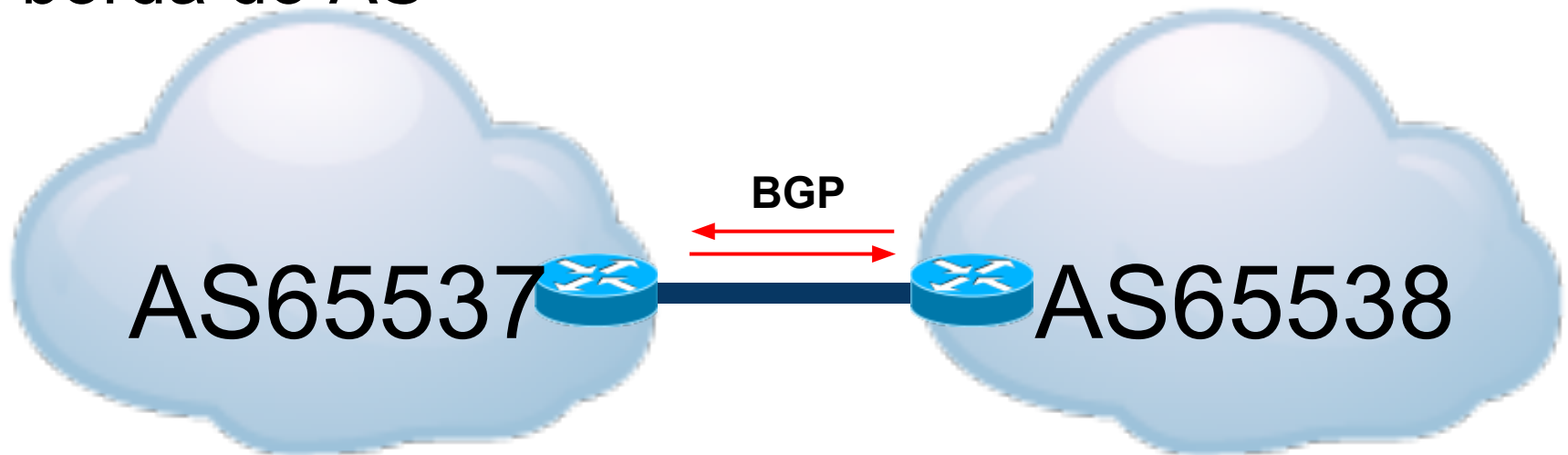
O que é BGP?

Sua comunicação é feita através do protocolo BGP



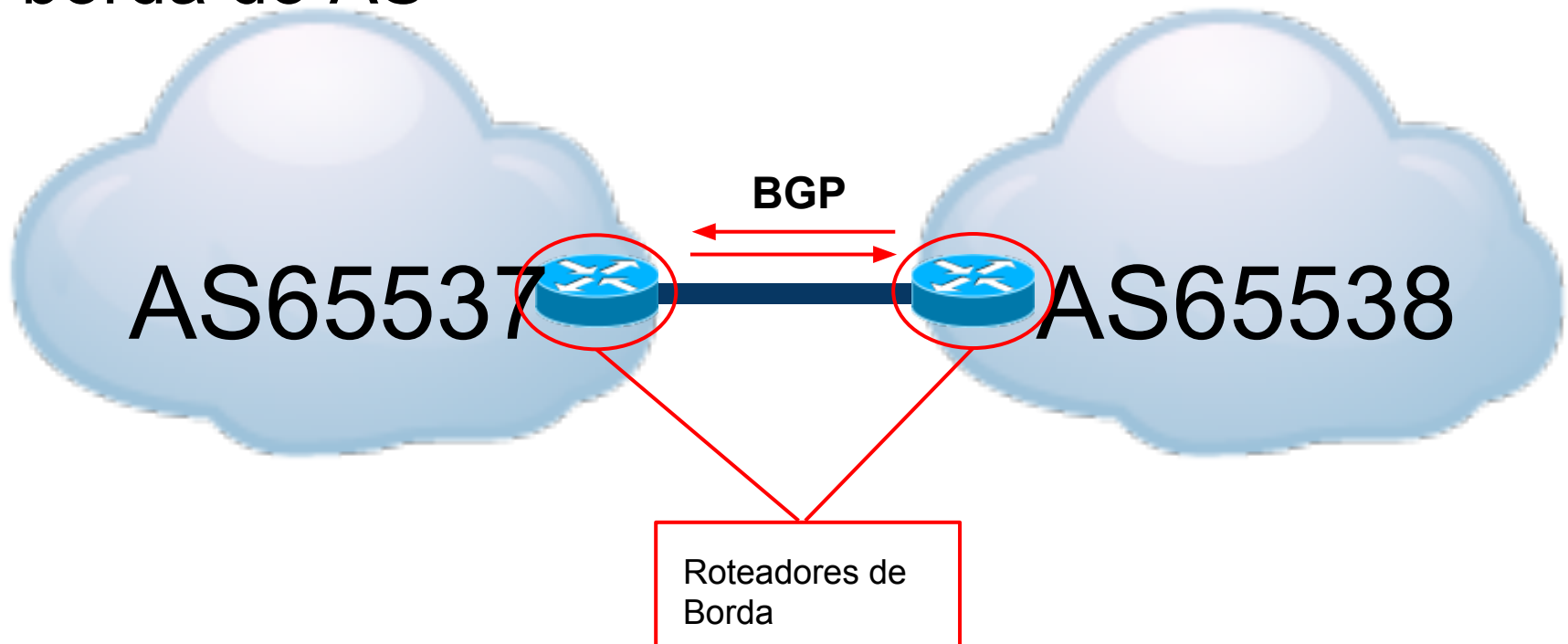
O que é BGP?

O protocolo BGP é utilizado nos roteadores de borda do AS



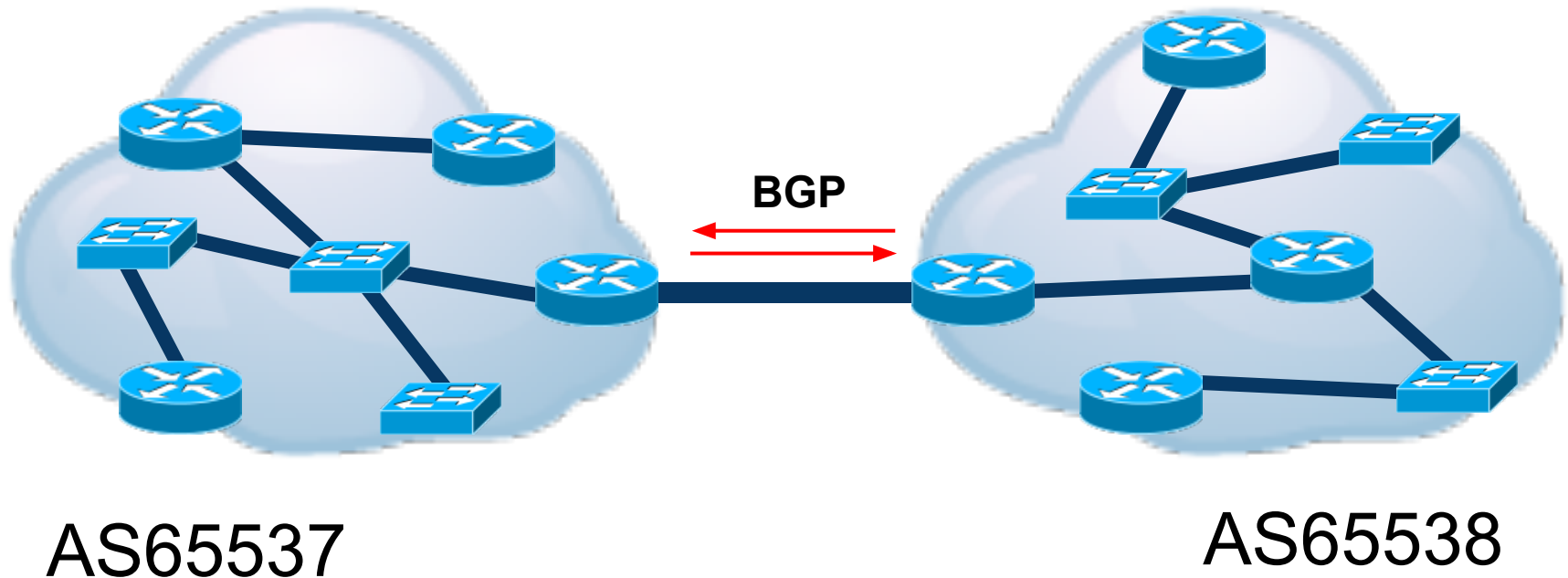
O que é BGP?

O protocolo BGP é utilizado nos roteadores de borda do AS



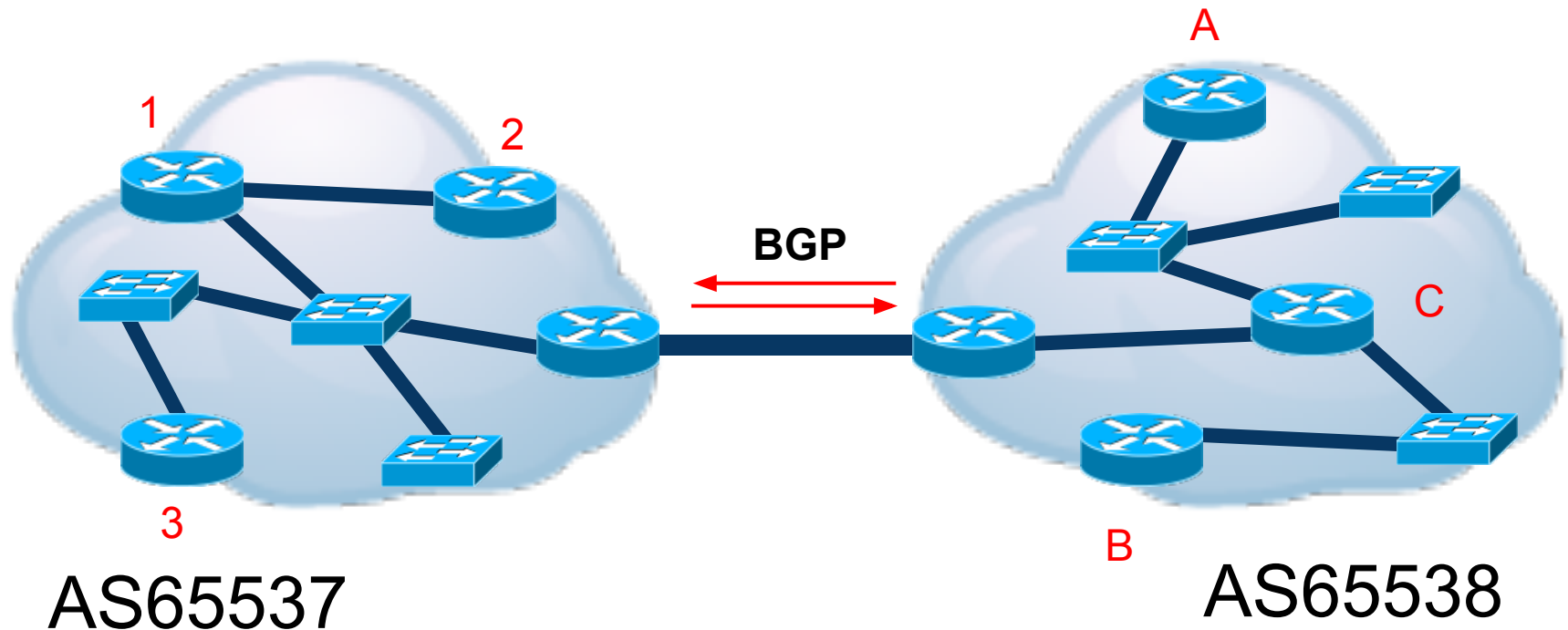
O que é BGP?

Detalhando a rede interna de cada AS



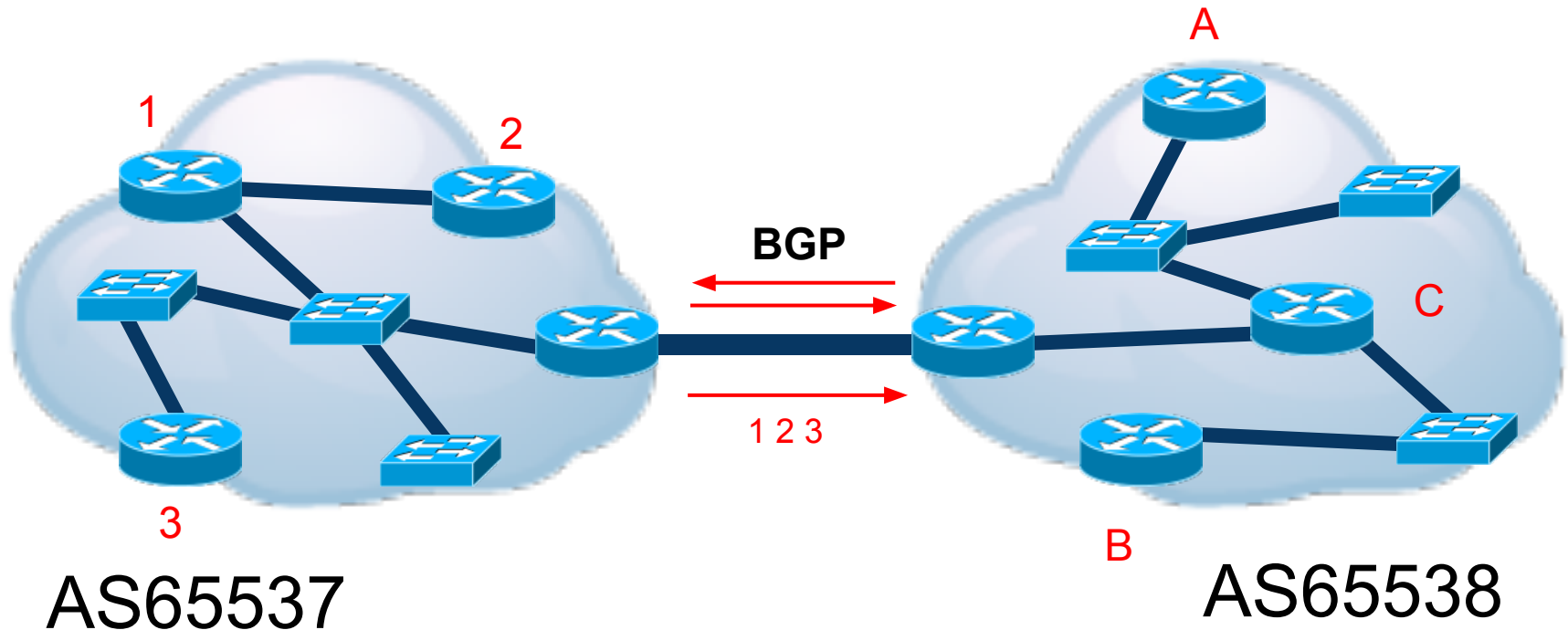
O que é BGP?

Colocando nomes nas máquinas de cada rede



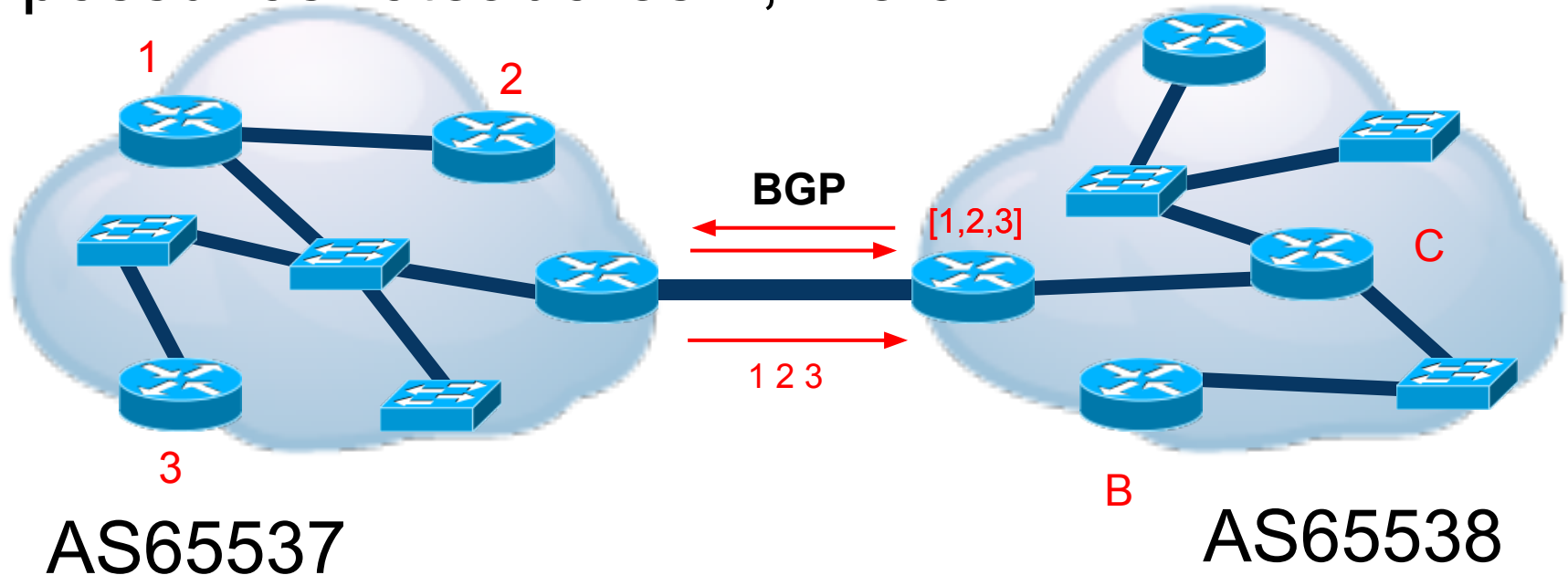
O que é BGP?

AS65537 envia informações sobre sua rede



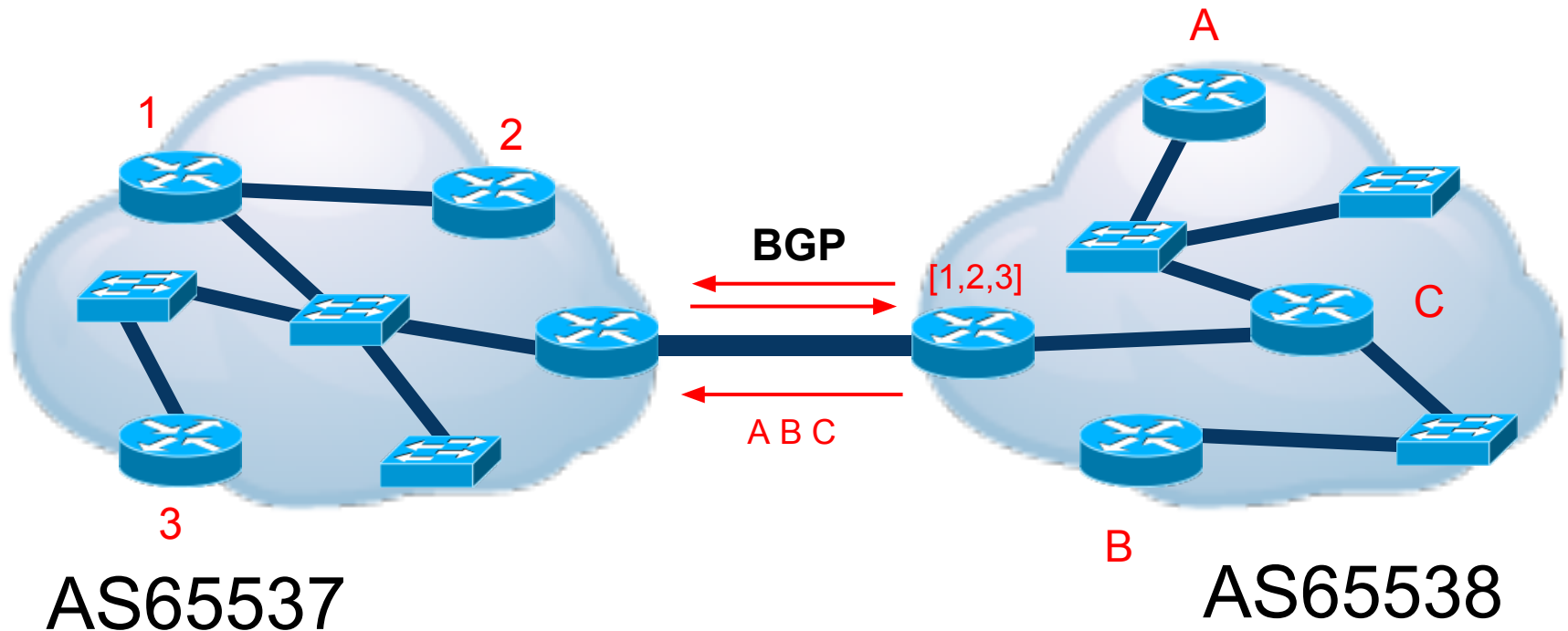
O que é BGP?

Assim o AS65538 descobre que o AS65537 possui os roteadores 1, 2 e 3



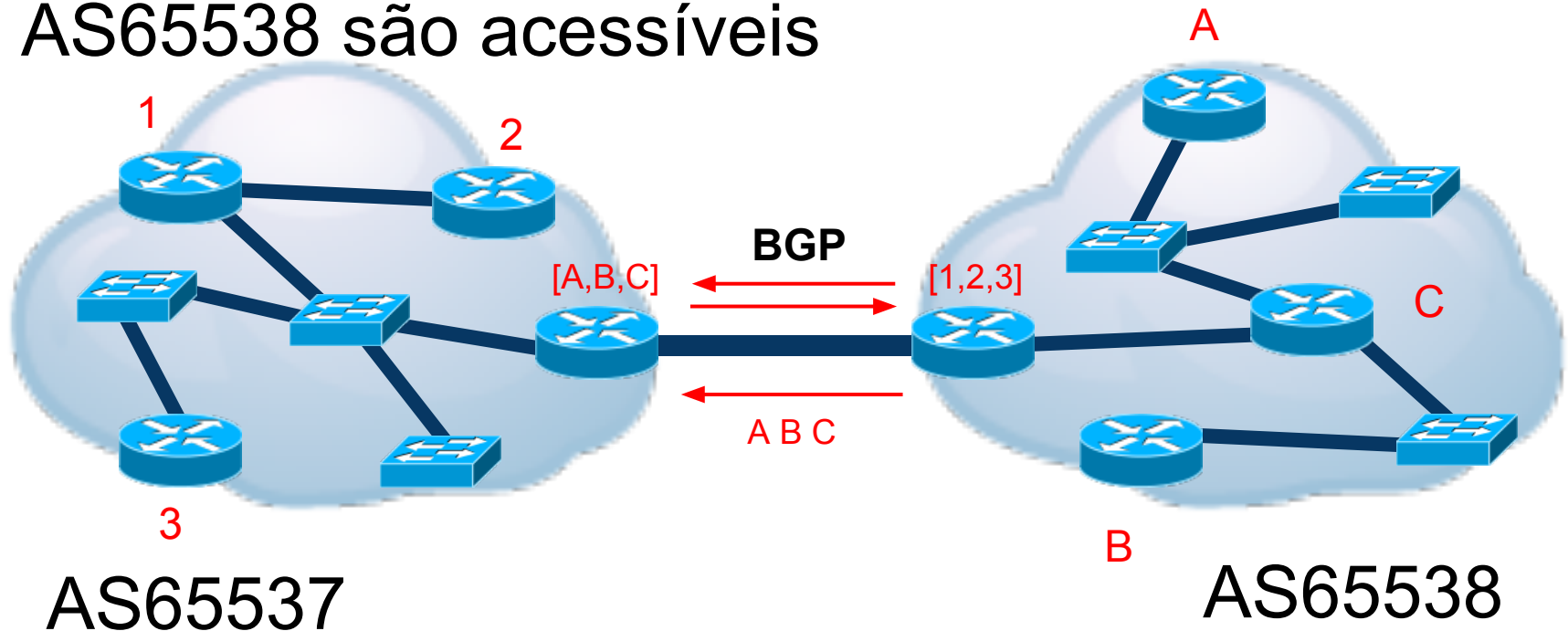
O que é BGP?

AS65538 também faz a mesma coisa



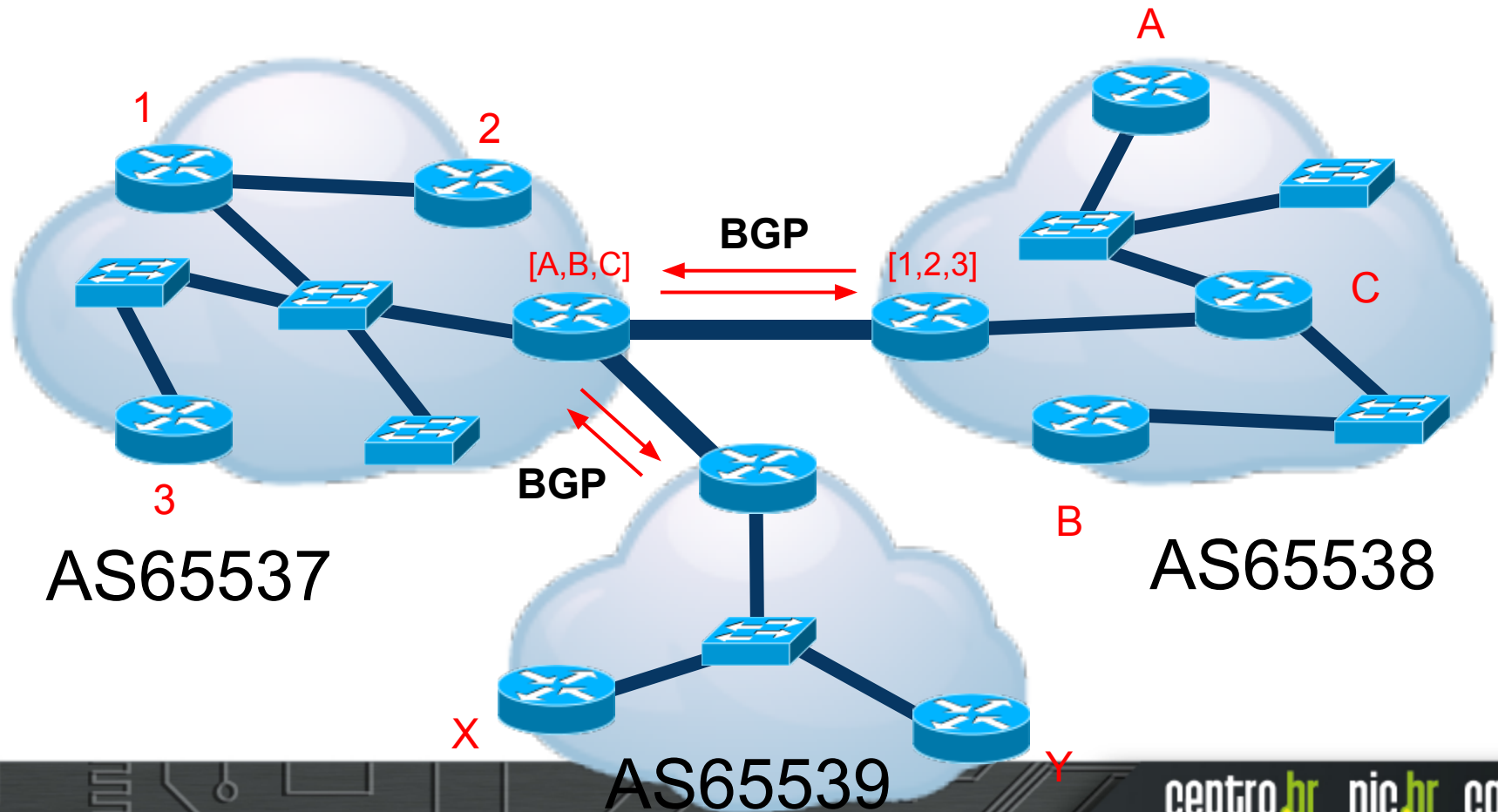
O que é BGP?

E o AS65537 descobre quais máquinas do AS65538 são acessíveis



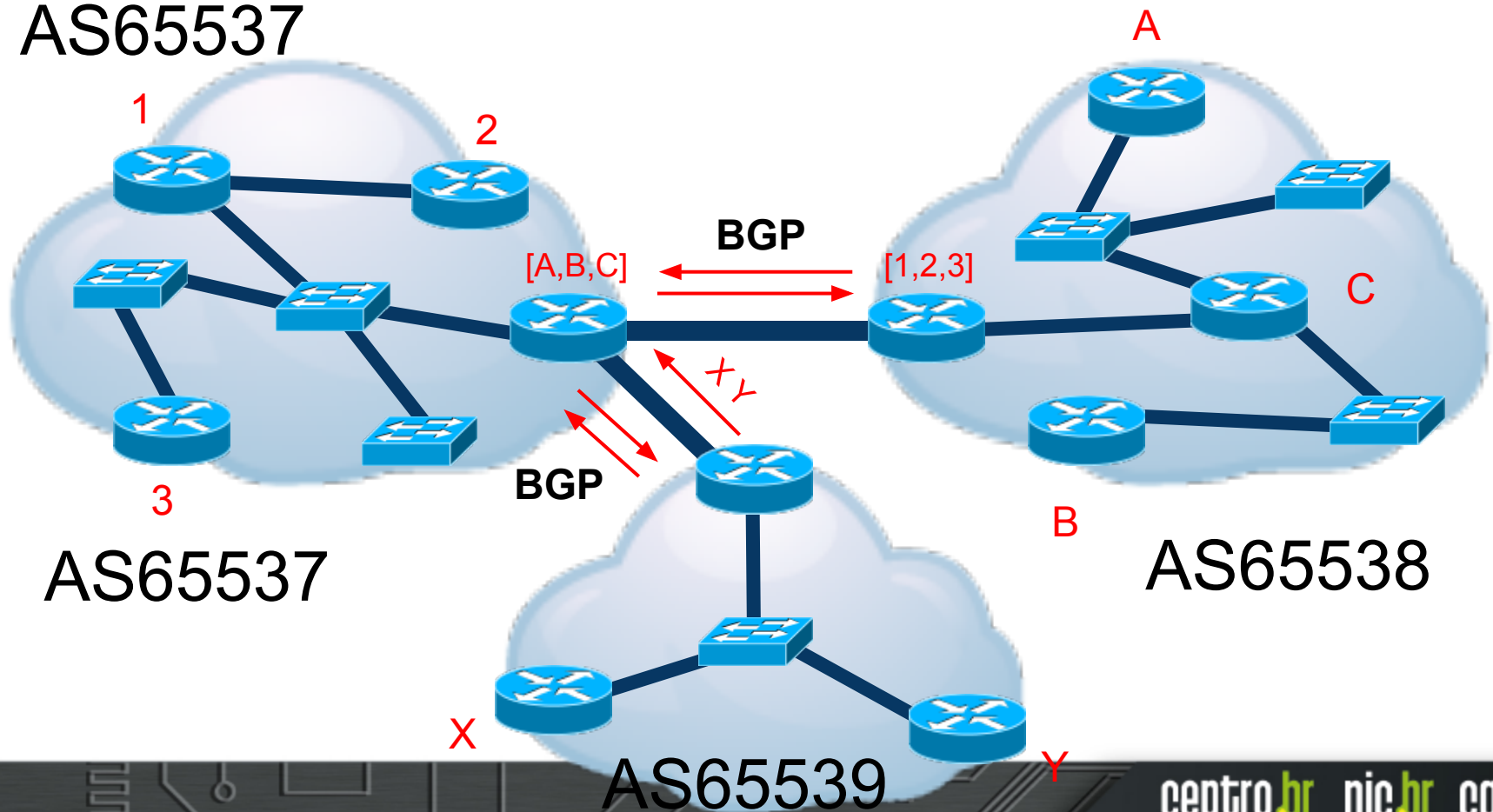
O que é BGP?

Com mais um AS no exemplo



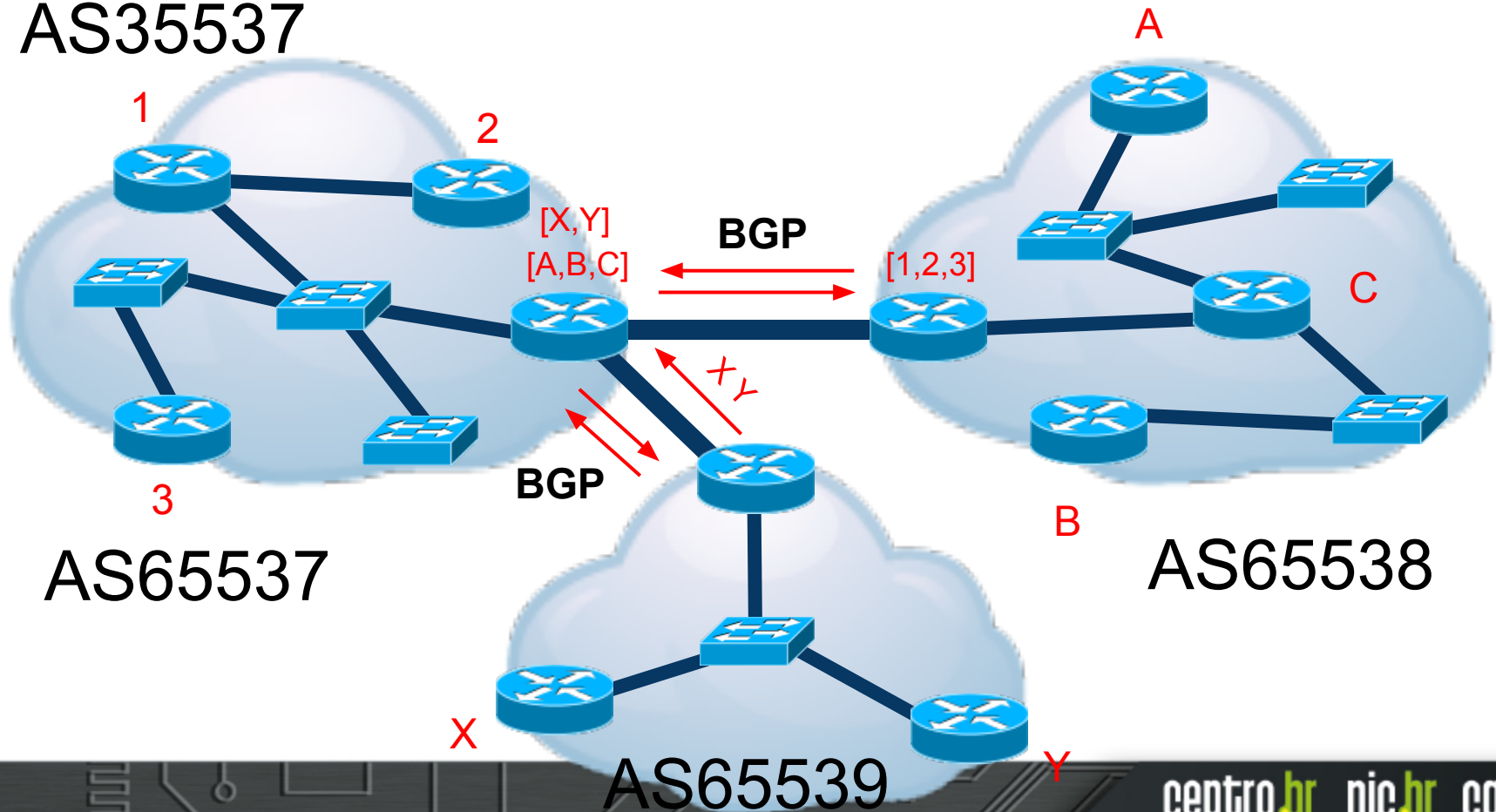
O que é BGP?

O AS novo envia suas informações para o AS65537



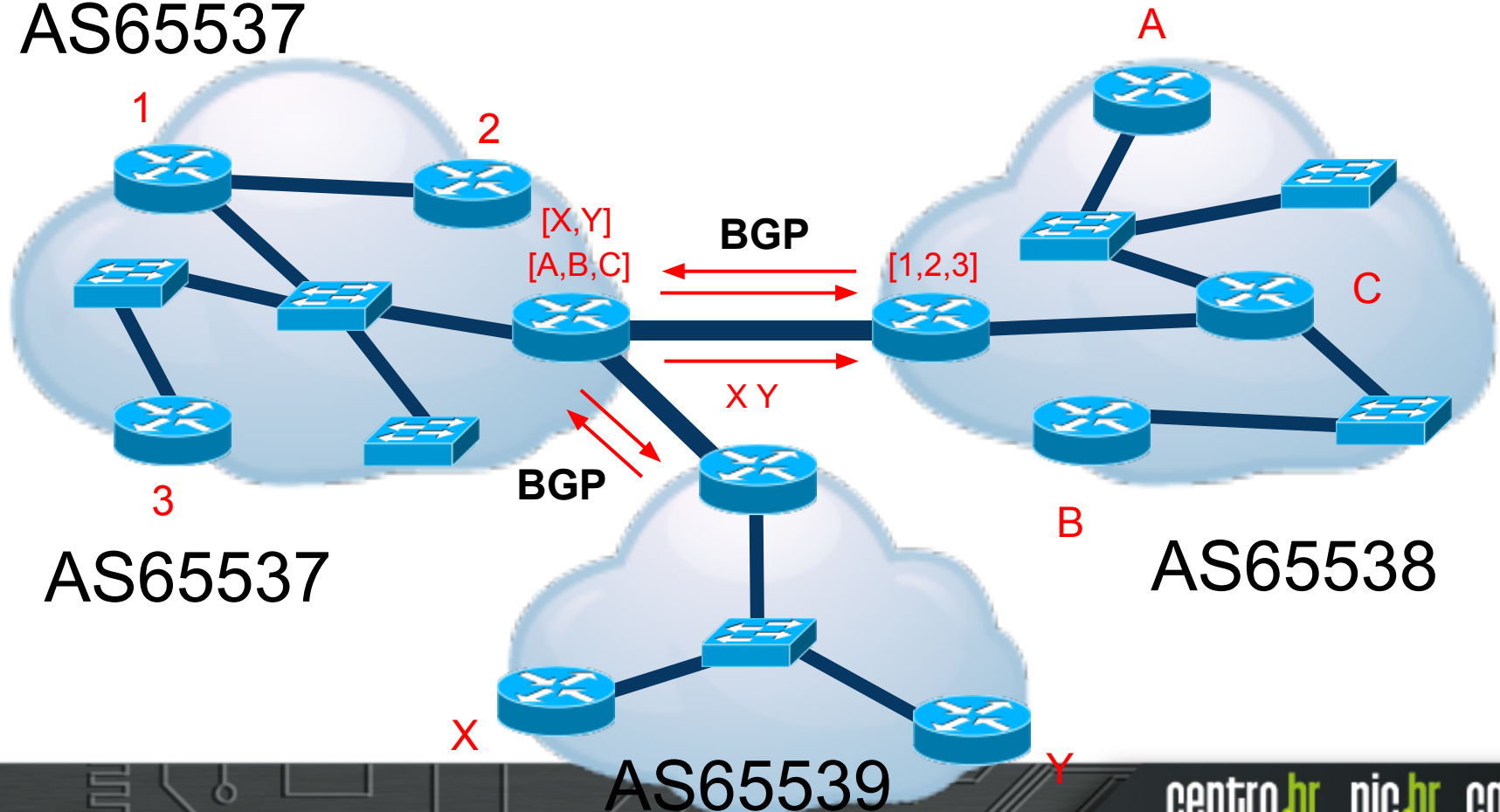
O que é BGP?

O AS novo envia suas informações para o AS35537



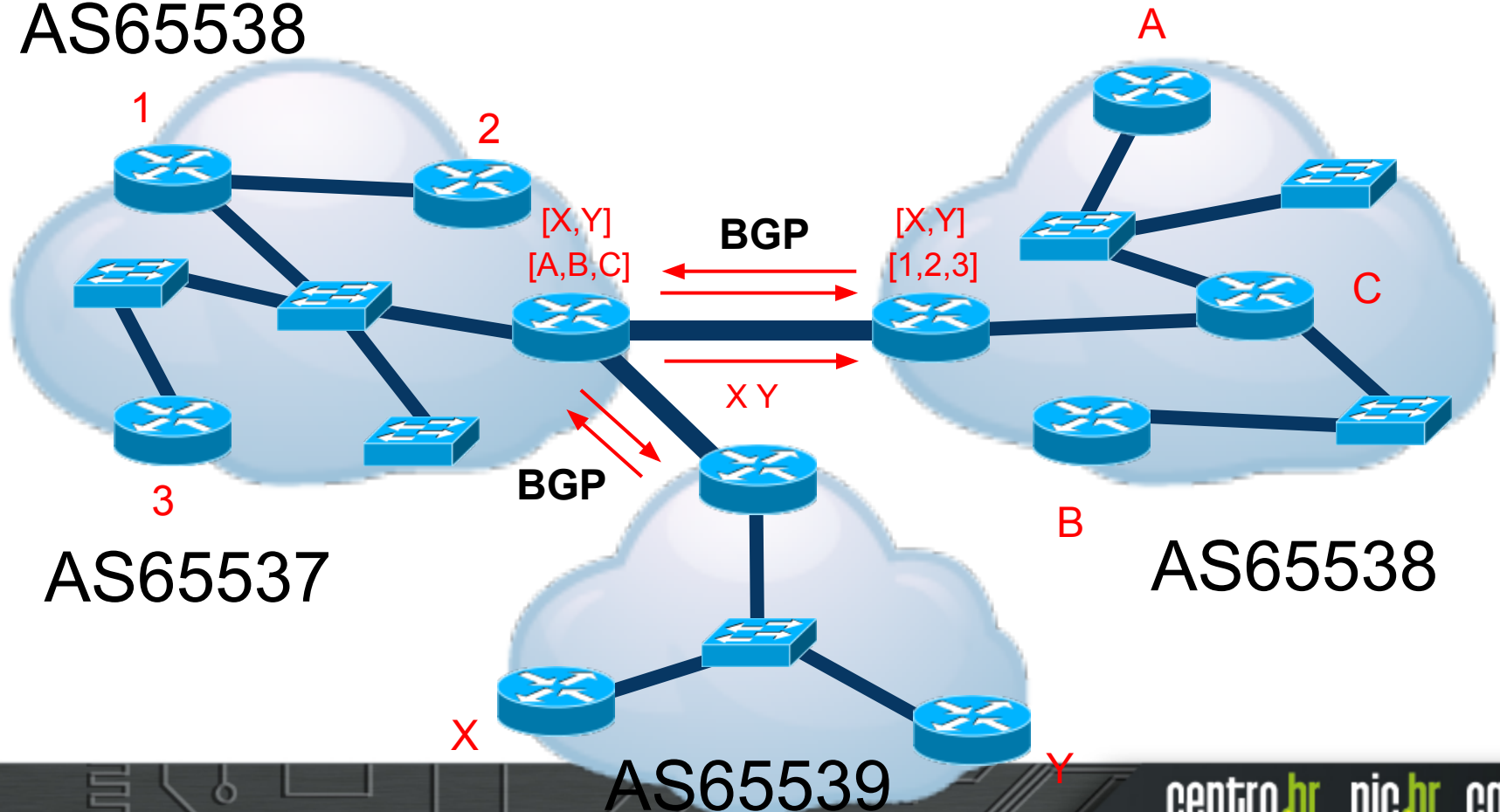
O que é BGP?

O AS novo envia suas informações para o AS65537



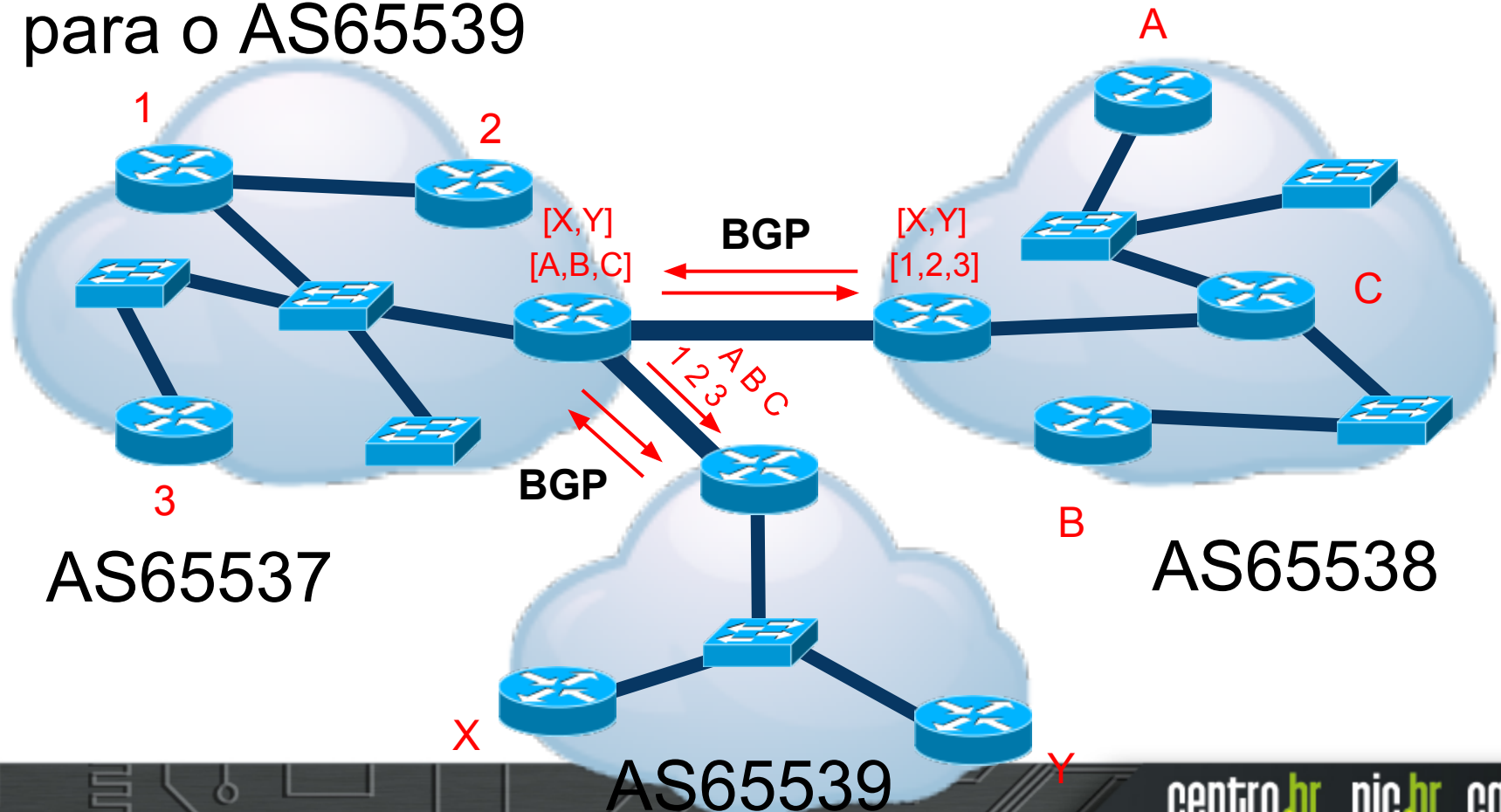
O que é BGP?

E o AS65537 repassa os dados para o AS65538



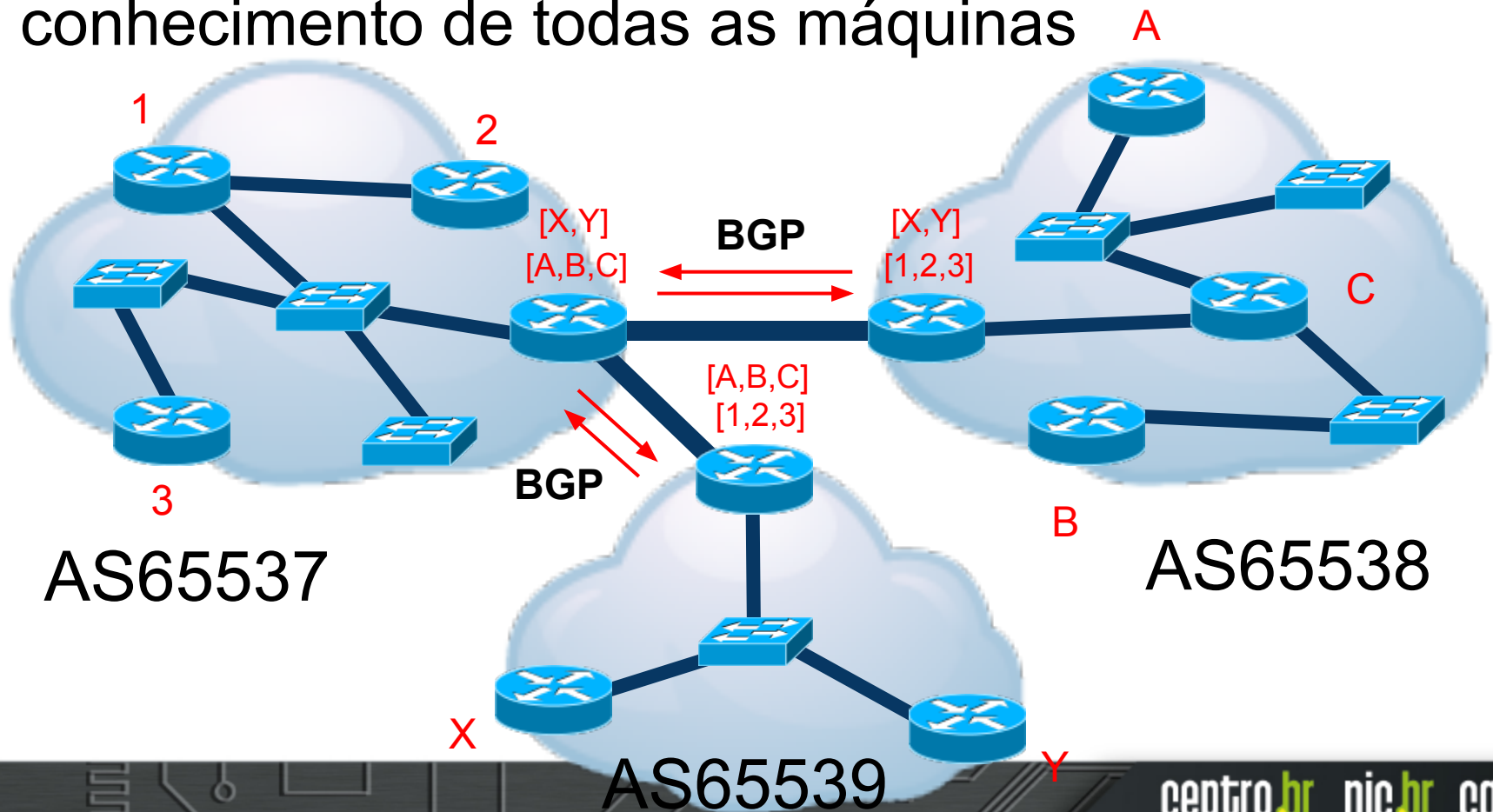
O que é BGP?

O AS65537 também repassa suas informações para o AS65539



O que é BGP?

Ao final do processo todos os AS tem conhecimento de todas as máquinas



Introdução ao Gerenciamento de Redes

- Motivação
- Conceitos Importantes
- Protocolos Importantes
- Tipos de Ferramentas
- Extras

Motivação

Motivação

→ Gerenciar para que?

- ◆ Melhorar a organização
- ◆ Detectar problemas desconhecidos na rede
- ◆ Aumentar a disponibilidade do sistema
- ◆ Aumentar a performance do sistema
- ◆ Diminuir custos
- ◆ Conhecer a sua rede

O que é gerência de redes?

- Garantir o funcionamento correto da rede
 - ◆ Qualidade
 - ◆ Desempenho
 - ◆ Resolução de problemas
- Redução de custos
- Tomada de decisão
 - ◆ Troca de equipamentos
 - ◆ Novas ferramentas

O que é gerência de redes?

- Monitorar a disponibilidade e tempo de resposta
- Automatizar processos
- Segurança
- Controle de tráfego
- Detecção e correção de falhas
- Prever possíveis problemas
- Log de informação para análise

Modelos de referência

- Permitem organizar diferentes funções de um sistema ou tecnologia
- Modelos conceituais de gerenciamento de redes:
 - ◆ FCAPS
 - ◆ OAMP

FCAPS

- Fault
- Configuration
- Accounting
- Performance
- Security

OAMP

- Operations
- Administration
- Maintenance
- Provisioning
- Troubleshooting

Conceitos Importantes

Confiabilidade vs. Disponibilidade

→ Confiabilidade é o mesmo que Disponibilidade?

Confiabilidade vs. Disponibilidade

→ Confiabilidade é o mesmo que Disponibilidade?

- ◆ **Confiabilidade:** probabilidade de falha em um determinado intervalo de tempo
- ◆ **Disponibilidade:** probabilidade do sistema estar disponível em um determinado instante de tempo

Alertas vs. Logs

- Alertas indicam quando algo fora do normal está acontecendo
- Logs ajudam a identificar a causa desse acontecimento

Ferramentas Ativas vs. Passivas

→ **Ativas:** causam interferência no sistema para poder obter informações. Ex:

- ◆ snmpwalk
- ◆ ping
- ◆ traceroute

→ **Passivas:** coletam dados já existentes. Ex:

- ◆ awstats
- ◆ nfdump
- ◆ swatch

Baseline

- **Baseline:** como sua rede é hoje?
- **Fundamental para qualquer gerenciamento de redes**
 - ◆ Primeiro passo para um bom gerenciamento
 - ◆ Como saber o que é estranho sem saber o que é normal?

Protocolos Importantes

Protocolos de monitoramento

→ **ICMP**: Internet Control Message Protocol

- ◆ Utilizado para debug da rede, através de pings e traceroutes
 - **ping**: utiliza o ICMP para verificar a acessibilidade de equipamentos

Protocolos de monitoramento

→ Syslog

- ◆ Padrão criado pela IETF
- ◆ Forma padronizada de registrar mensagens do sistema
- ◆ É boa prática configurá-lo em um repositório central para facilitar o gerenciamento

Protocolos de monitoramento

→ **SNMP**: Simple Network Management Protocol

- ◆ Protocolo padrão para gerenciar dispositivos em redes IP
- ◆ Com ele é possível monitorar diversos recursos
 - Carga na CPU
 - Uptime
 - Temperatura
 - Espaço em disco
 - Processos
 - Usuários logados

Protocolos de monitoramento

→ NetFlow

- ◆ Desenvolvido pela Cisco
- ◆ Define fluxos
 - Pacotes são agrupados de acordo com suas características em comum
- ◆ Utilizado para:
 - Análise de tráfego
 - Largura de banda

Tipos de Ferramentas

Tipos de ferramentas

→ Coletores

- ◆ Utilizados para colher e guardar diferentes tipos de informação de rede. Ex:
 - nfdump (NetFlow)
 - tcpdump (TCP/IP)

Tipos de ferramentas

→ Sistemas de detecção de invasão (IDS)

- ◆ Detectam padrões suspeitos que são característicos de comportamento malicioso
- ◆ Podem analisar o tráfego da rede, alarmes, logs, etc. além de tomar ações para mitigar os efeitos
- ◆ Ex:
 - Snort

Tipos de ferramentas

→ Sistema de análise de performance

- ◆ Permite analisar dados de tráfego e performance.
- ◆ Dados em gráficos para permitir o entendimento dos usuários.
- ◆ Permite planejamento de novos recursos e identificação de gargalos na rede.
- ◆ Ex:
 - Cacti
 - Zabbix

Tipos de ferramentas

→ Cacti

- ◆ A principal função do Cacti é armazenar e mostrar de forma simples as informações disponibilizadas pelos equipamentos, em geral através do protocolo SNMP
- ◆ O fato de utilizar RRD facilita muito na geração de gráficos simples e concisos

Tipos de ferramentas

console graphs

Console -> Devices -> (Edit) Logged in as admin (Logout)

Save Successful.

n4 (192.0.0.12)

SNMP Information
System: Linux n4 3.8.0-19-generic #30-Ubuntu SMP Wed May 1 16:36:13 UTC 2013
i686
Uptime: 12610 (0 days, 0 hours, 2 minutes)
Hostname: n4
Location: NIC.br
Contact: teste@teste

Ping Results
IOMP Ping Success (0.043 ms)

Devices [edit: n4]

General Host Options

Description
Give this host a meaningful description.

Hostname
Fully qualified hostname or IP address for this device.

Host Template
Choose the Host Template to use to define the default Graph Templates and Data Queries associated with this Host.

Number of Collection Threads
The number of concurrent threads to use for polling this device. This applies to the Spine poller only.

Disable Host
Check this box to disable all checks for this host. Disable Host

Availability/Reachability Options

Downed Device Detection
The method Cacti will use to determine if a host is available for polling.
NOTE: It is recommended that, at a minimum, SNMP always be selected.

Ping Method
The type of ping packet to send.
NOTE: ICMP on Linux/UNIX requires root privileges.

Ping Timeout Value
The timeout value to use for host ICMP and UDP ping. This host SNMP timeout value applies for SNMP pings.

Ping Retry Count
After an initial failure, the number of ping retries Cacti will attempt before failing.

SNMP Options

SNMP Version
Choose the SNMP version for this device.

SNMP Community
SNMP read community for this device.

SNMP Port
Enter the UDP port number to use for SNMP (default is 161).


SNMP Timeout
The maximum number of milliseconds Cacti will wait for an SNMP response (does not work with php-snmp support).

Maximum OID's Per Get Request
Specified the number of OID's that can be obtained in a single SNMP Get request.

Additional Options

Management

- New Graphs
- Graph Management
- Graph Trees
- Data Sources
- Devices**
- Collection Methods
- Data Queries
- Data Input Methods
- Templates
- Graph Templates
- Host Templates
- Data Templates
- Import/Export
- Import Templates
- Export Templates
- Configuration
- Settings
- Plugin Management
- Utilities
- System Utilities
- User Management
- Logout User



Create Graphs for this Host

- Data Source List
- Graph List

Tipos de ferramentas

→ Sistema de gerenciamento de alarmes

- ◆ Coletam e monitoram alarmes da rede.
- ◆ Melhor visualização dos alarmes para o usuário.
- ◆ Diagnóstico inicial
- ◆ Ex:
 - Nagios
 - Icinga
 - Zabbix

Tipos de ferramentas

Current Network Status

Last Updated: Mon Jun 3 09:52:28 BRT 2013 - Update in 86 seconds [pause]
Icinga 1.9.0 - Logged in as icingadmin

- ▶ View Alert History For All Hosts
- ▶ View Notifications For All Hosts
- ▶ View Host AND Services For All Hosts
- ▶ View Host Status Detail For All Hosts

Commands for checked services

Select command

Display Filters:

Service Status Details For All Hosts

Page 1 of 1 Results: 50

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	06-03-2013 09:49:16	5d 22h 59m 42s	1/4	OK - load average: 0.81, 0.68, 0.59
	Current Users	OK	06-03-2013 09:49:51	13d 13h 14m 54s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	06-03-2013 09:50:26	13d 13h 14m 20s	1/4	HTTP OK: HTTP/1.1 200 OK - 454 bytes in 0.000 second response time
	Icinga Startup Delay	OK	06-03-2013 09:51:02	13d 13h 13m 20s	1/4	OK: Icinga started with 2 seconds delay
	PING	OK	06-03-2013 09:51:37	13d 13h 13m 14s	1/4	PING OK
	SSH	OK	06-03-2013 09:47:48	13d 13h 17m 7s	1/4	SSH OK
	Swap Usage	OK	06-03-2013 09:48:23	13d 13h 16m 34s	1/4	SWAP OK
	Total Processes	OK	06-03-2013 09:48:58	13d 13h 15m 51s	1/4	PROC OK
serverB	Current Load	OK	06-03-2013 09:49:33	0d 1h 42m 55s	1/4	OK - load average: 2.32, 2.47, 2.90
	Current Users	OK	06-03-2013 09:50:09	10d 0h 41m 32s	1/4	USERS OK
	Icinga Startup Delay	OK	06-03-2013 09:51:19	10d 0h 40m 21s	1/4	OK: Icinga started with 2 seconds delay
	Total Processes	OK	06-03-2013 09:48:41	10d 0h 38m 0s	1/4	PROC OK
	SSH	CRITICAL	06-03-2013 09:47:48	13d 13h 17m 7s	1/4	SSH CRITICAL

Page 1 of 1 Results: 50

Displaying Result 1 - 12 of 12 Matching Services

Host	Service	Status	Timestamp	Output	Attempt
localhost	Current Load	OK	2013-05-17 14:43:33	OK - load average: 2.32, 2.47, 2.90	4 / 4
localhost	Current Load	WARNING	2013-05-17 14:23:33	WARNING - load average: 2.01, 3.66, 3.95	4 / 4
localhost	Current Load	CRITICAL	2013-05-17 14:13:34	CRITICAL - load average: 5.29, 6.54, 3.90	4 / 4
localhost	Current Load	CRITICAL	2013-05-17 14:12:33	CRITICAL - load average: 12.70, 7.76, 4.09	3 / 4
localhost	Current Load	WARNING	2013-05-17 14:11:33	WARNING - load average: 7.37, 5.16, 3.02	2 / 4
localhost	Current Load	CRITICAL	2013-05-17 14:10:33	CRITICAL - load average: 13.91, 5.48, 2.98	1 / 4
localhost	Current Load	OK	2013-05-17 14:00:33	OK - load average: 2.73, 3.22, 1.97	3 / 4
localhost	Current Load	WARNING	2013-05-17 13:59:33	WARNING - load average: 5.49, 3.67, 2.02	2 / 4
localhost	Current Load	WARNING	2013-05-17 13:58:33	WARNING - load average: 6.56, 3.20, 1.76	1 / 4
localhost	Current Load	OK	2013-05-17 11:13:33	OK - load average: 0.41, 1.62, 2.78	4 / 4
localhost	Current Load	WARNING	2013-05-17 11:08:33	WARNING - load average: 1.54, 3.95, 3.74	4 / 4
localhost	Current Load	WARNING	2013-05-17 11:07:33	WARNING - load average: 3.79, 4.77, 3.97	3 / 4
localhost	Current Load	WARNING	2013-05-17 11:06:33	WARNING - load average: 2.36, 4.66, 3.88	2 / 4
localhost	Current Load	WARNING	2013-05-17 11:05:33	WARNING - load average: 2.85, 5.22, 4.00	1 / 4

Tipos de ferramentas

→ Sistema de tickets

- ◆ Rastrear como os problemas estão sendo resolvidos.
- ◆ Cadastro dos problemas
- ◆ Alocação de recursos
- ◆ Estatísticas de resolução
- ◆ Ex:
 - Redmine
 - Trac

Tipos de ferramentas

→ Ferramentas de acesso

- ◆ SSH e telnet
- ◆ Acesso à máquinas remotas, permite a troca de informação entre a ferramenta de gerenciamento e os dispositivos.
- ◆ Ex:
 - OpenSSH
 - PuTTY

Tipos de ferramentas

→ Ferramentas de depuração

- ◆ **ping**: verifica a conectividade entre as máquinas
- ◆ **traceroute**: verifica as rotas feitas por um pacote
- ◆ **ps/top**: monitora os processos da máquina
- ◆ **nmap**: verifica quais portas estão habilitadas em certo host
- ◆ **wireshark**: analisa pacotes da rede em tempo real

Tipos de ferramentas

→ Ferramentas de log

- ◆ **syslog-ng, rsyslog**: implementam o protocolo syslog
- ◆ **Log Analyzer**: permite visualizar o conteúdo dos logs de maneira inteligível
- ◆ **tenshi, swatch**: permitem a criação de filtros para os logs

Tipos de ferramentas

→ Gerenciamento de configurações

- ◆ Manual
 - CVS
 - SVN
 - Mercurial
- ◆ Automático
 - RANCID (roteadores)

Tipos de ferramentas

→ RANCID

- ◆ Conecta ao roteador (SSH ou Telnet)
- ◆ Executa e coleta dados de comandos
- ◆ Salva os dados em CVS/SVN
- ◆ Cria um diff entre a configuração anterior e a atual
- ◆ Envia um e-mail com o diff das configurações aos interessados.

Tipos de ferramentas

→ Performance

- ◆ **IPerf**: ferramenta para medir o throughput da rede
- ◆ **Ntop**: Mostra o uso a rede de forma similar ao top

Tipos de ferramentas

→ Gerenciamento de endereços

- ◆ IPplan
- ◆ PhpIPAM
- ◆ NetDot
- ◆ GestióIP

Tipos de ferramentas

phpipam IP address management

Search string Search

H. Usuario Um
Logged in as User
Logout

Customers Users

Available subnets

Add new subnet +

Add subnet

Subnet: subnet in CIDR Enter subnet in CIDR format (e.g. 192.168.0.0/24)

Description: subnet description Enter subnet description

VLAN: No VLAN Select VLAN

Master Subnet: Root subnet Enter master subnet if you want to nest it in a subnet, or select root to create root subnet

VRF: None Add this subnet to VRF

IP Requests: Allow or deny IP requests for this subnet

Show as name: Show Subnet name instead of subnet IP

Cancel

show networks networks VLANs importexport manage help

create new networks

GestiiIP

networks advanced

hosts advanced

create one network

IPv4 + IPv6

network: (e.g. 192.168.0.0)

BM: 24 (255.255.255.0 - 254 hosts)

description:

comment:

site:

category:

Root network:

include networks within automatic update:

create calculate

IPPlan - IP Address Management and Tracking

User Manager

Main Customers Network DNS Options Admin Help

Logged in as admin

Current Users/Groups

New User | New Group

Search

Search

Edit Users/Groups

Click on a group or user

No groups have been created.

Orphan Users

Create group

Group name:

Group description:

Group can create/modify/delete customers?

No

Create group

Group data?

Yes

IPPlan v4.9.2b

192.0.0.0/24 - 192.0.0.0/24

Children Sites Zones DHCP Access Rights Attributes Comments All

Address: 192.0.0.0/24

Status: Subnet

Description: Use Network/Broadcast?: No

First Created 2013-07-01 17:27:22

Last Modified 2013-07-01 17:27:22

Owner: Network Services [edit]

Used by: UCCO-SNMP [edit]

Netmask: 255.255.255.0

Broadcast: 192.0.0.255

Usable Addresses: 254 (192.0.0.1 - 192.0.0.254)

Utilization: Used 2 of 254 Available: 252 (-99%)

Legend	Available	Discovered	Dynamic	Reserved
0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	21	22	23	24
25	26	27	28	29
30	31	32	33	34
35	36	37	38	39
40	41	42	43	44
45	46	47	48	49
50	51	52	53	54
55	56	57	58	59
60	61	62	63	64
65	66	67	68	69
70	71	72	73	74
75	76	77	78	79
80	81	82	83	84
85	86	87	88	89
90	91	92	93	94
95	96	97	98	99
100	101	102	103	104
105	106	107	108	109
110	111	112	113	114
115	116	117	118	119
120	121	122	123	124
125	126	127	128	129
130	131	132	133	134
135	136	137	138	139
140	141	142	143	144
145	146	147	148	149
150	151	152	153	154
155	156	157	158	159
160	161	162	163	164
165	166	167	168	169
170	171	172	173	174
175	176	177	178	179
180	181	182	183	184
185	186	187	188	189
190	191	192	193	194
195	196	197	198	199
200	201	202	203	204
205	206	207	208	209
210	211	212	213	214
215	216	217	218	219
220	221	222	223	224
225	226	227	228	229
230	231	232	233	234
235	236	237	238	239
240	241	242	243	244
245	246	247	248	249
250	251	252	253	254
255				

© GPL, Netbox: NB Team Documentation Tool v1.8.4

Introdução ao uso de Flows

Introdução ao uso de Flows

- O que é Flow?
- Para que serve?
- Quando é útil?
- Como eu utilizo?
- Conclusões

O que é Flow?

O que é Flow?

→ Flow: do inglês, significa **fluxo**

◆ E o que é fluxo?

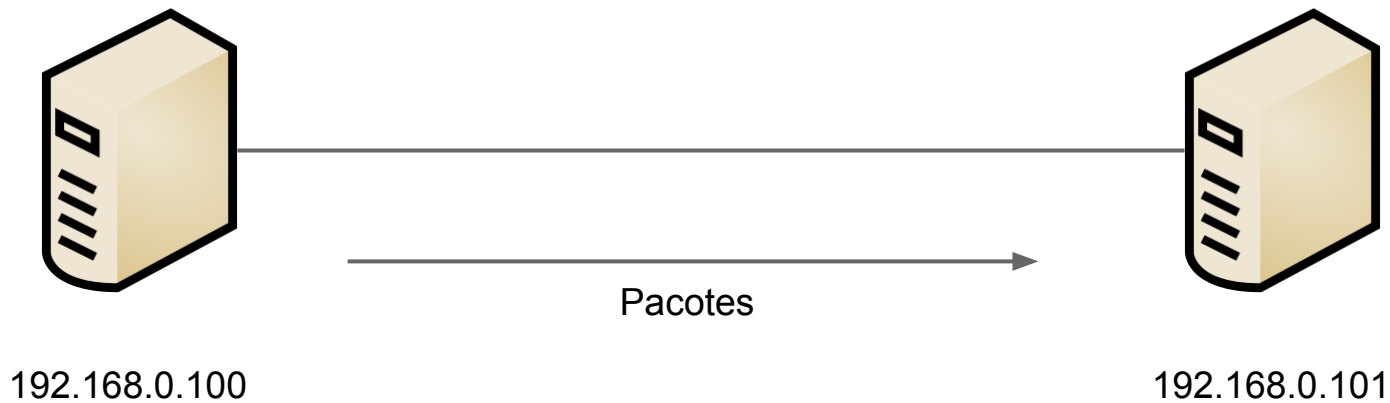
- Fluxo de pessoas
- Fluxo de caixa
- Fluxo magnético
- Fluxo de dados

O que é Flow?

- Fluxo indica uma taxa de entrada/saída de um determinado objeto dentro de uma referência fixa
- Em redes de computadores: sequência unidirecional ou bidirecional de pacotes com características em comuns entre uma origem e um destino

O que é Flow?

Exemplo de Flow:



flow: 1 origem:192.168.0.100 destino:192.168.0.101

Para que serve?

Para que serve?

- Necessidade de **mais informações** sobre o uso da rede
- ◆ Análises tradicionais de rede, como MRTG/cacti informam apenas o total de tráfego utilizado

Para que serve?

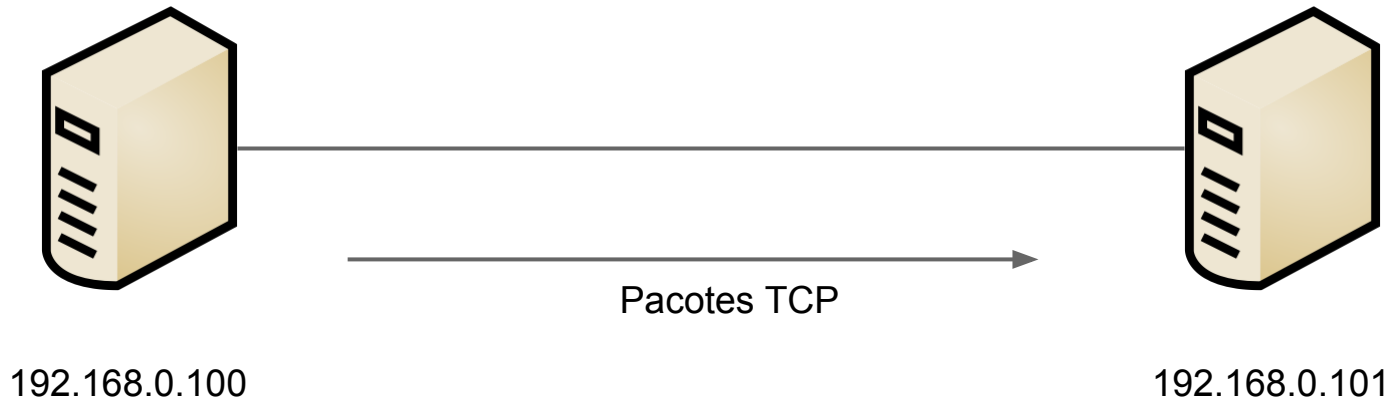
- Necessidade de um mecanismo **eficiente** de coleta de dados
- ◆ Análise pacote a pacote como no tcpdump se torna inviável em grande escala

Para que serve?

- Nesse sentido o que queremos é um meio termo
- ◆ Ao invés de guardar pacote a pacote, agrupar esses pacotes por **características semelhantes**
 - Origem e destino
 - Porta de origem e destino
 - Protocolo de camada de transporte

O que é Flow?

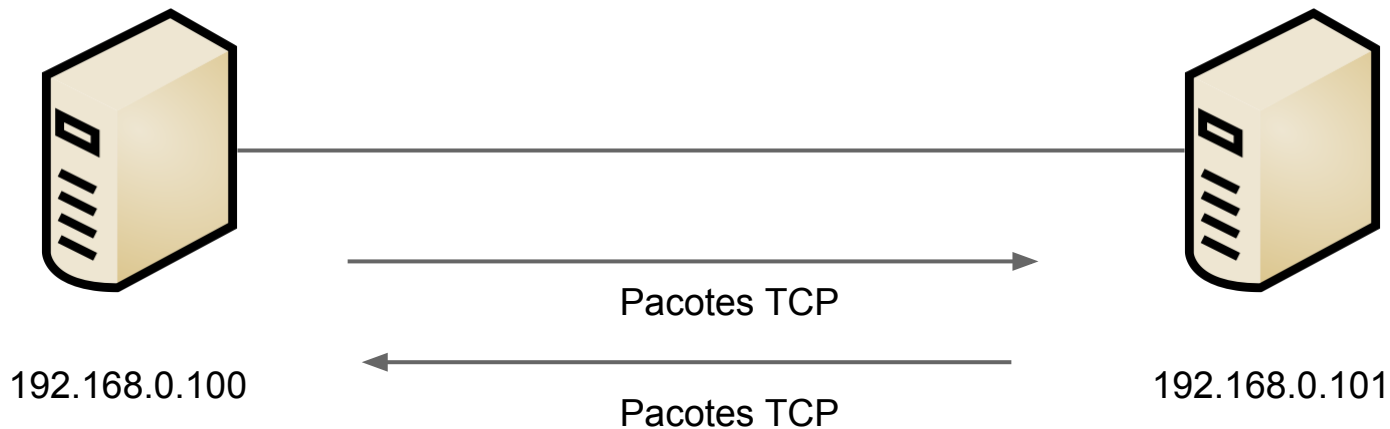
Exemplo de Flow:



flow: 1 origem:192.168.0.100 destino:192.168.0.101 protocolo: tcp

O que é Flow?

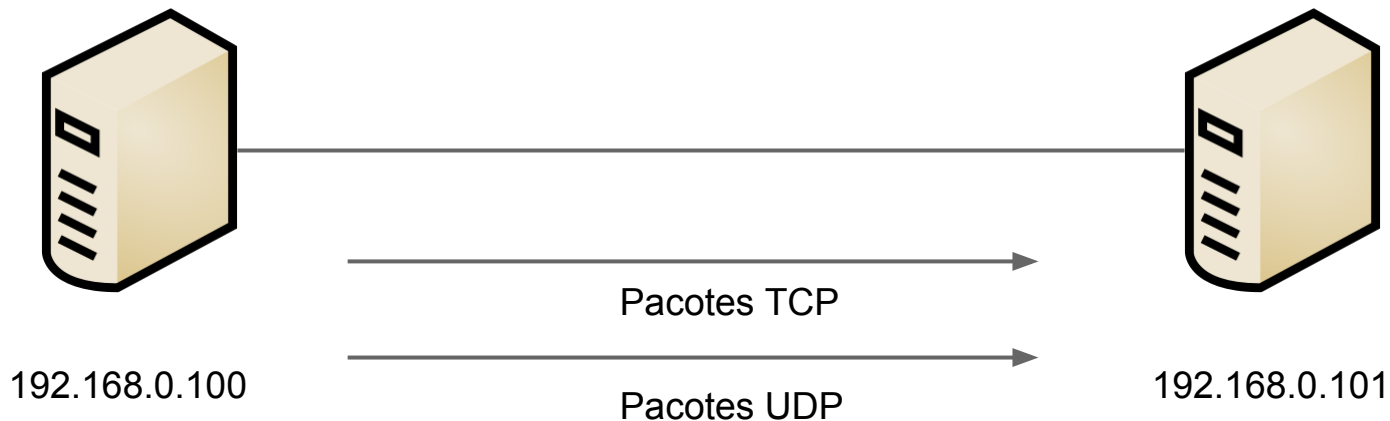
Exemplo de Flow:



flow: 1	origem:192.168.0.100	destino:192.168.0.101	protocolo: tcp
flow: 2	origem:192.168.0.101	destino:192.168.0.100	protocolo: tcp

O que é Flow?

Exemplo de Flow:



flow: 1	origem:192.168.0.100	destino:192.168.0.101	protocolo: tcp
flow: 2	origem:192.168.0.100	destino:192.168.0.101	protocolo: udp

Quando é útil?

Quando é útil?

- Engenharia de tráfego
- Top Talkers
- Monitoramento de redes ocultas
- Lista de IPs maliciosos
- Análise de dados históricos
- Violações de política de uso

Engenharia de tráfego

- Quero entender como minha rede se comporta para dimensionar corretamente as estruturas
- ◆ Vale a pena participar do PTT?
- ◆ Quanto de tráfego meus clientes trocam com redes sociais ou torrent?
- ◆ Quanto de tráfego da minha rede é via IPv6?

Top Talkers

- Quem são os usuários mais ativos dentro da minha rede e quais recebem maior atividade
- ◆ Pode detectar anomalias na rede
 - Ataques de negação de serviço
 - Tentativas de intrusão
 - Proxy mal configurado
 - DNS recursivo aberto

Monitoramento de redes ocultas

- Monitorar equipamentos com IPs não divulgados e que não deveriam ser acessados por qualquer um
 - ◆ Acessos a esse equipamento **podem** indicar ataques de varredura
 - ◆ Verificar atividade das máquinas suspeitas

Lista de IPs maliciosos

- Verificar se algum equipamento está se comunicando com IPs conhecidos maliciosos
- ◆ Se um equipamento acessa um IP de um controlador de botnet conhecida, possivelmente o equipamento está comprometido

Análise de dados históricos

- Uma das funcionalidades mais importantes
 - ◆ Caso ocorra algum incidente, é possível olhar os dados passados e analisá-los para tentar descobrir o que ocorreu naquele momento

Violações de política de uso

- Caso a empresa possua uma política de uso, os flows podem ajudar a identificar os usuários que estão violando as políticas de uso
 - ◆ Torrent
 - ◆ Sites inapropriados
 - ◆ Realização de ataques

Como eu utilizo?

Tipos de Flow

Tipos de Flow

- NetFlow
- IPFIX
- sFlow

NetFlow

- Padrão proposto pela Cisco
 - ◆ Exportado via UDP
 - ◆ Possui diversas versões em uso (cuidado)

NetFlow

- Flow é criado quando se recebe um pacote diferente dos flows já existentes
- Expira quando
 - ◆ Inativo por mais de 15 segundos
 - ◆ Duração acima de 30 minutos
 - ◆ Conexão encerrada
 - ◆ Tabela de Flows cheia

NetFlow

→ Versões

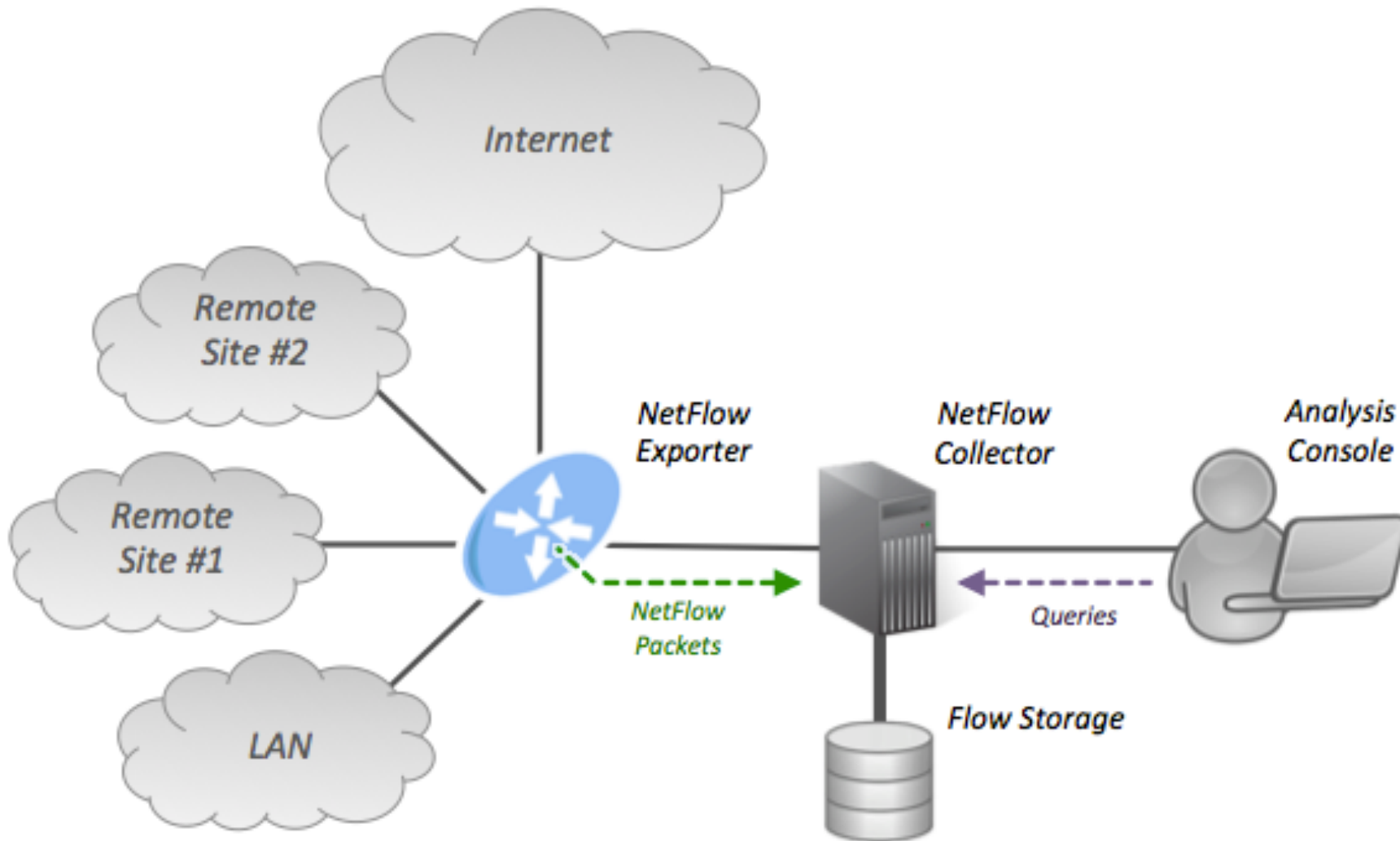
- ◆ V1: obsoleto
- ◆ V5: mais comum, sem suporte a IPv6
- ◆ V9: permite agrupamento de flows
- ◆ V10: IPFIX

sFlow

- Quando o fluxo de informações é muito alto, não é viável analisar todos os pacotes
 - ◆ sFlow trabalha com amostragem (sampling)
 - Temporal
 - Aleatória
- Funcionamento parecido com NetFlow

Equipamentos necessários

- Exportador de flows
 - ◆ Equipamento que analisa os pacotes, gera os flows e os envia ao coletor
- Coletor de flows
 - ◆ Recebe os flows do exportador, armazena e pré-processa os dados
- Analisador de flows
 - ◆ Analisa os dados armazenados no coletor de flows



fonte: http://en.wikipedia.org/wiki/File:NetFlow_Architecture_2012.png

Ferramentas

- nfdump (coletor e analisador de dados de flow)
- nfsen (frontend para dados coletados via nfdump)
- ntop (monitora NetFlow através do nprobe)
- softflowd (exportador de flows para Linux)

Conclusões

Conclusões

- Flows são importantes para engenharia de tráfego e segurança da rede
- Grande auxílio para montar o baseline
- Requer certo conhecimento de análise, pois elas são diferentes para cada tipo de rede
- Cuidado com os falsos positivos

Conclusões

→ Para que gerenciar?

- ◆ Para garantir uma rede funcional e clientes satisfeitos

→ Como gerenciar?

◆ Ferramentas de Gerenciamento

- Logs (rsyslog, log analyzer, tenshi)
- Alertas (Icinga, Nagios, Zabbix)
- Performance (Cacti)
- Tickets (trac, redmine)
- Endereços (IPPlan, NetDot, GestióIP)
- Configuração (SVN, Rancid)

Obrigado(a)

www.nic.br

 ipv6@nic.br

 [@ComuNICbr](https://twitter.com/ComuNICbr)

 facebook.com/nic.br

São Paulo, SP
16 de julho de 2015

nic.br **cgi.br**

www.nic.br | www.cgi.br