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

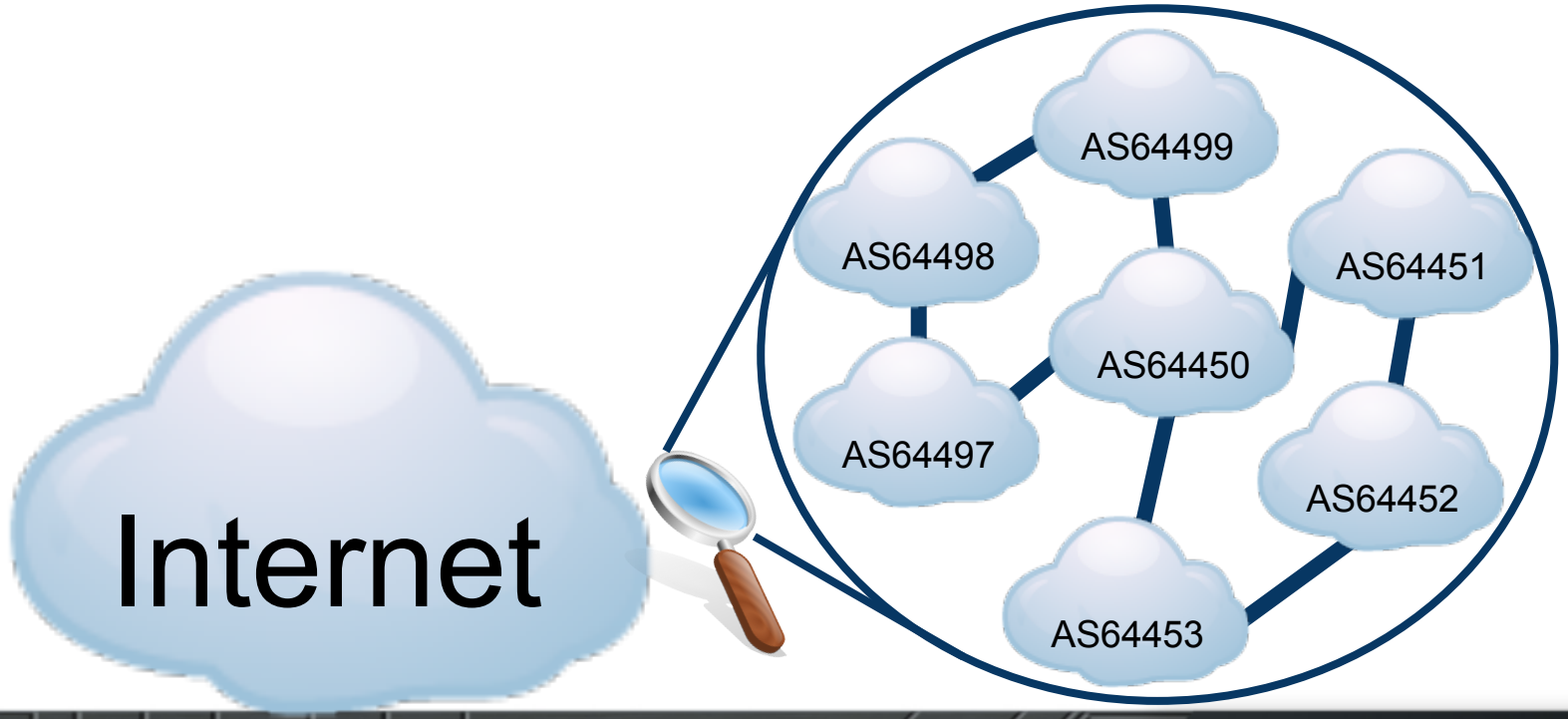
Nuvem

O que é a Internet?

Do ponto de vista do usuário

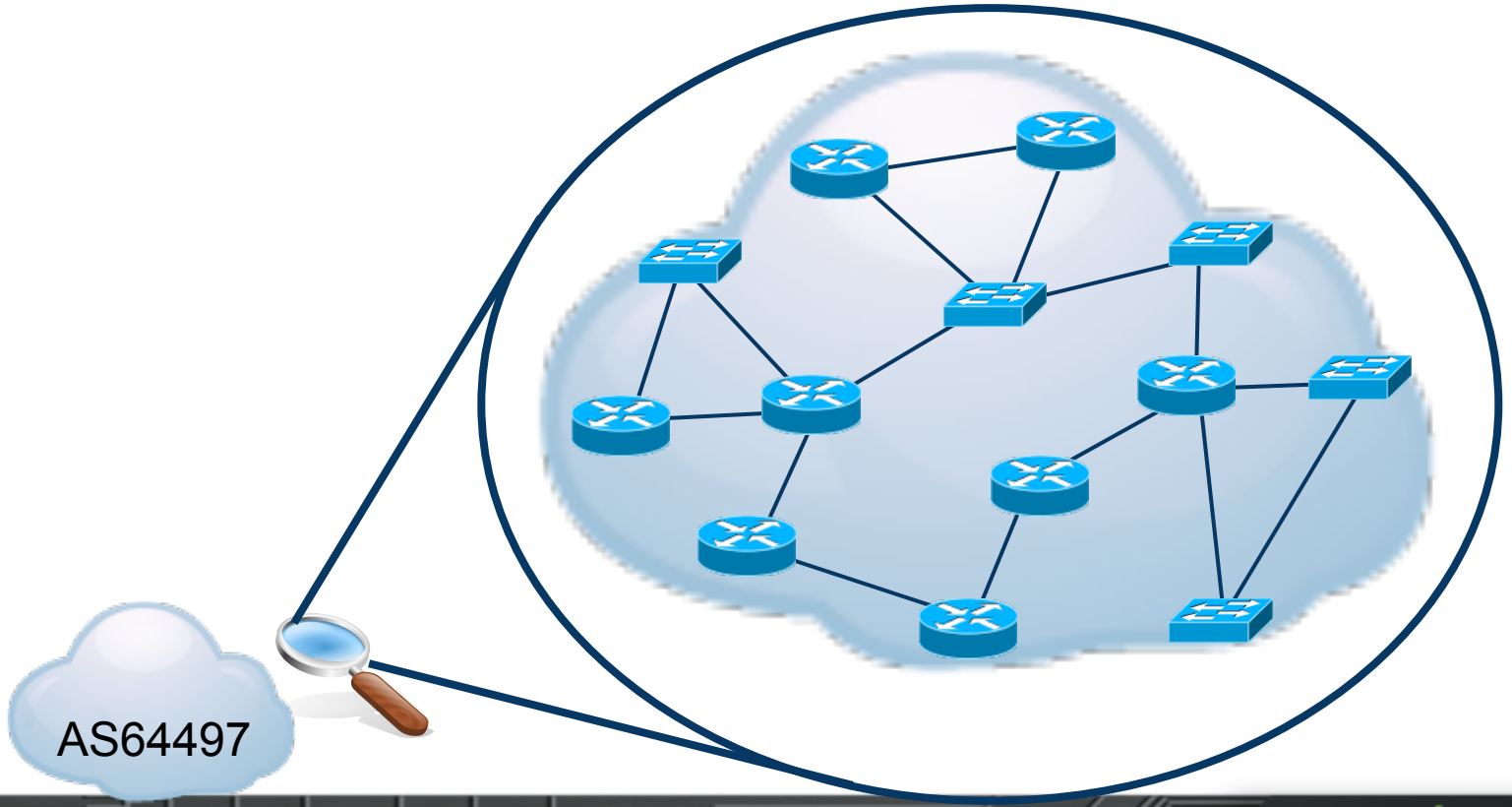
O que é a Internet?

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?

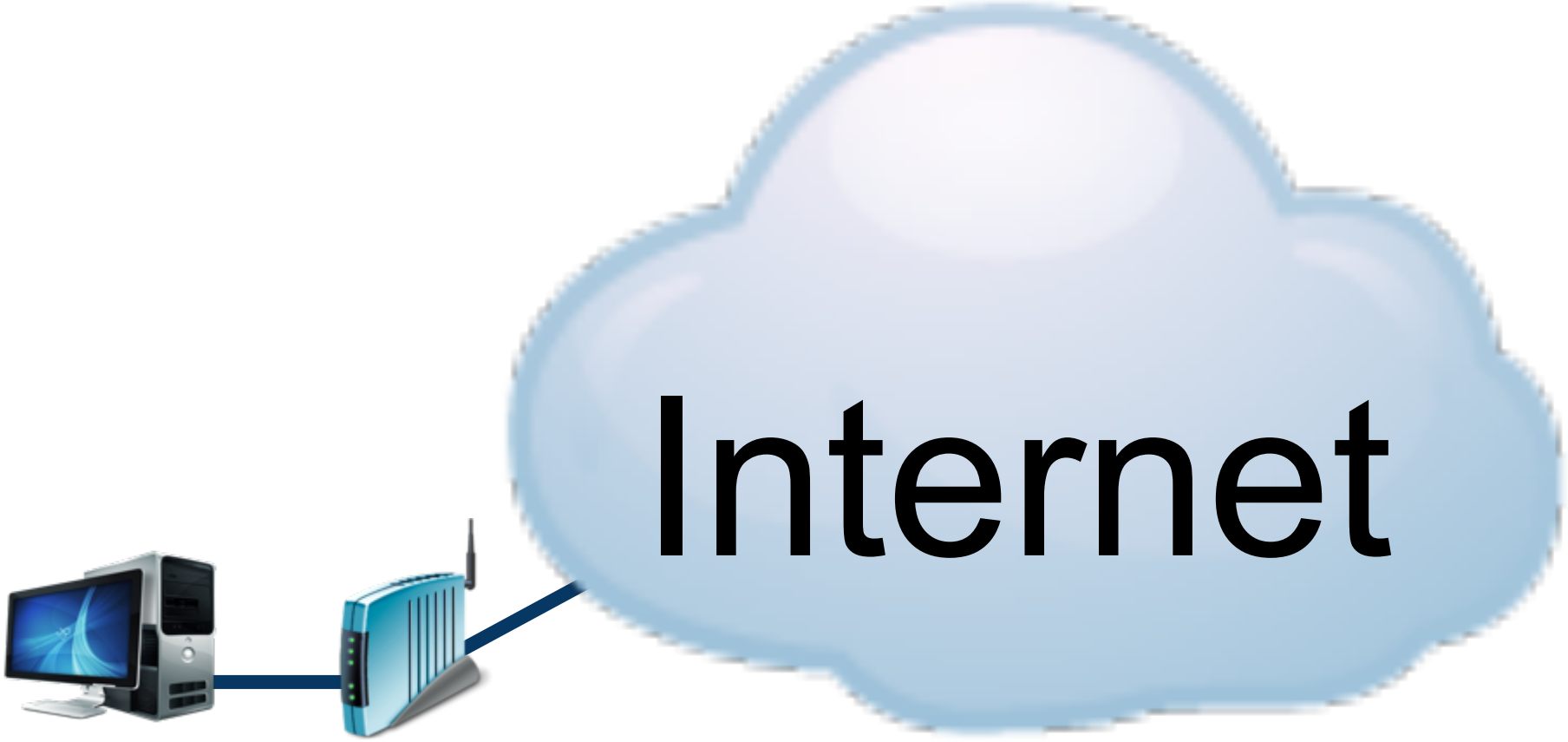
O que é um ISP?

ISP = Internet Service Provider

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

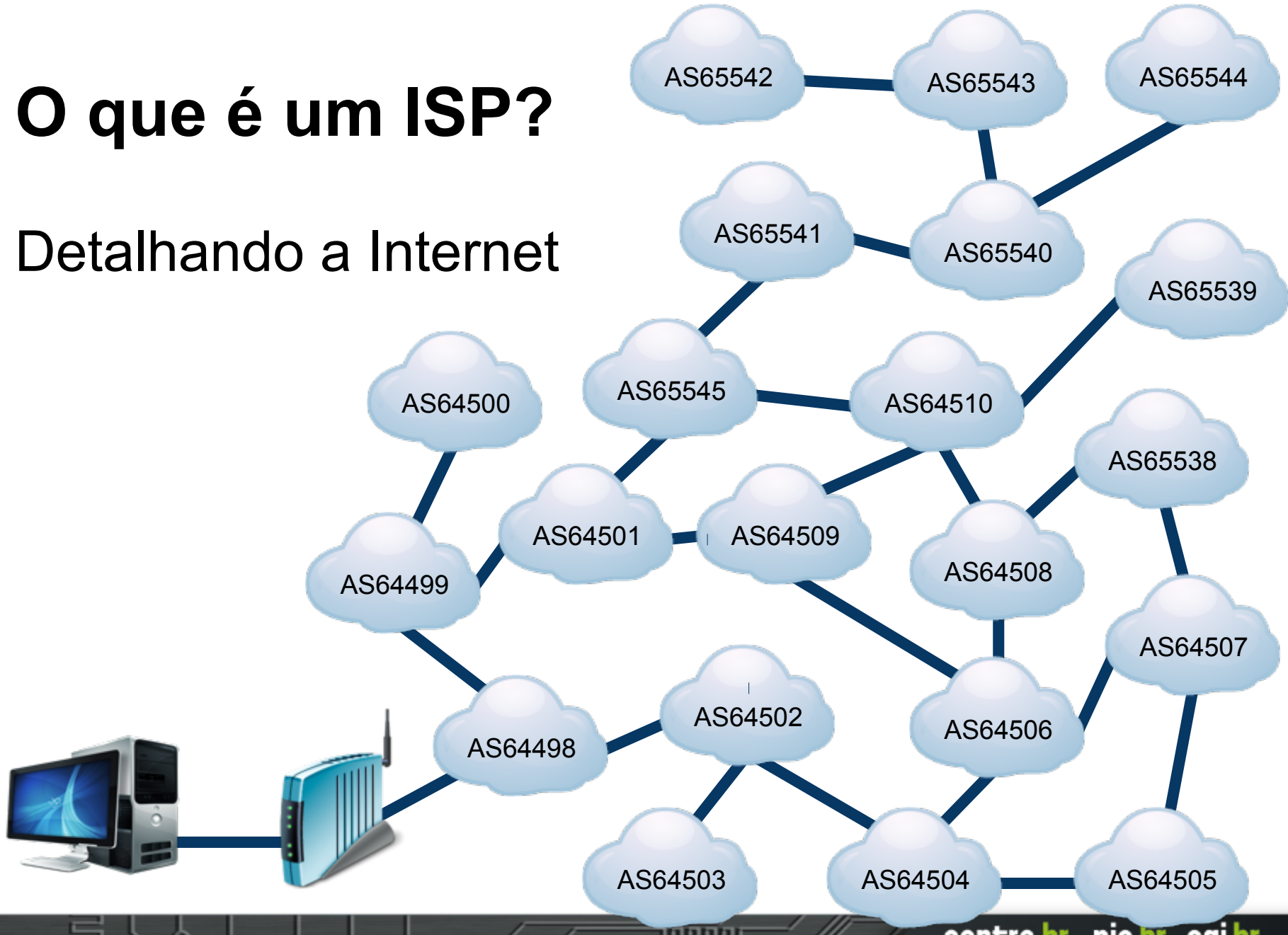
O que é um ISP?

Do ponto de vista do usuário



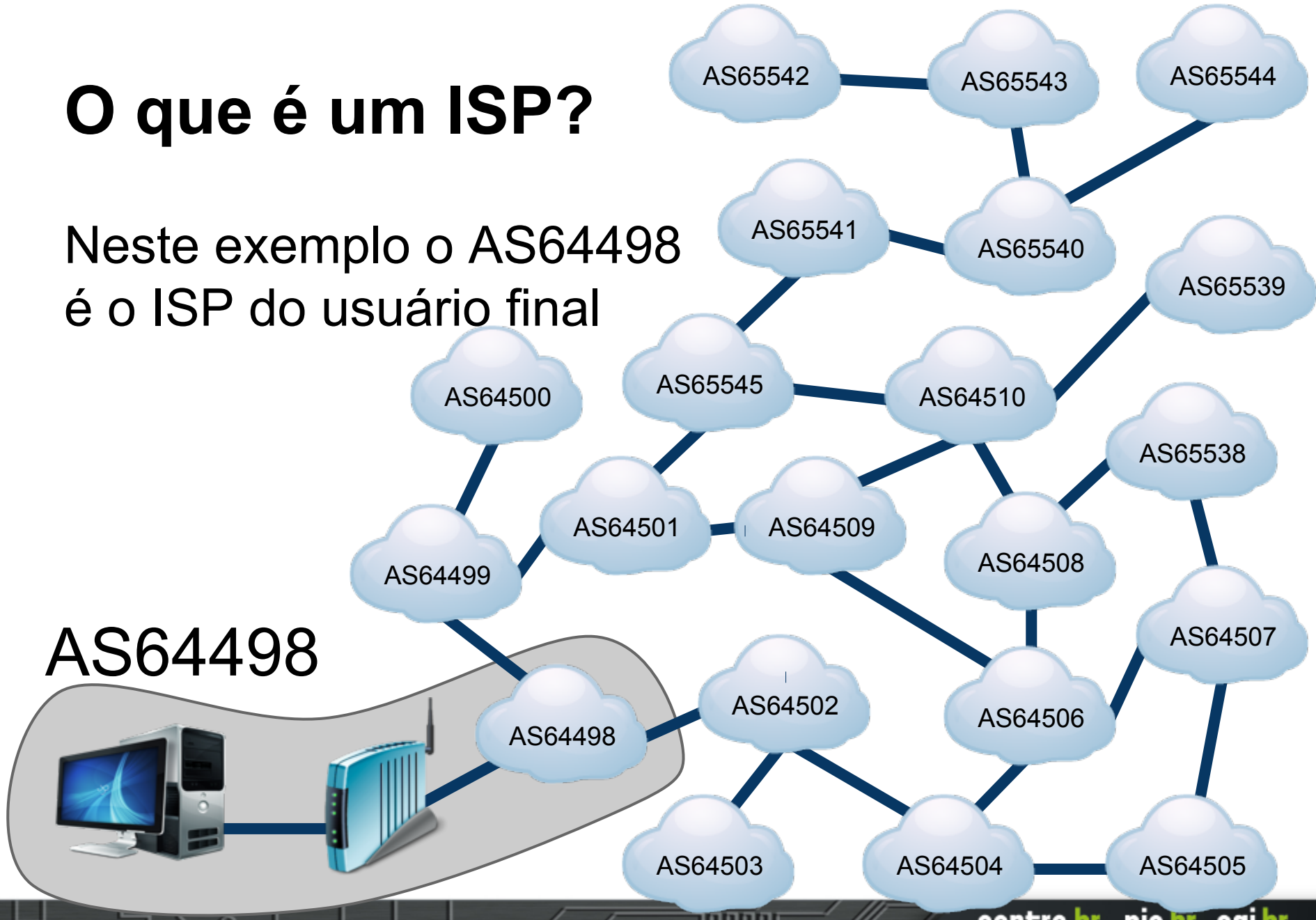
O que é um ISP?

Detalhando a Internet



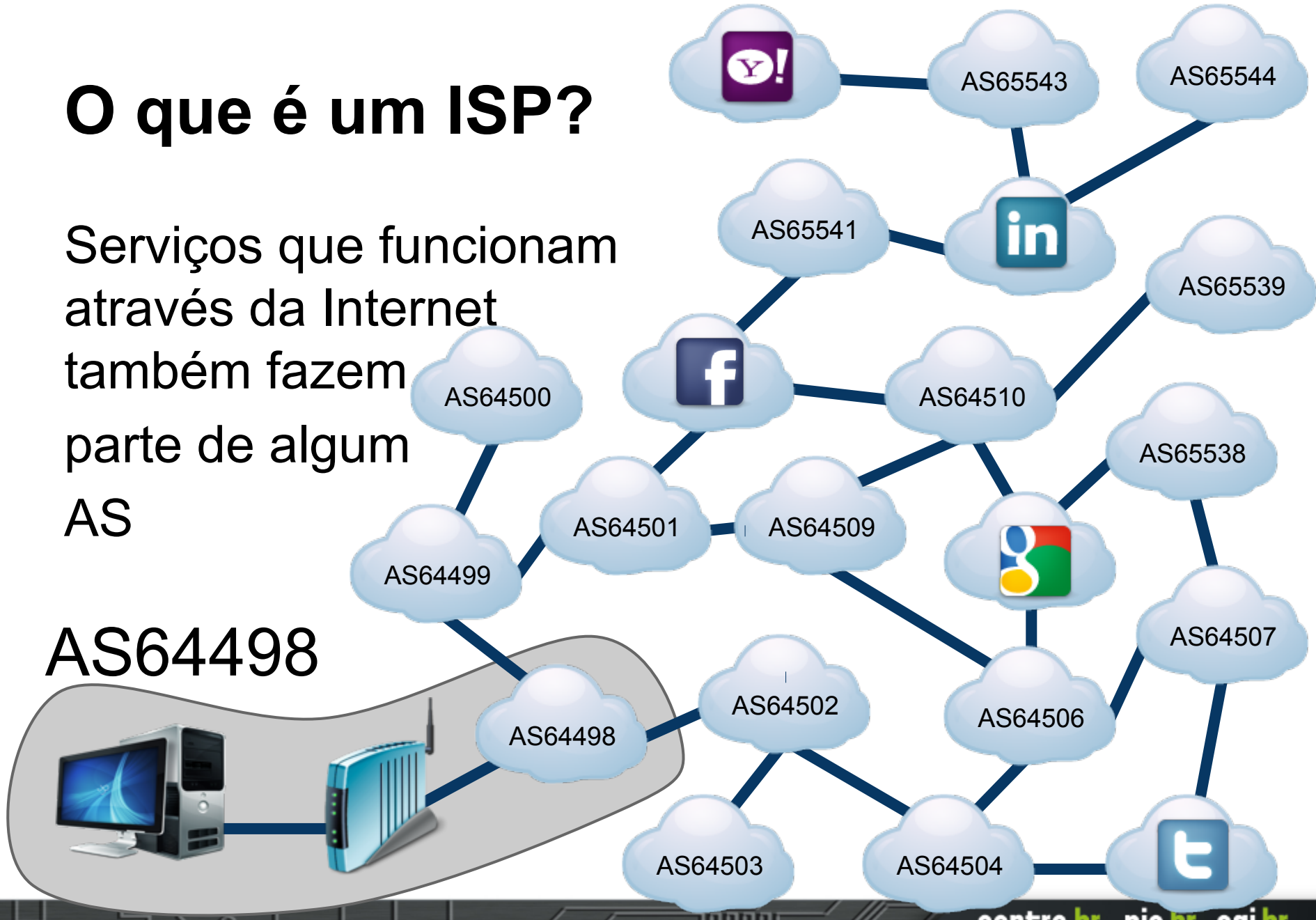
O que é um ISP?

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



O que é BGP?

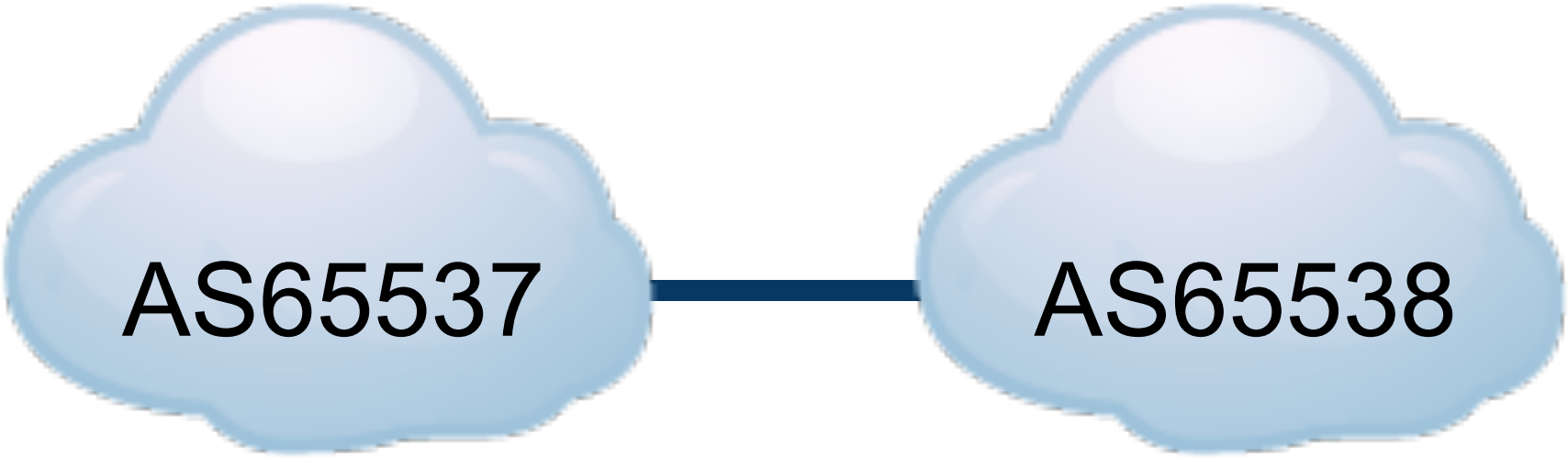
O que é BGP?

BGP = Border Gateway Protocol

Protocolo que os AS usam para comunicar entre si

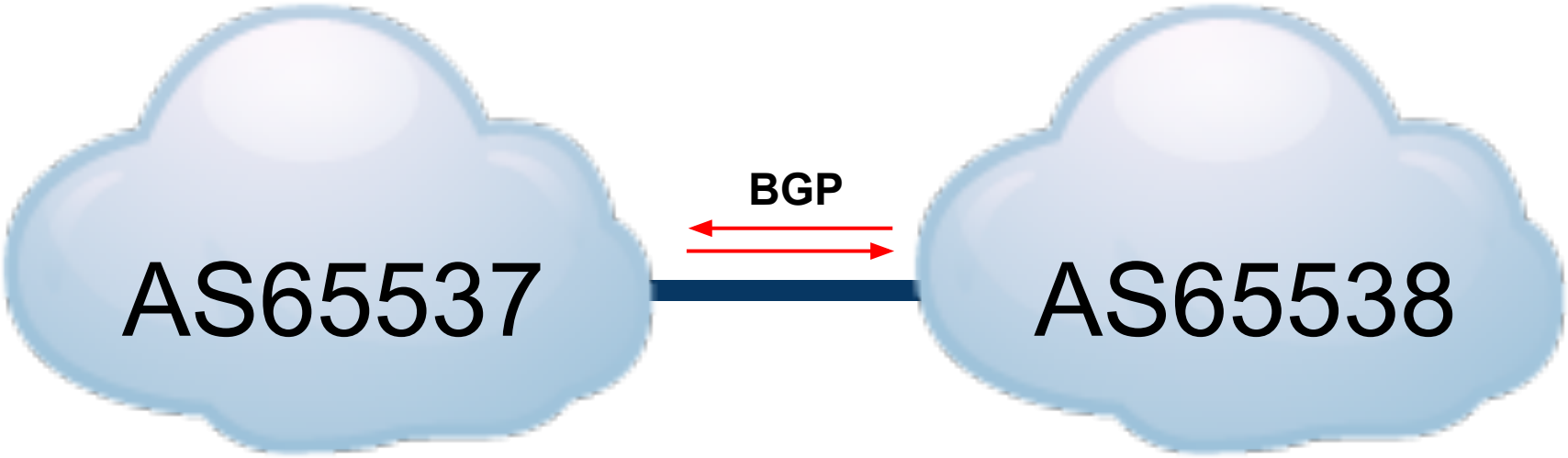
O que é BGP?

Exemplo: 2 AS conectados entre si



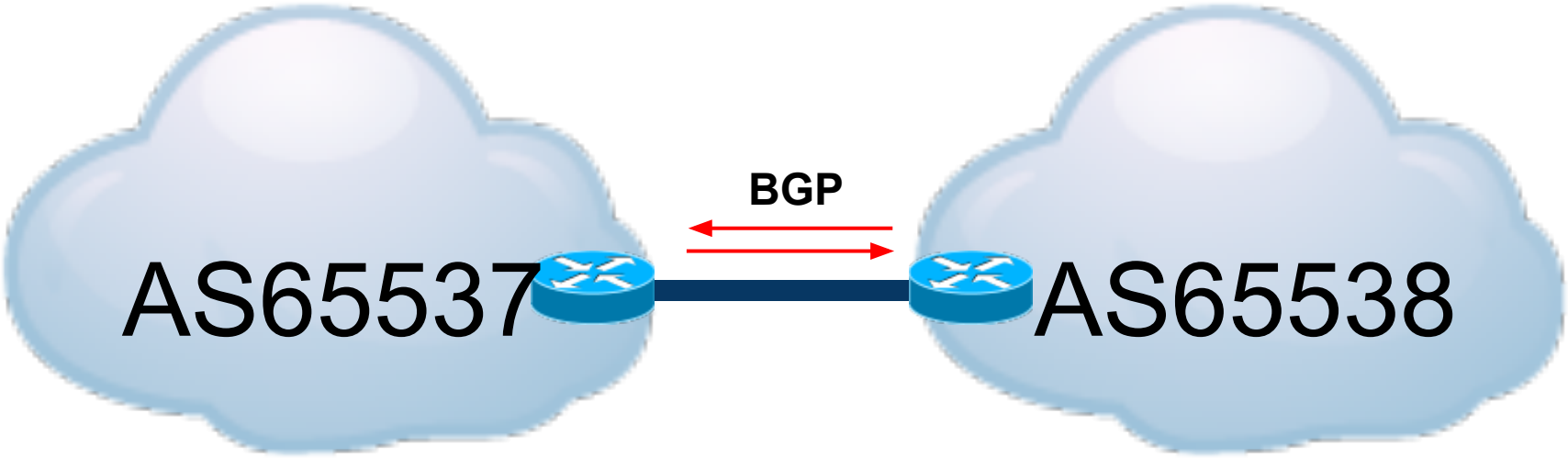
O que é BGP?

Sua comunicação é feita atraveś do protocolo BGP



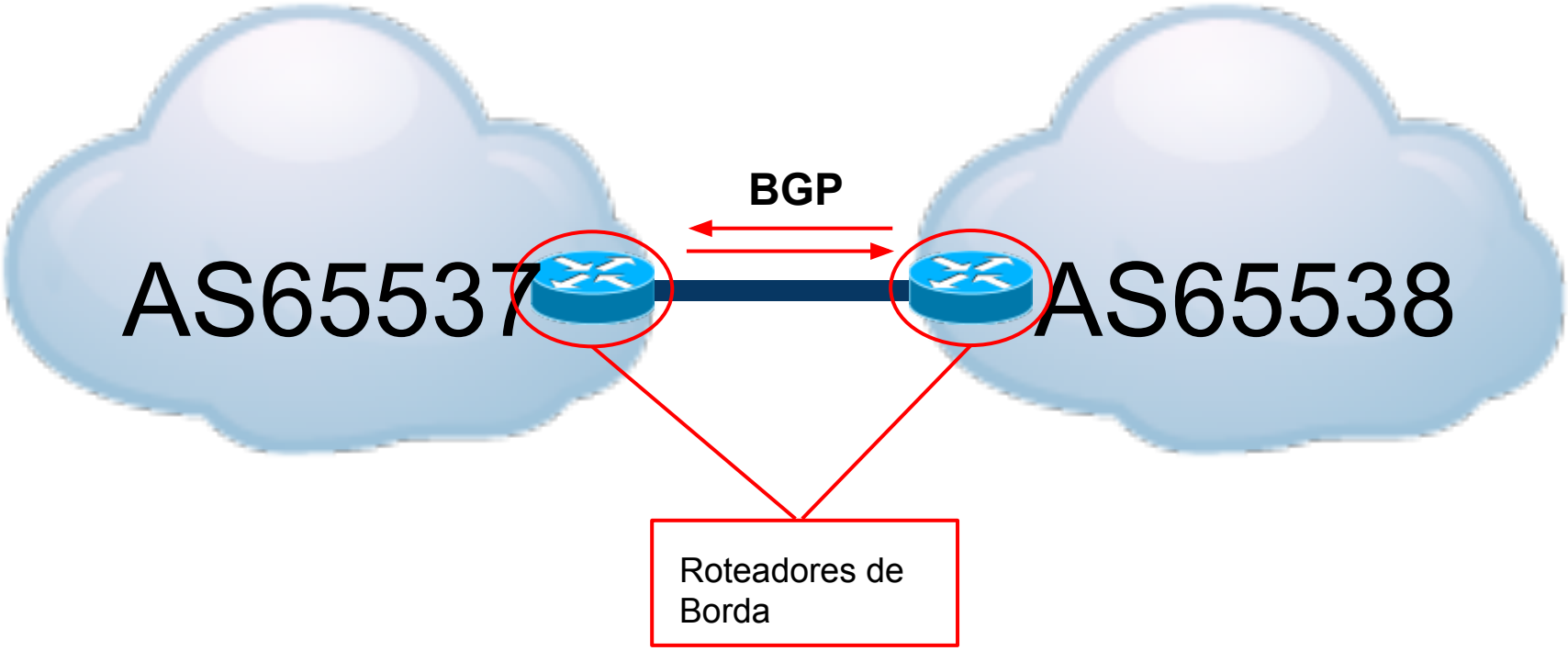
O que é BGP?

O protocolo BGP é utilizado nos roteadores de borda do AS



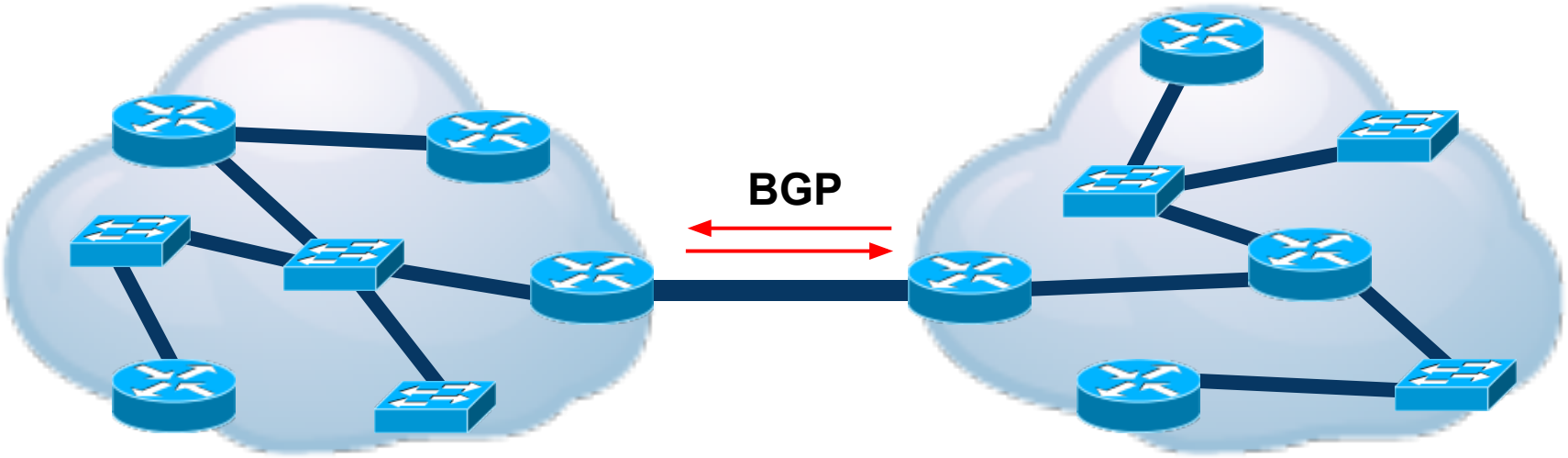
O que é BGP?

O protocolo BGP é utilizado nos roteadores de borda do AS



O que é BGP?

Detalhando a rede interna de cada AS

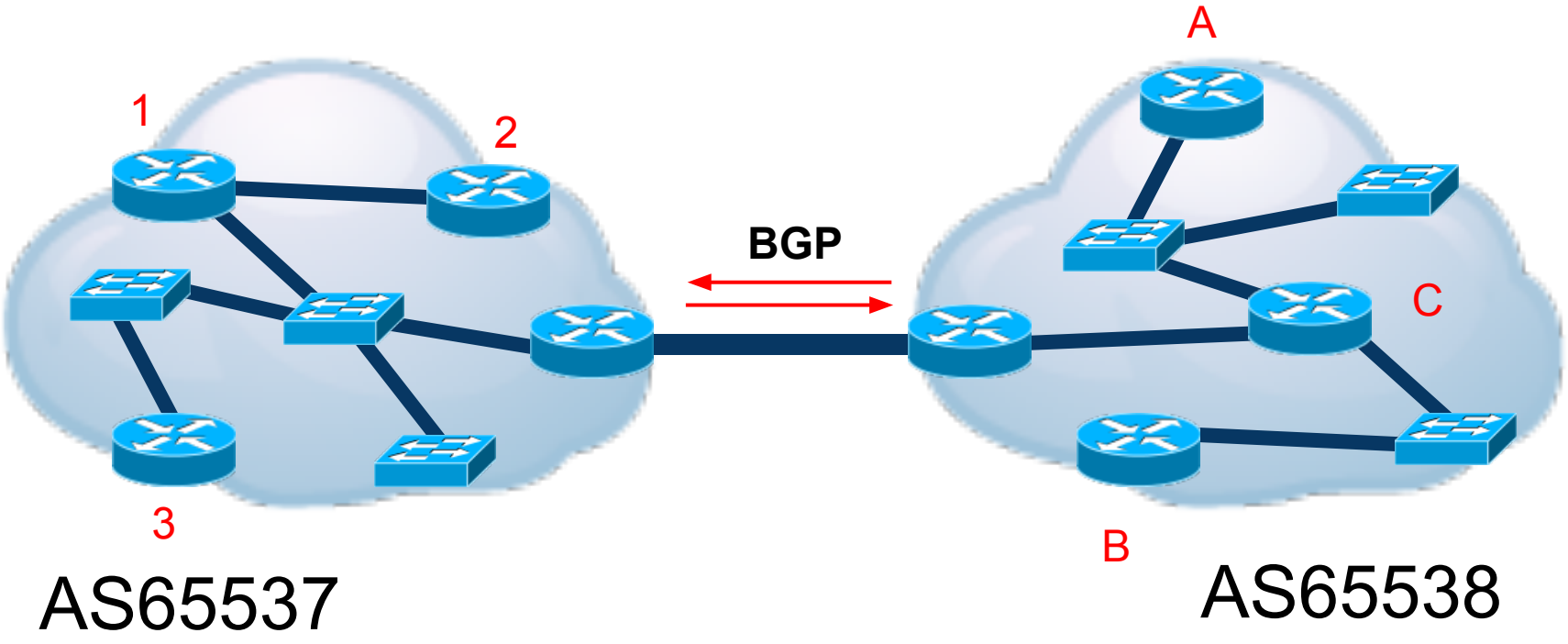


AS65537

AS65538

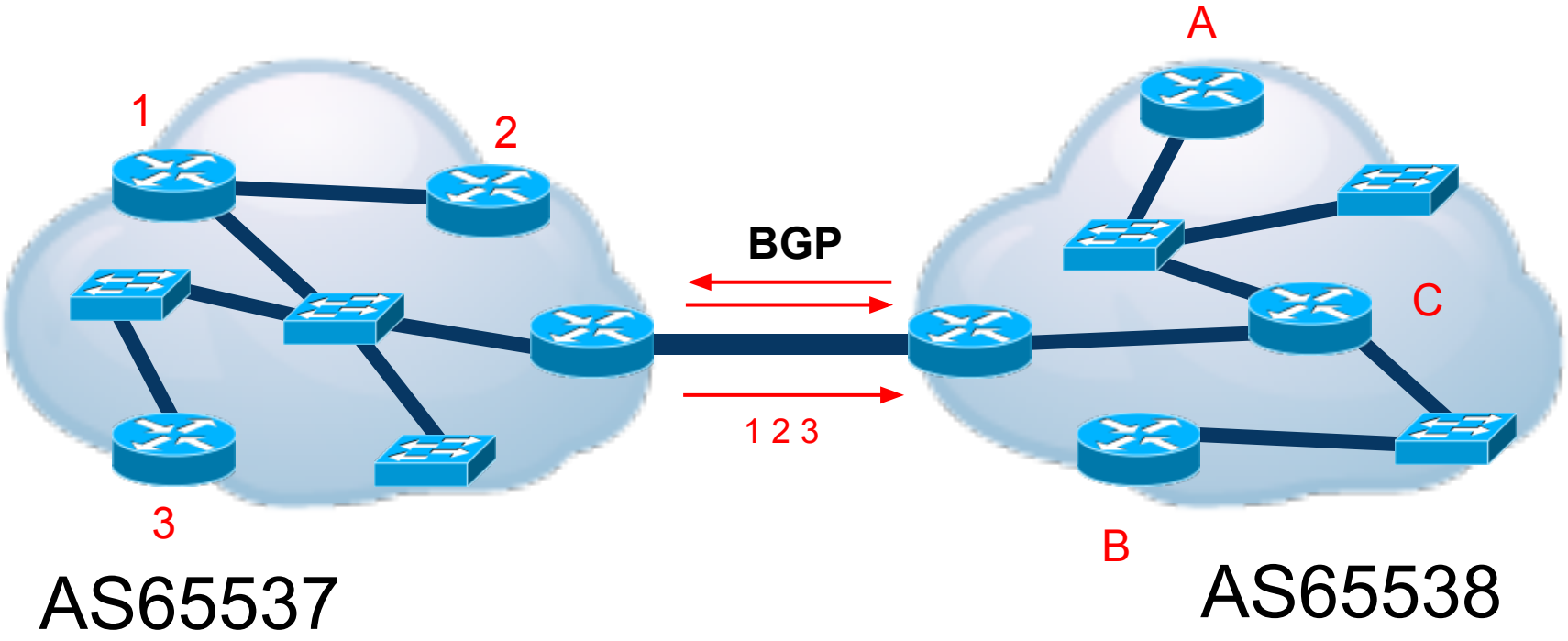
O que é BGP?

Colocando nomes nas máquinas de cada rede



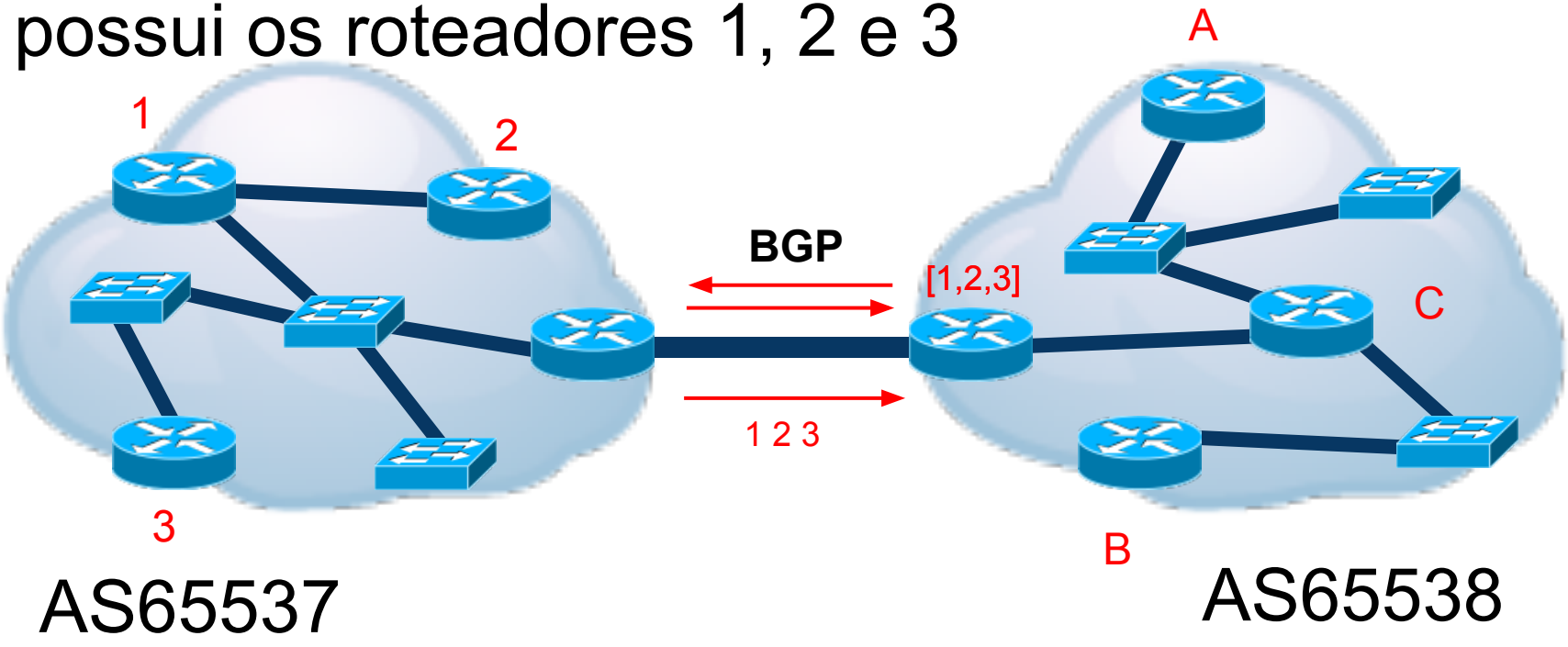
O que é BGP?

AS65537 envia informações sobre sua rede



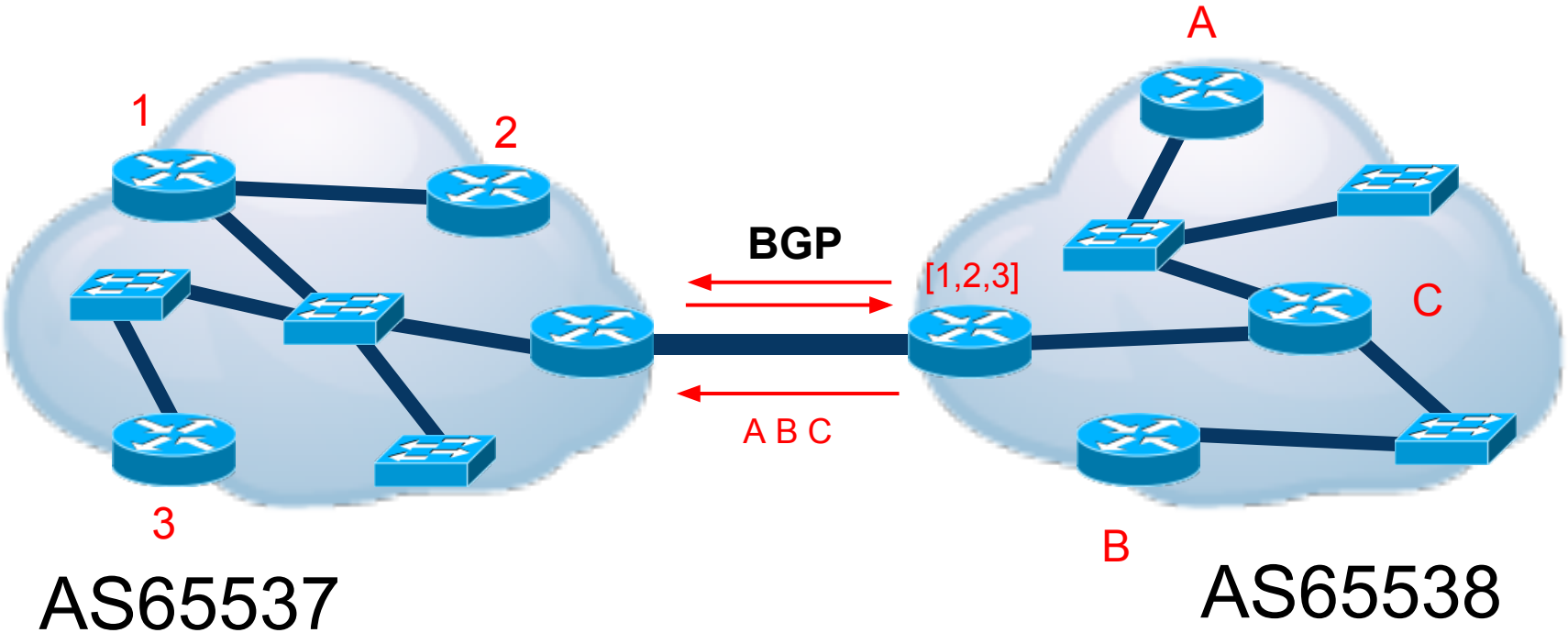
O que é BGP?

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



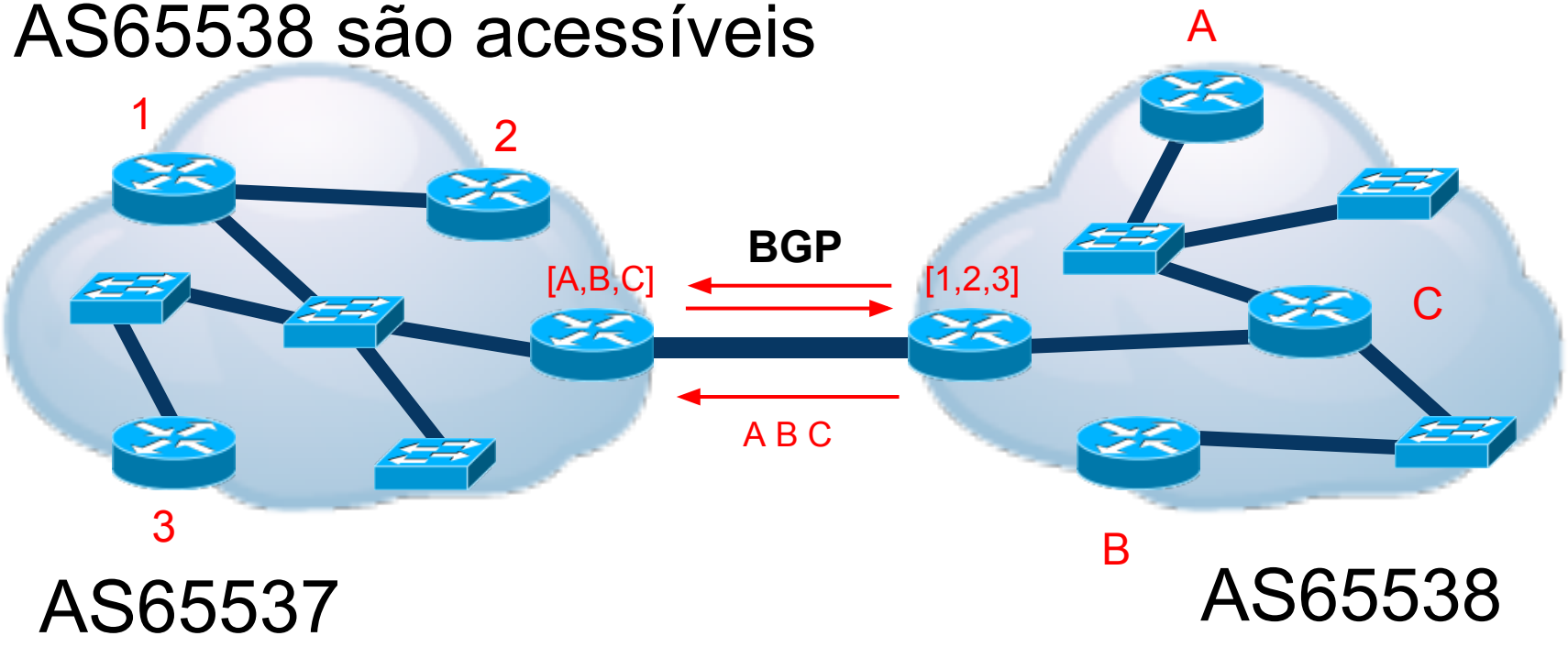
O que é BGP?

AS65538 também faz a mesma coisa



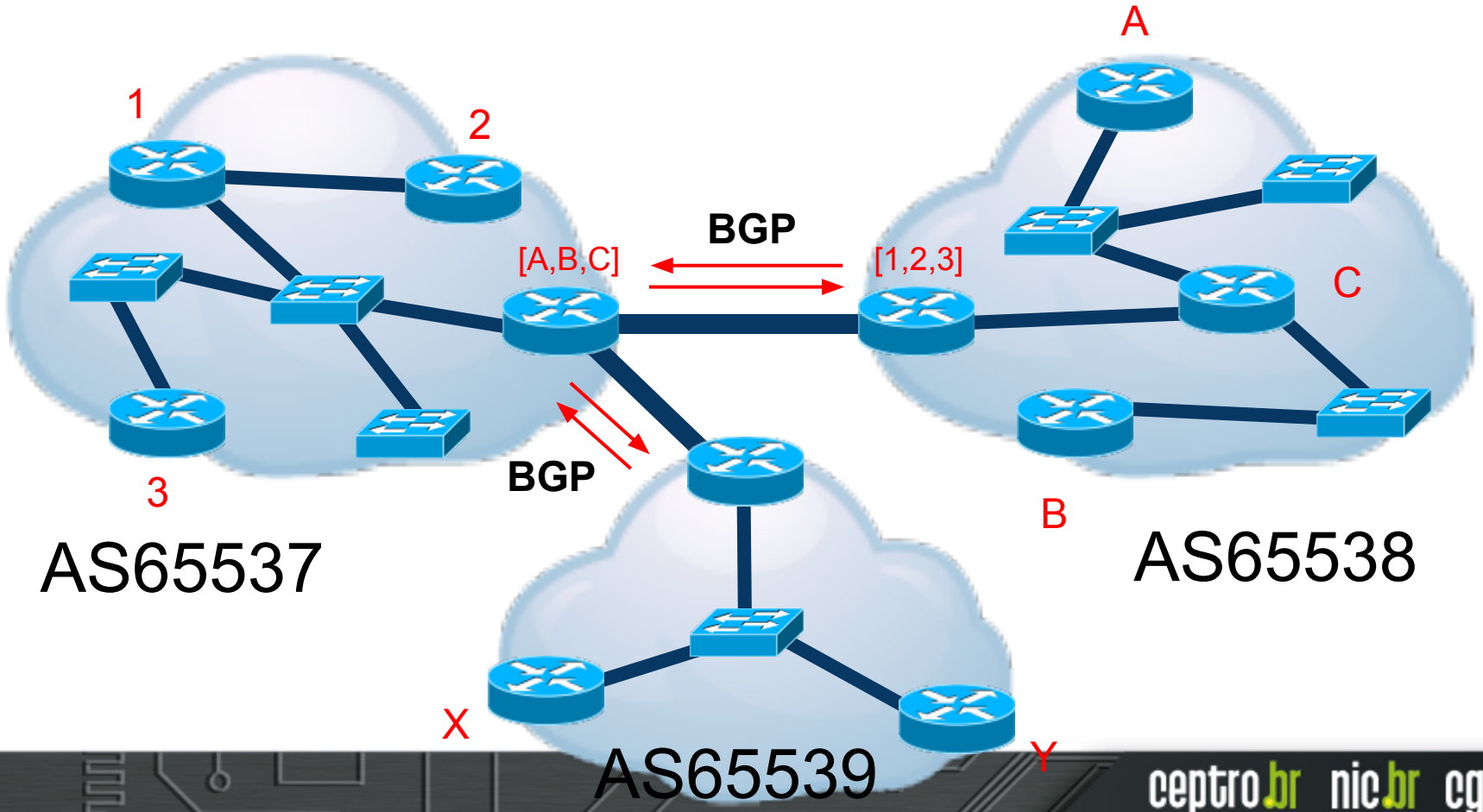
O que é BGP?

E o AS65537 descobre quais máquinas do AS65538 são acessíveis



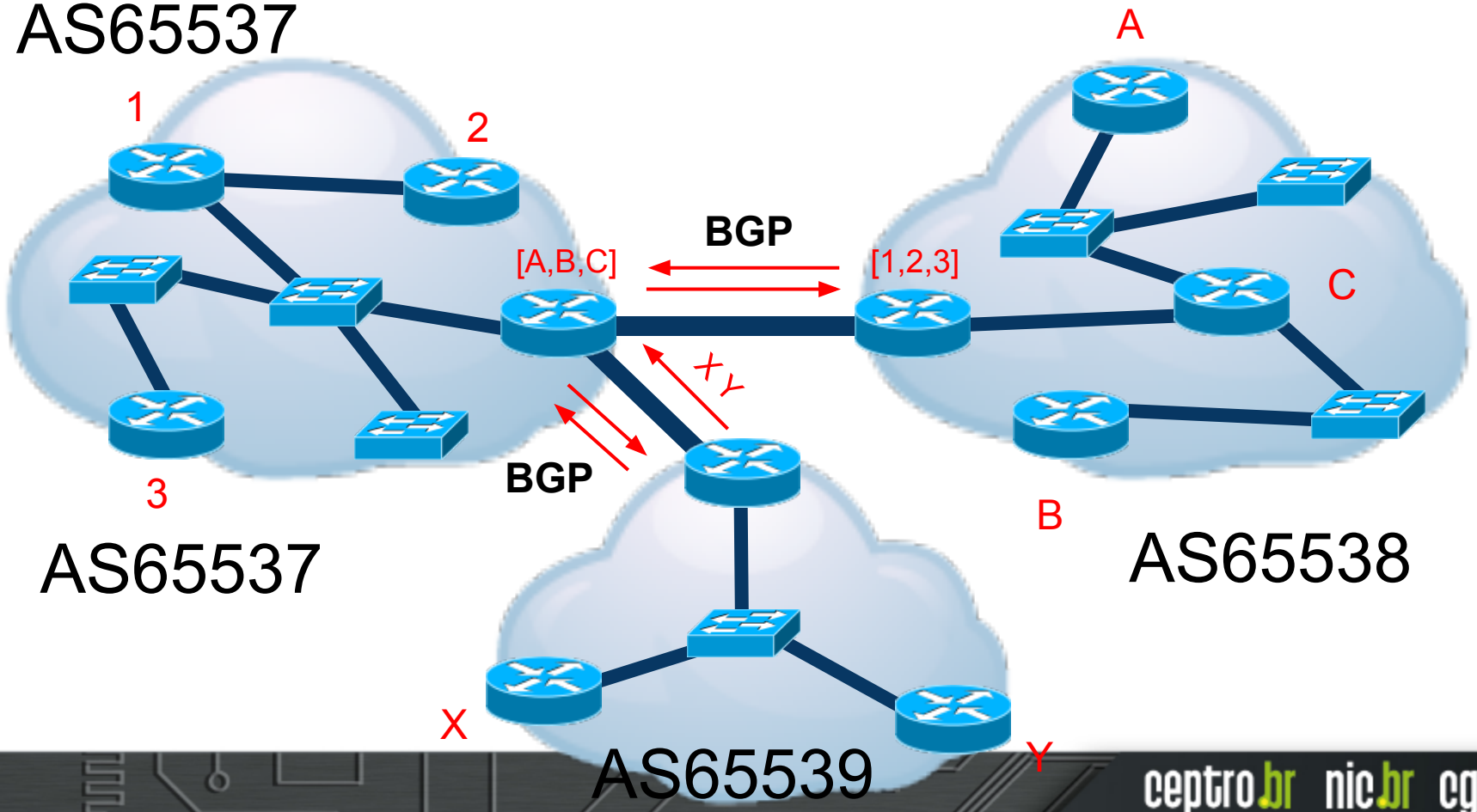
O que é BGP?

Com mais um AS no exemplo



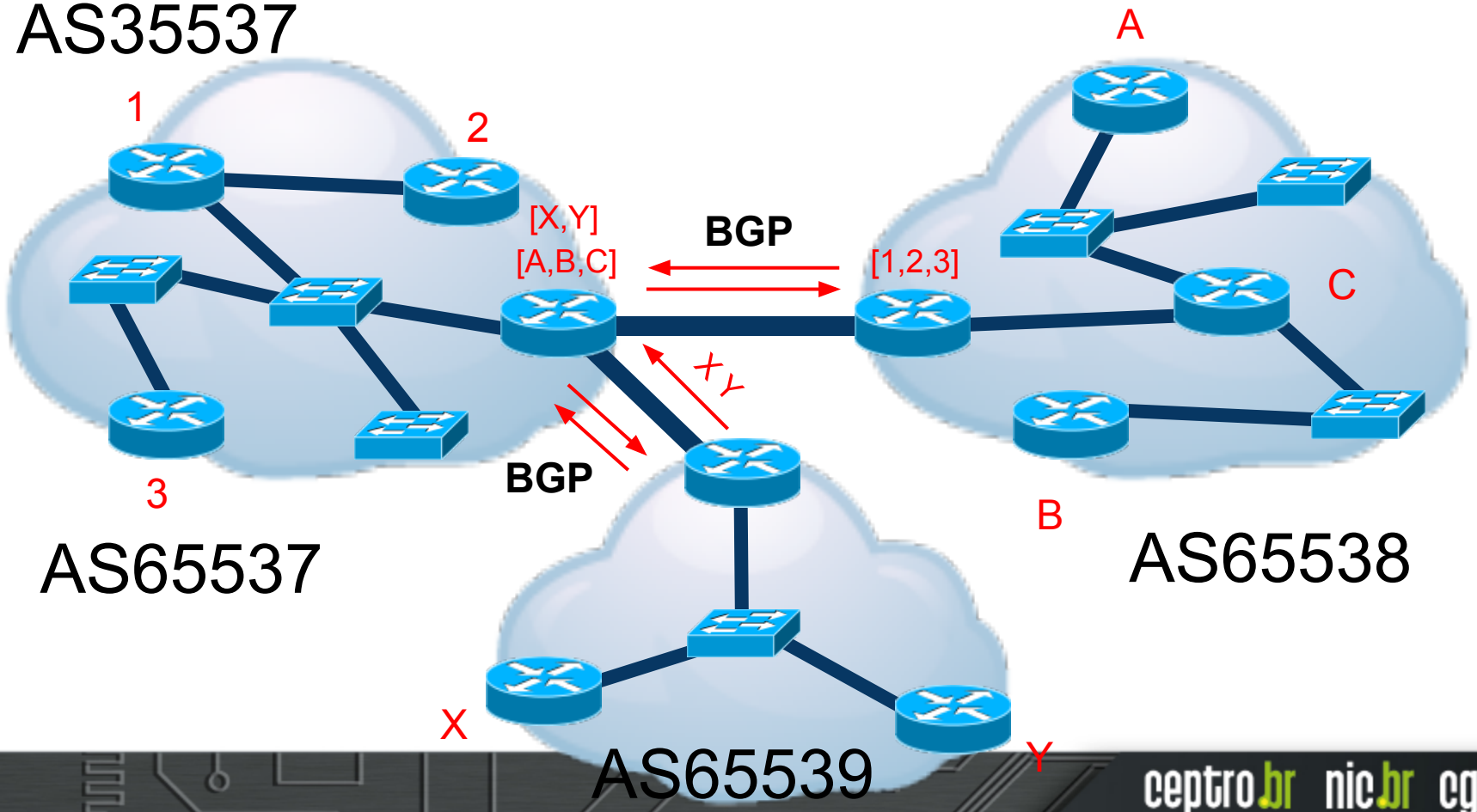
O que é BGP?

O AS novo envia suas informações para o AS65537



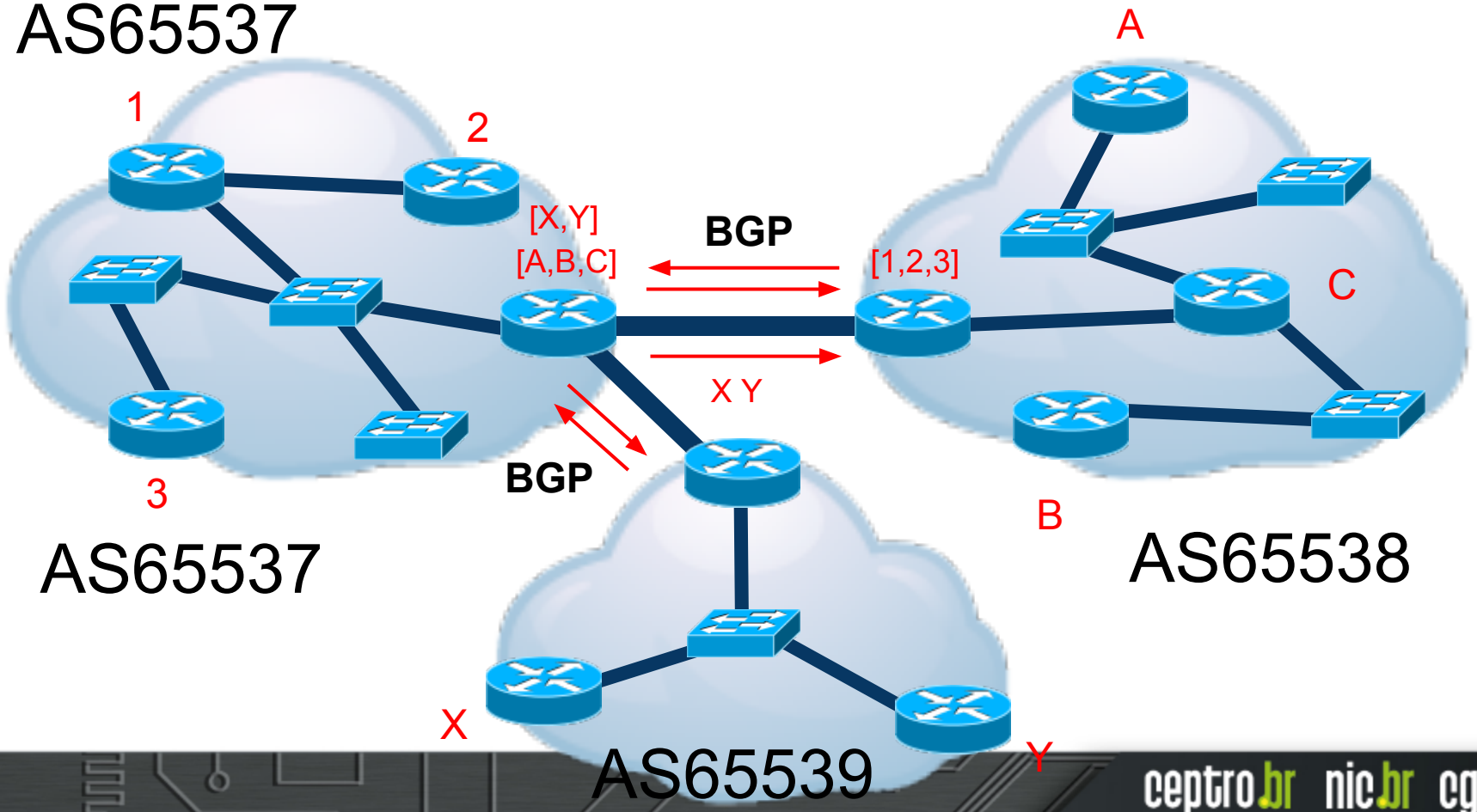
O que é BGP?

O AS novo envia suas informações para o AS35537



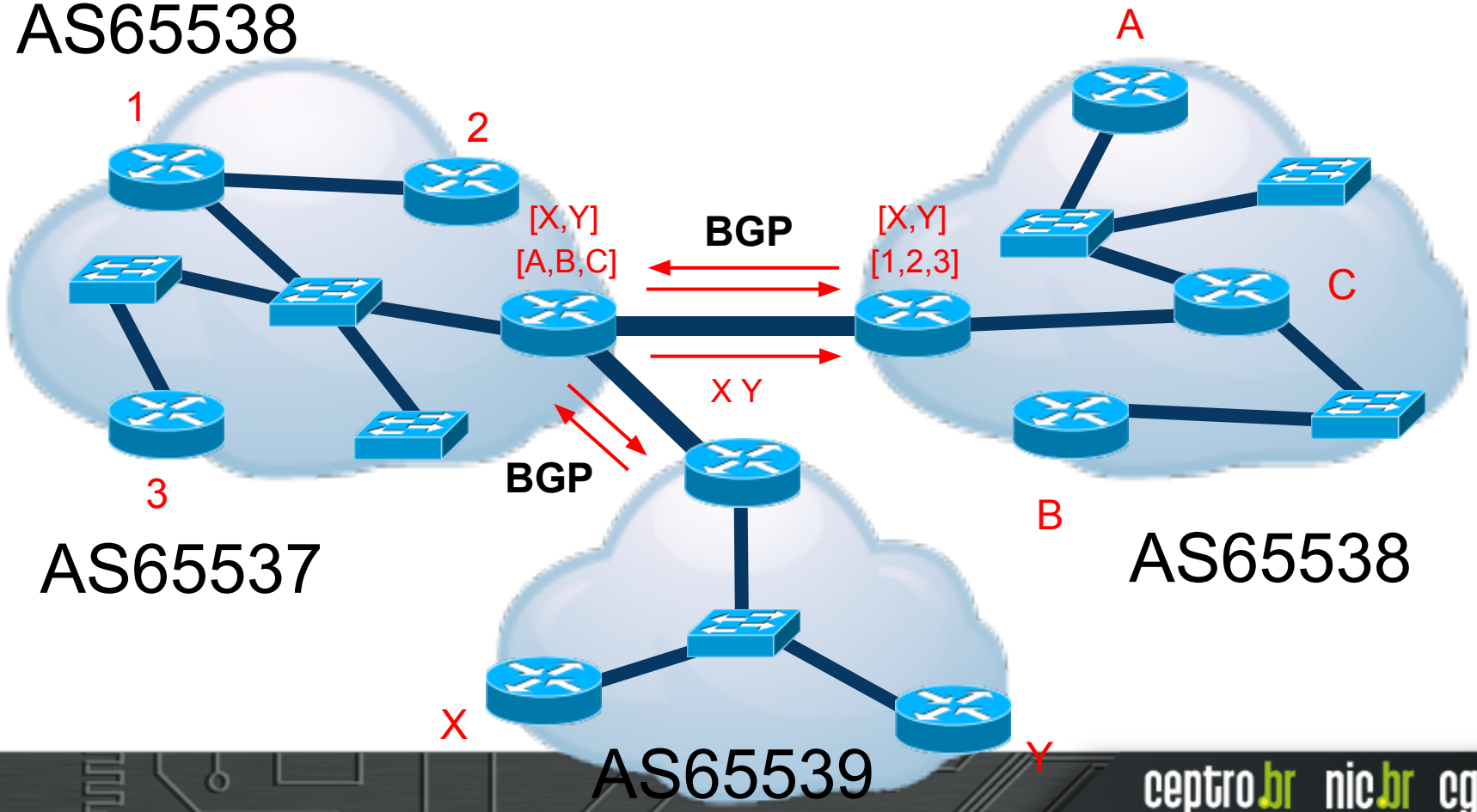
O que é BGP?

O AS novo envia suas informações para o AS65537



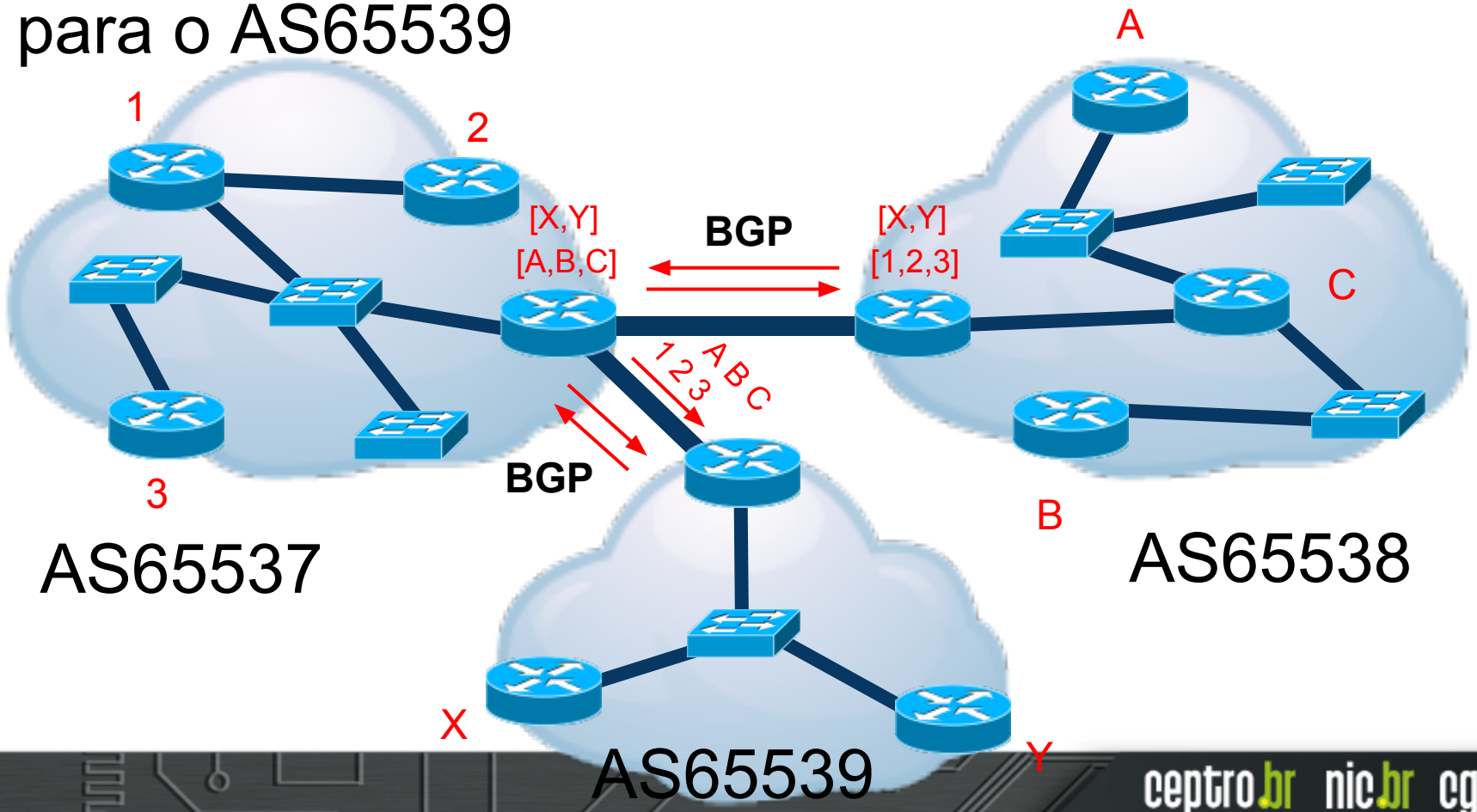
O que é BGP?

E o AS65537 repassa os dados para o AS65538



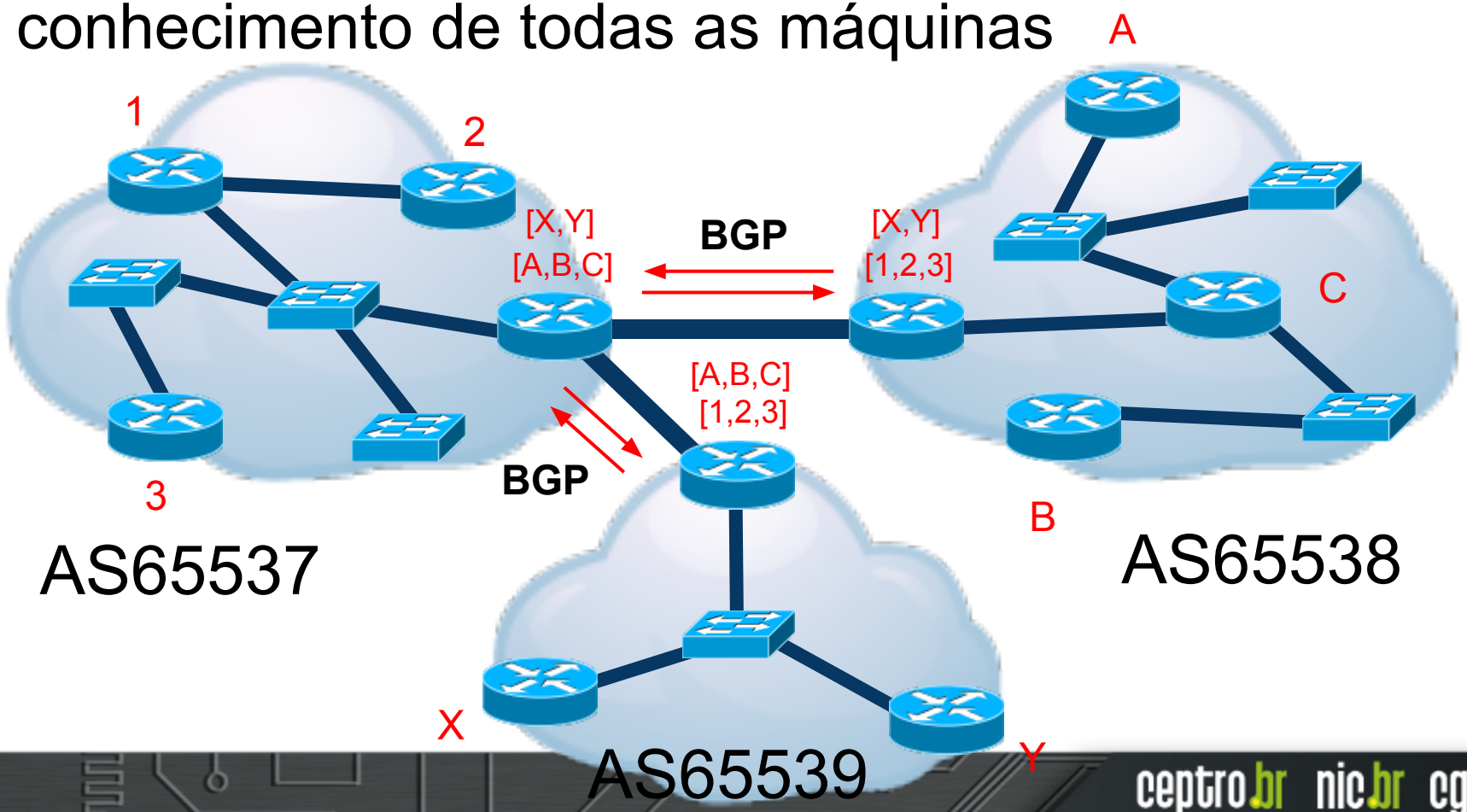
O que é BGP?

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

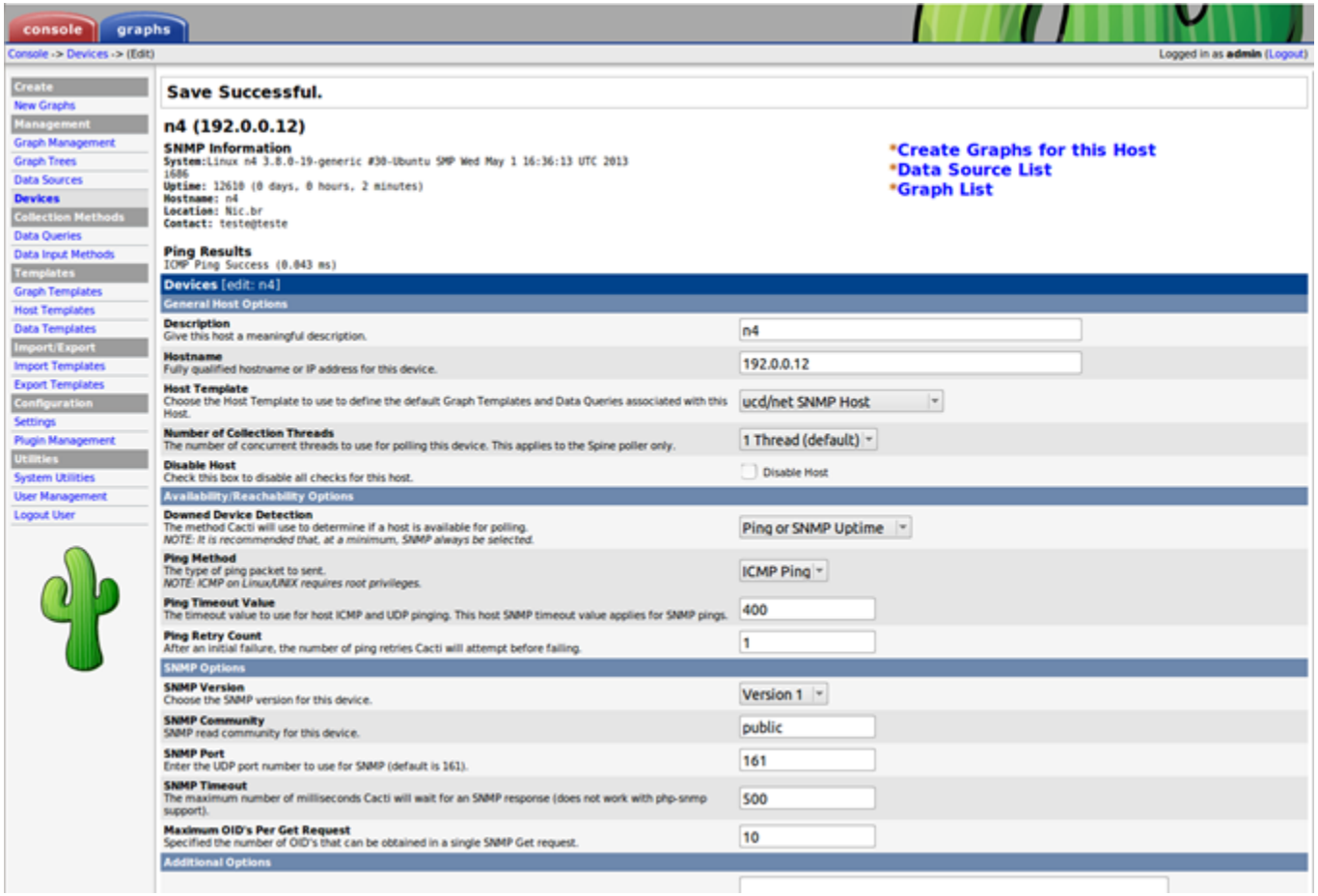
- Permite analisar dados de tráfego e performance.
- Dados em gráficos para permitir o entendimento dos usuários.
- Permite planejamento de novos recursos e identificação de gargalos na rede.
- Ex:
  - Cacti
  - Zabbix

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

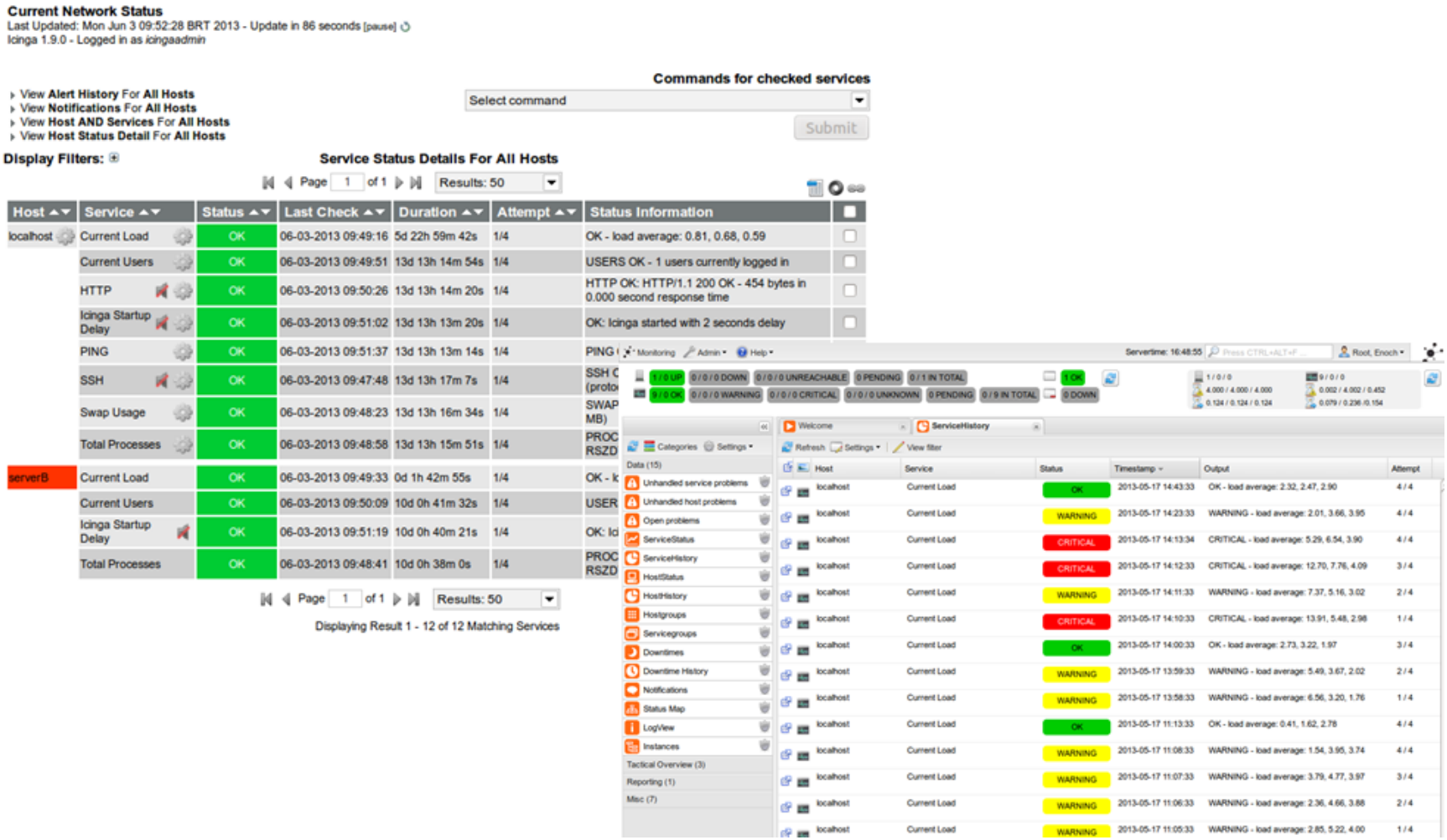


Tipos de ferramentas

➔ 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



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

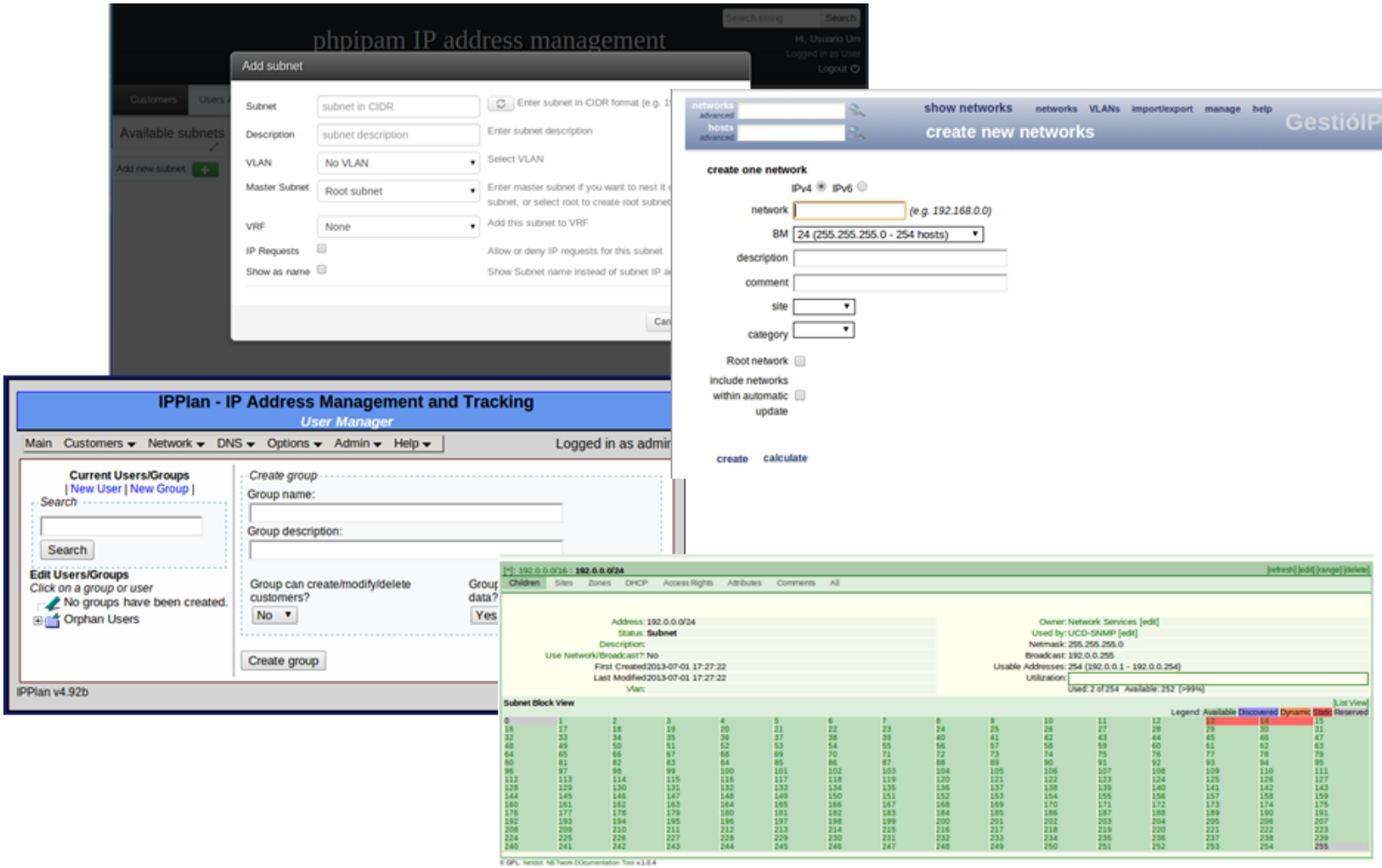
➔ Performance

- **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



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?

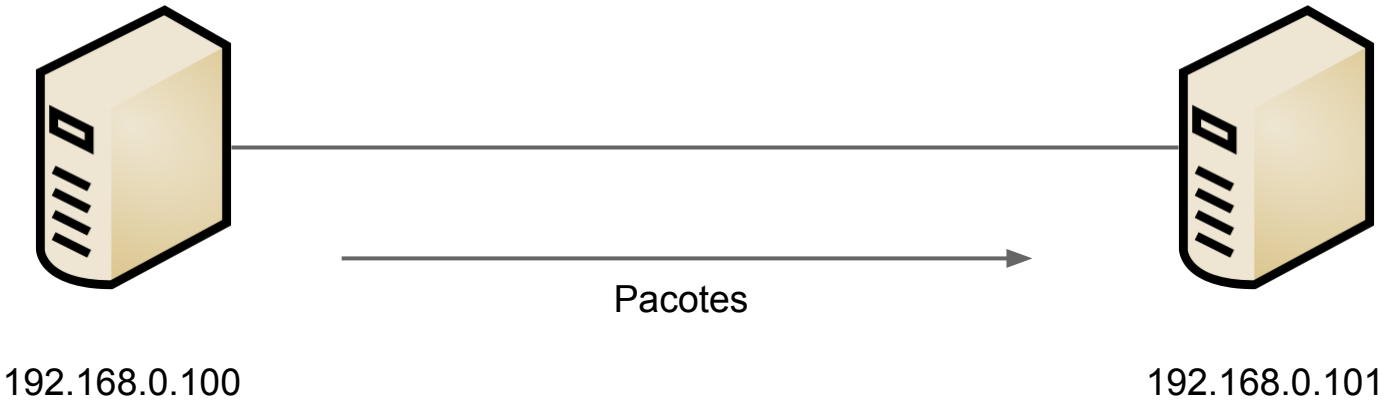
- ➔ Flow: do inglês, significa **fluxo**
  - ◆ E o que é fluxo?
    - Fluxo de pessoas
    - Fluxo de caixa
    - Fluxo magnético
    - Fluxo de dados

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

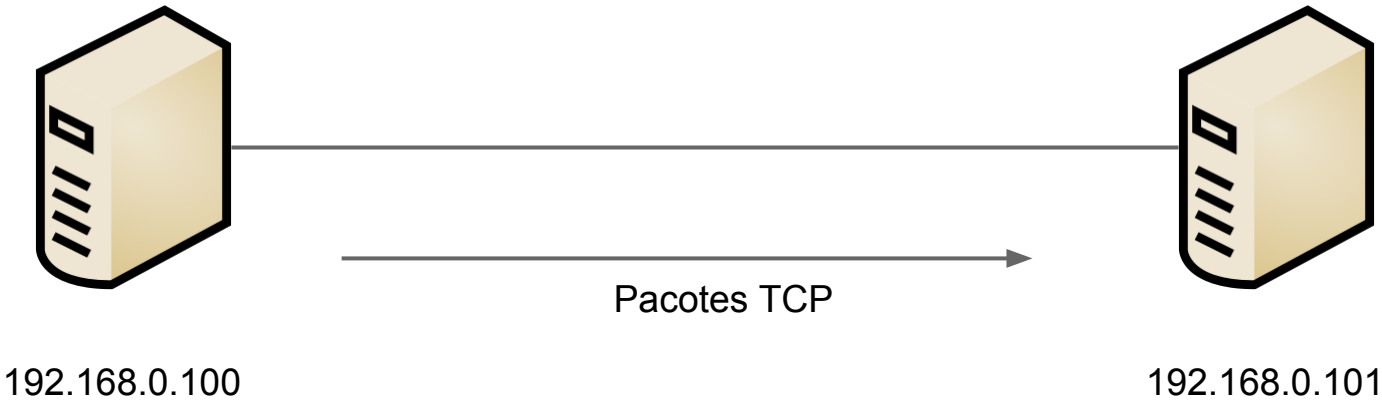
Para que serve?

➔ 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?

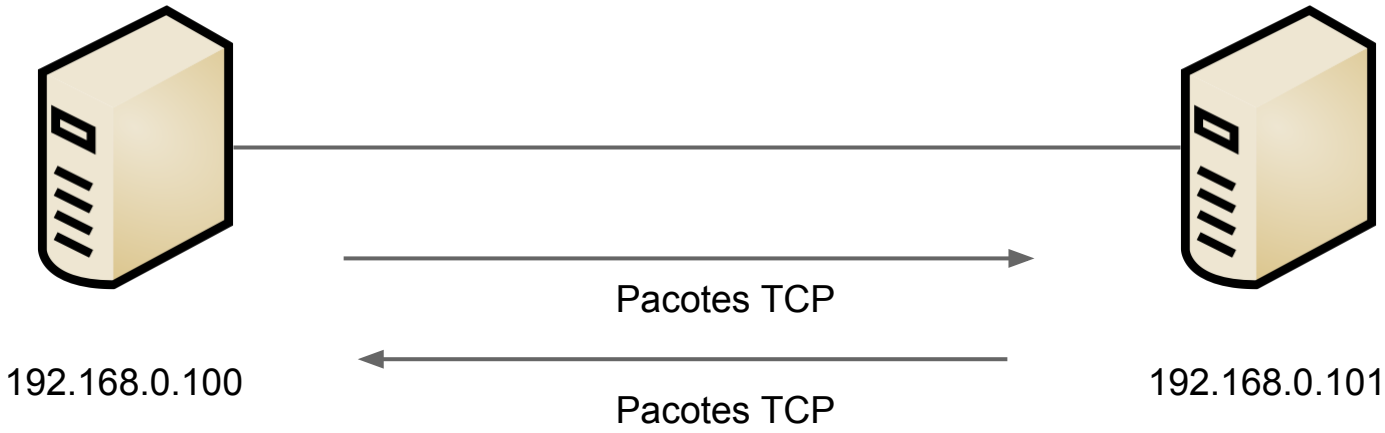
Exemplo de Flow:



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

O que é Flow?

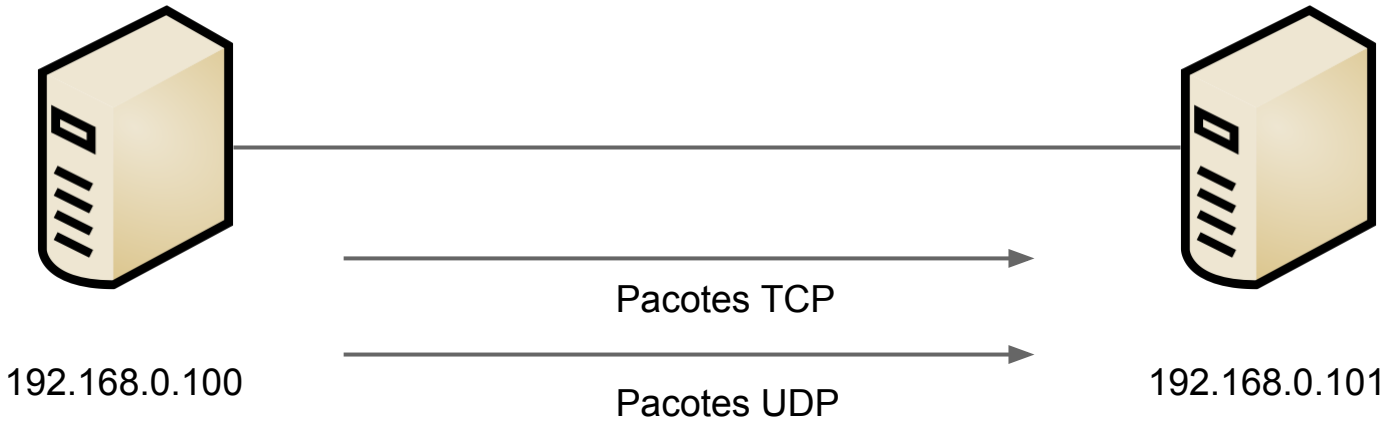
Exemplo de Flow:



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

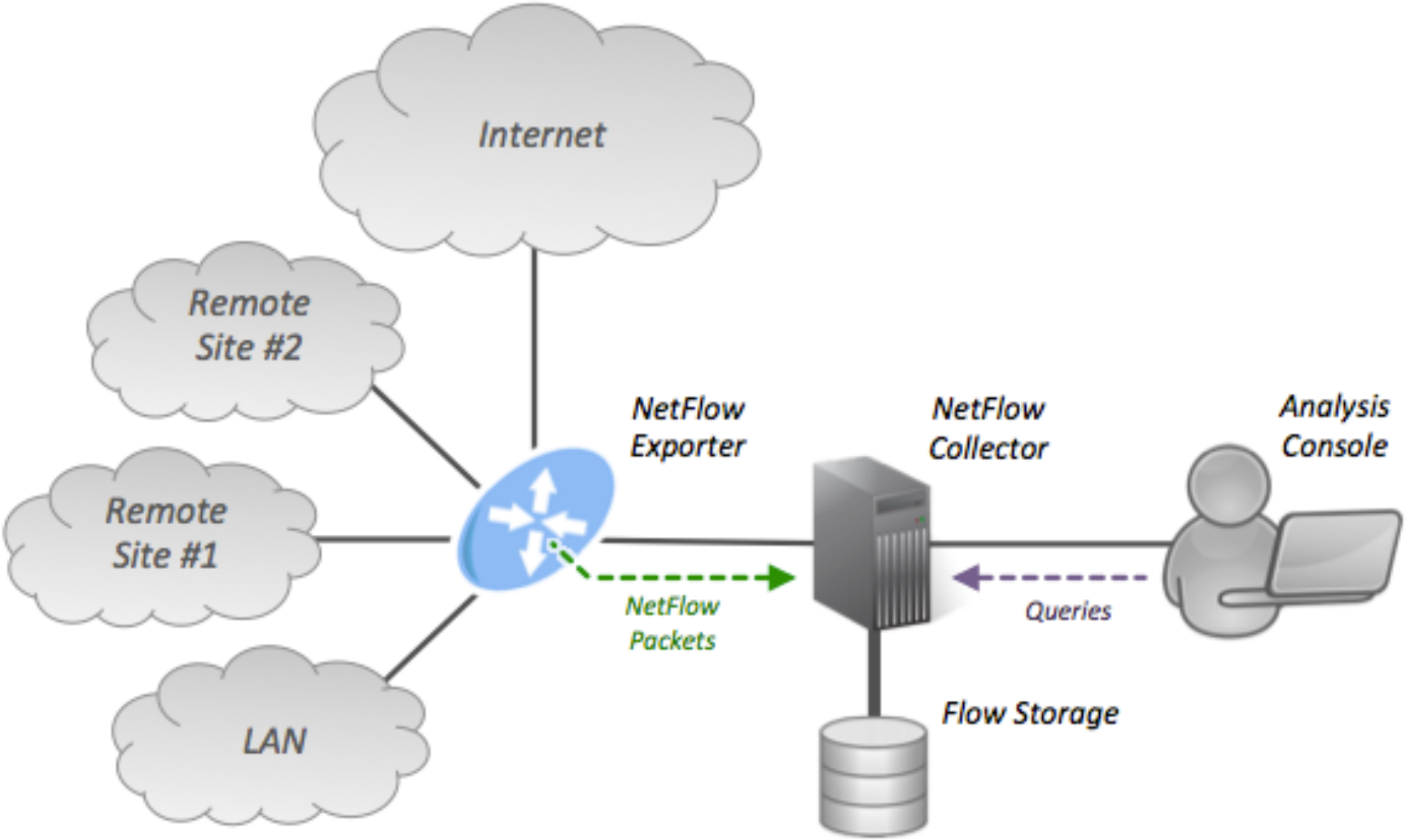
- Versões
  - V1: obsoleto
  - V5: mais comum, sem suporte a IPv6
  - V9: permite agrupamento de flows
  - V10: IPFIX

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

 facebook.com/nic.br

São Paulo, SP

16 de julho de 2015

nic.br cgi.br

www.nic.br | www.cgi.br