Análise de Vulnerabilidades de Redes em Conexões com PTT

27ª Reunião GTER

Eduardo Ascenço Reis
<eascenco@nic.br>
<eduardo@intron.com.br>

2009-06-19

Agenda

- Resumo
- Informações Preliminares
- Modelo Tradicional de Conexão a PTT
- Novo Modelo de Conexão a PTT – Links Família Ethernet
  - Vantagens
  - Alguns Efeitos Negativos
- Análise Links Ethernet para PTT
  - Problemas L2
  - Problemas L3

Resumo

Com a proliferação da adoção de redes Metro Ethernet para prover conexões L2 entre Sistemas Autônomos (AS) e Pontos de Troca de Tráfego (PTT), muitos benefícios foram obtidos, tais como: simplificação da conexão, tecnologia familiar e uniforme (família Ethernet), menor custo, menor número de pontos de falha, maior flexibilidade, etc.

Por outro lado, a utilização dessas conexões pode expor o AS a pontos de vulnerabilidades nas áreas de segurança e de redes.

Esta apresentação pretende focar a discussão em algumas potenciais vulnerabilidades de redes e em sugestões de como um AS pode se proteger, com o objetivo de manter uma rede mais controlada, segura e estável.

Os pontos chaves que serão endereçados nesta apresentação são: vulnerabilidades de roteamento em engenharia de tráfego externo e proteções na estrutura Ethernet (L2), ambas considerando como referência o AS participante de PTTs.

Apontamento

Esta apresentação é uma continuação da palestra abaixo:

Reunião LACNIC XII
http://lacnic.net/pt/eventos/lacnicxii/

Fórum de Interconexão Regional NAPLA 2009
http://lacnic.net/pt/eventos/lacnicxii/napla2009.html

Algumas Considerações sobre Modelos de Conexão dos Participantes de IXP
http://lacnic.net/documentos/lacnicxii/presentaciones/napla/06_Eduardo_Ascenco_Reis.pdf

Informação - IXP / PTT

IXP - Internet eXchange Point

PTT – Ponto de Troca de Tráfego

O foco desta apresentação é no participante do PTT,

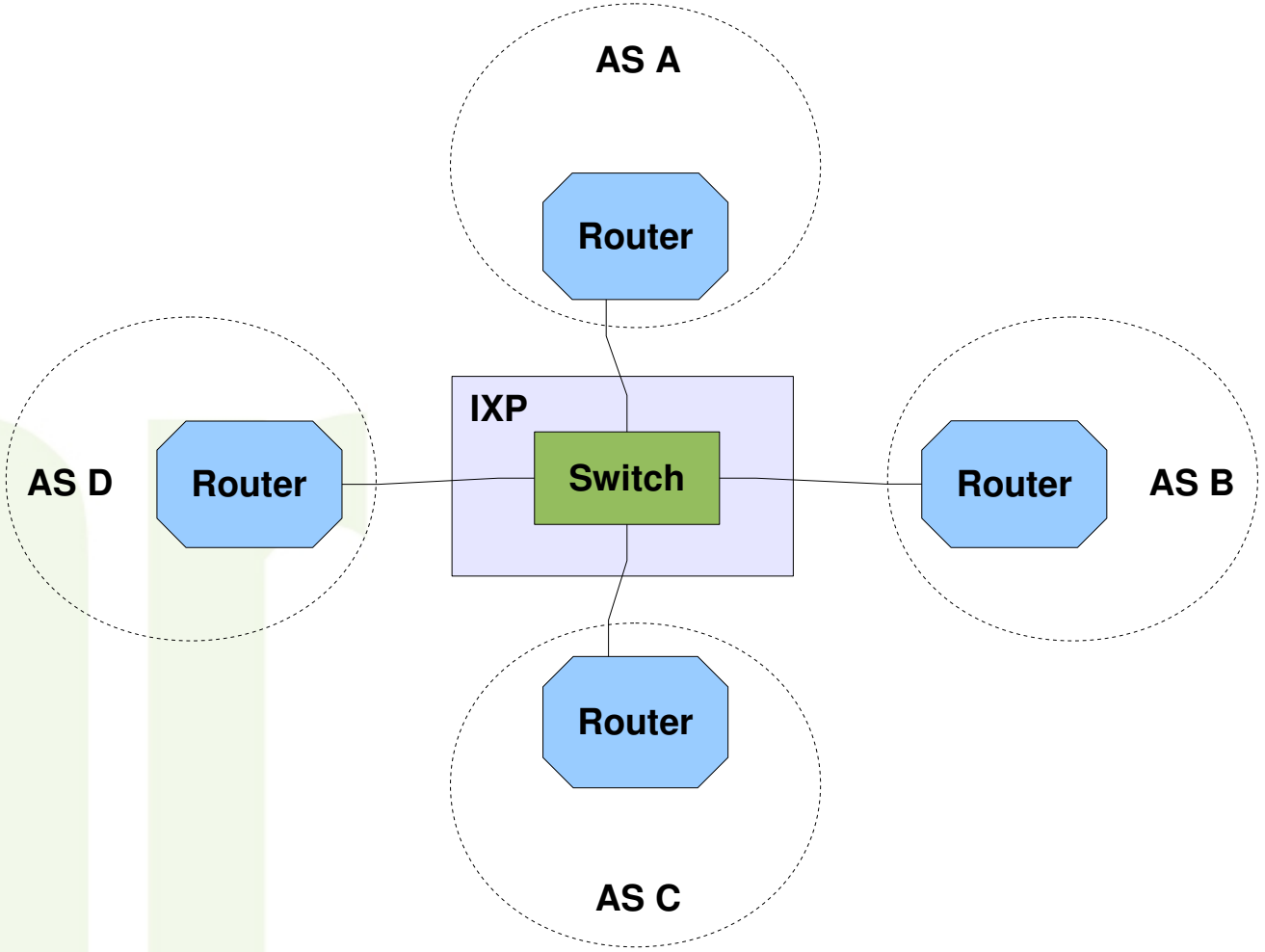
e não no PTT em si.

PTT – Matriz de Comutação (switching fabric / peering fabric)

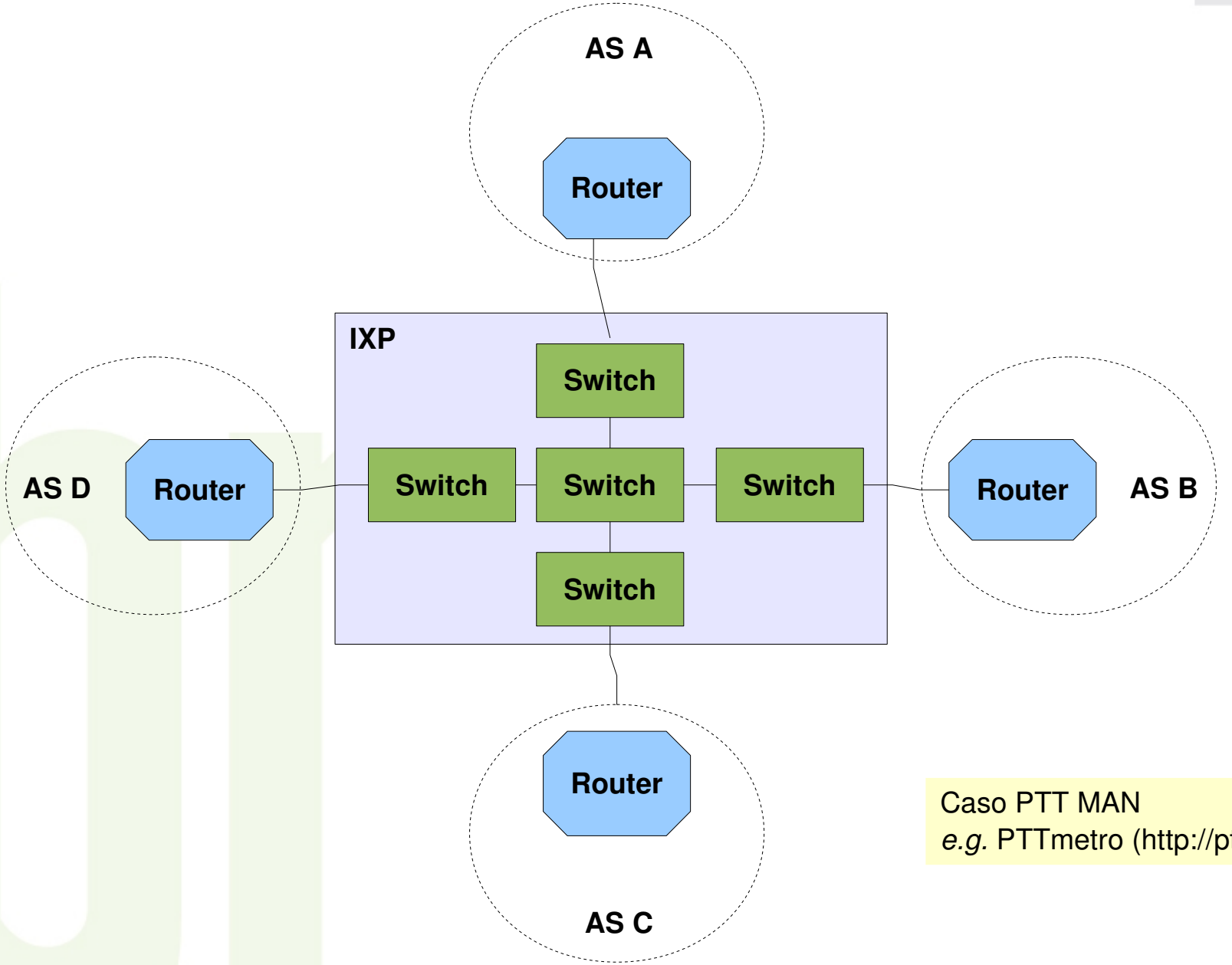
Tradicionalmente baseada em equipamentos da família Ethernet (switches)

O modelo de um PTT pode ser simplificado como um único switch LAN.

Informações Preliminares – PTT – Modelo LAN Switch



Informações Preliminares – PTT – Modelo Rede Metro Ethernet



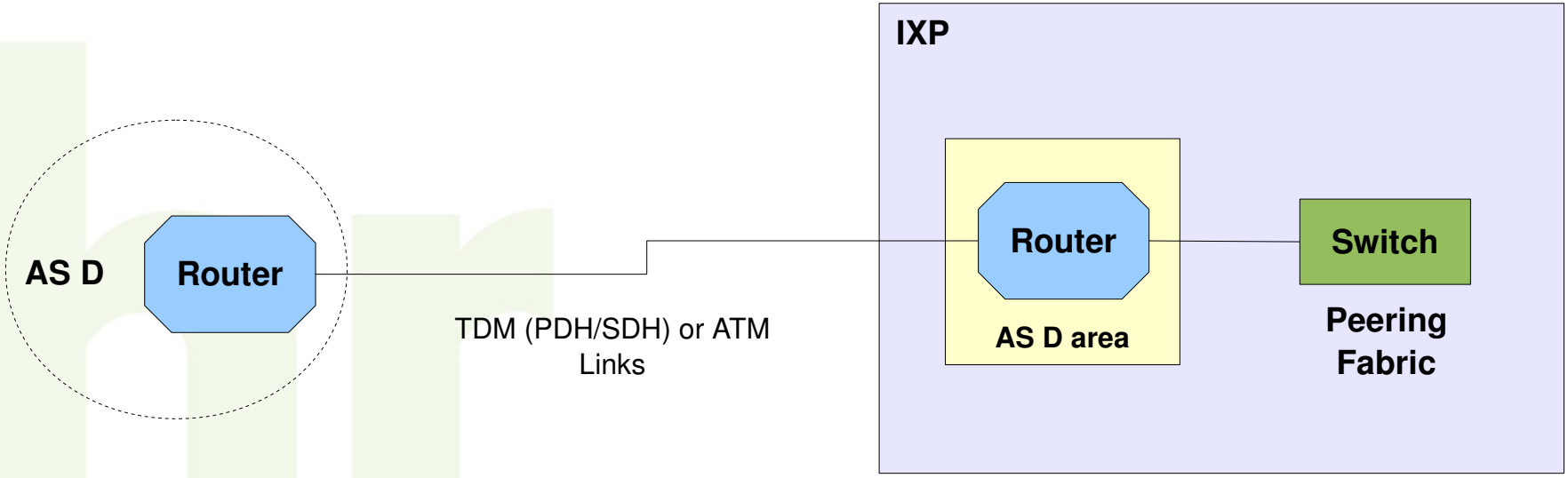
Caso PTT MAN
e.g. PTTmetro (http://ptt.br)

Informações Preliminares – AS

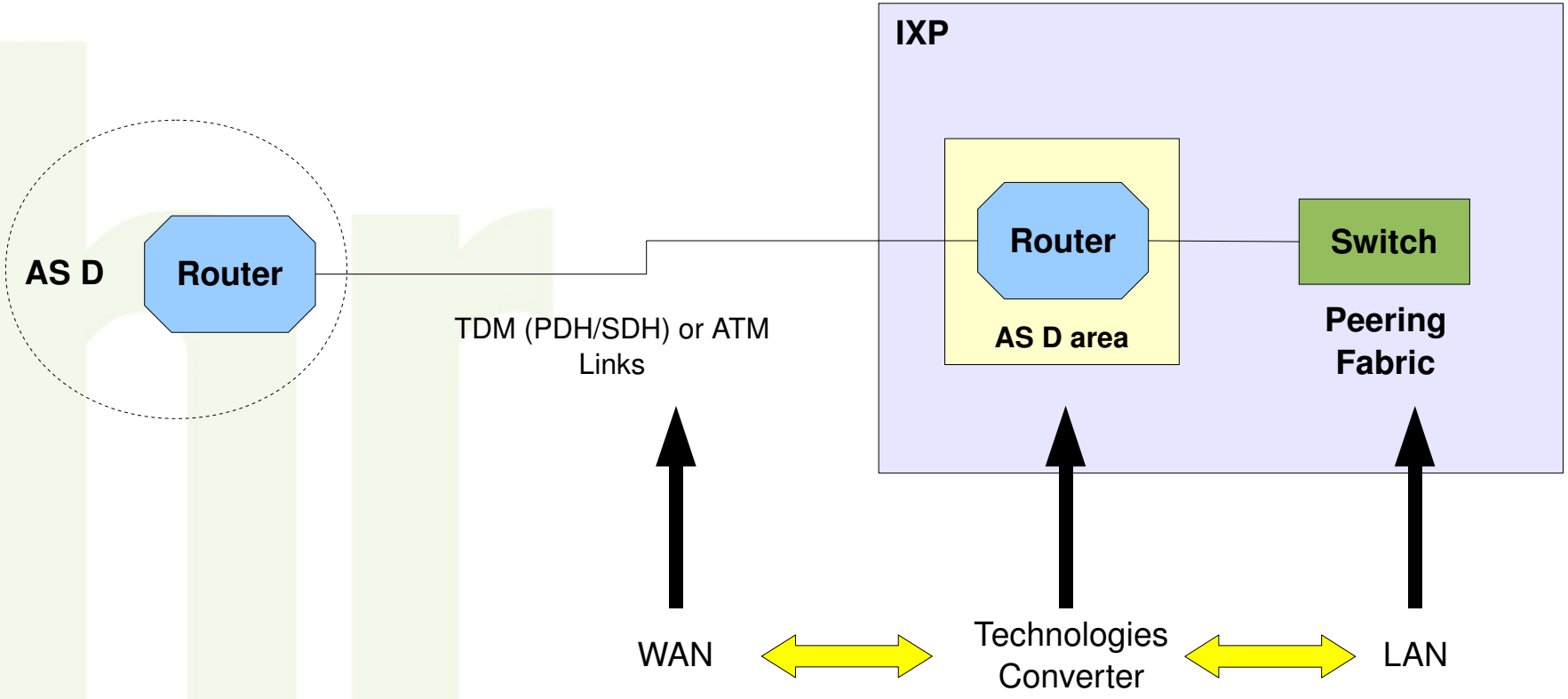
Os Sistemas Autônomos (Autonomous System- AS) normalmente utilizam redes internas baseadas em equipamentos da família Ethernet (switches).

As redes internas de um AS podem ser simplificadas como uma rede local (LAN).

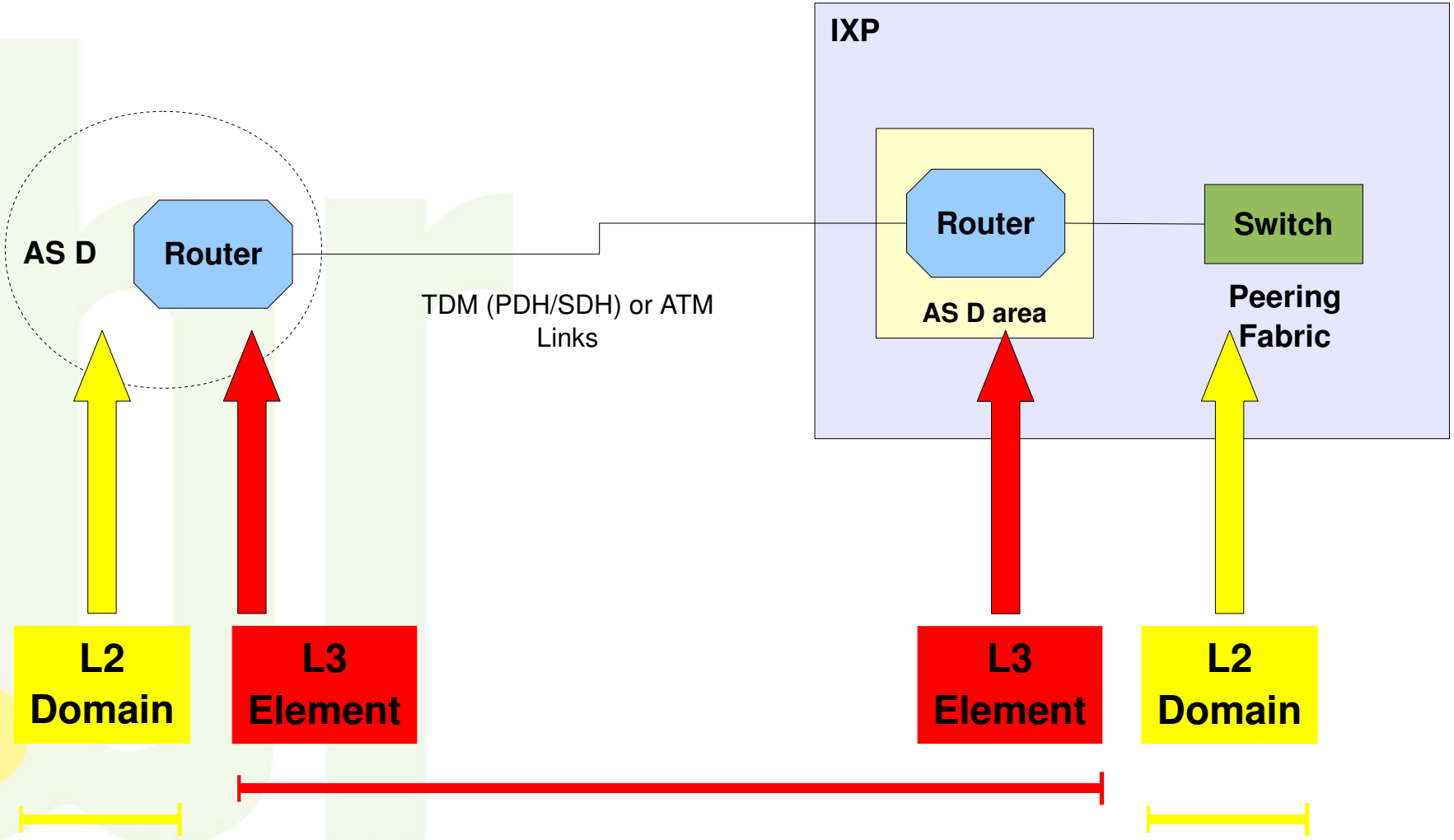
PTT – Modelo Tradicional de Conexão



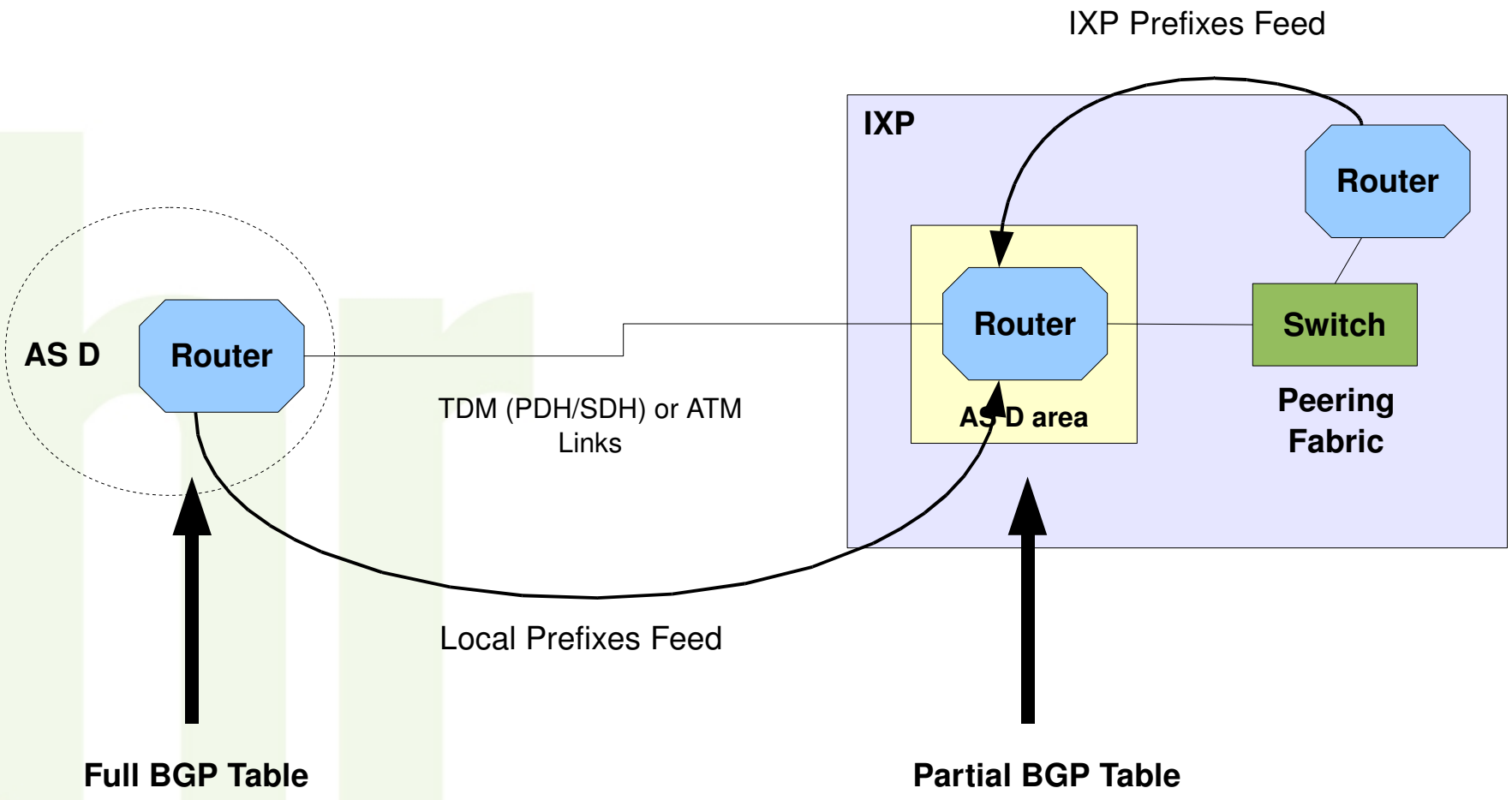
PTT – Modelo Tradicional de Conexão



PTT – Modelo Tradicional de Conexão



PTT – Modelo Tradicional de Conexão



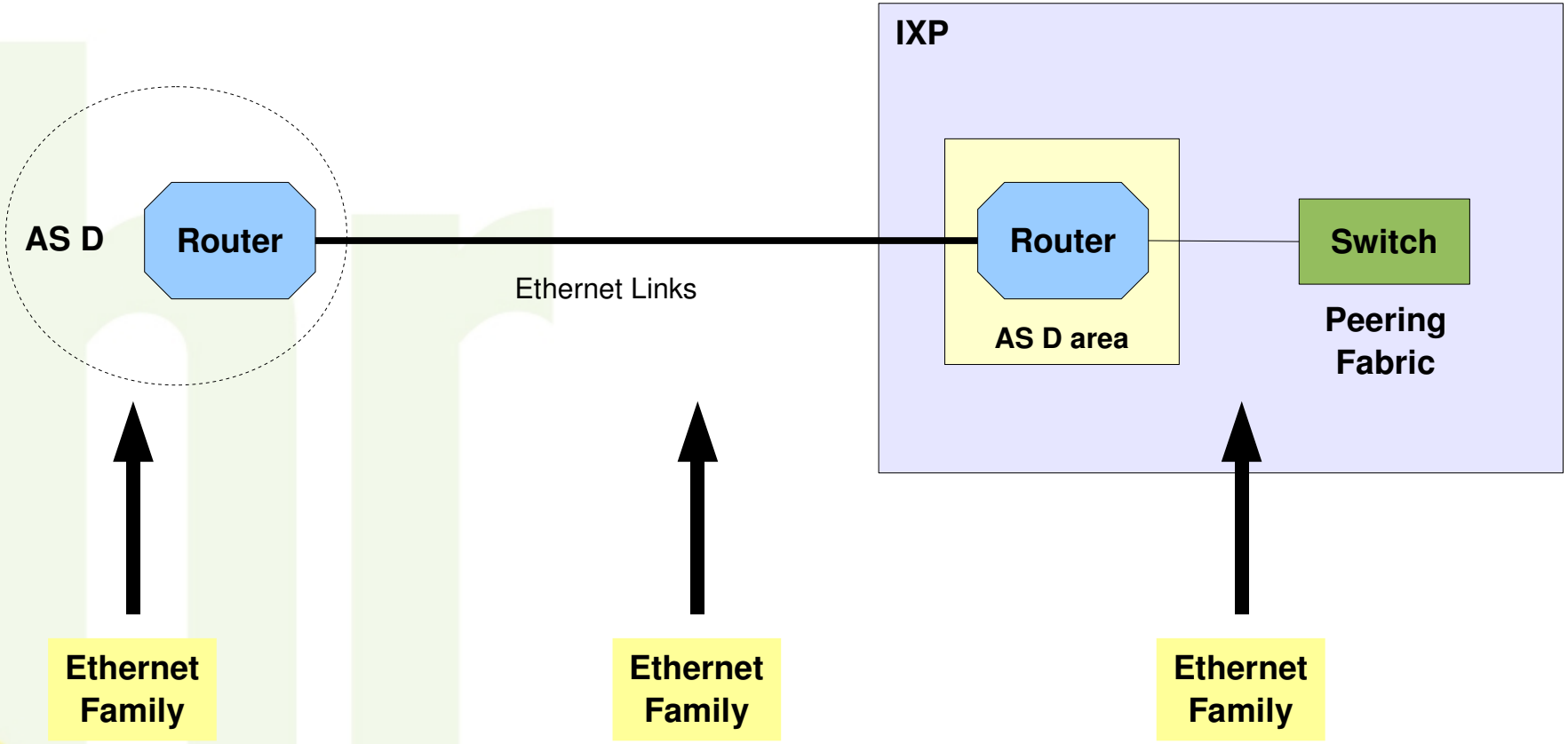
PTT – Modelo Novo de Conexão – Links Família Ethernet

Links da família Ethernet (Gigabit Ethernet e 10 Gibabit Ethernet)

tornaram-se uma tecnologia comum para uso externo em Redes Metropolitanas (MAN),

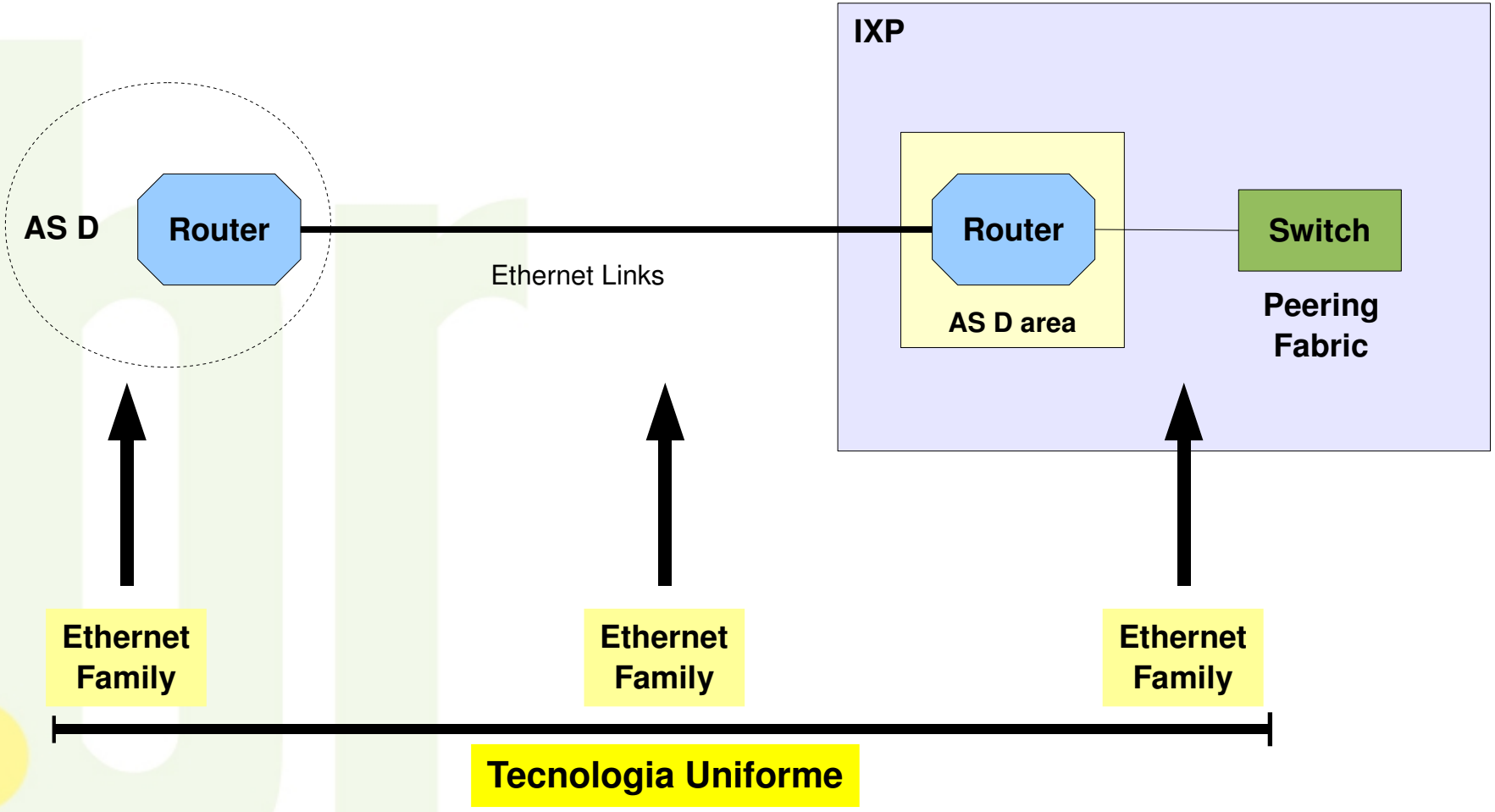
além de também serem utilizados em conexões de longa distância (WAN).

PTT – Modelo Novo de Conexão – Links Família Ethernet - Vantagens



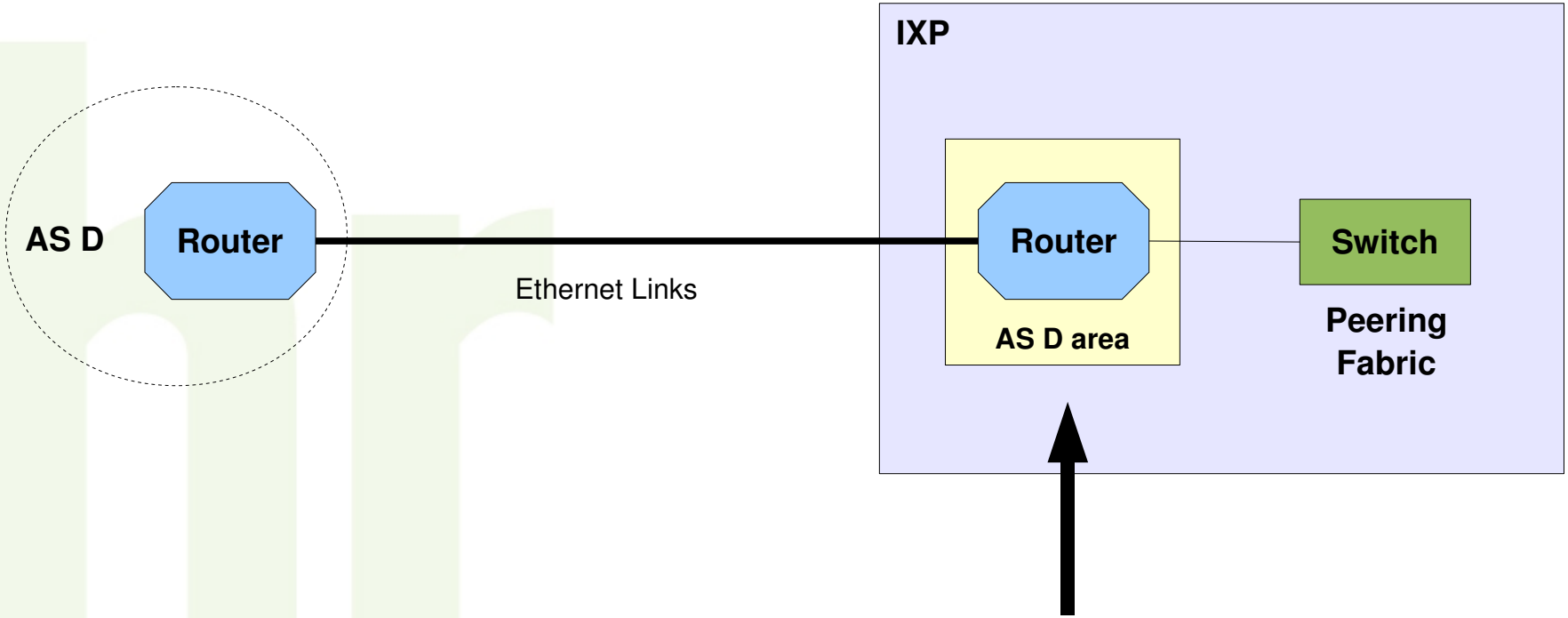
PTT – Modelo Novo de Conexão – Links Família Ethernet - Vantagens

✔ Simplificação
✔ Menor Custo Operacional



PTT – Modelo Novo de Conexão – Links Família Ethernet - Vantagens

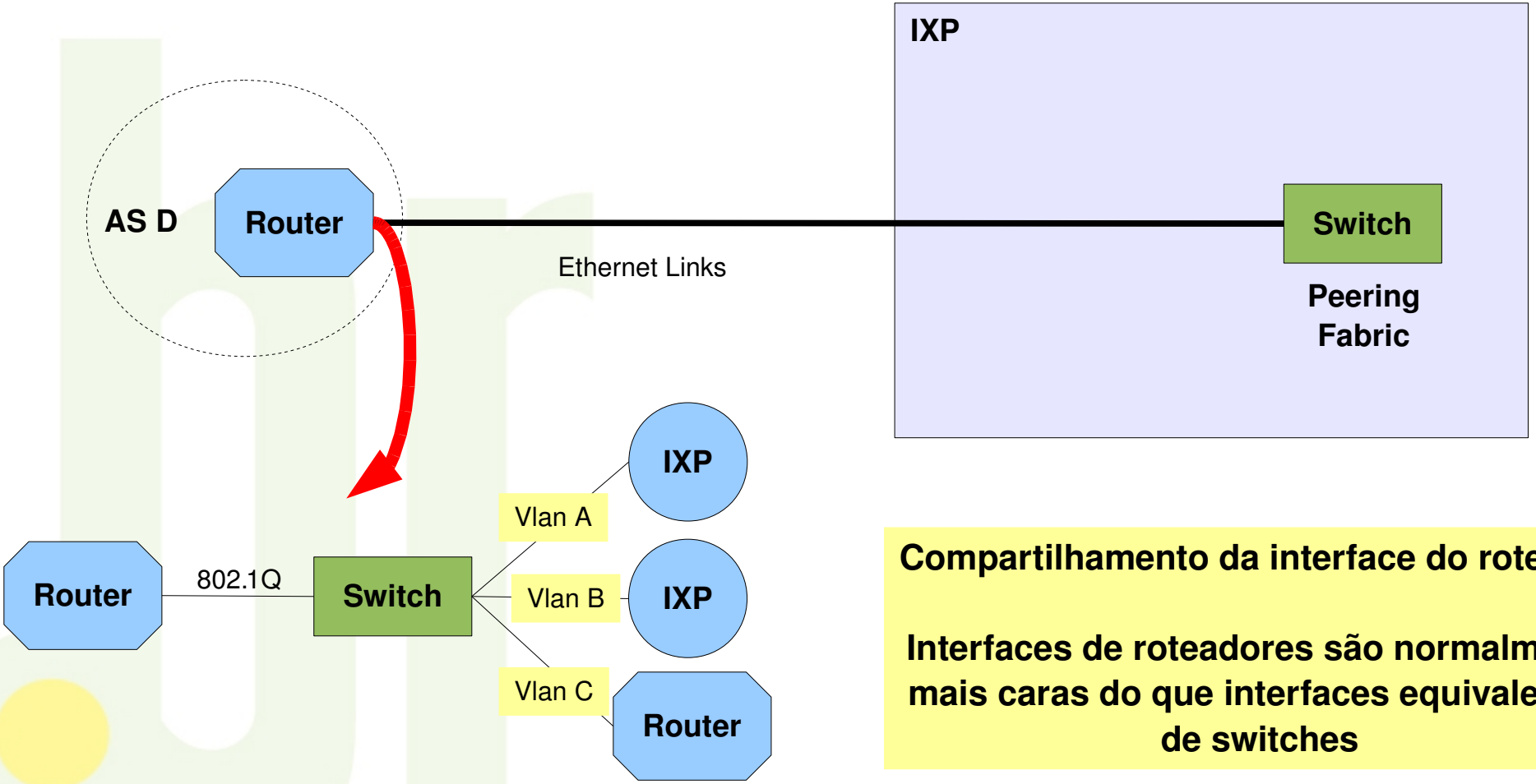
✔ **Menor Custo**
✔ **Menos Equipamentos Envolvidos**
(menor número de pontos de falha, simplificação de gerenciamento e suporte)



Não há mais necessidade de roteador remoto e eventualmente de espaço de Data Center no local do PTT.

PTT – Modelo Novo de Conexão – Links Família Ethernet - Vantagens

✔ Menor Custo
✔ Otimização de Equipamentos



Compartilhamento da interface do roteador

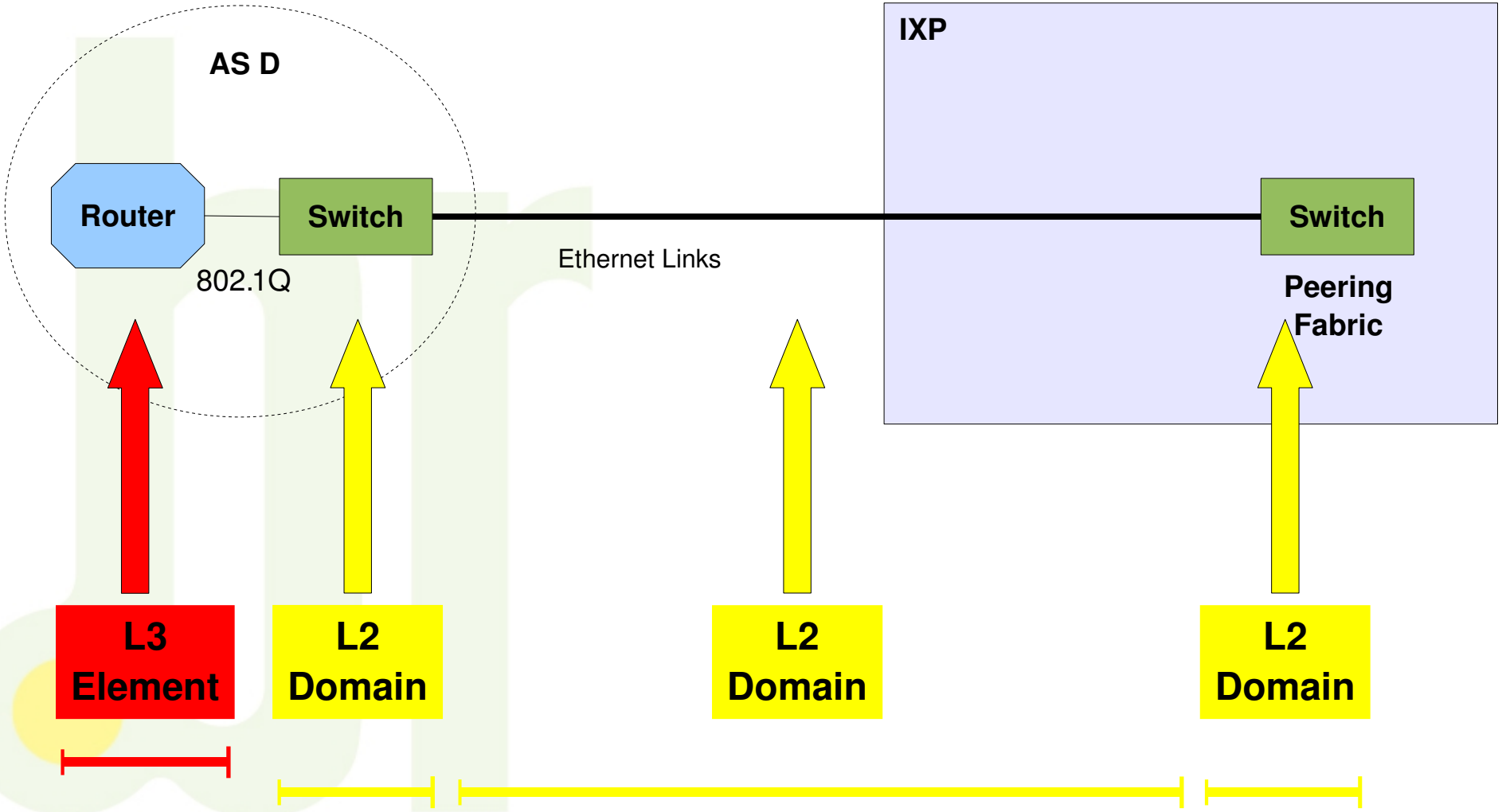
Interfaces de roteadores são normalmente mais caras do que interfaces equivalentes de switches

PTT – Modelo Novo de Conexão – Links Família Ethernet – Efeitos Negativos

Ao menos dois possíveis grupos de problemas podem ser observados

- ✗ **Perda de isolamento lógico simples entre domínios L2**
- ✗ **Perda de isolamento das tabelas BGP (PTT e Global) dentro do AS**

✗ **Perda de isolamento lógico simples entre domínios L2**

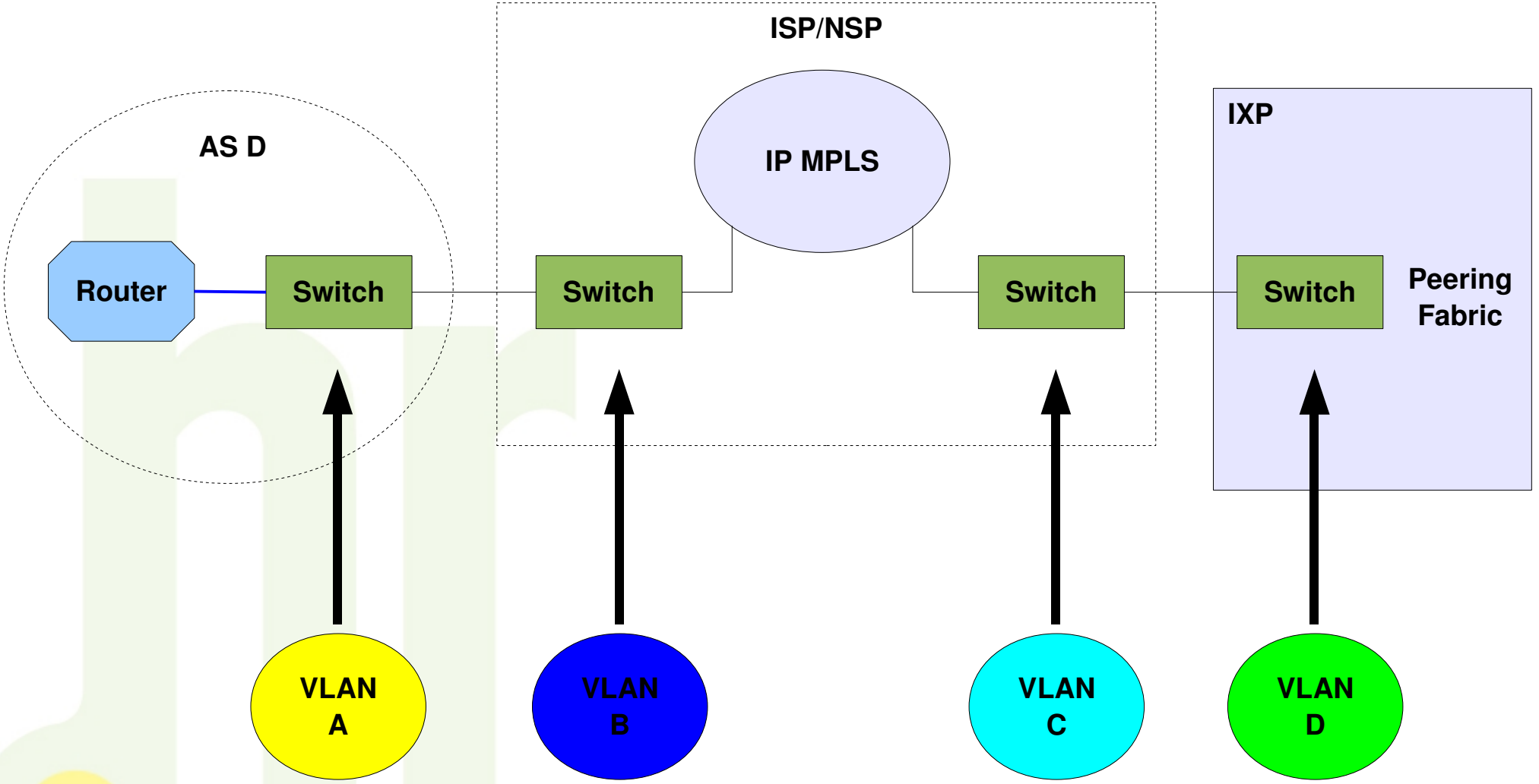


PTT – Links Ethernet – Problemas na Camada de Enlace (L2)

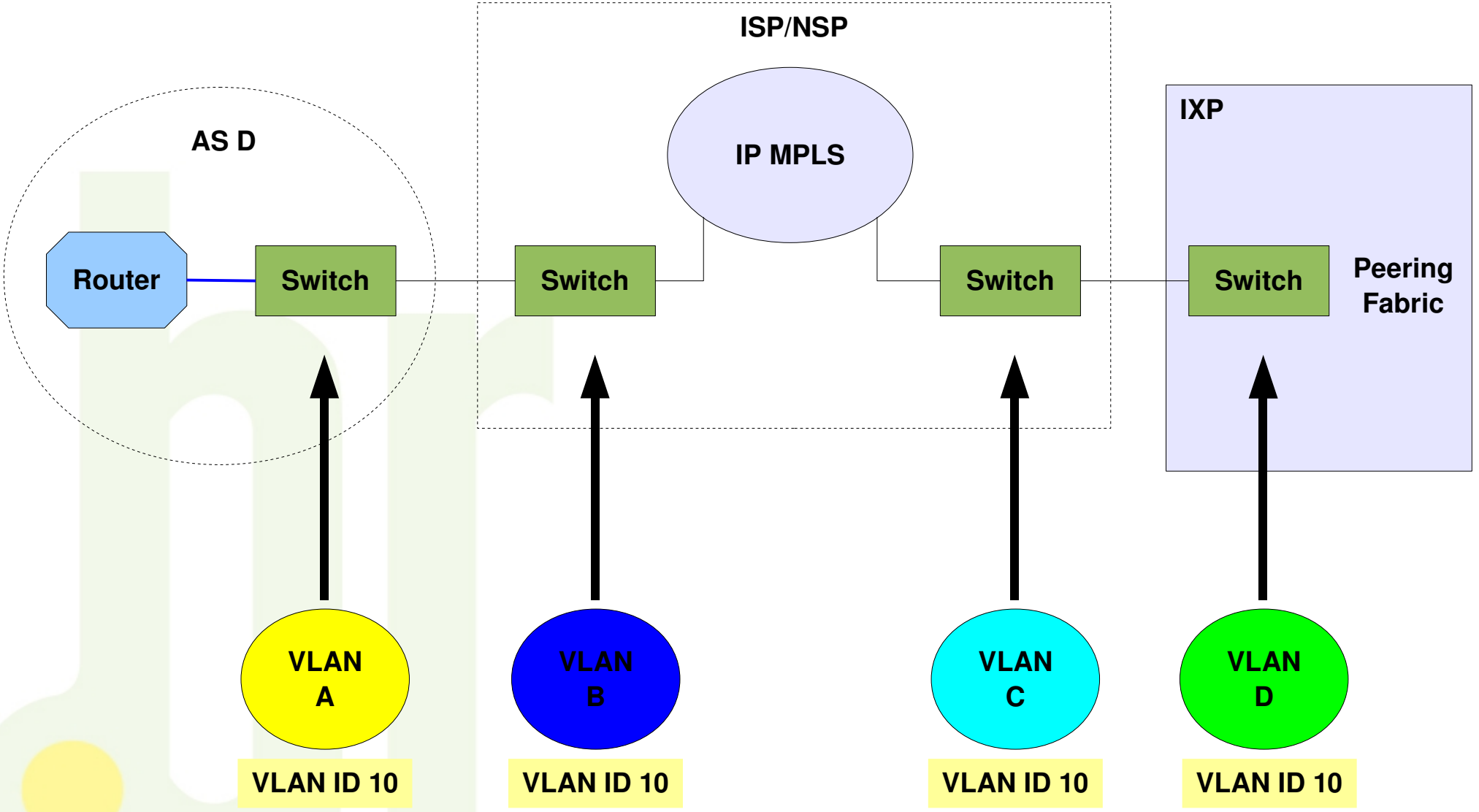
As redes Ethernet não foram originariamente concebidas para prevenir problemas Decorrentes da interconexão entre redes L2 sob administrações diferentes.

Recursos especiais podem ser necessários para conferir proteções e atualmente algumas soluções podem depender de funcionalidades proprietárias.

As VLANs conferem isolamento lógico em redes Ethernet

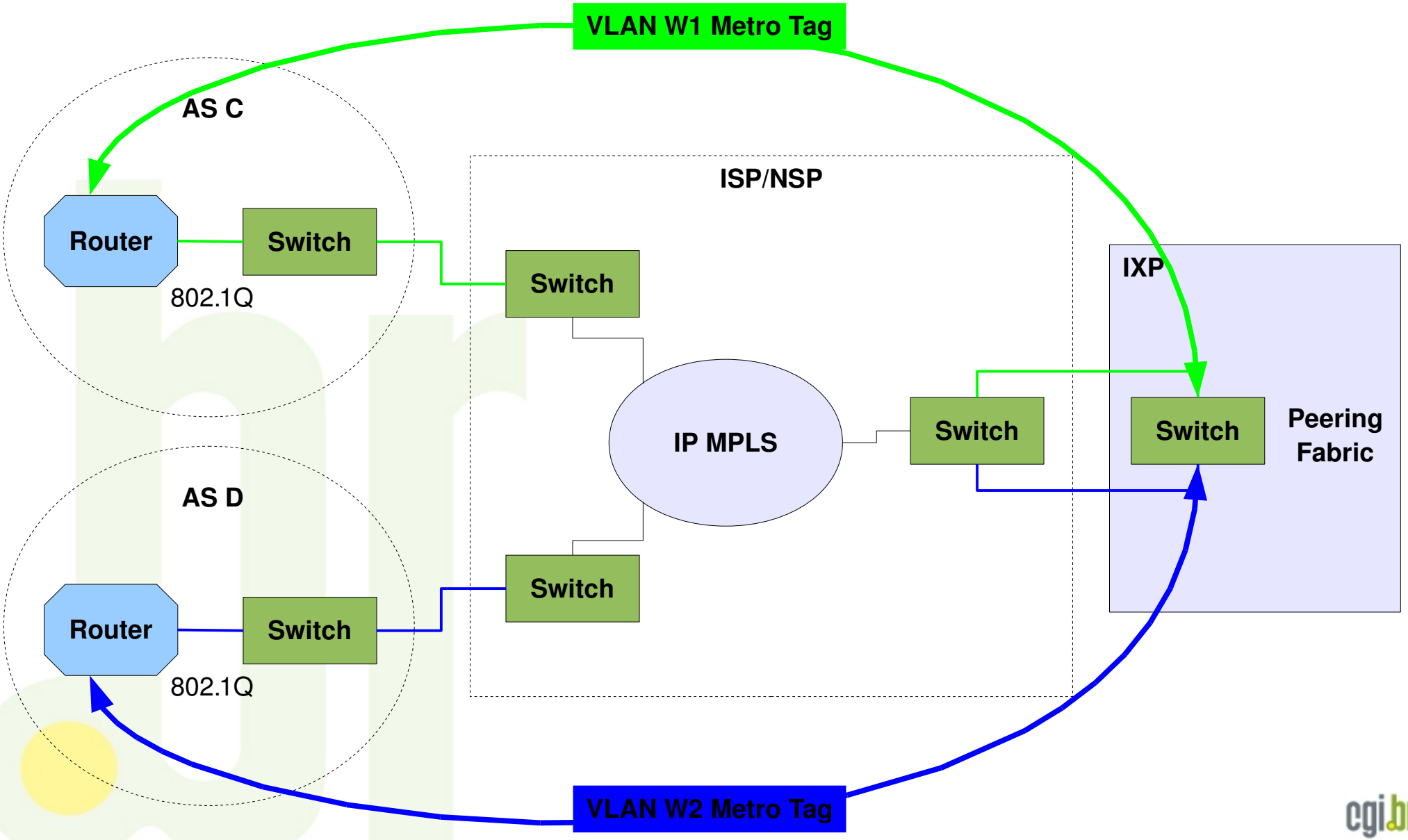


VLANs independentes e conectadas podem ter a mesma identificação (ID)

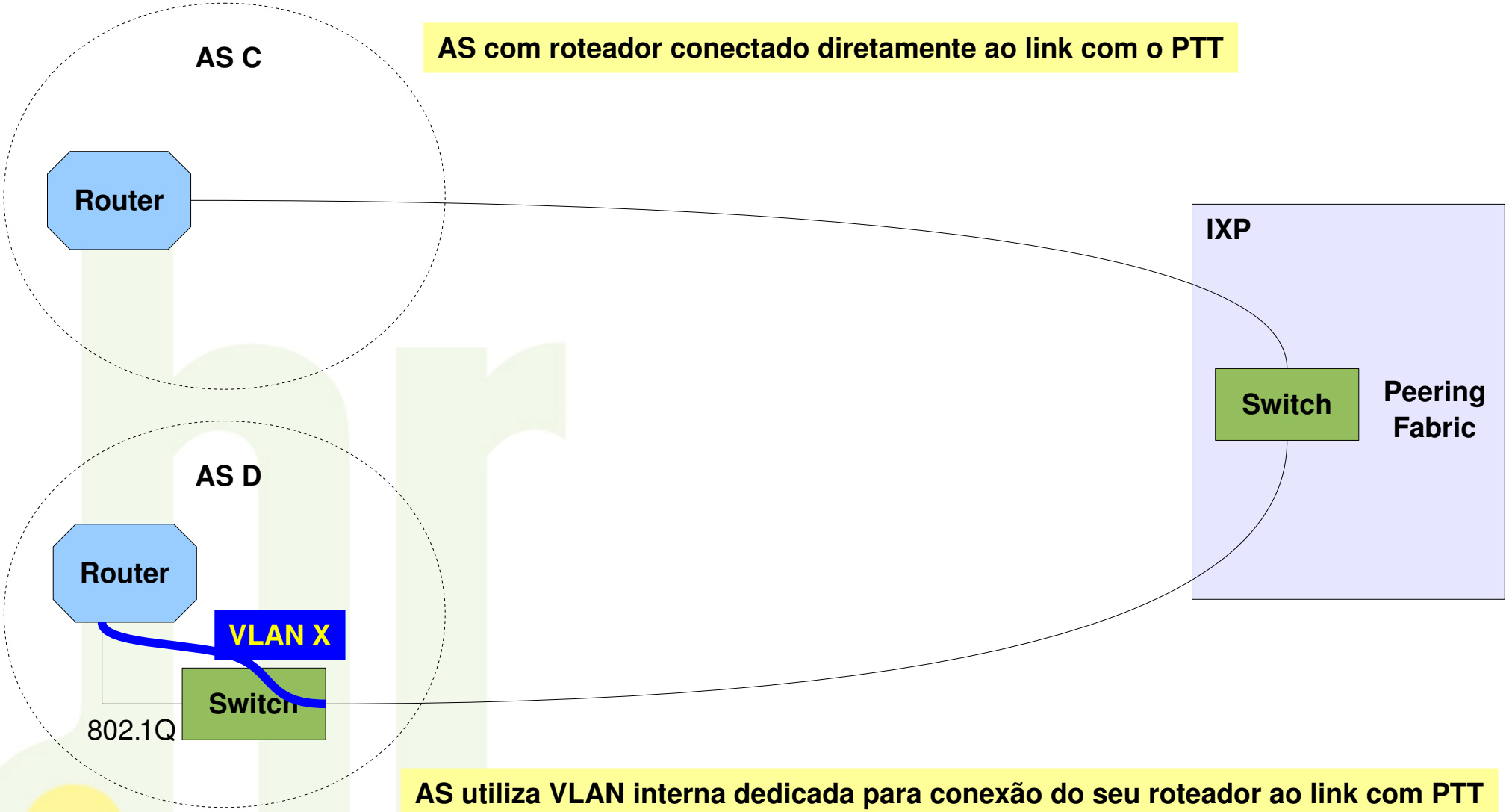


Conexões tipo trunk (802.1Q) entre diferentes domínios L2 podem exigir cuidados especiais.

Isolamento Lógico Ethernet no ISP/NSP - 802.1ad (QinQ)



PTT – Links Ethernet – Problemas na Camada de Enlace (L2)



Algumas Sugestões de Pontos de Proteções Ethernet

- Definição explícita do modo de operação de trunk (802.1Q) na interconexão de domínios L2
  (evitar a utilização de configuração automática ou dinâmica)

- Definição explícita das condições de controle de links agregados
  (LACP - 802.3ad)

- Utilização de filtros de entrada e saída para bloquear certos tipos de quadros Ethernet
  - Protocolos de descoberta de vizinhança (e.g. CDP, EDP, etc)
  - Protocolos de redundância L2 (e.g. STP, EAPS, REP, etc)
  - Broadcast diferentes de ARP

Operação Restritiva para Permissão de Quadros Ethernet

AS permite apenas determinados tipos de quadros, com Ethertypes específicos, na conexão com links para PTT:

- 0x0800 - IPv4
- 0x0806 - ARP
- 0x86dd - IPv6

Proteções Ethernet – Exemplos Switches Extreme Networks

Filtro de quadros STP

```
configure stpd <stpd_name> ports edge-safeguard enable <port_list>
```

Controle de broadcast por porta

```
configure ports <port_list> rate-limit flood [broadcast | multicast |
unknown-destmac] [no-limit | <pps>]
```

Exemplos de scripts de configuração e implementações reais.

http://www.extremenetworks.com/solutions/widget-central/?refID=3

Proteções Ethernet – Exemplos Switches Extreme Networks

```
ACL para filtrar quadros ethernet por ethertypes:

entry entry1 {
if {
ethernet-type <number> --> coloca o ethertype desejado
} then {
deny;
count contador;  --> coloca a ação desejada permit/deny ou algum action
}              modifier.
}

Exemplos de ethertype são:

ETHER-P-IP (0x0800), ETHER-P-8021Q (0x8100),
ETHER-P-IPV6 (0x86DD), ARP (0x806)
```

Proteções Ethernet – Exemplos Switches Cisco

```
!
interface aa/x/y
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/
    configuration/guide/layer2.html


!
Interface aa/x/y
Switchport port-security
Switchport port-security violation protect
Switchport port-security maximum z vlan w
Switchport port-security mac-address dddd.dddd.dddd vlan w
!

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/
    configuration/guide/port_sec.html
```

Proteções Ethernet – Exemplos Switches Cisco

```
! Port ACLs (PACLs):
!
Mac access-list extended BLOCK-L2-FRAMES
Deny any 0180.c200.0000 0000.0011.1111
Permit any any 0x0800
Permit any any 0x0806
Permit any any 0x86dd
!
Interface aa/x/y
Mac Access-group BLOCK-L2-FRAMES in
!


http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/
    configuration/guide/vacl.html
```

Proteções Ethernet – Exemplos Switches Foundry

Habilitar BPDU Guard

```
NetIron(config) interface ethe 2/1
NetIron(config-if-e1000-2/1)# spanning-tree protect
```

Habilitar Root Guard

```
NetIron(config)# interface ethernet 5/5
NetIron(config-if-e10000-5/5) spanning-tree root-protect
```

Proteções Ethernet – Exemplos Switches Foundry

Exemplo de Configuração de Layer 2 ACL com filtros de Ethertype

```
NetIron(config)# access-list 400 permit any any any etype ipv4
NetIron(config)# access-list 400 permit any any any etype arp
NetIron(config)# access-list 400 permit any any any etype ipv6
NetIron(config)# access-list 400 deny any any 100
```

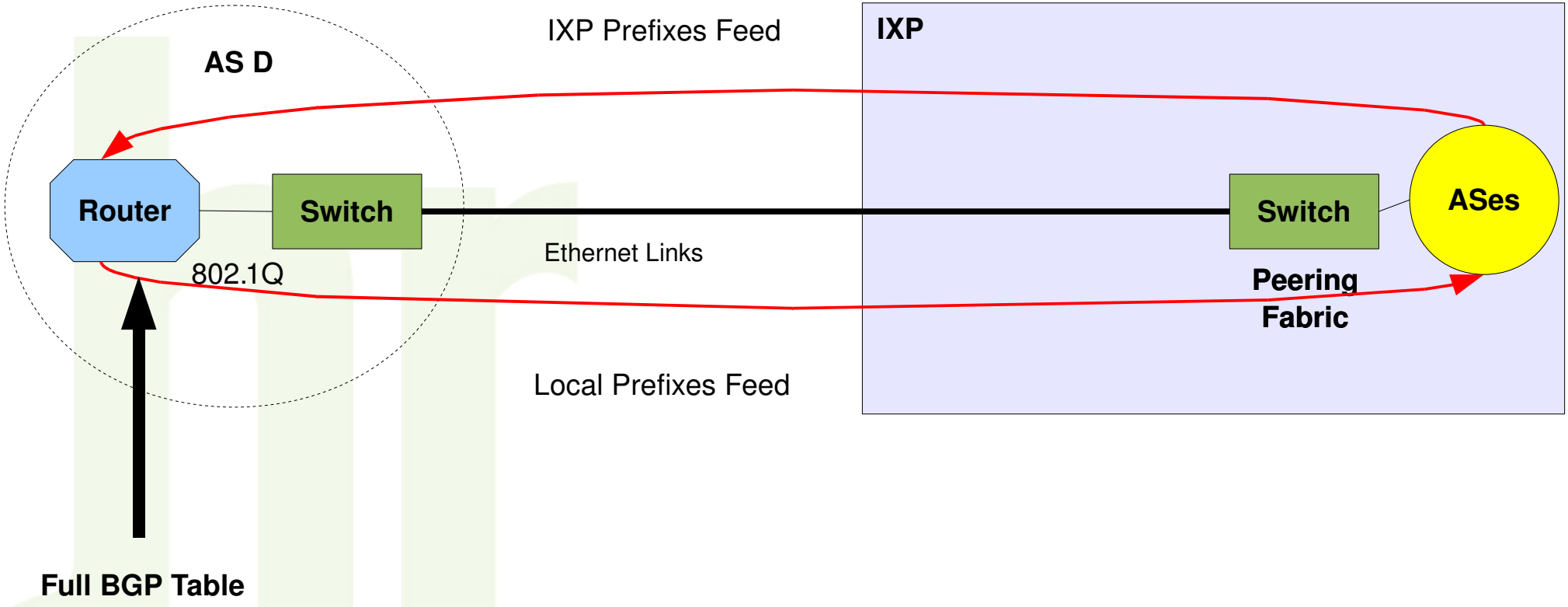
Proteções Ethernet – Exemplos Switches Juniper

Port Security Overview
http://www.juniper.net/techpubs/en_US/junos9.5/information-products/pathway-pages/ex-series/port-security.html

802.1X Overview
http://www.juniper.net/techpubs/en_US/junos9.5/information-products/pathway-pages/ex-series/access-control.html

Rate Limiting Overview
http://www.juniper.net/techpubs/en_US/junos9.5/information-products/pathway-pages/ex-series/device-security.html

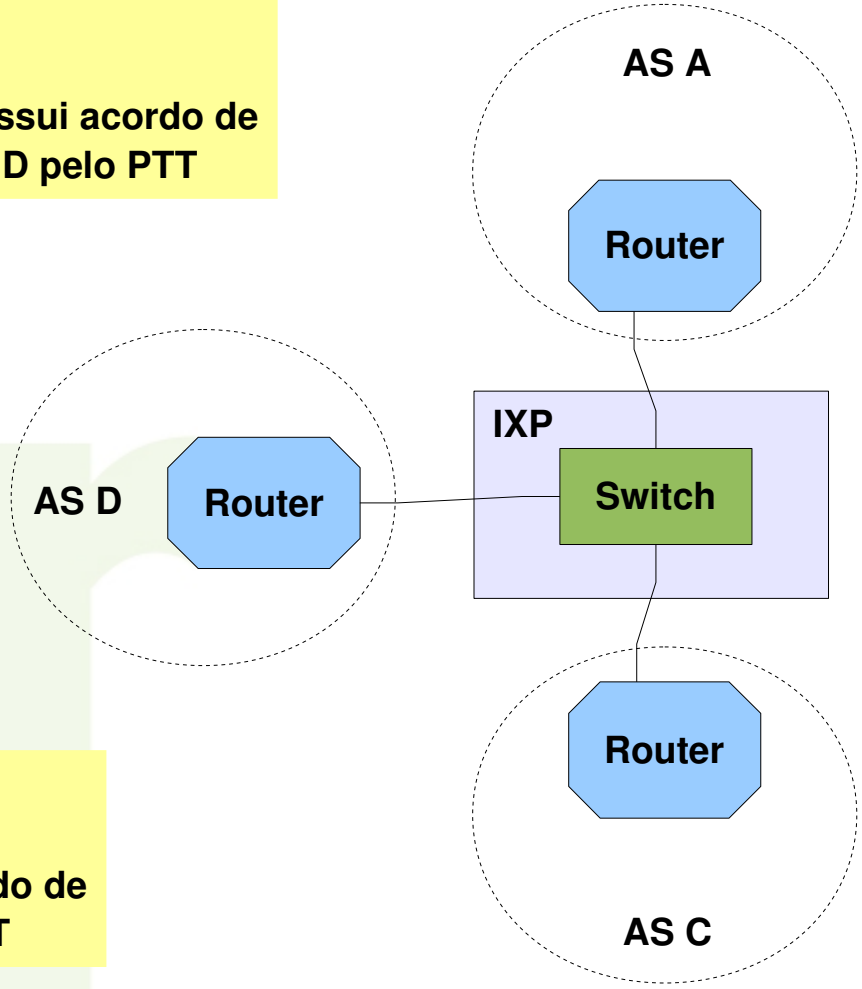
✗ **Perda de isolamento das tabelas BGP (PTT e Global) dentro do AS**



PTT – Links Ethernet – Problemas na Camada de Rede (L3)

Situação 1

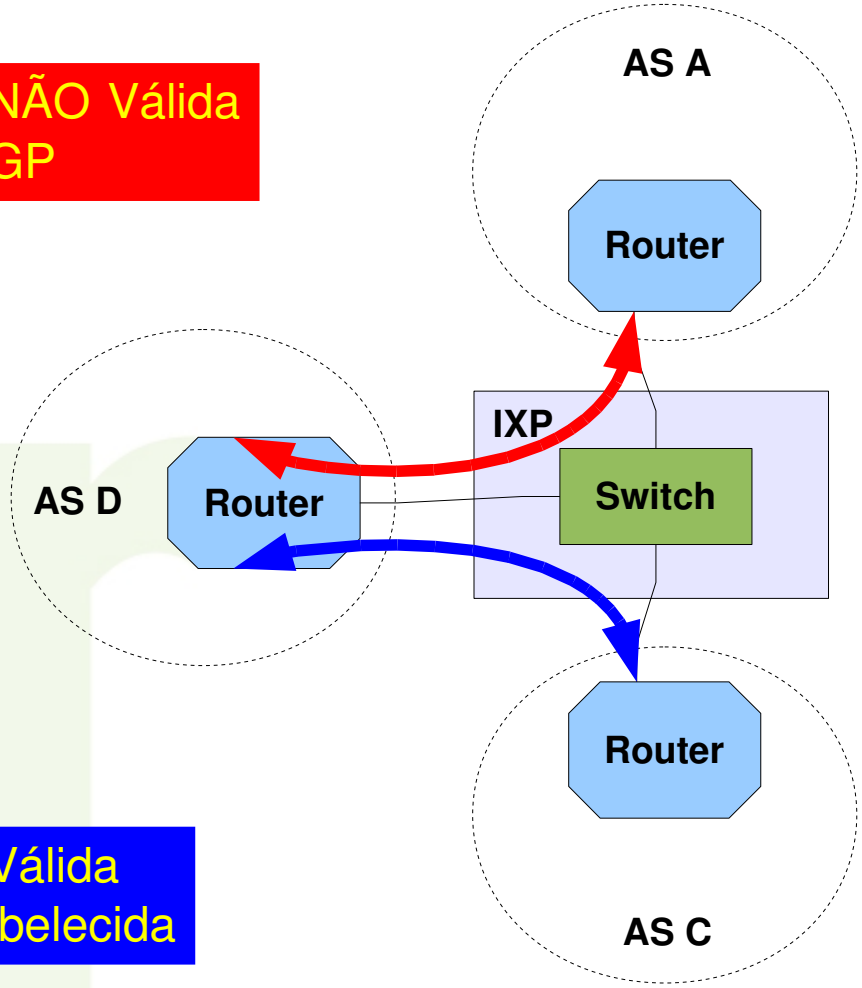
- **AS A gostaria, mas NÃO possui acordo de troca de tráfego com AS D pelo PTT**



Situação 2

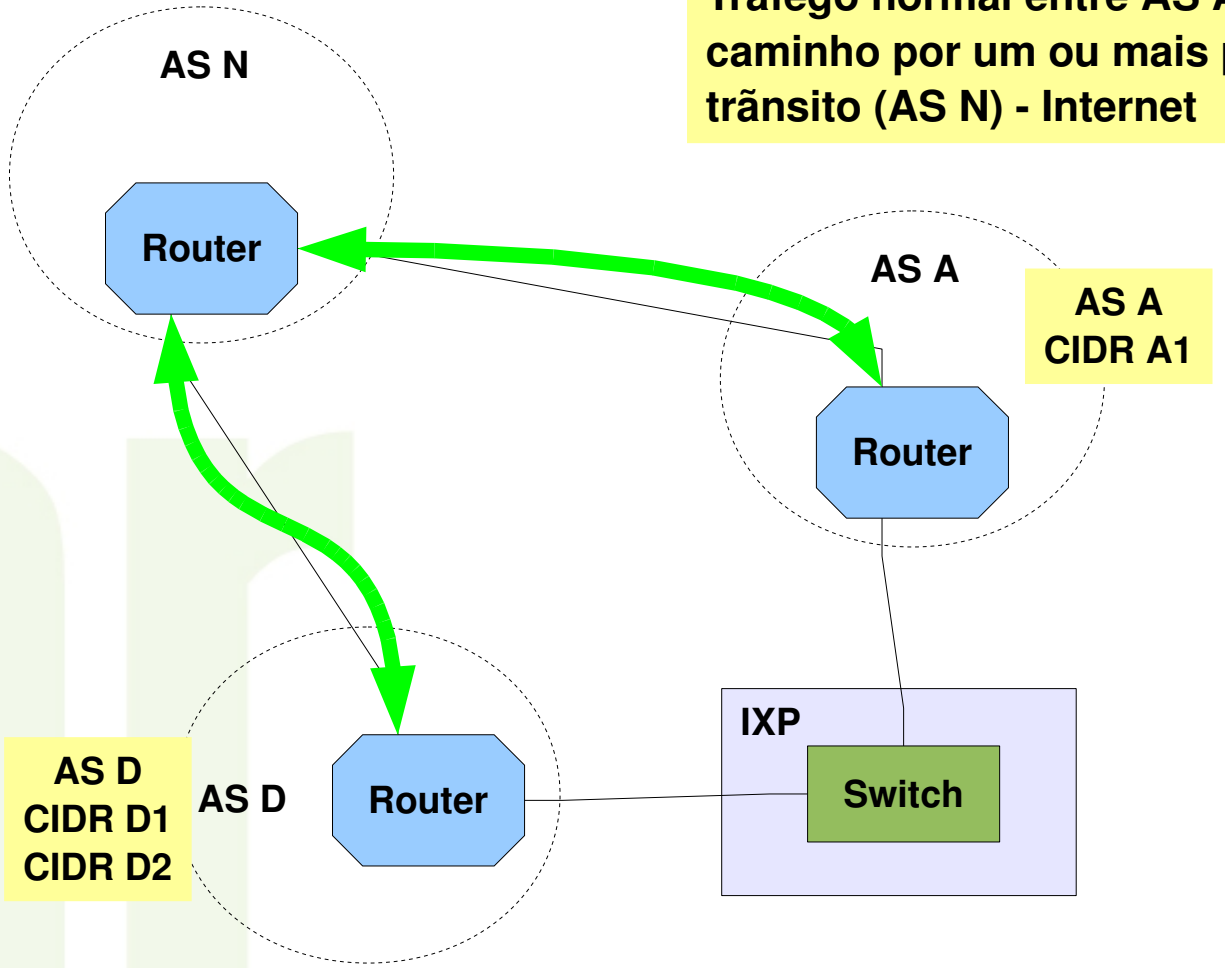
- **AS D e AS C possuem acordo de troca de tráfego pelo PTT**

Troca de Tráfego NÃO Válida
Não há Sessão BGP

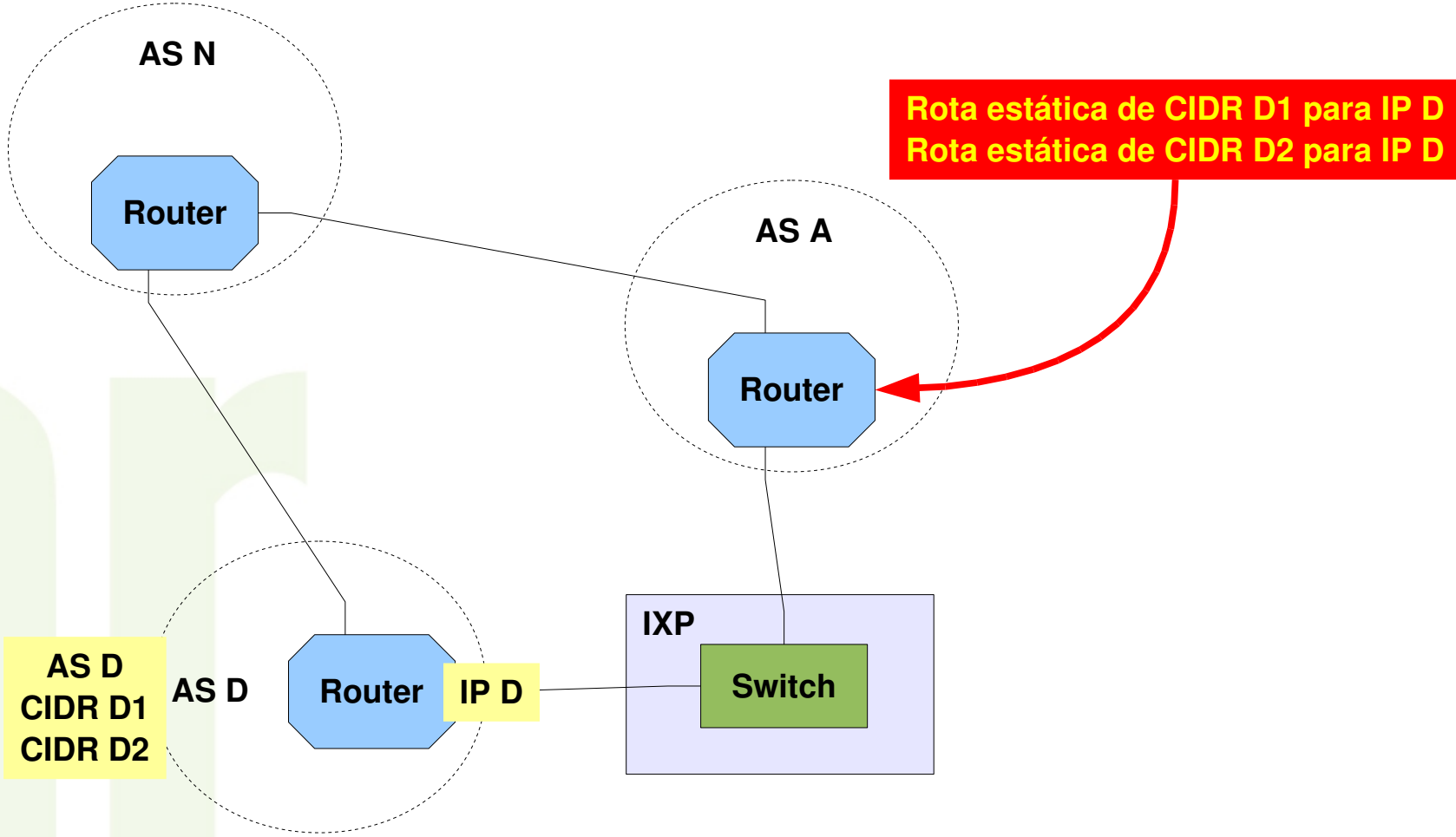


Troca de Tráfego Válida
Sessão BGP Estabelecida

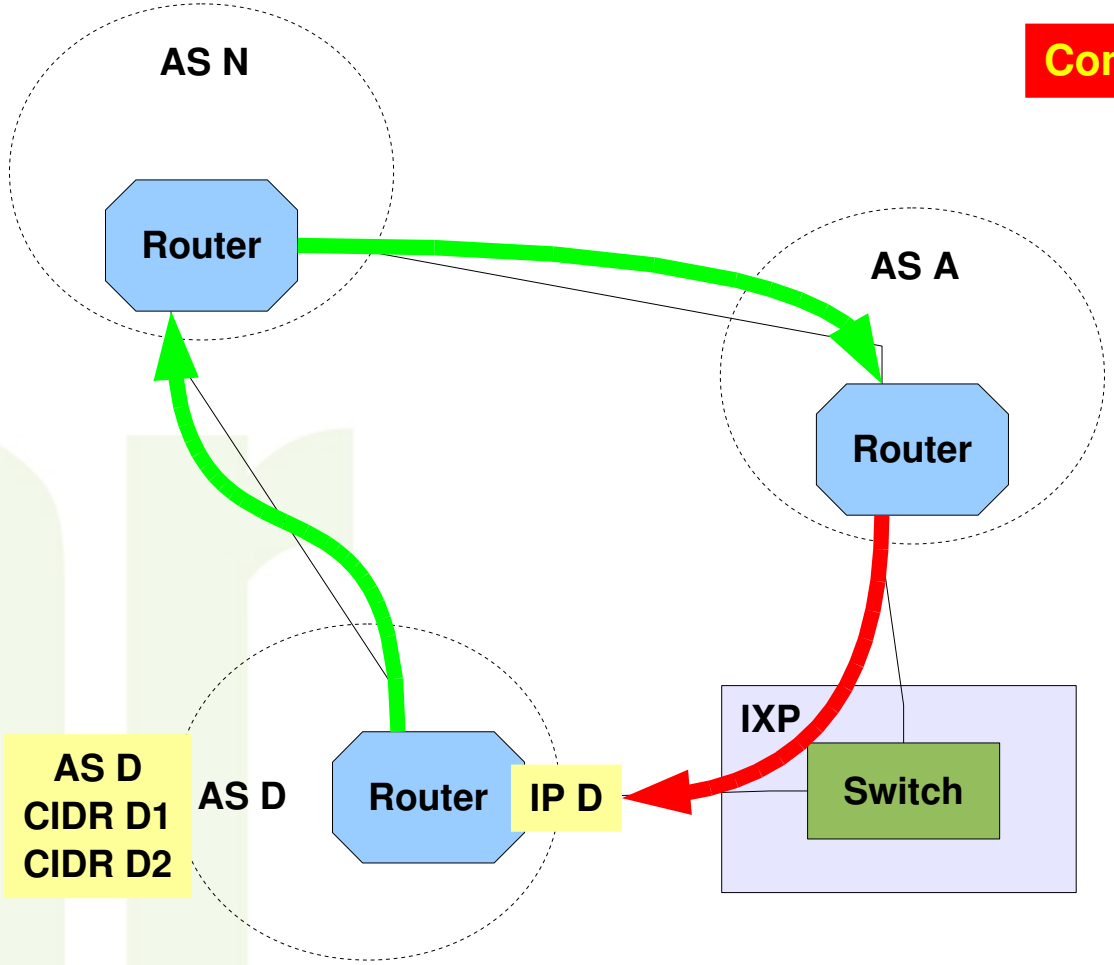
Tráfego normal entre AS A e AS D utiliza caminho por um ou mais provedores de trãnsito (AS N) - Internet



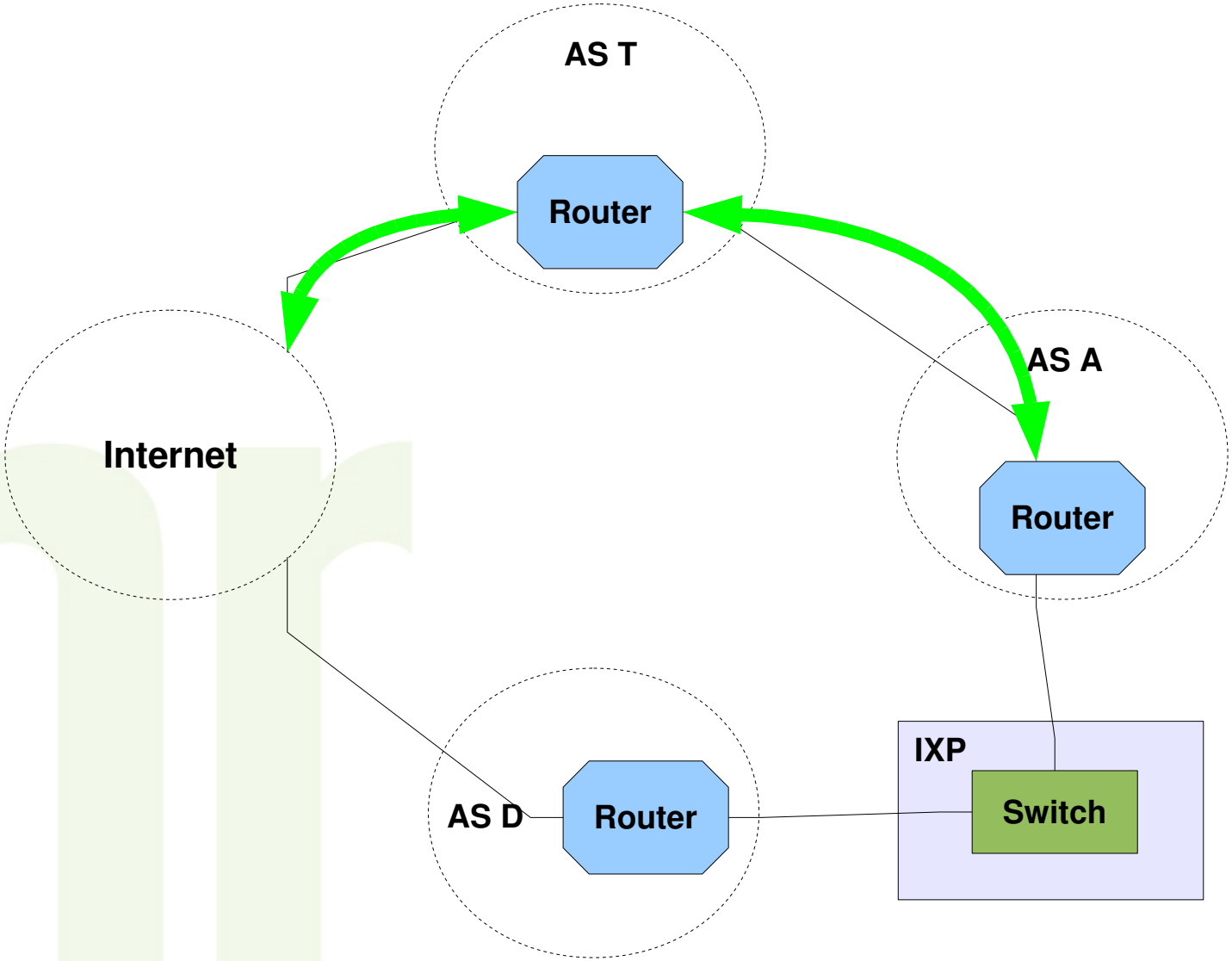
PTT – Links Ethernet – Problemas na Camada de Rede (L3)



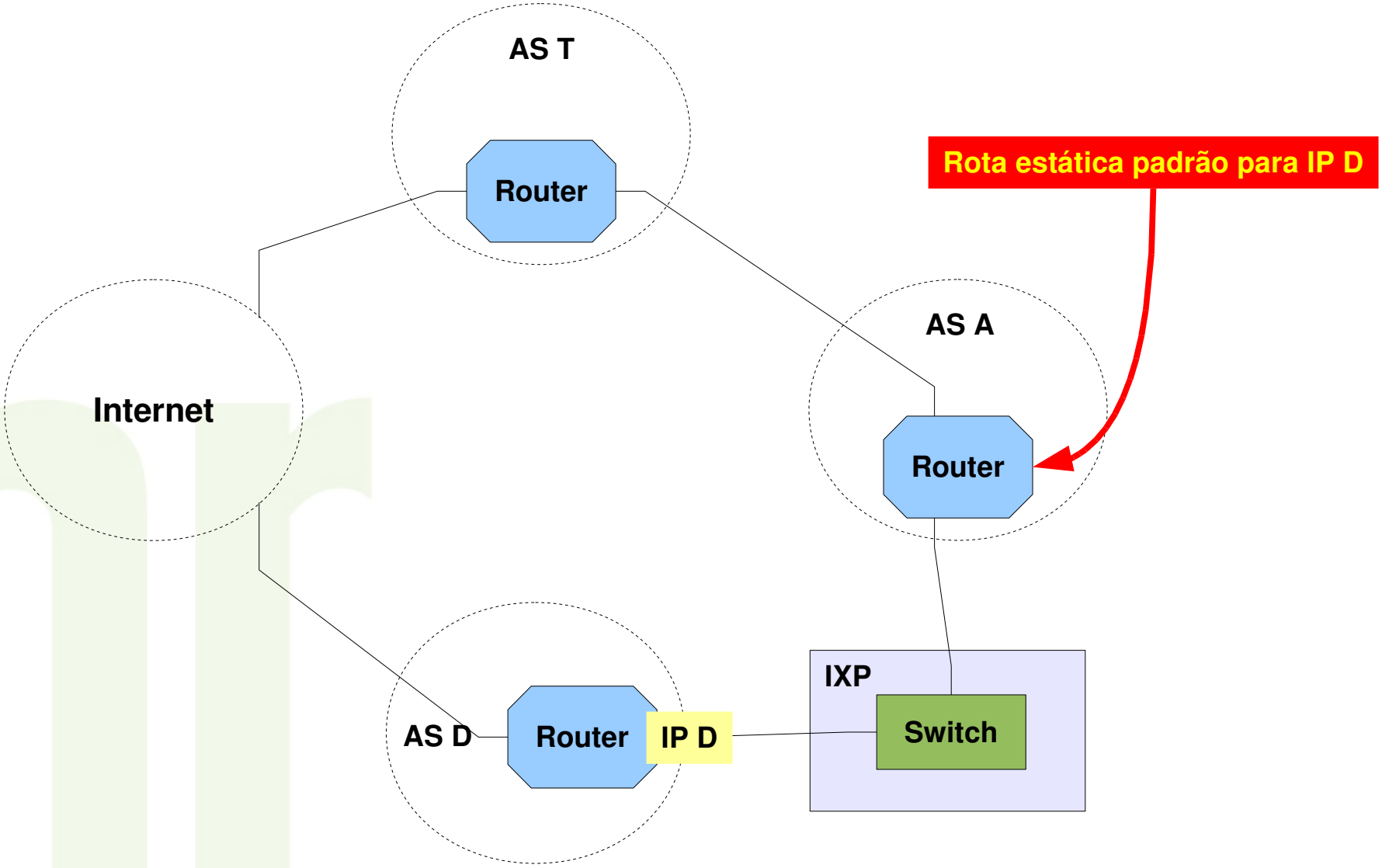
PTT – Links Ethernet – Problemas na Camada de Rede (L3)



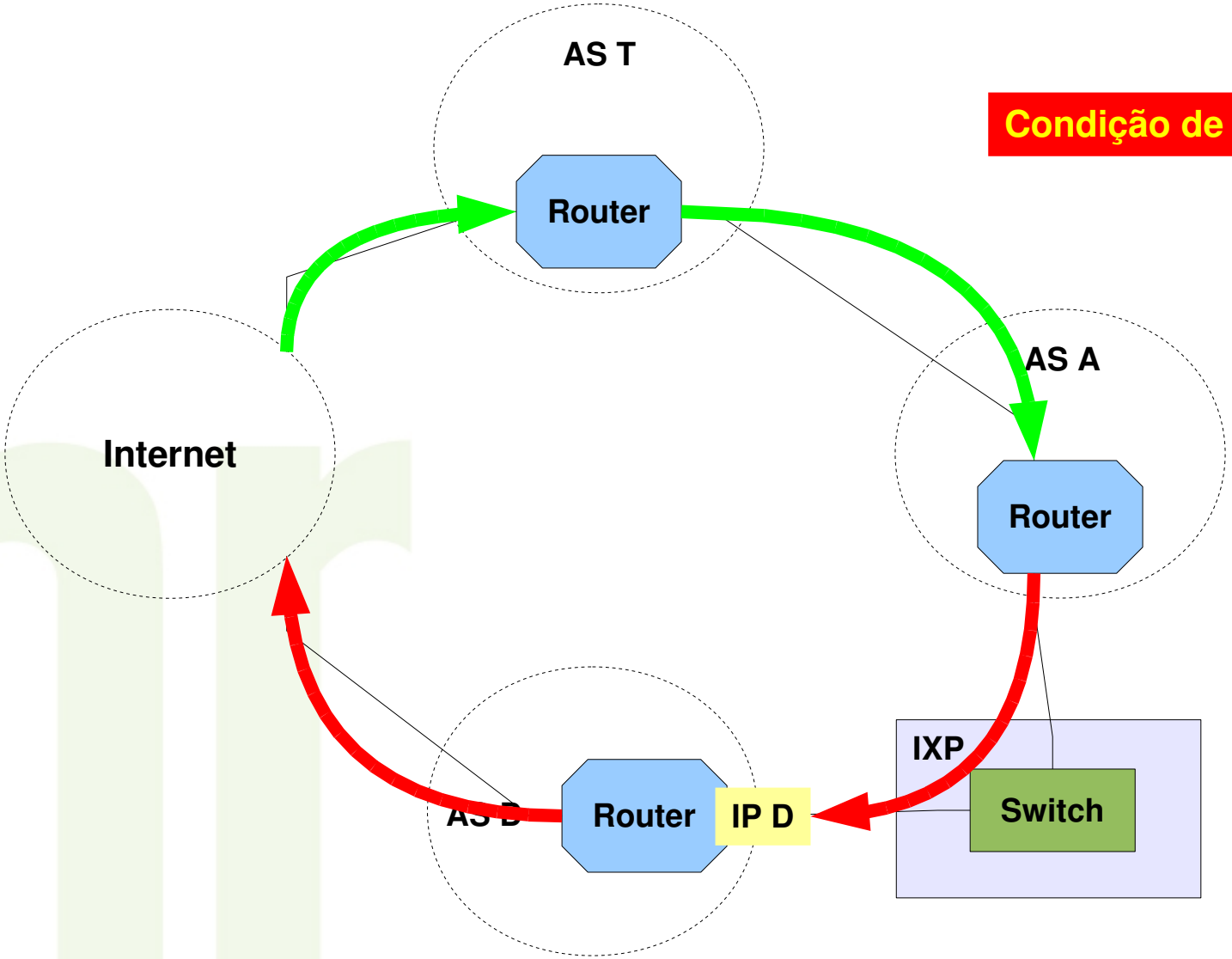
PTT – Links Ethernet – Problemas na Camada de Rede (L3)



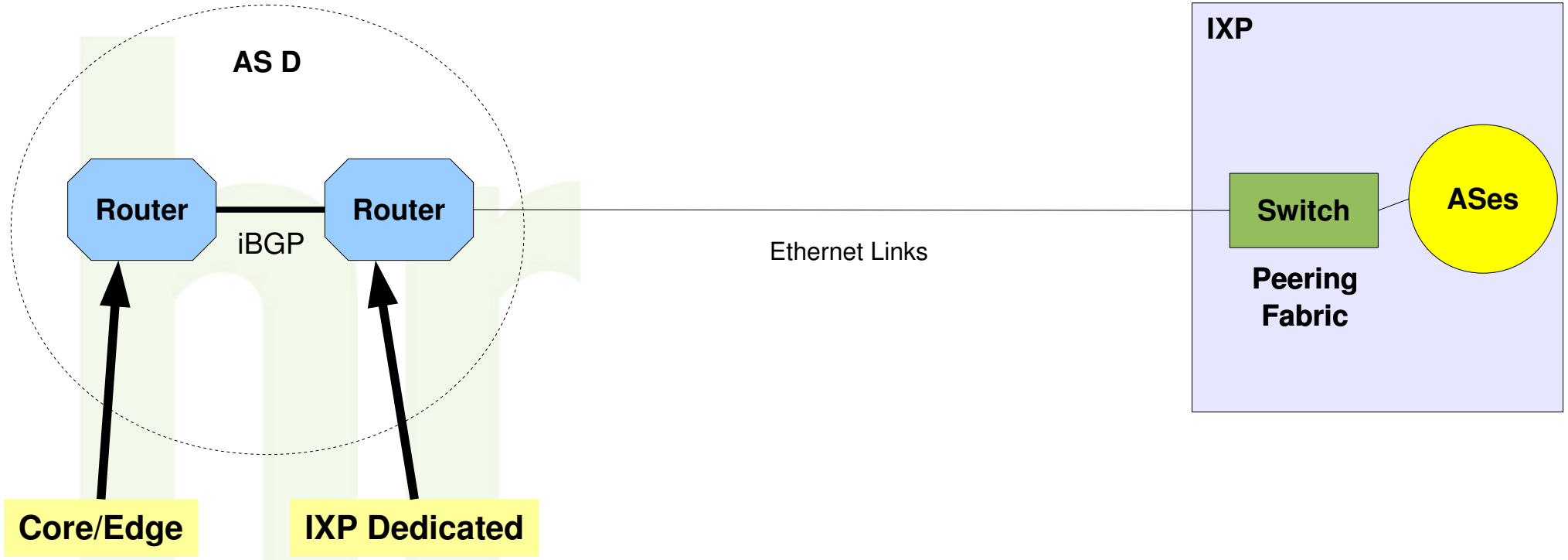
PTT – Links Ethernet – Problemas na Camada de Rede (L3)



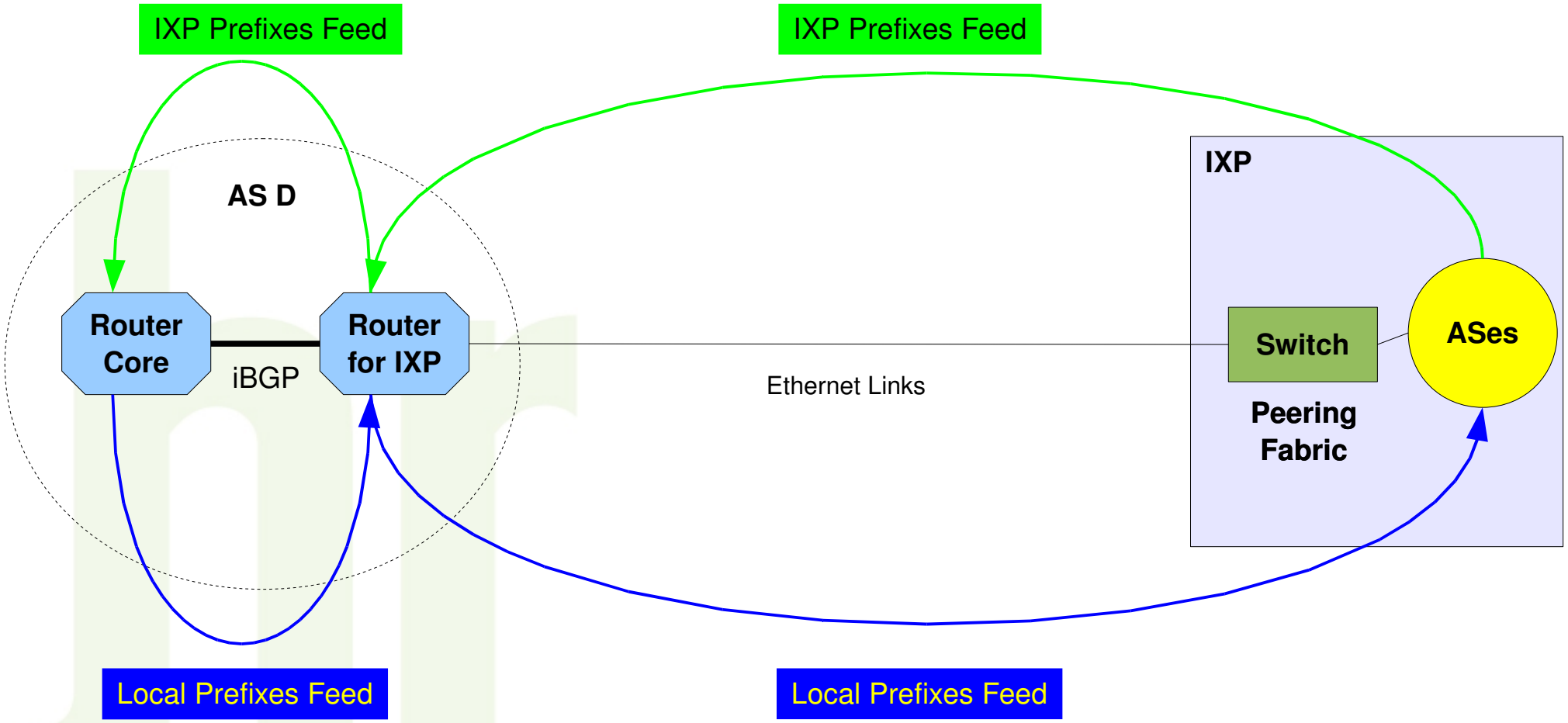
PTT – Links Ethernet – Problemas na Camada de Rede (L3)



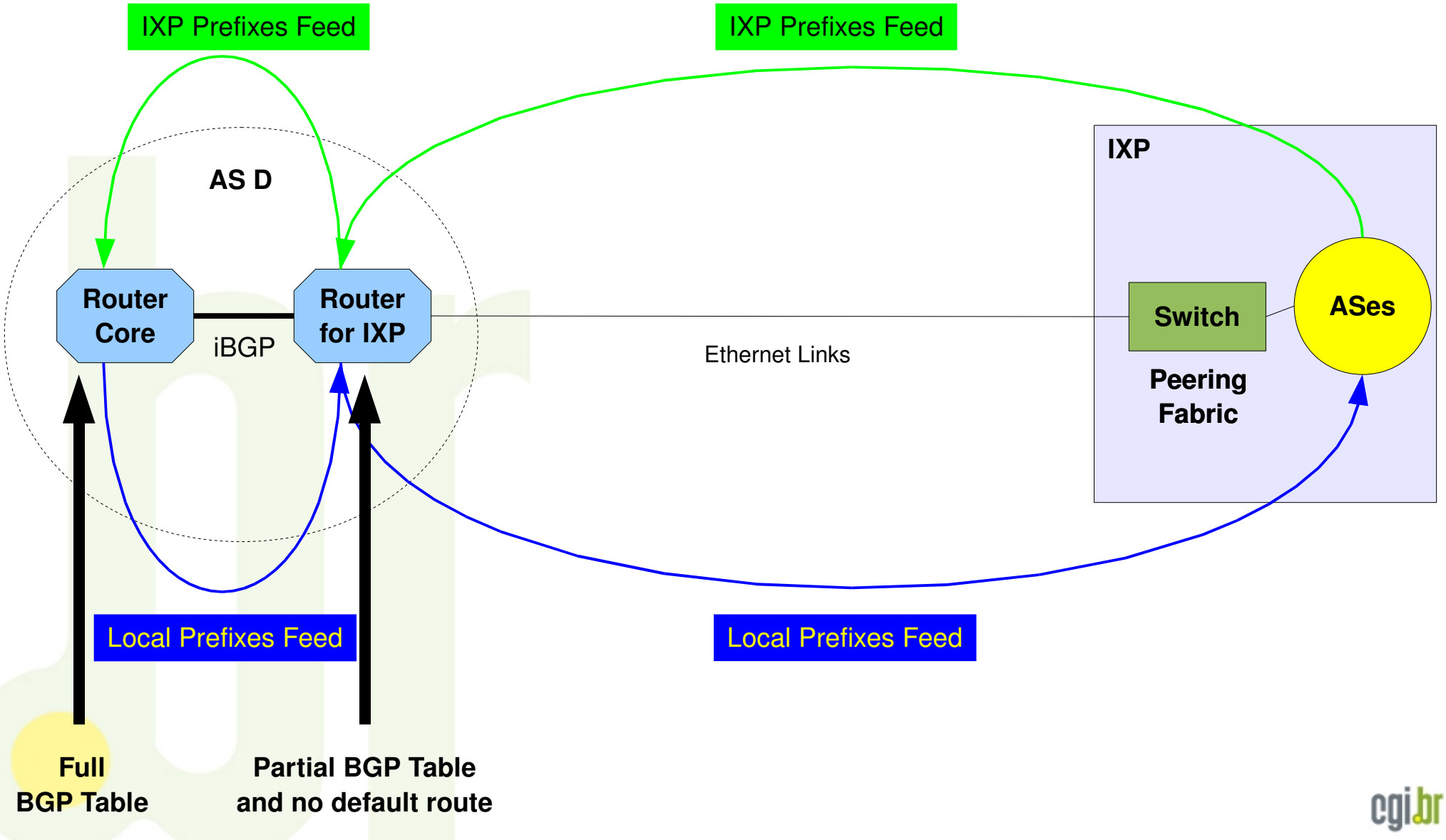
Exemplo de Solução



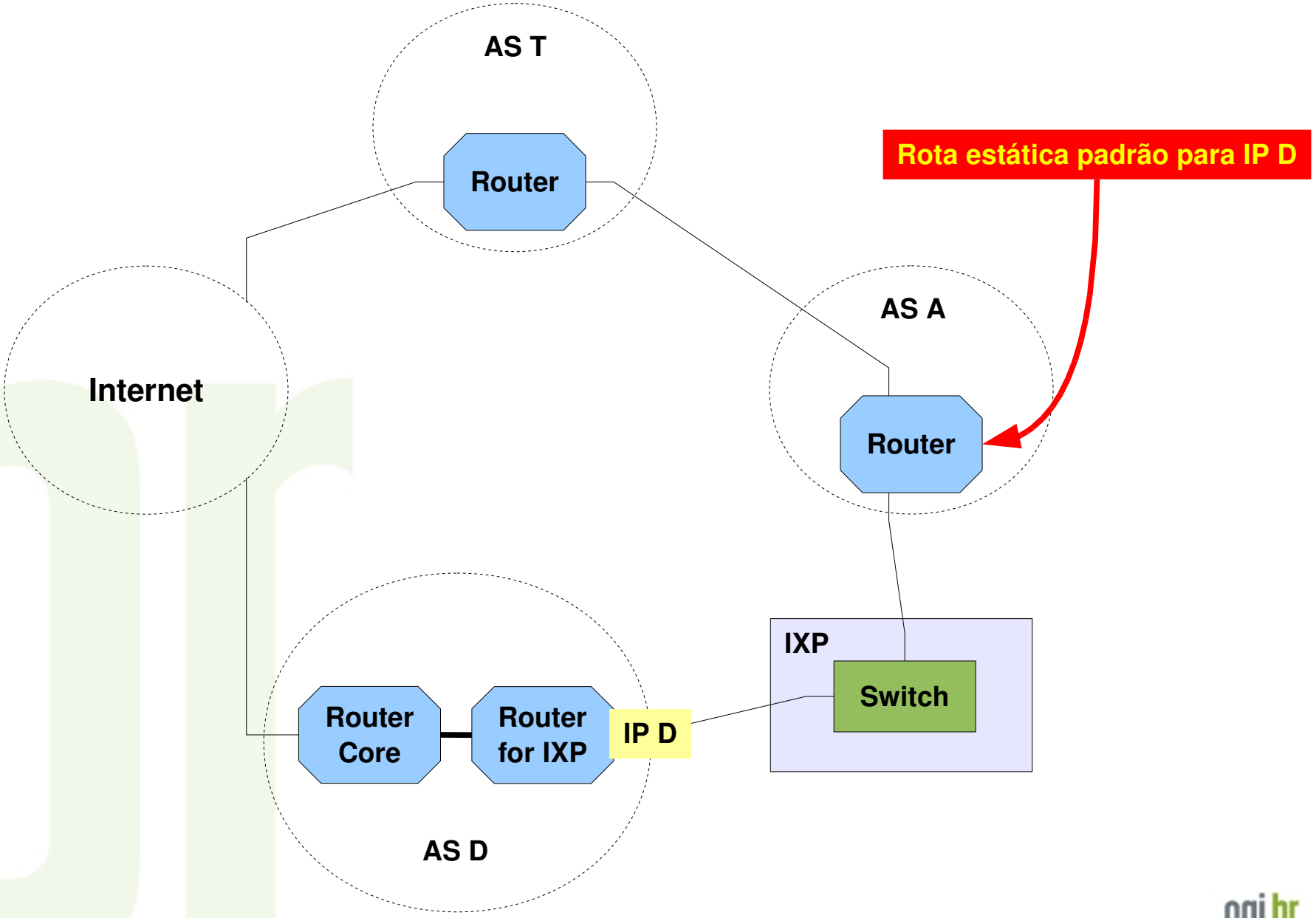
Exemplo de Solução



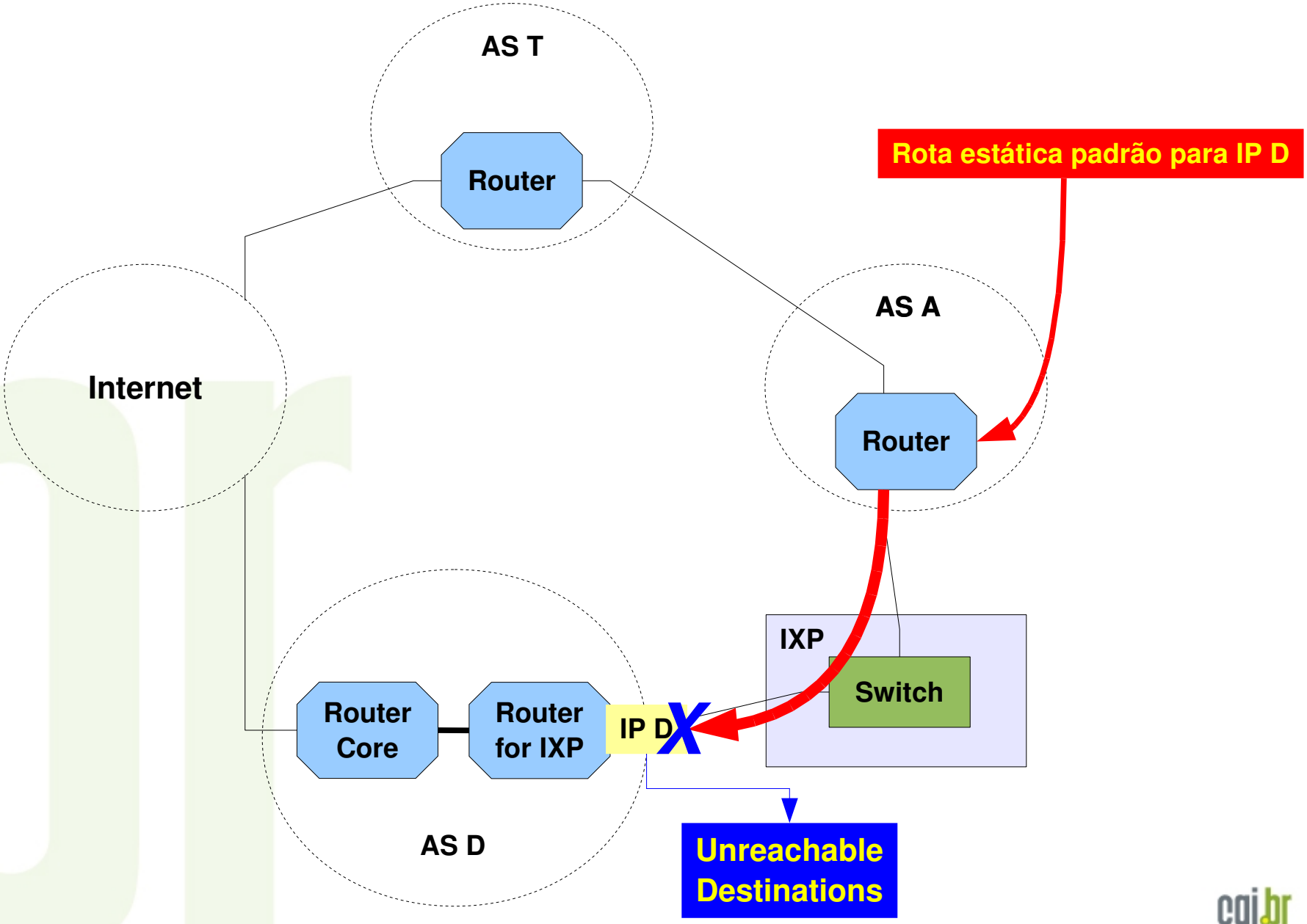
Exemplo de Solução



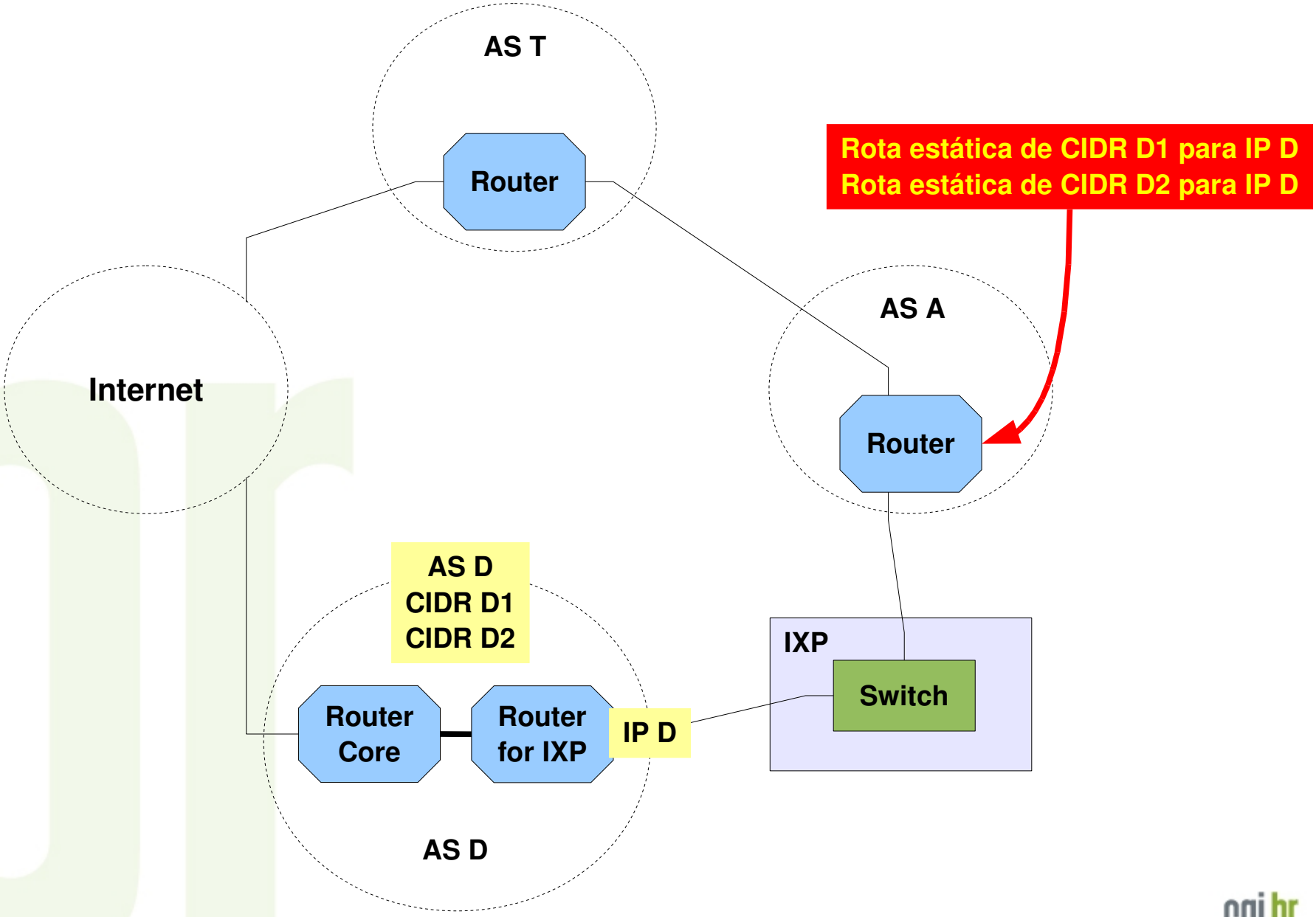
Exemplo de Solução



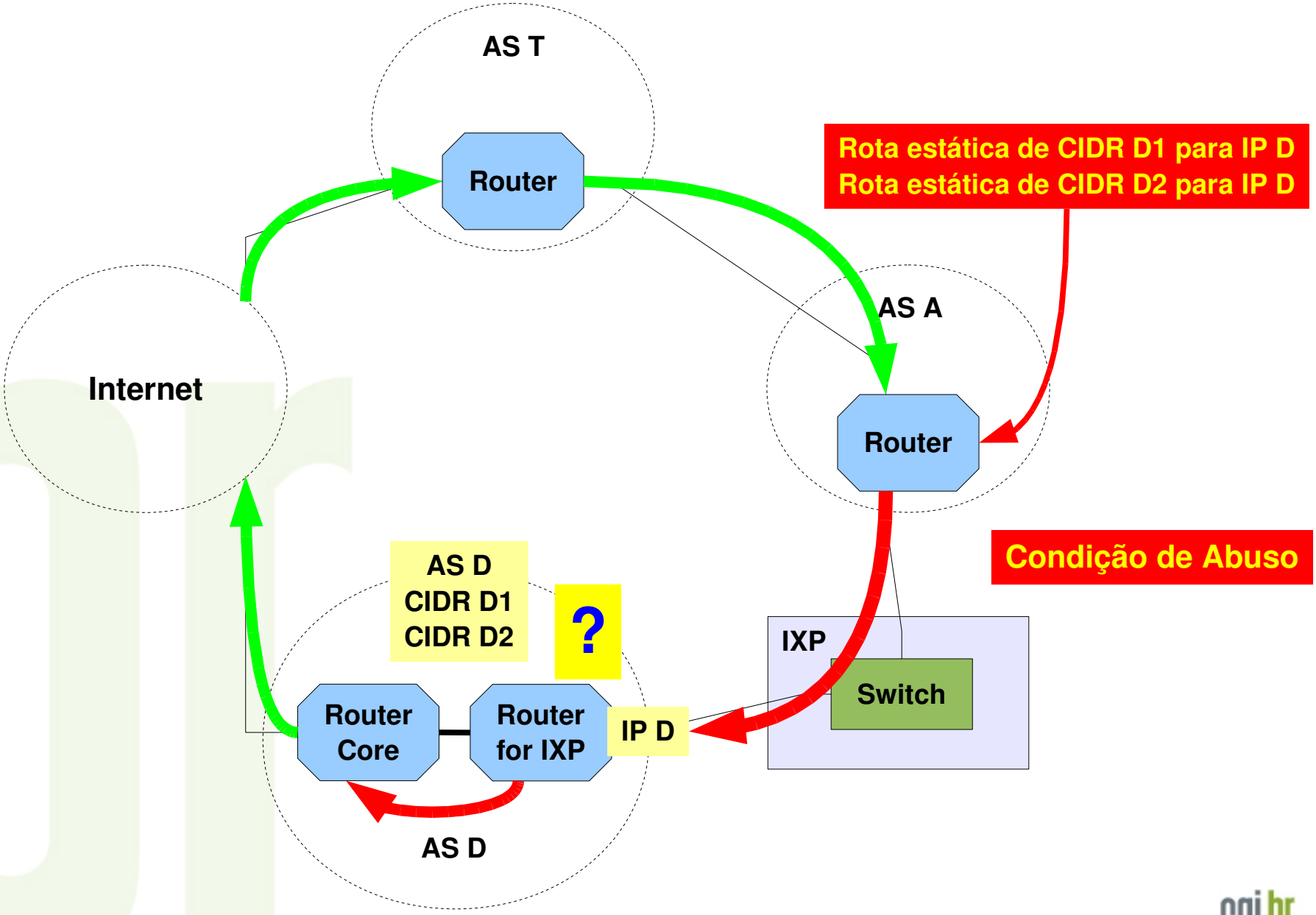
Exemplo de Solução



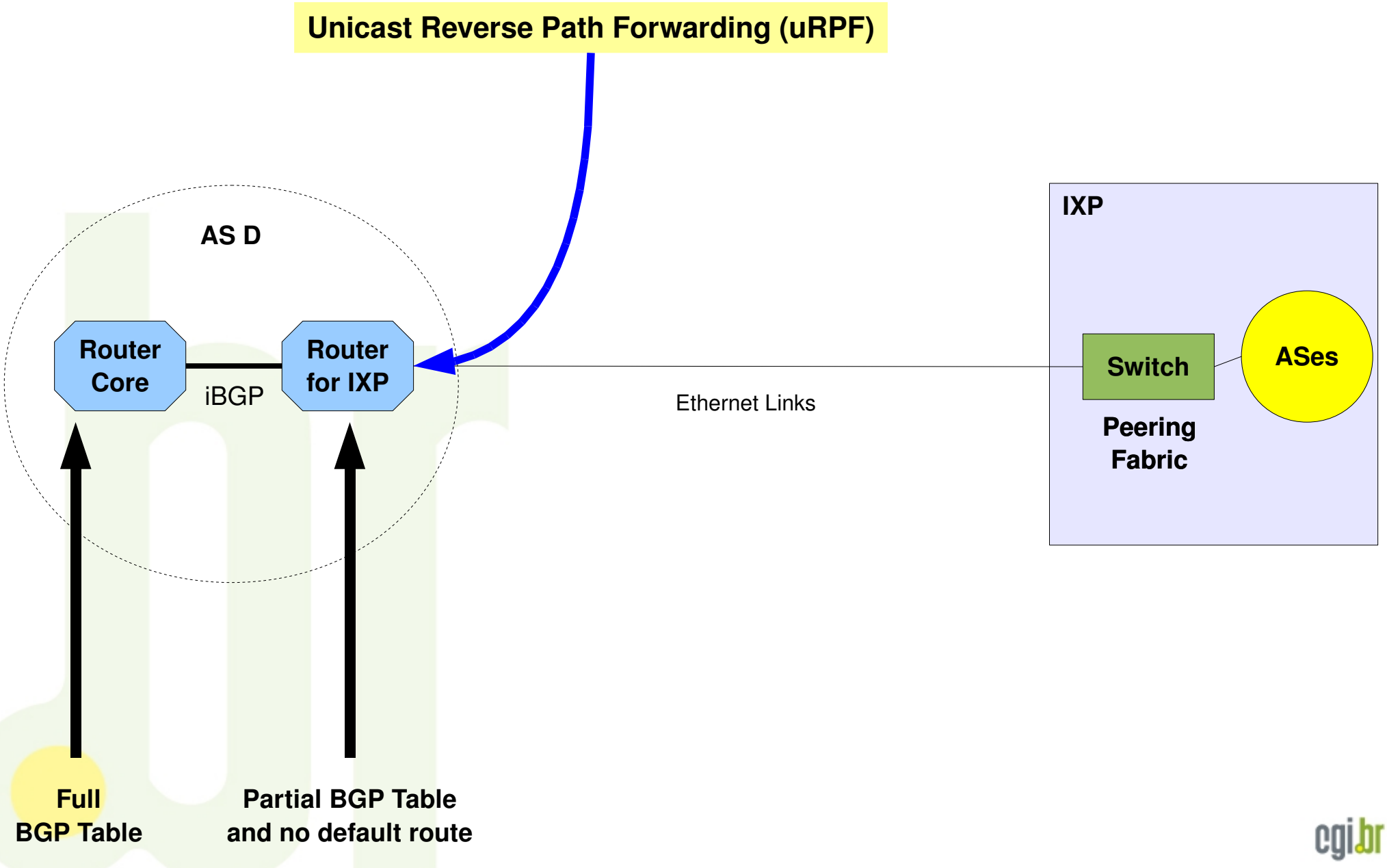
Exemplo de Solução



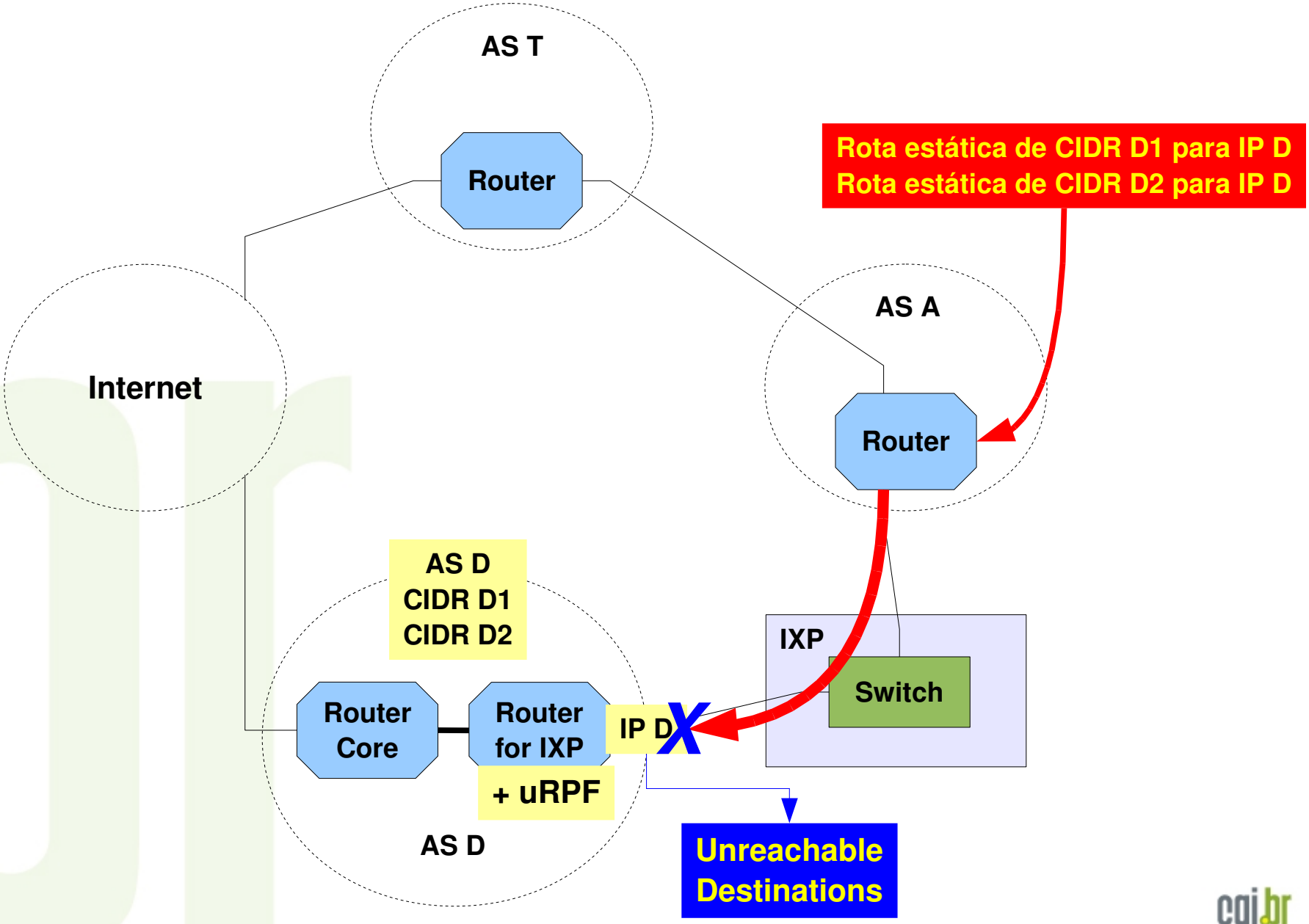
Exemplo de Solução



Exemplo de Solução



Exemplo de Solução



Unicast Reverse Path Forwarding

RFC3704 - Ingress Filtering for Multihomed Networks
BCP: 84
http://www.ietf.org/rfc/rfc3704.txt

RFC2827 - Network Ingress Filtering: Defeating Denial of Service Attacks
which employ IP Source Address Spoofing
BCP: 38
http://www.ietf.org/rfc/rfc2827.txt

uRPF - Exemplo Cisco

```
interface FastEthernet 0/0
ip verify unicast source reachable-via
       {rx | any} [allow-default] [allow-self-ping] [list]
ipv6 verify unicast source reachable-via
       {rx | any} [allow-default] [allow-self-ping] [access-list-name]

Understanding Unicast Reverse Path Forwarding
http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html

Unicast RPF for IPv6 on the Cisco 12000 Series
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/urpf_gsr.html

Service Provider Security Best Practices
http://www.cisco.com/security/sp
```

uRPF - Exemplo Juniper

```
You must enable unicast RPF check on an interface.
To do so, include the rpf-check statement:

rpf-check <fail-filter filter-name>;

You can include this statement at the following hierarchy levels:

[edit interfaces interface-name unit logical-unit-number
    family (inet | inet6)]
[edit logical-systems logical-system-name interfaces interface-name
    unit logical-unit-number family (inet | inet6)]

For more information about configuring unicast RPF on an interface,
see the JUNOS Network Interfaces Configuration Guide.

Configuring Unicast Reverse-Path-Forwarding Check
http://www.juniper.net/techpubs/software/junos/junos95/
    swconfig-routing/id-10460803.html#id-10460803
```

uRPF - Exemplo BSD

The uRPF check can be performed on packets by using the urpf-failed keyword in filter rules:

```
block in quick from urpf-failed label uRPF
```

Note that the uRPF check only makes sense in an environment where routing is symmetric.

OpenBSD - PF: Packet Filtering
Unicast Reverse Path Forwarding
http://www.openbsd.org/faq/pf/filter.html#urpf

BSD PF IPv6 and IPv4 /etc/pf.conf Firewall Script
http://bash.cyberciti.biz/firewall/
pf-ipv6-ipv4-firewall-for-freebsd-openbsd-netbsd/

uRPF - Exemplo Linux

Reverse Path Filter (rp_filter)

```
# sysctl -w net.ipv4.conf.ifname.rp_filter=1

# echo 1 > /proc/sys/net/ipv4/conf/<ifname>/rp_filter
```

[PATCH] RP filter support for IPv6, kernel 2.6.15
http://linux.derkeiler.com/pdf/Mailing-Lists/Kernel/2006-01/msg05334.pdf

Agradecimentos

Alexandre Ribeiro - Foundry / Blackit

Caio Klein – Juniper Networks

Igor Giangrossi - Cisco Systems

Leonardo Sambrana / Marcelo Pizzotti Maldi - Extreme Networks

Obrigado

Eduardo Ascenço Reis
<eascenco@nic.br>
<eduardo@intron.com.br>

nic.br ceptro.br ptt.br

cgi.br