

Some Considerations About IXP Customers Connection Models

LACNIC XII – NAPLA - Panama

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

2009-05-26

- Summary
- Preliminary Information
- IXP Traditional Connection Model
- IXP New Connection Model – Ethernet Family Links
 - Advantages
 - Some Negative Results
- IXP Ethernet Links
 - L2 Problem
 - L3 Problem

With the proliferation adoption of Metro Ethernet Networks to provide L2 links between Autonomous Systems (AS) and Internet eXchange Points (IXP) comes many benefits, like: connection simplification, uniform and familiar technology (Ethernet family), lower costs, less points of failures, etc.

On the other hand, directly connect Ethernet family links can expose the AS to vulnerabilities issues on security and network areas.

This presentation intends to focus the discussion on some network potential vulnerabilities and suggestions about how to protect the AS, looking forward a safe network.

The key points that will be addressed in the presentation are: routing vulnerabilities on external traffic engineering and Ethernet (L2) isolation/protection.

IXP - Internet eXchange Point

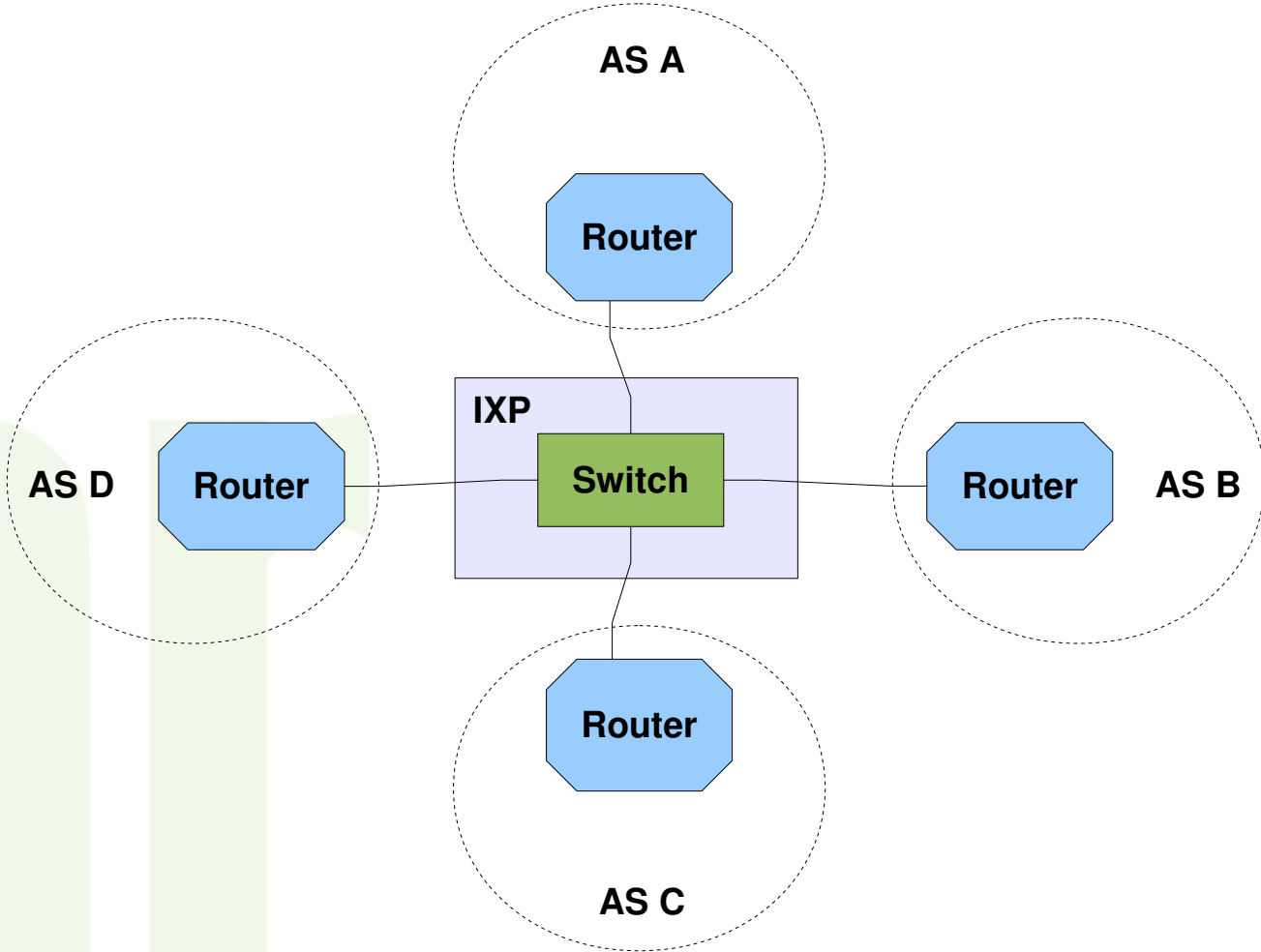
PTT – Ponto de Troca de Tráfego

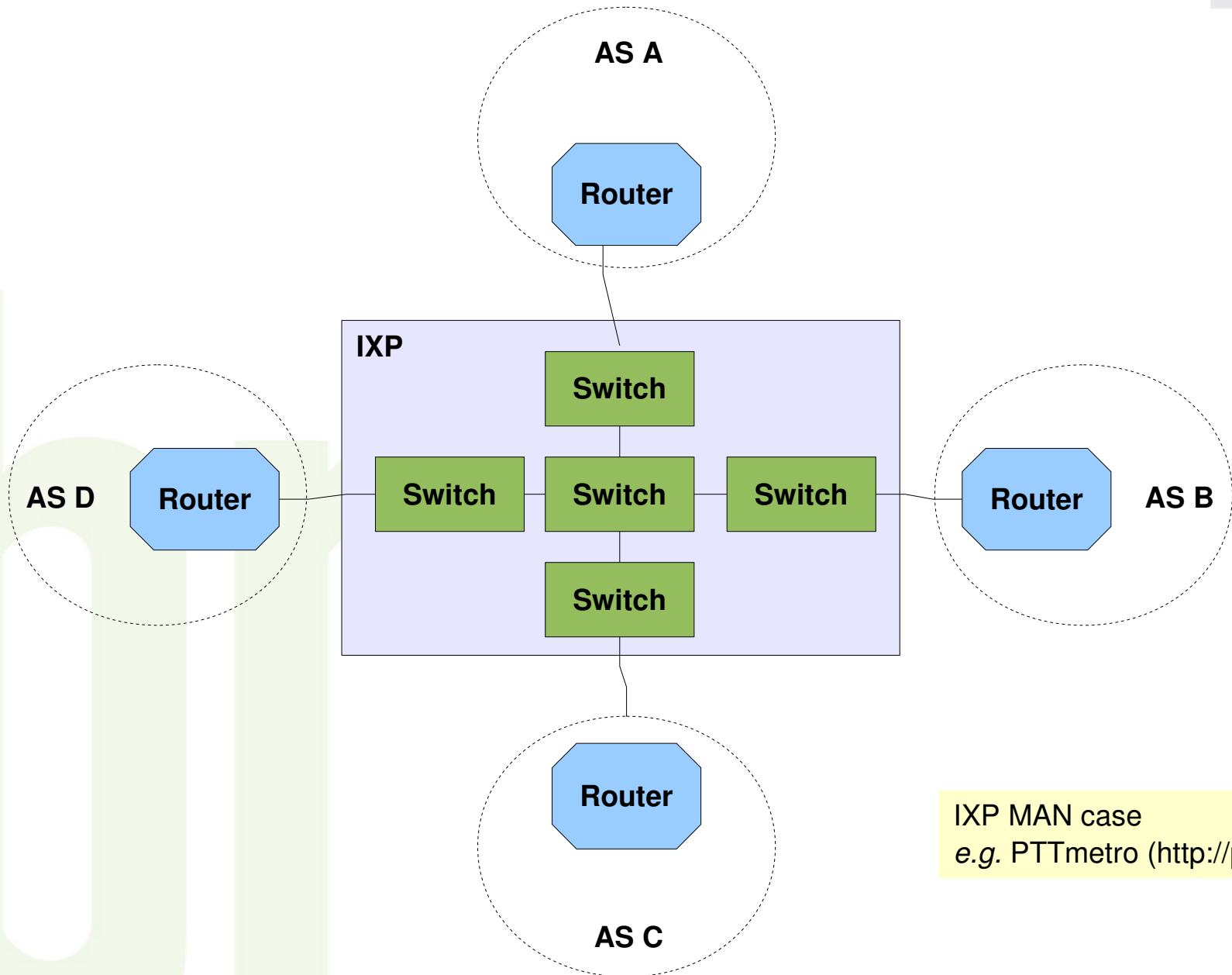
This presentation is focused on IXP participants and not on the IXP itself.

IXP - switching fabric / peering fabric

Traditionally based on exchange matrix Ethernet family equipments (switches)

IXP model can be simplified as a single LAN switch

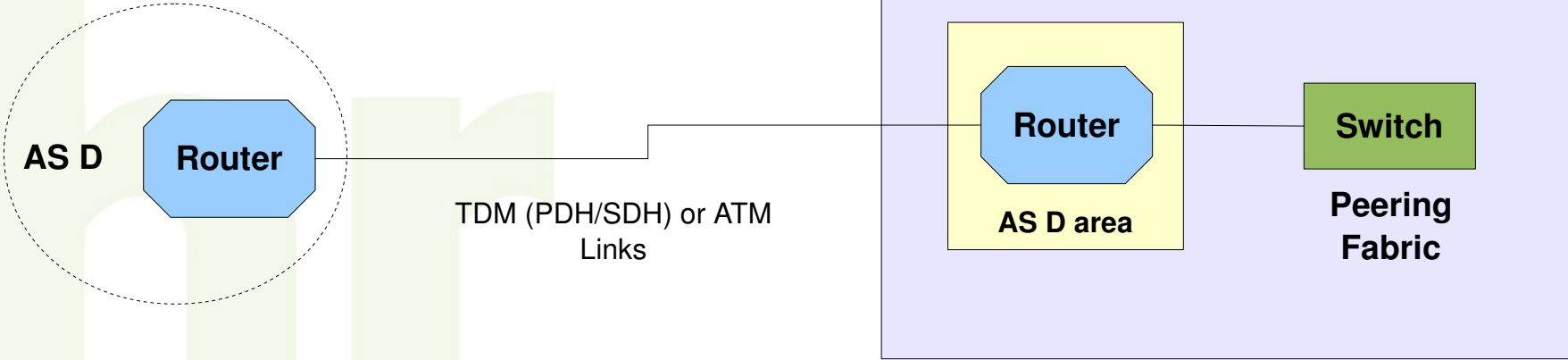


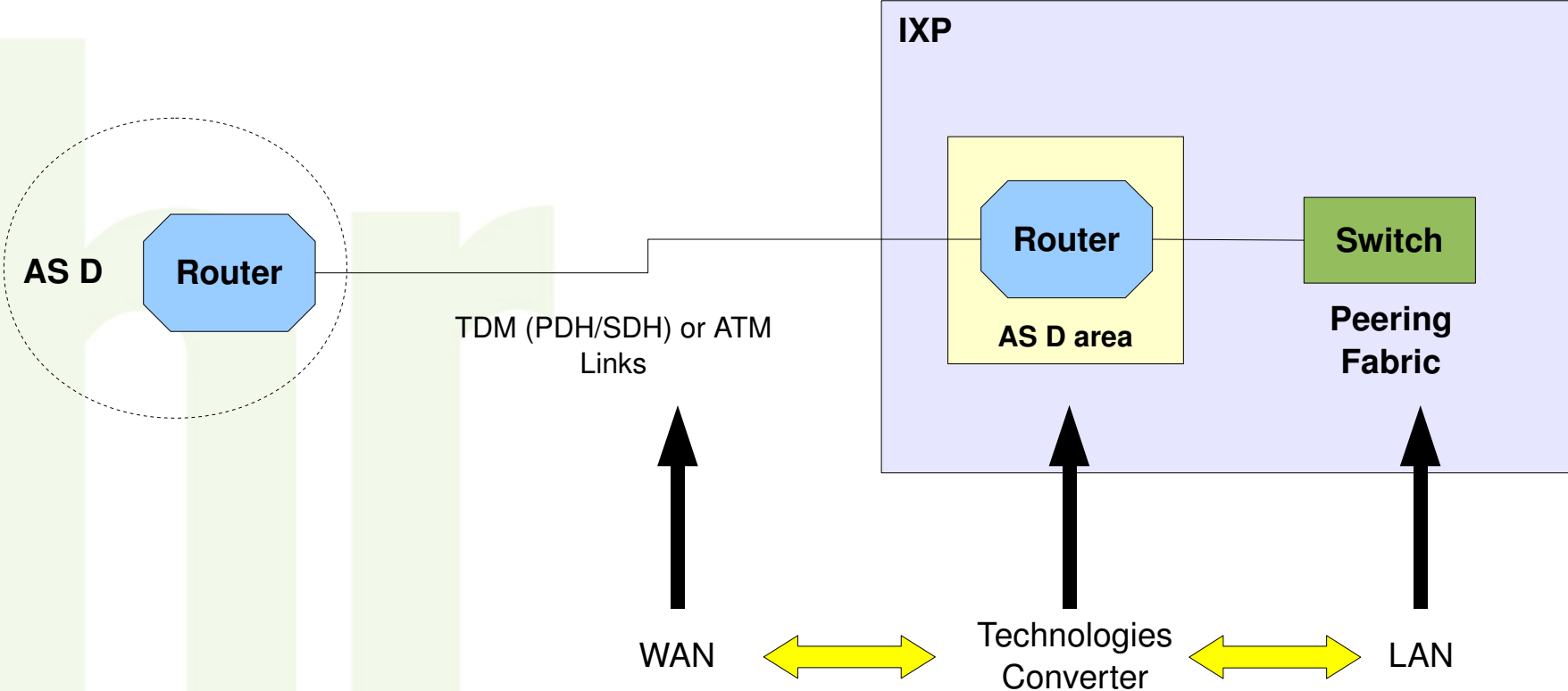


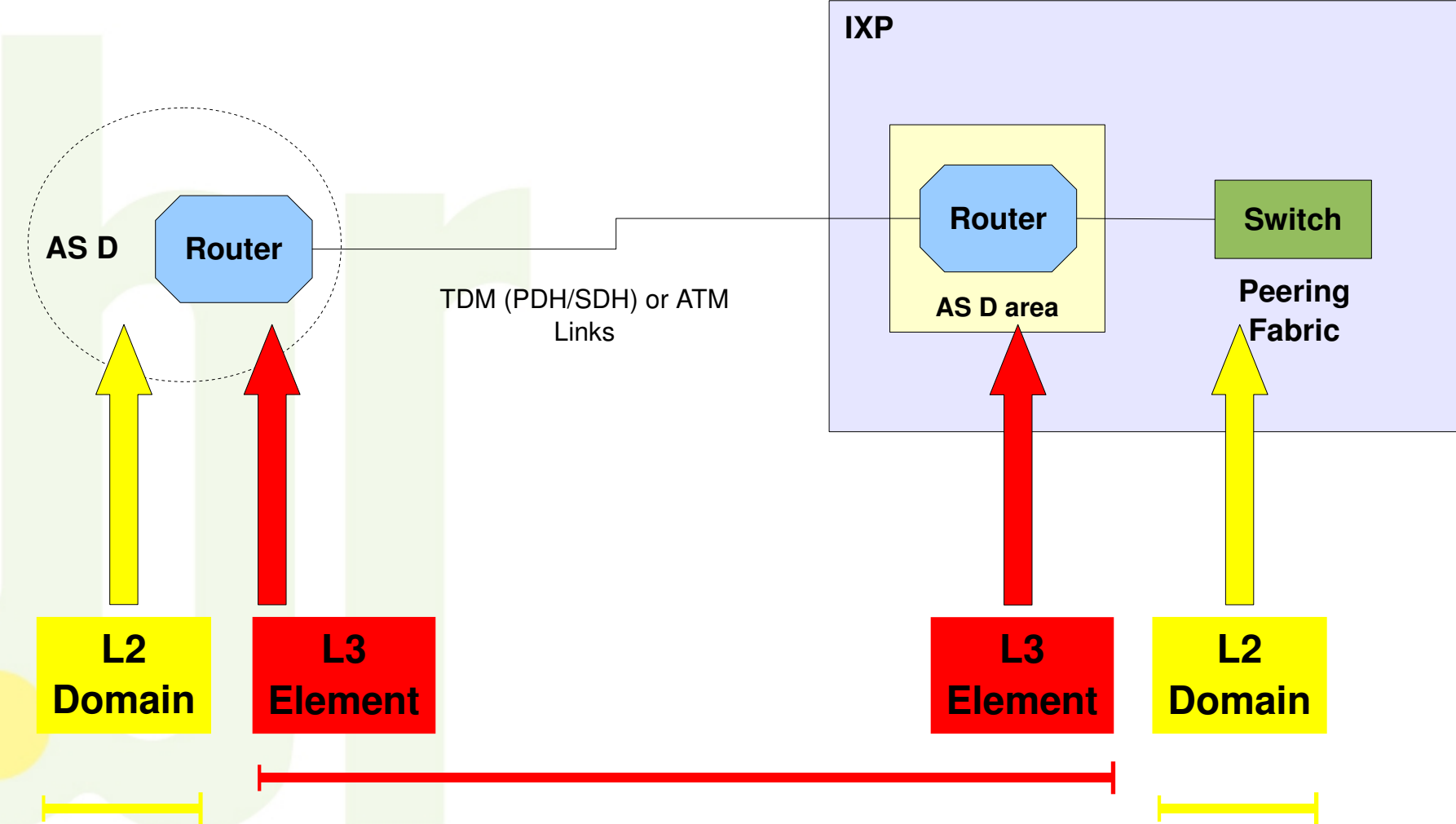
IXP MAN case
e.g. PTTmetro (<http://ptt.br>)

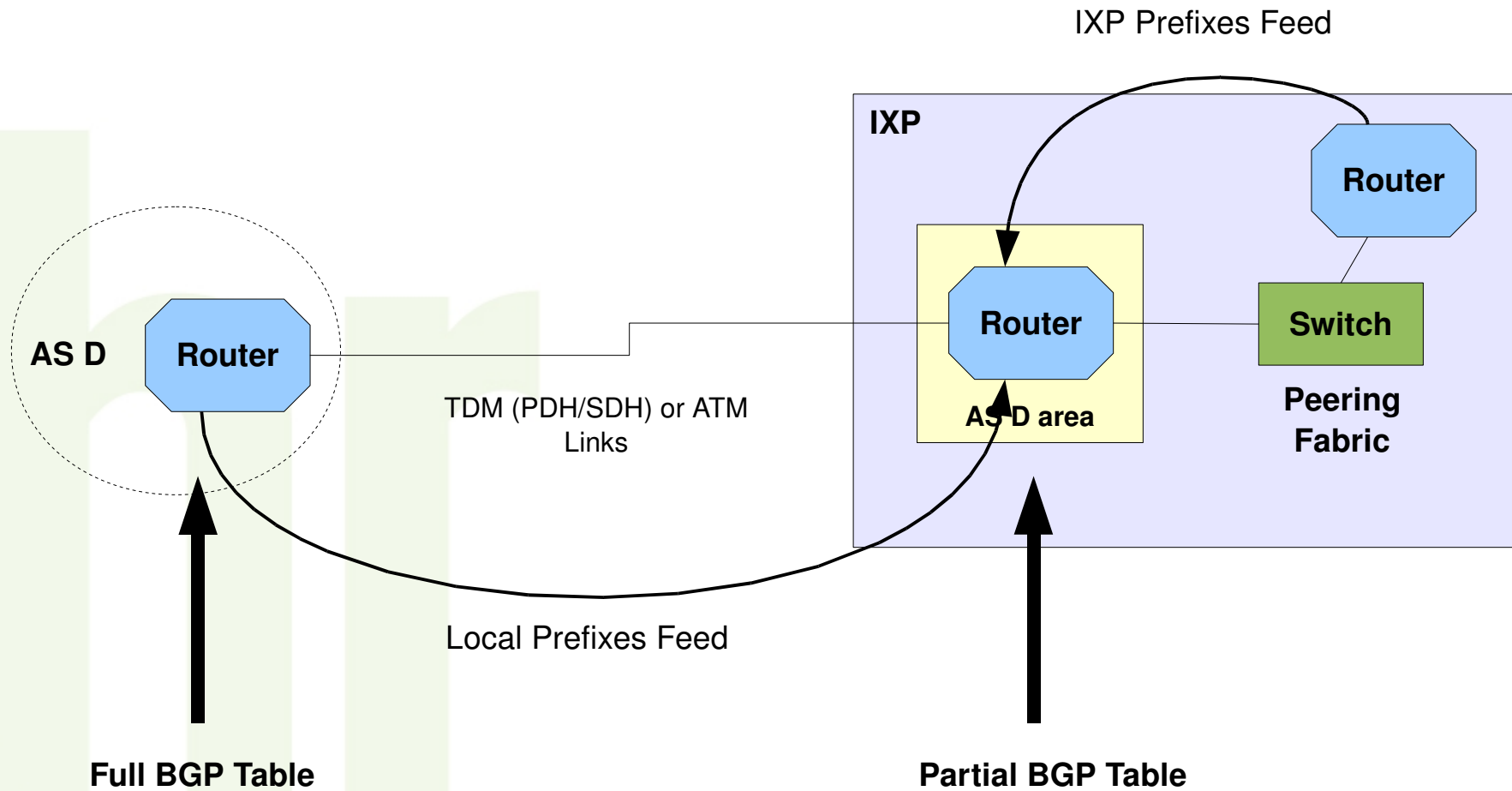
Autonomous System (AS) internal network also
normally based on Ethernet family equipments (switches)

AS internal network can be simplified as a LAN



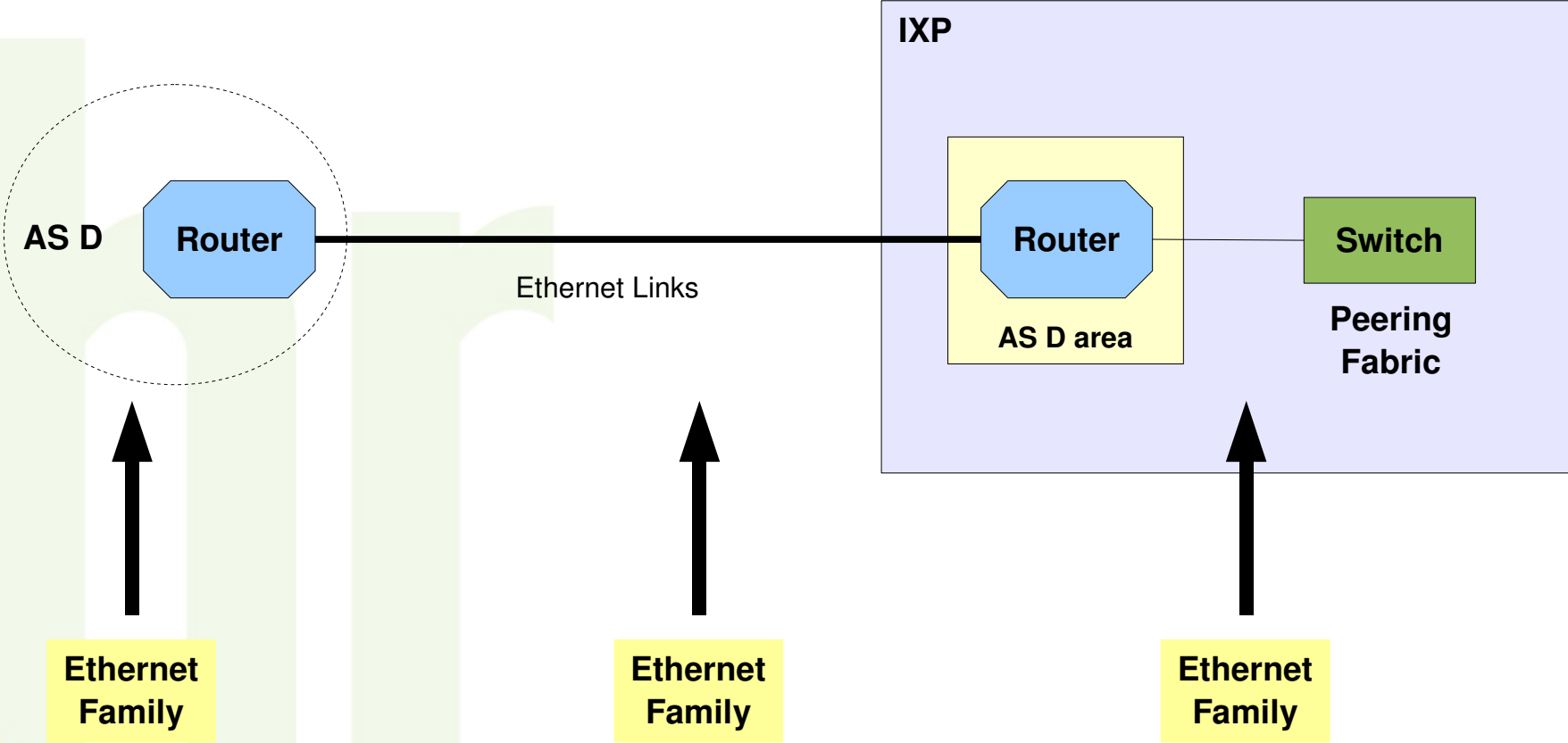




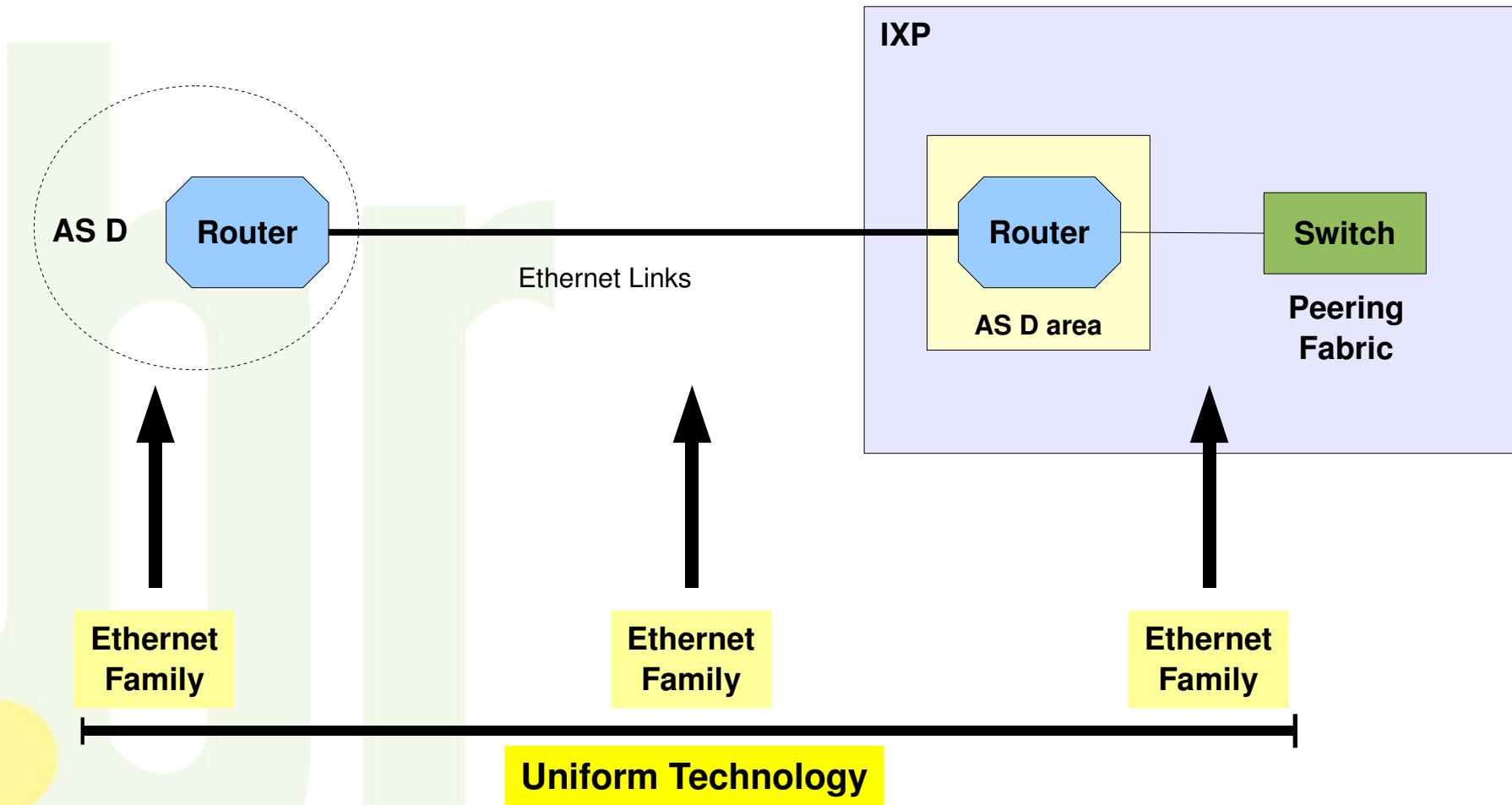


**Ethernet family (Gigabit Ethernet and 10 Gigabit Ethernet)
links become a familiar technology for outside use on
Metropolitan Networks (MAN) and even on long distance connections (WAN)**

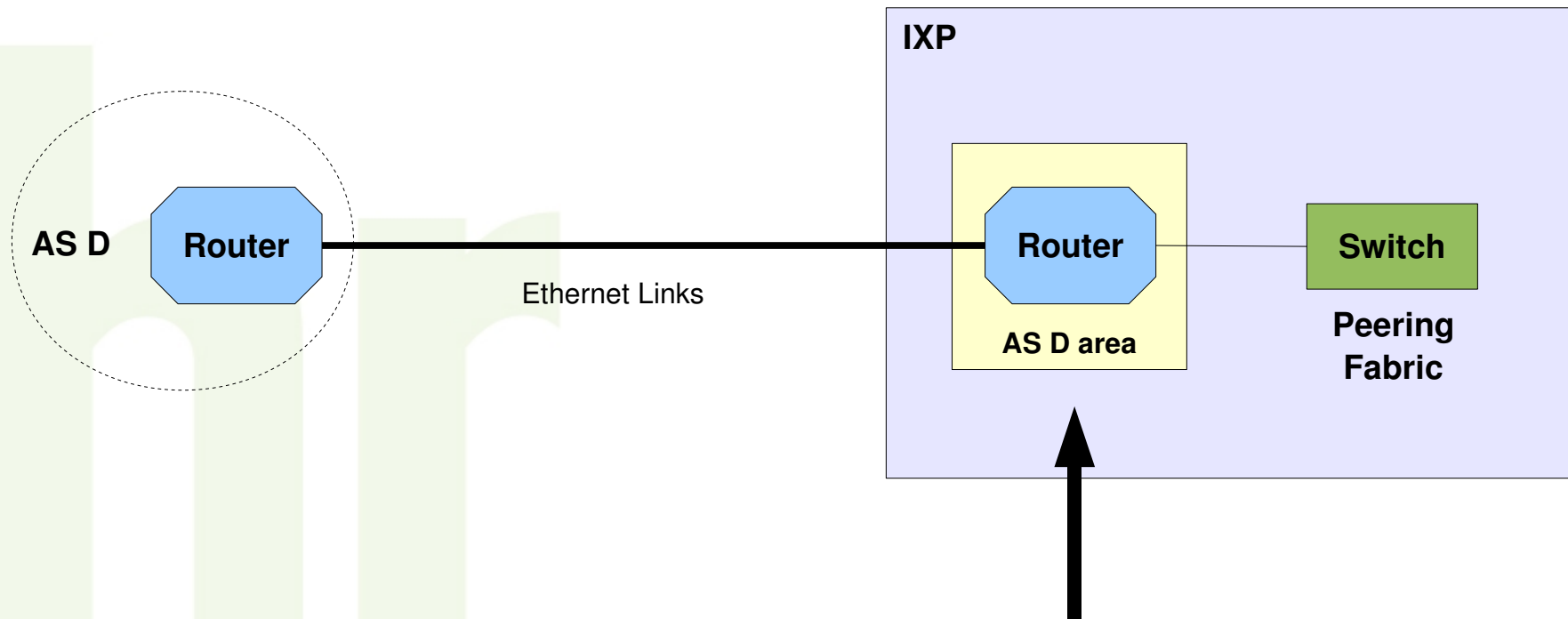
IXP New Connection Model – Ethernet Family Links - Advantages



- ✓ Simplification
- ✓ Lower Operational Cost

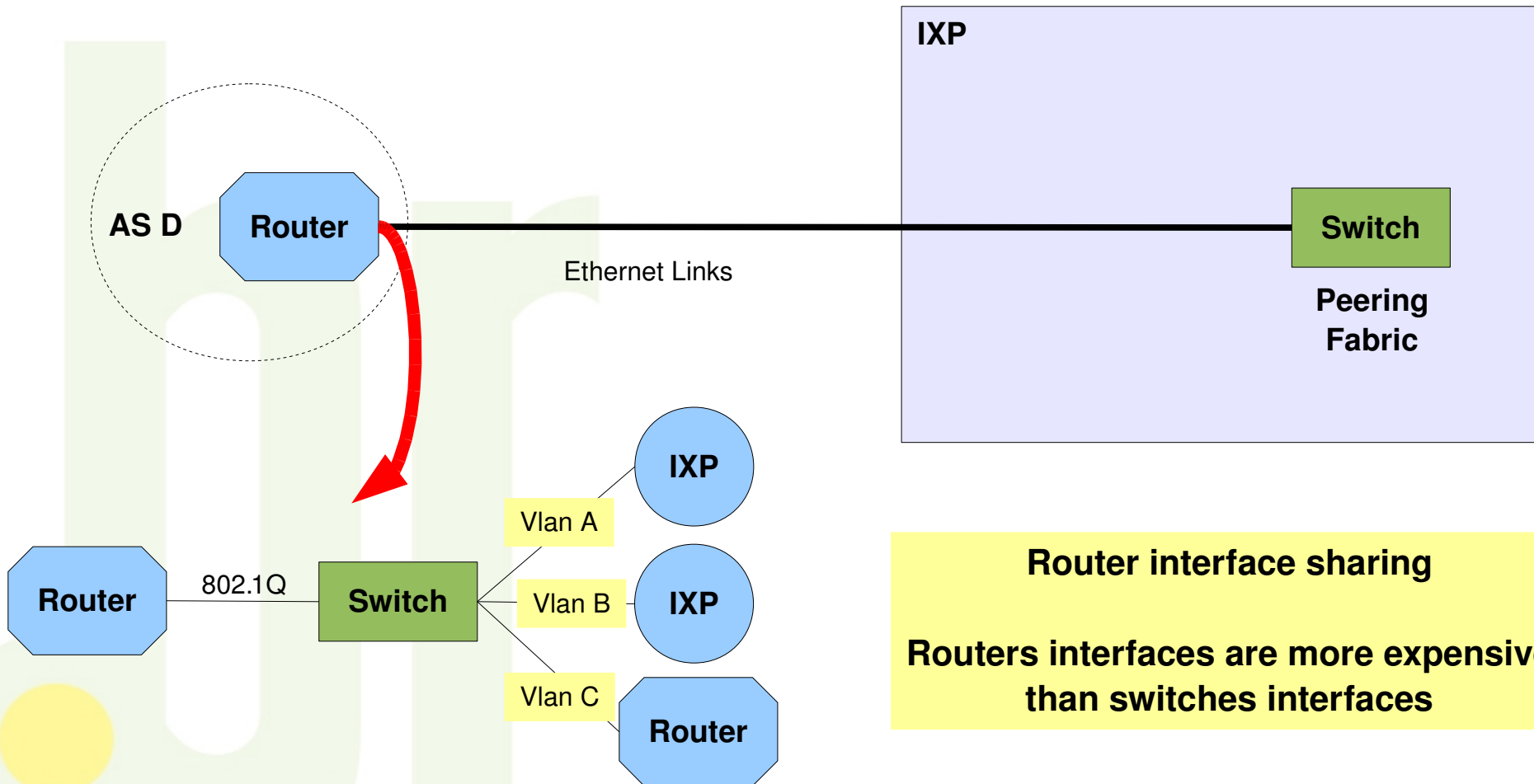


- ✓ Lower Cost
- ✓ Less equipments (less points of failure, simple management and support)



No more need for remote router and eventually data center collocation at IXP site

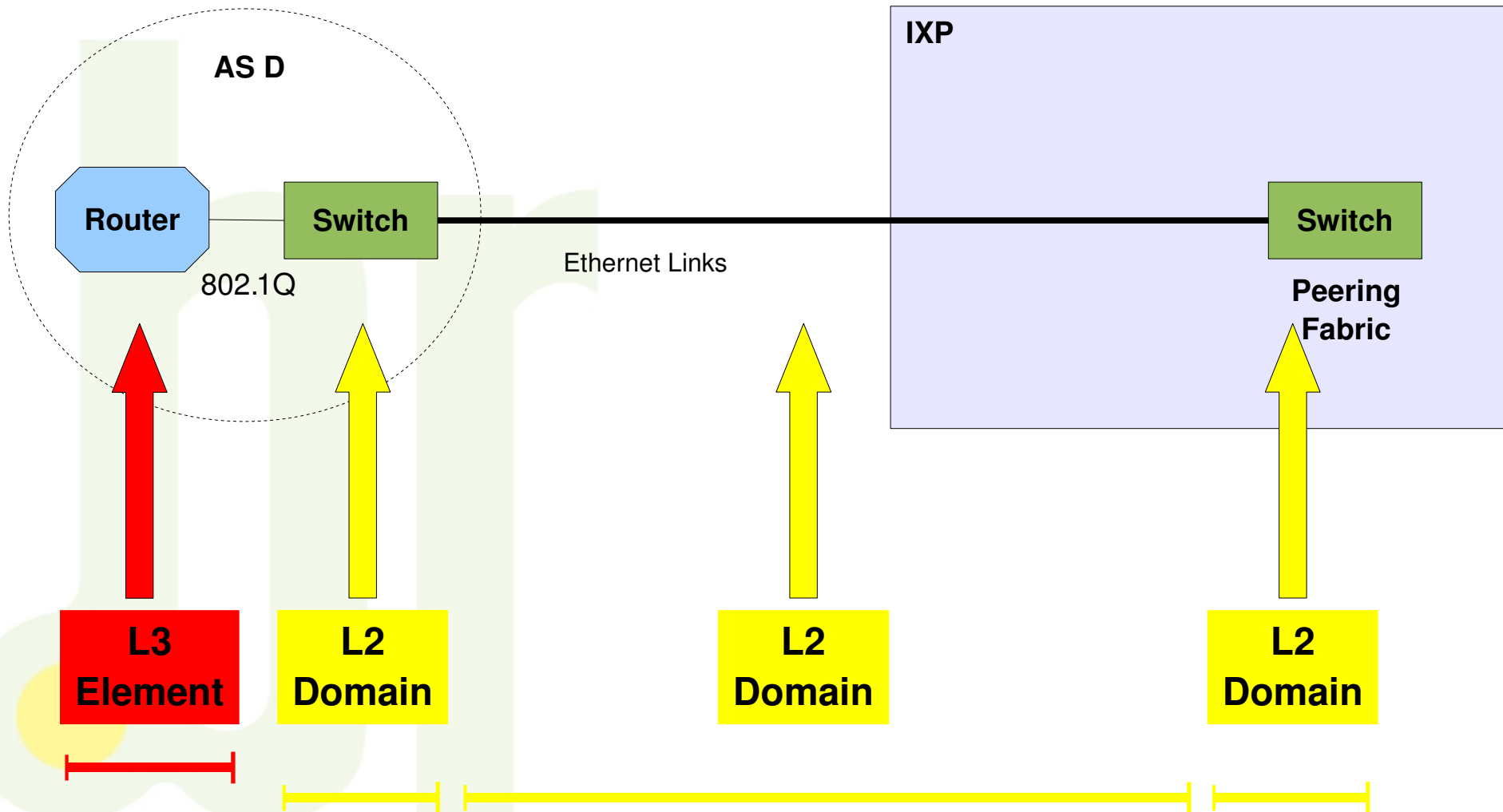
- ✓ Lower Cost
- ✓ Equipments Optimization



At Least Two Kinds of Possible Problems

- X** Lose of Simple Logical Isolation Between L2 Domains
- X** Lose of Intra AS BGP Tables Isolation (Global and IXP)

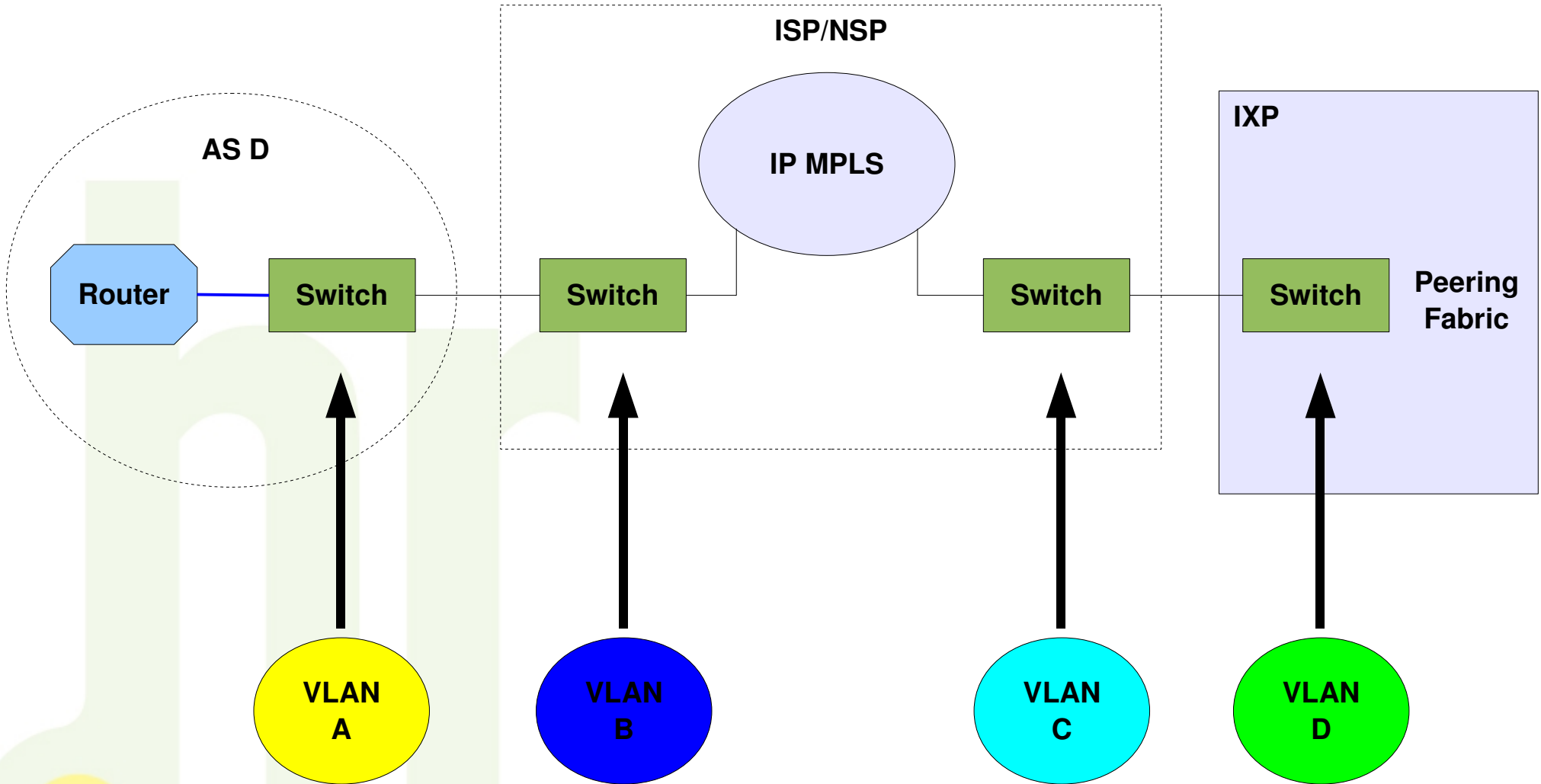
X Lose of Simple Logical Isolation Between L2 Domains



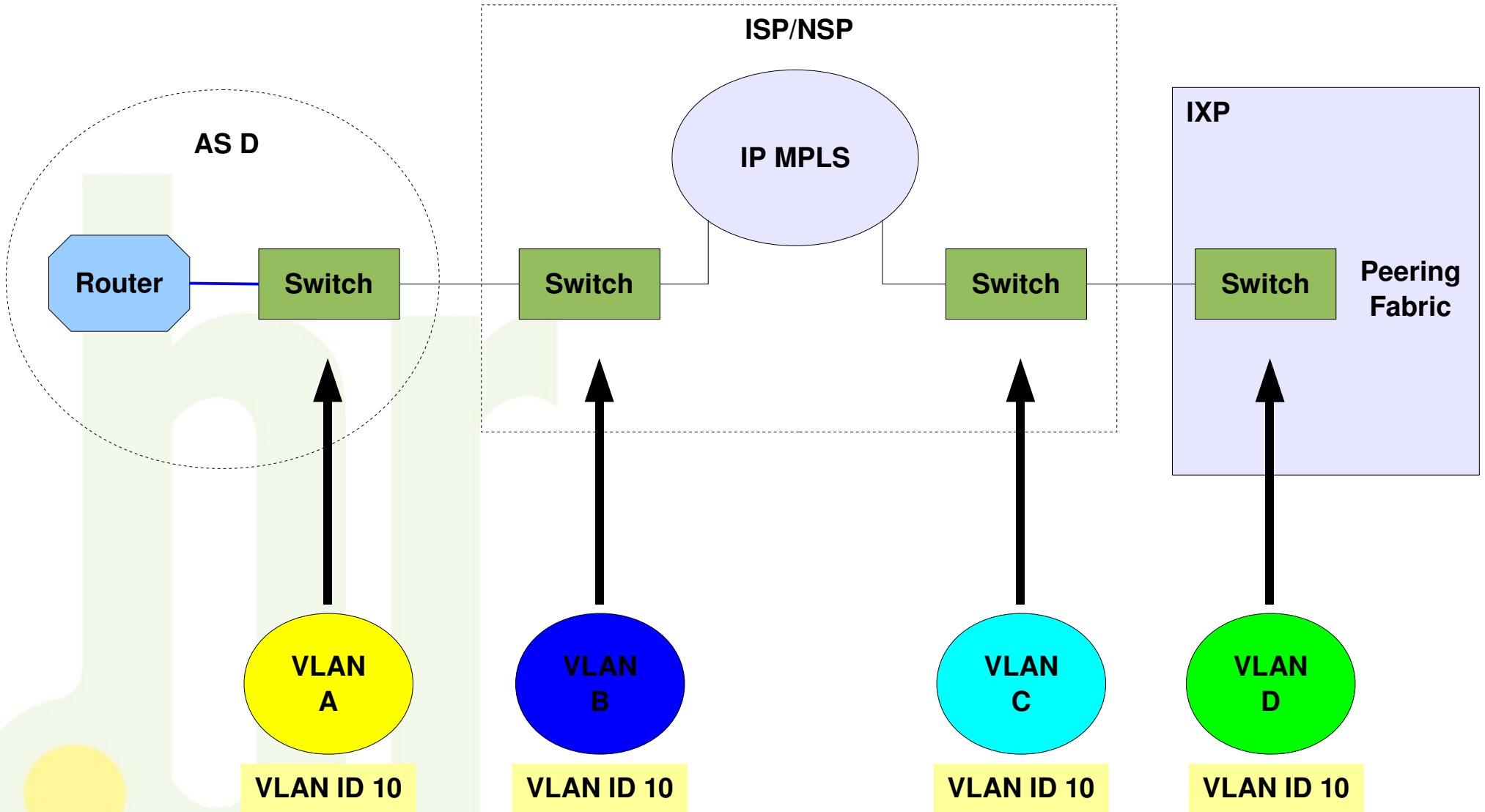
Ethernet networks were not originally design to prevent against problems on different administration networks L2 interconnection.

Special resources may be needed for protection and nowadays some solutions are only possible when using proprietary features.

Ethernet logical isolation is done by VLANs

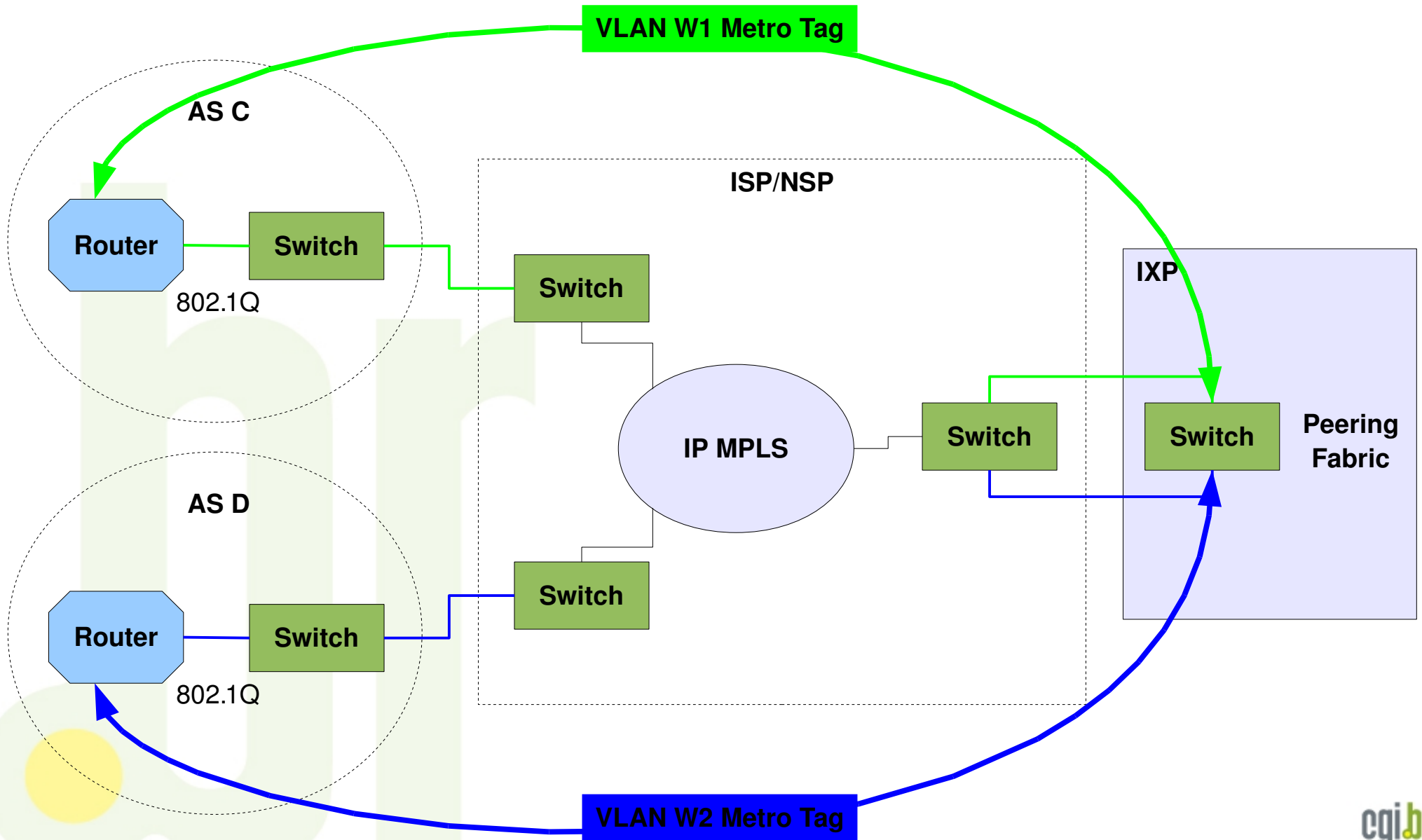


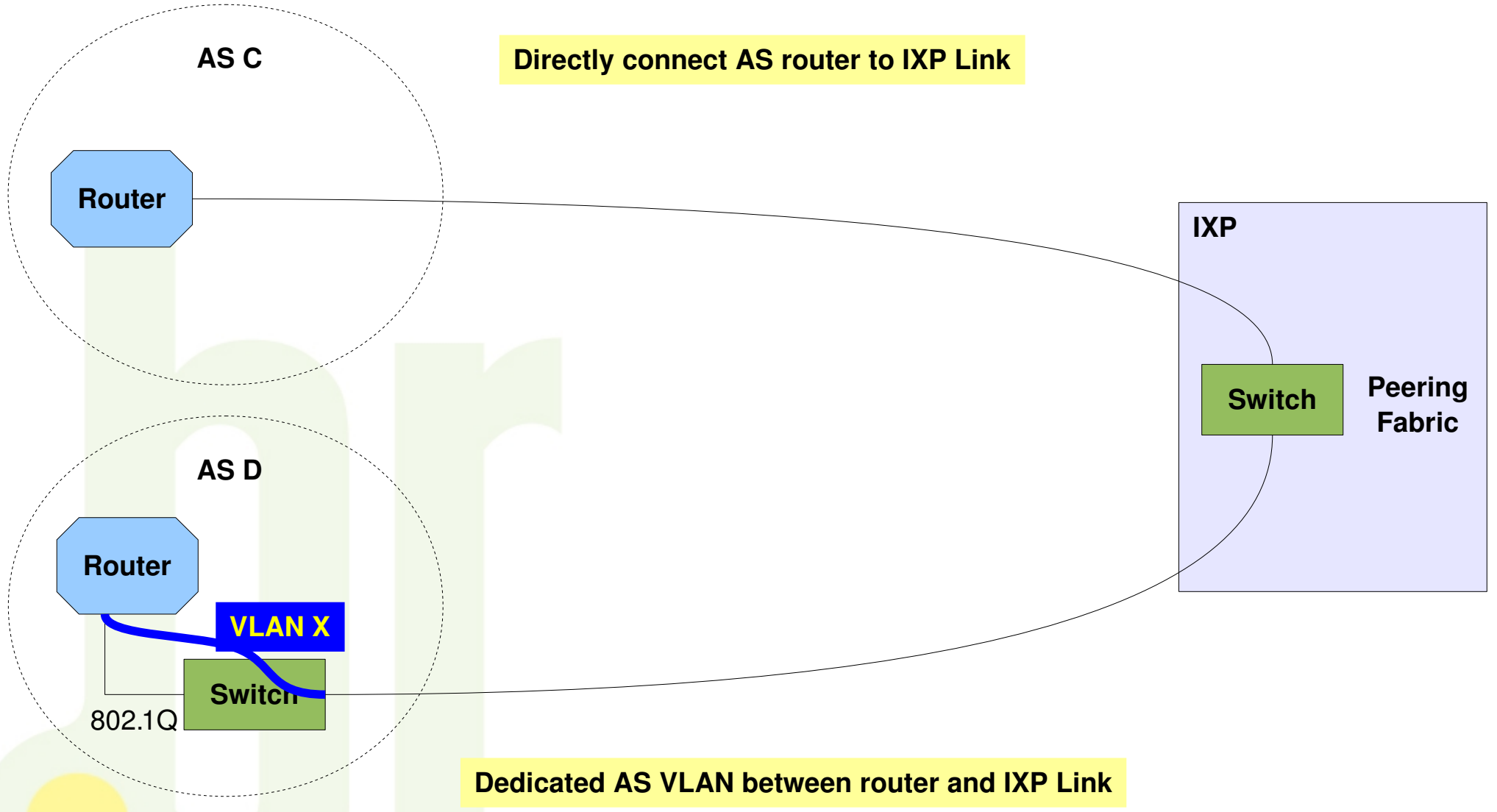
Independent connected VLANs may have the same ID



Special care must be taken when trunk (802.1Q) connections are used between L2 domains

Ethernet logical isolation on ISP/NSP - 802.1ad (QinQ)





Some Ethernet Protections Points

- Explicitly define trunk mode between L2 domains interconnection
(avoid auto / dynamic configuration)

- Explicitly define and control links aggregation conditions
(LACP - 802.3ad)

- Ethernet frames inbound and outbound filters
 - Neighbor discover protocols (e.g. CDP, EDP, etc)
 - Loop-free / Fault tolerant L2 protocols (e.g. STP, EAPS, REP, etc)
 - Non ARP Broadcast

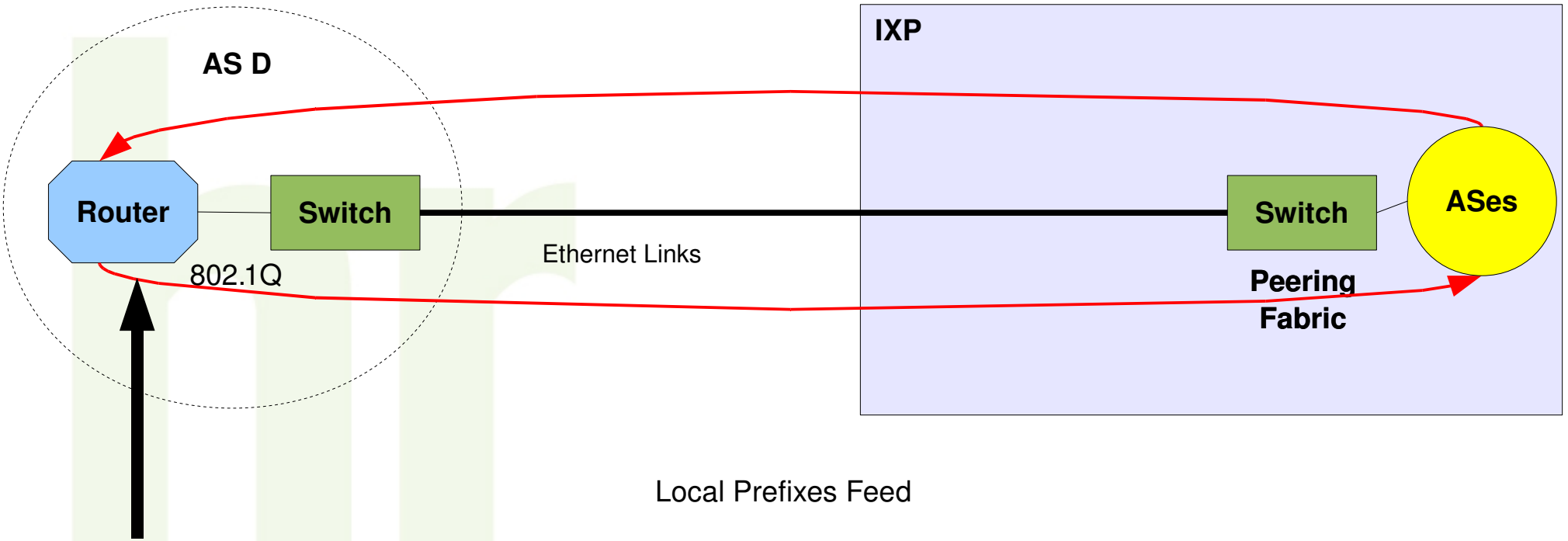
Restrictive Allowed Ethernet Frames Operation

AS permit only specific and expected Ethertypes frames on links to IXP

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

X BGP Table

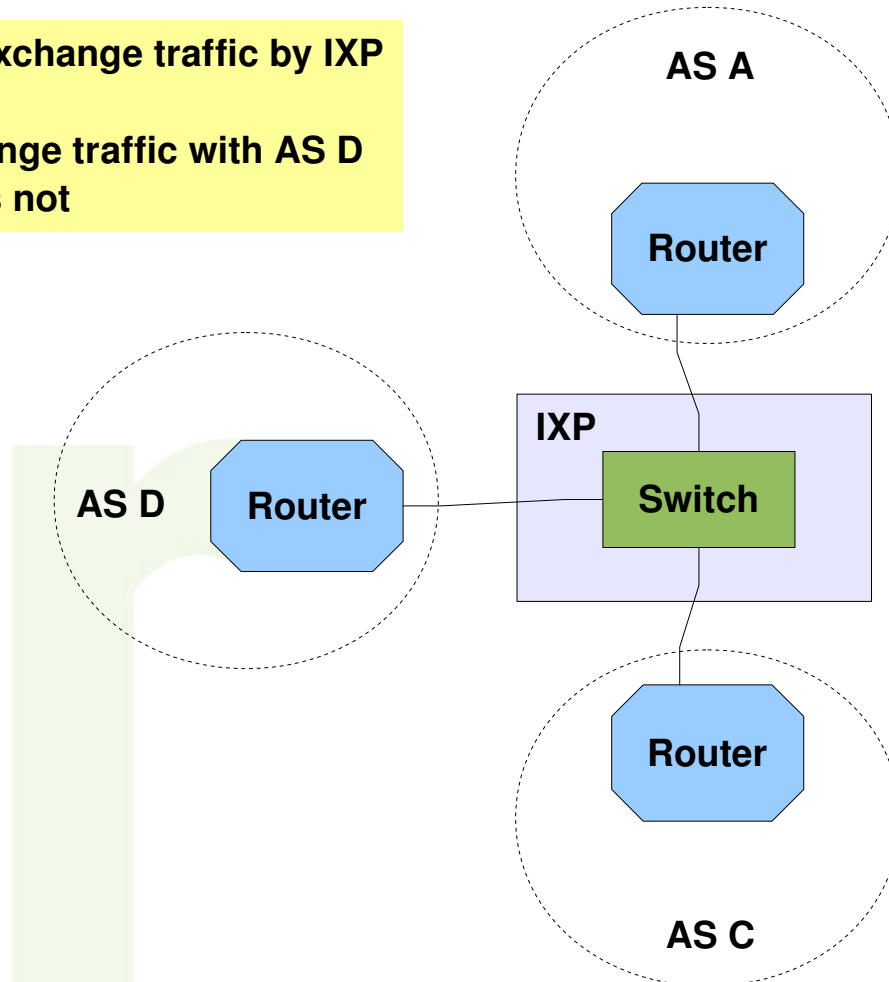
IXP Prefixes Feed



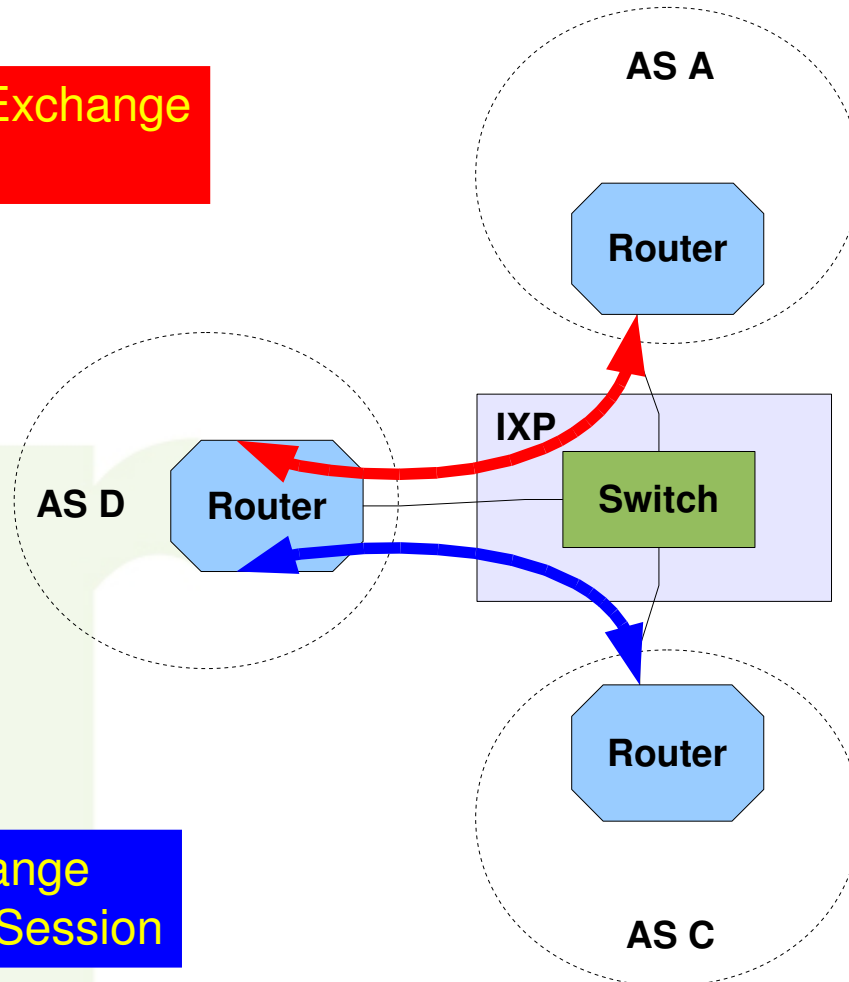
Local Prefixes Feed

Full BGP Table

- AS D and AS C want to exchange traffic by IXP
- AS A would like to exchange traffic with AS D by IXP, but AS D does not

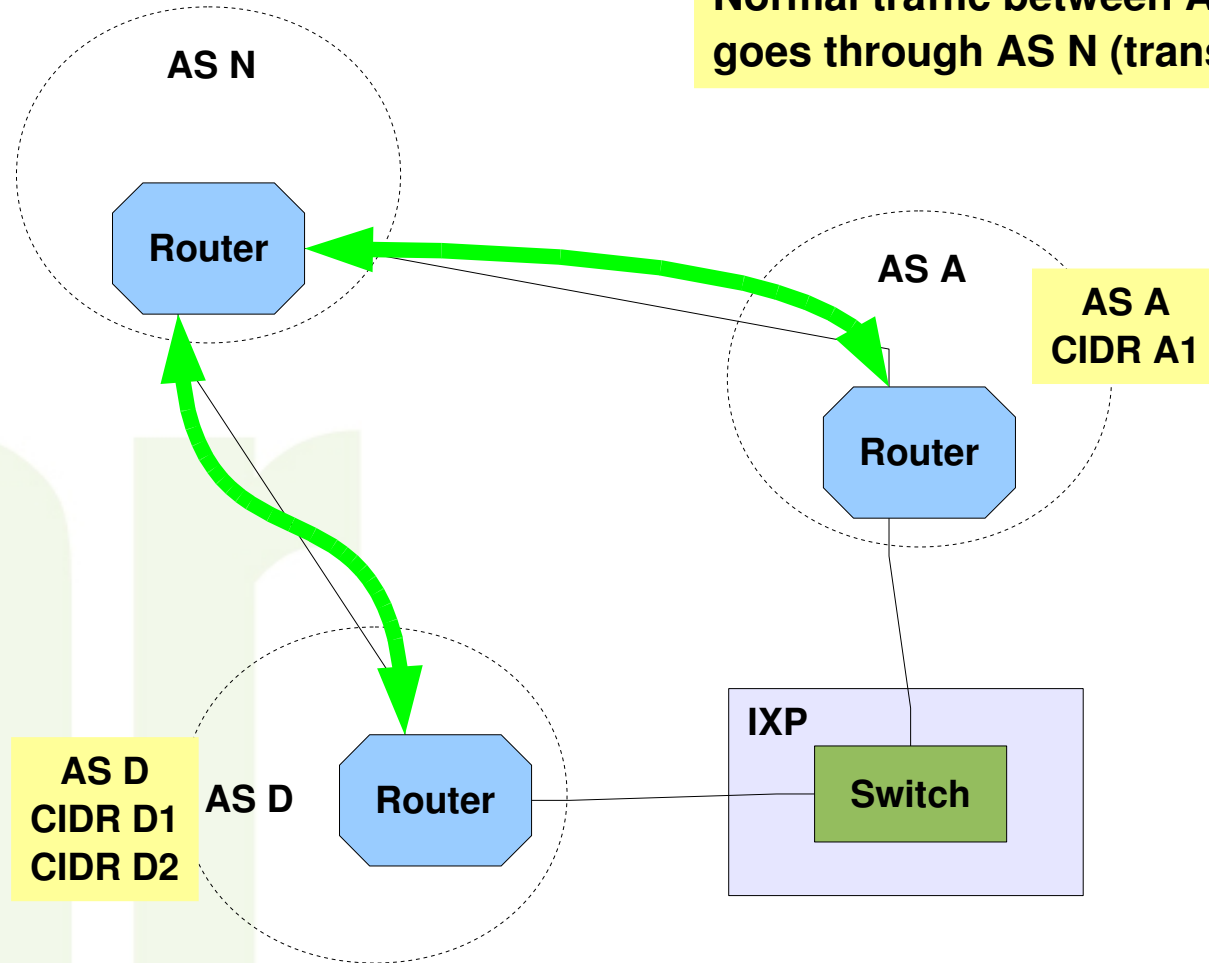


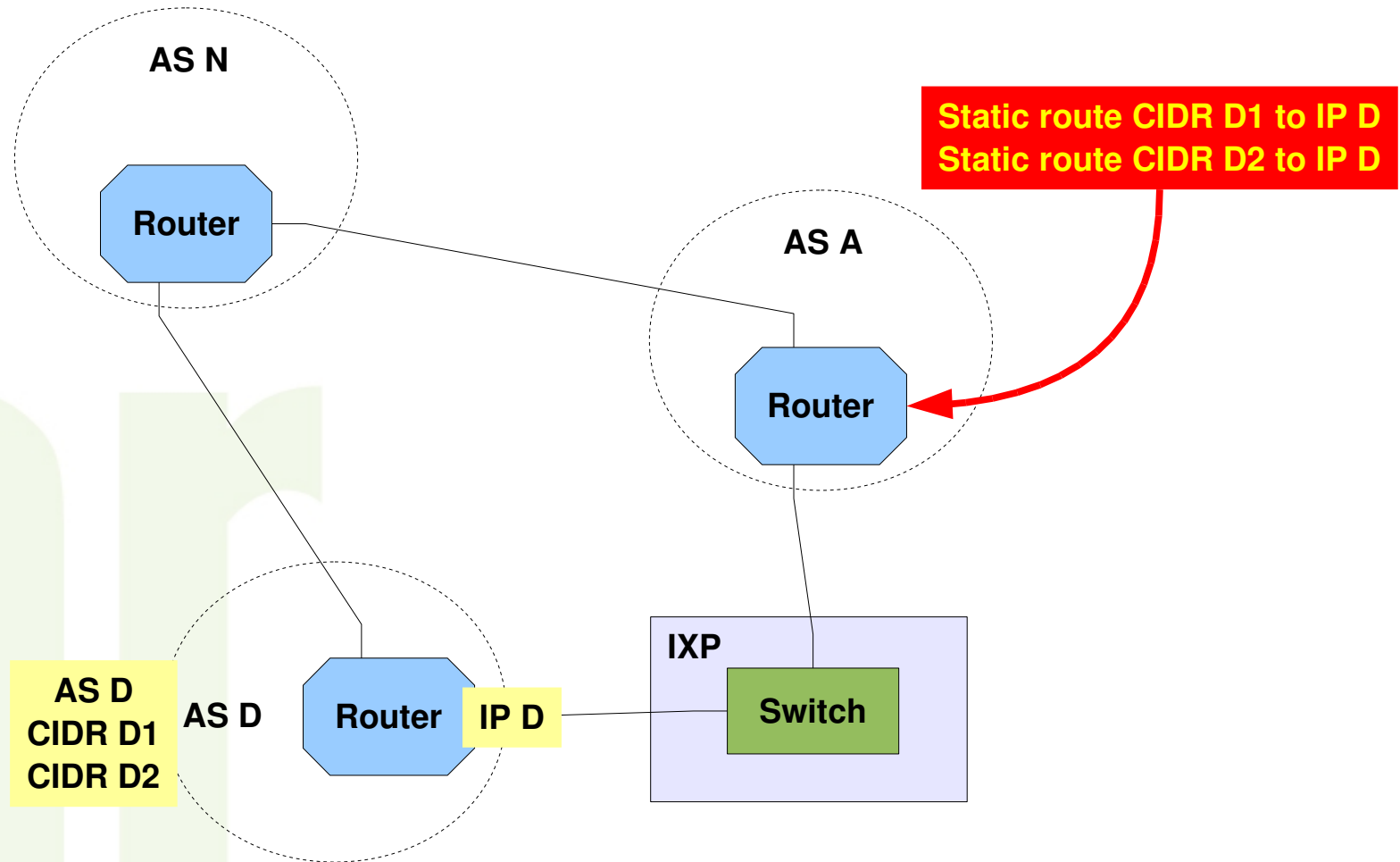
Non Valid Traffic Exchange
No BGP Session

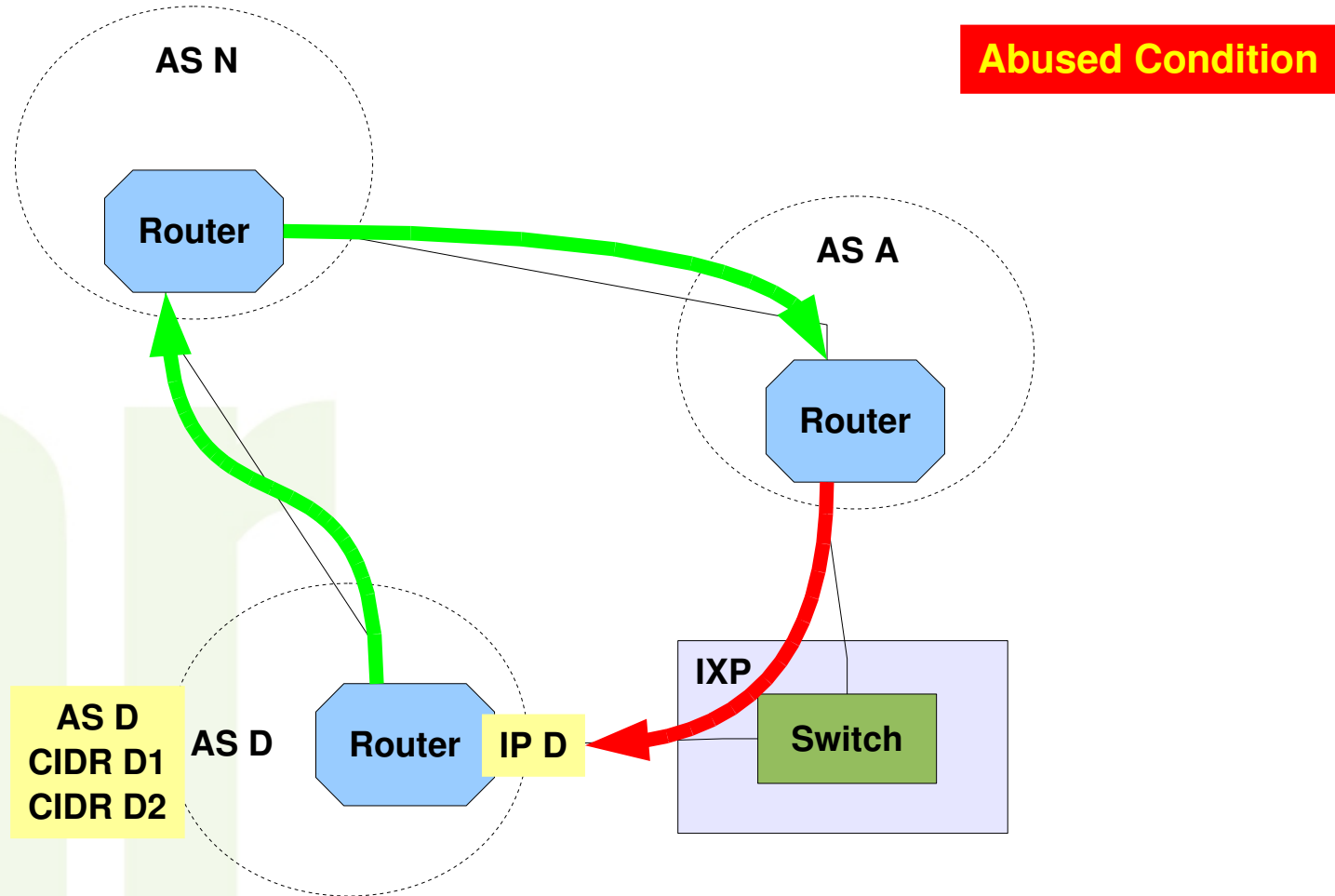


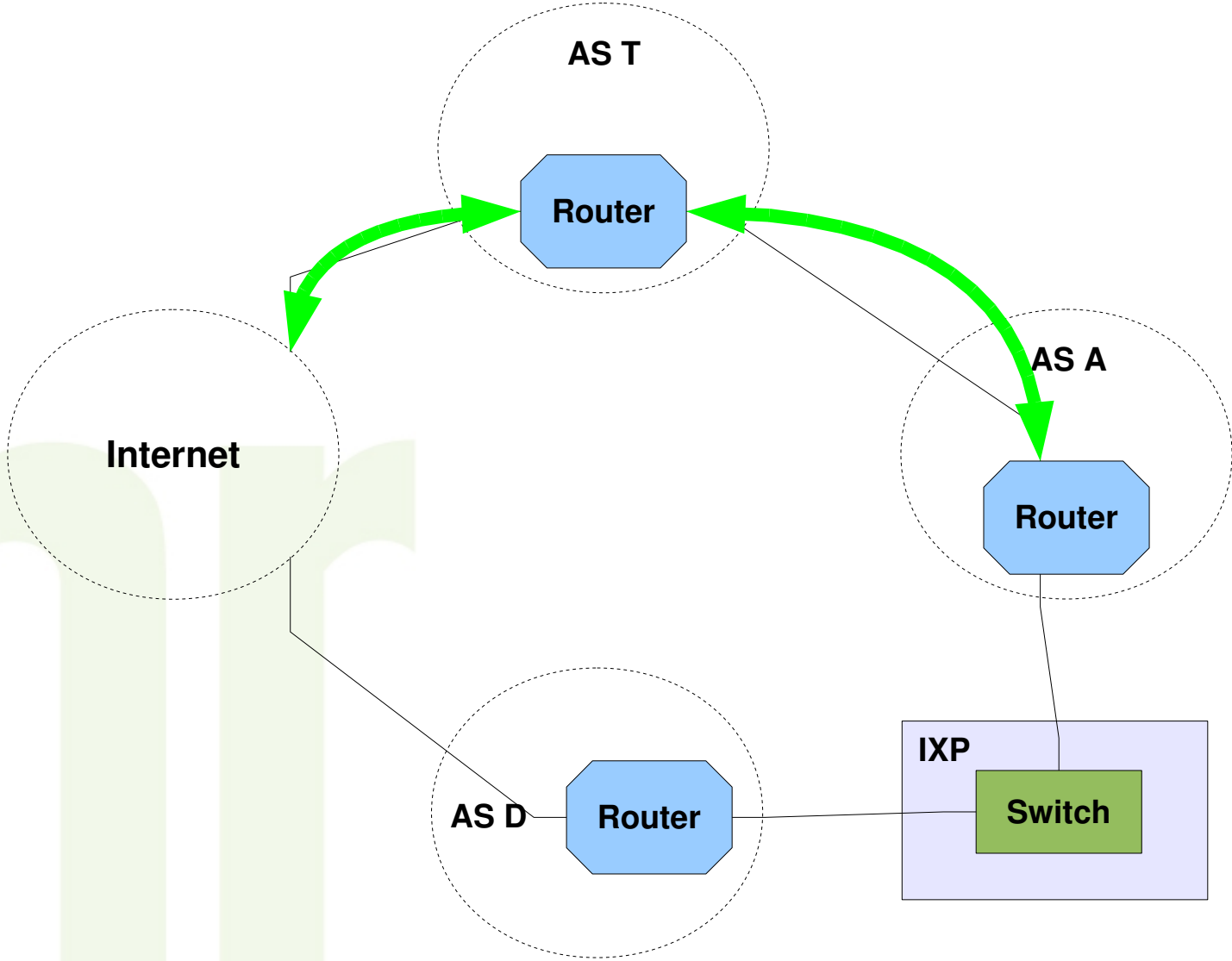
Valid Traffic Exchange
Established BGP Session

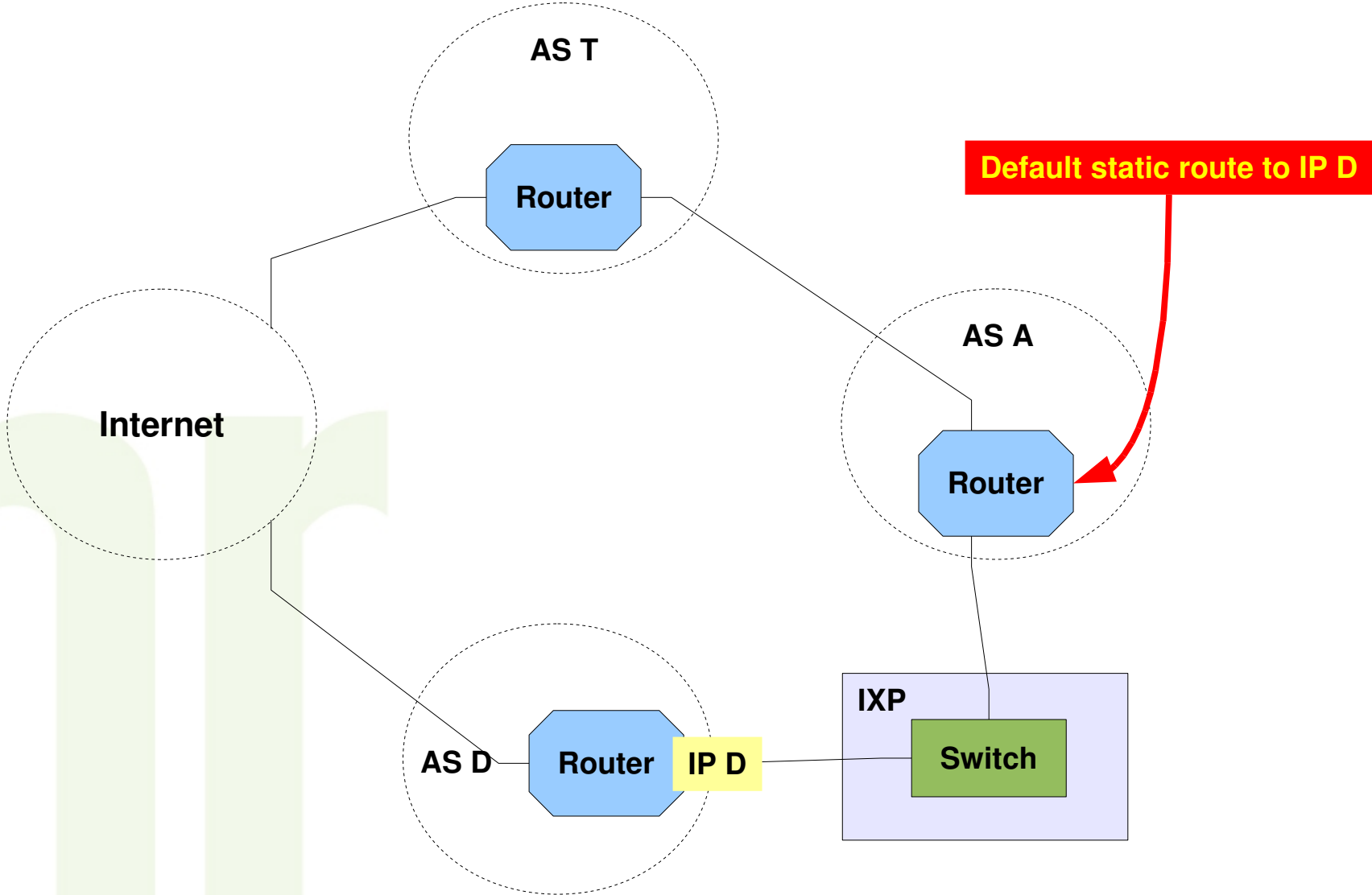
Normal traffic between AS A and AS D goes through AS N (transit)

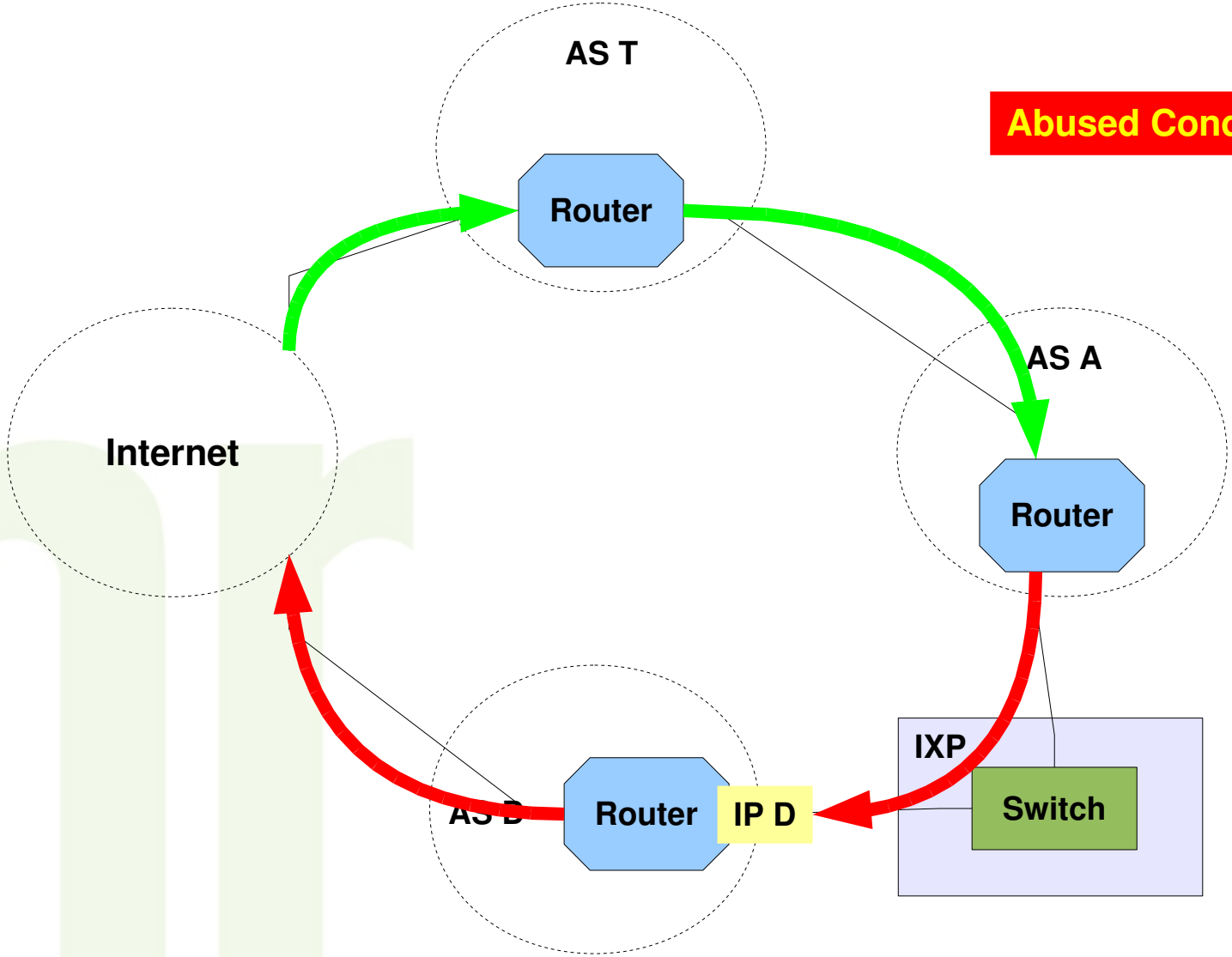




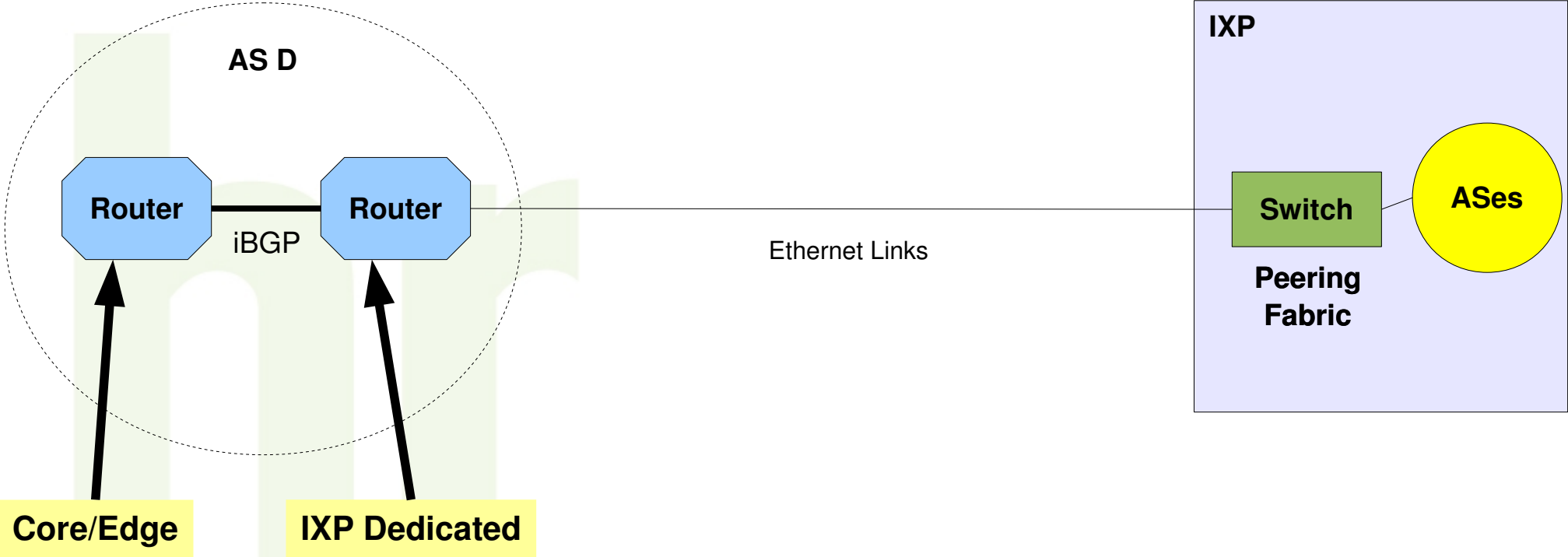


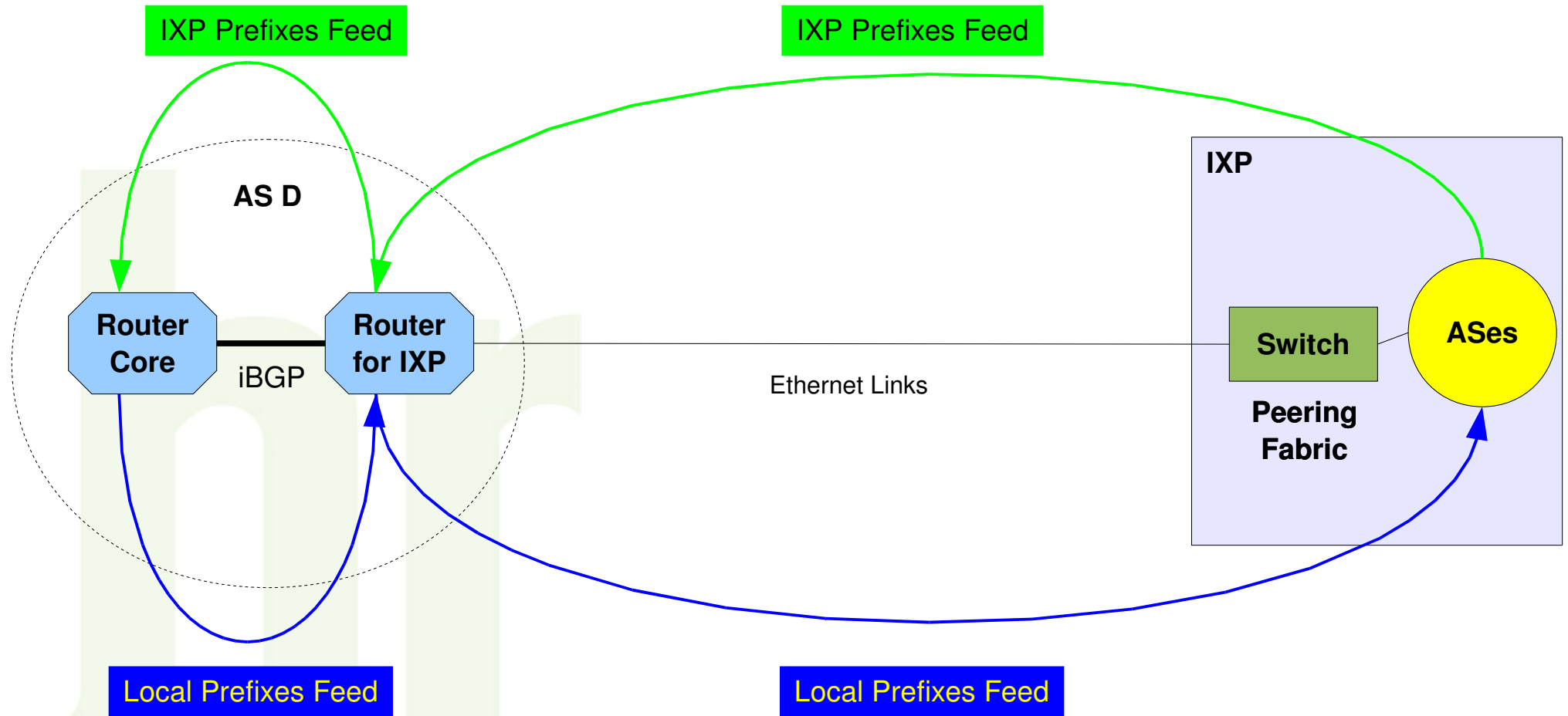


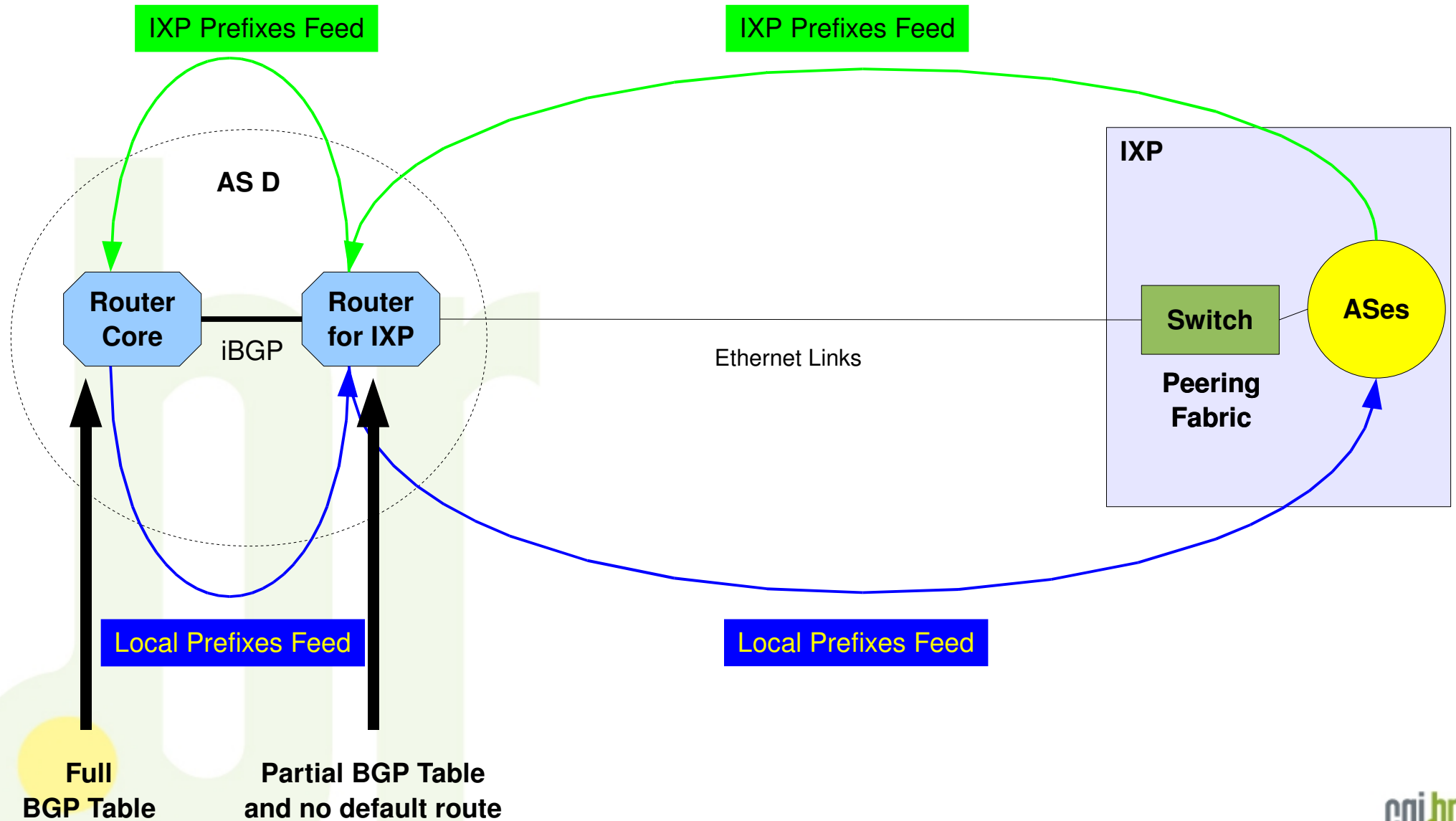


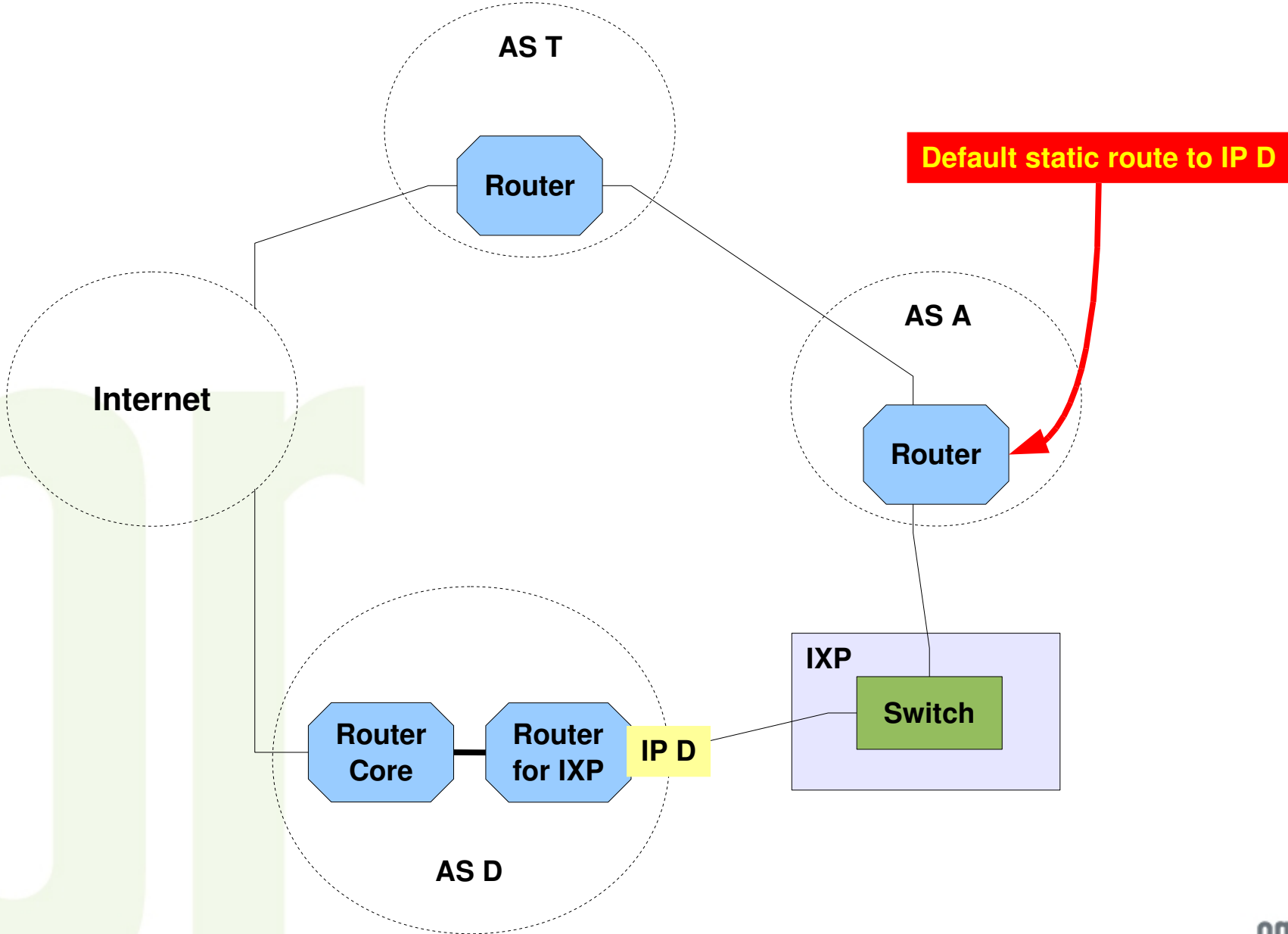


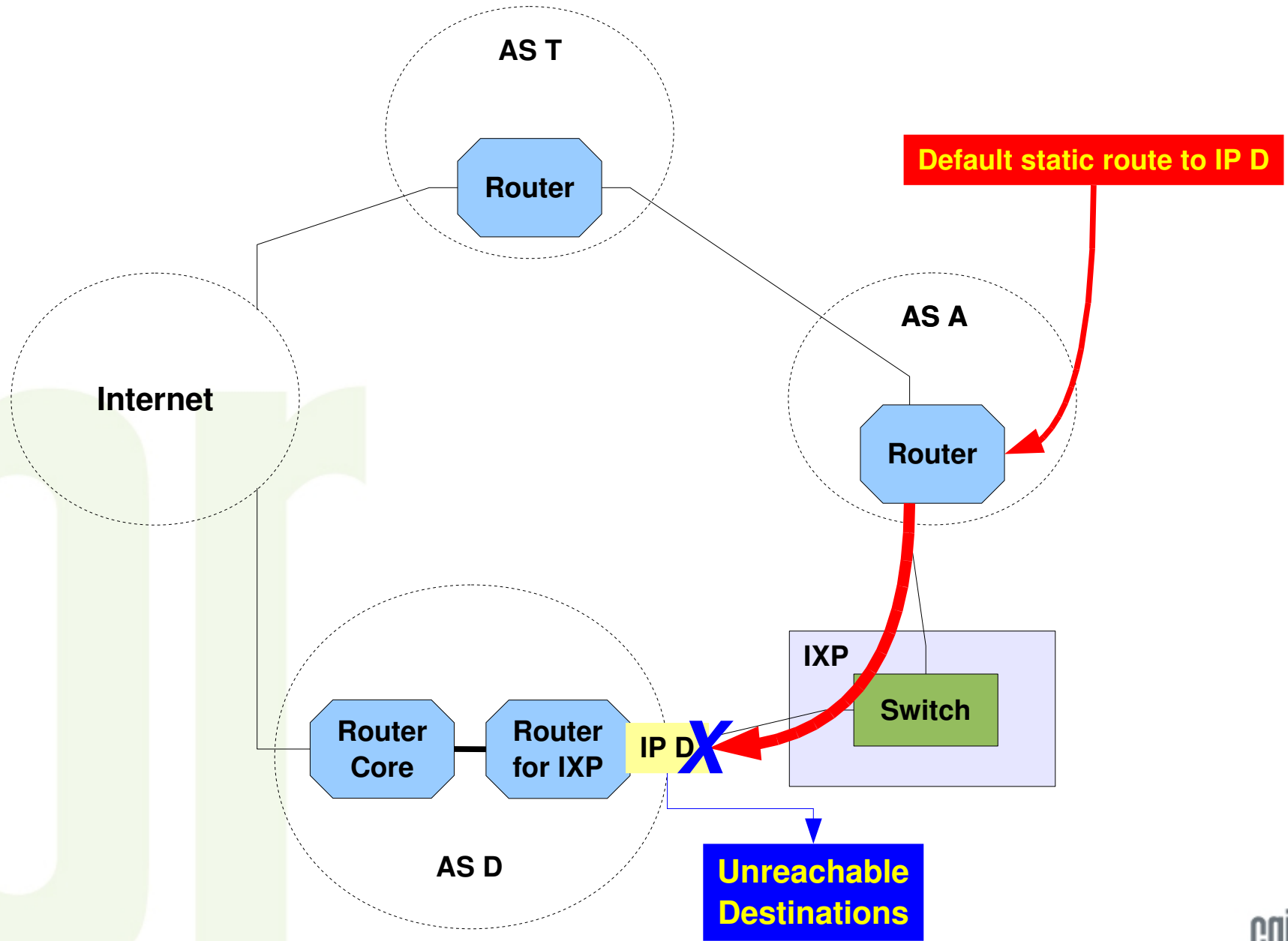
Abused Condition

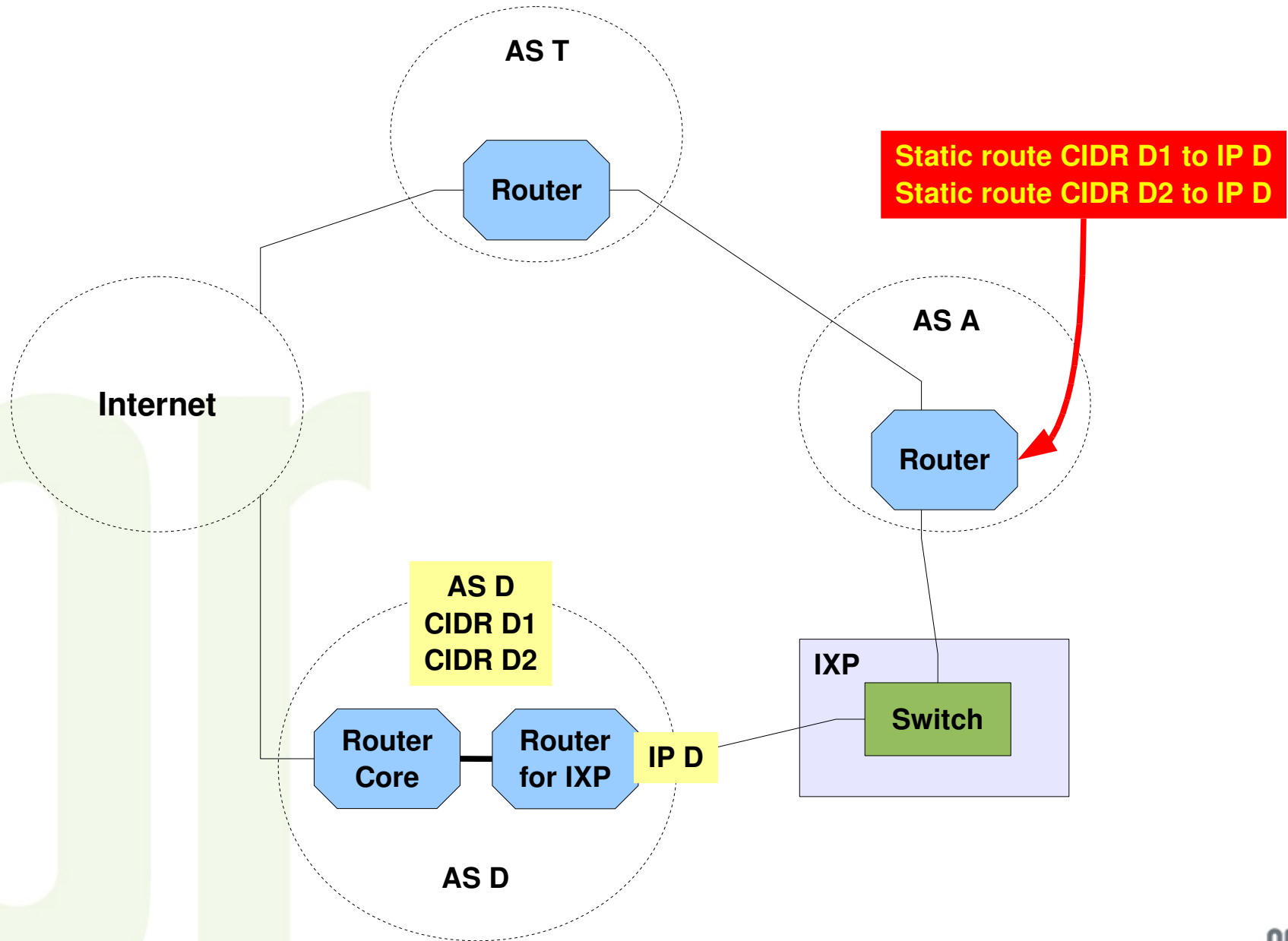


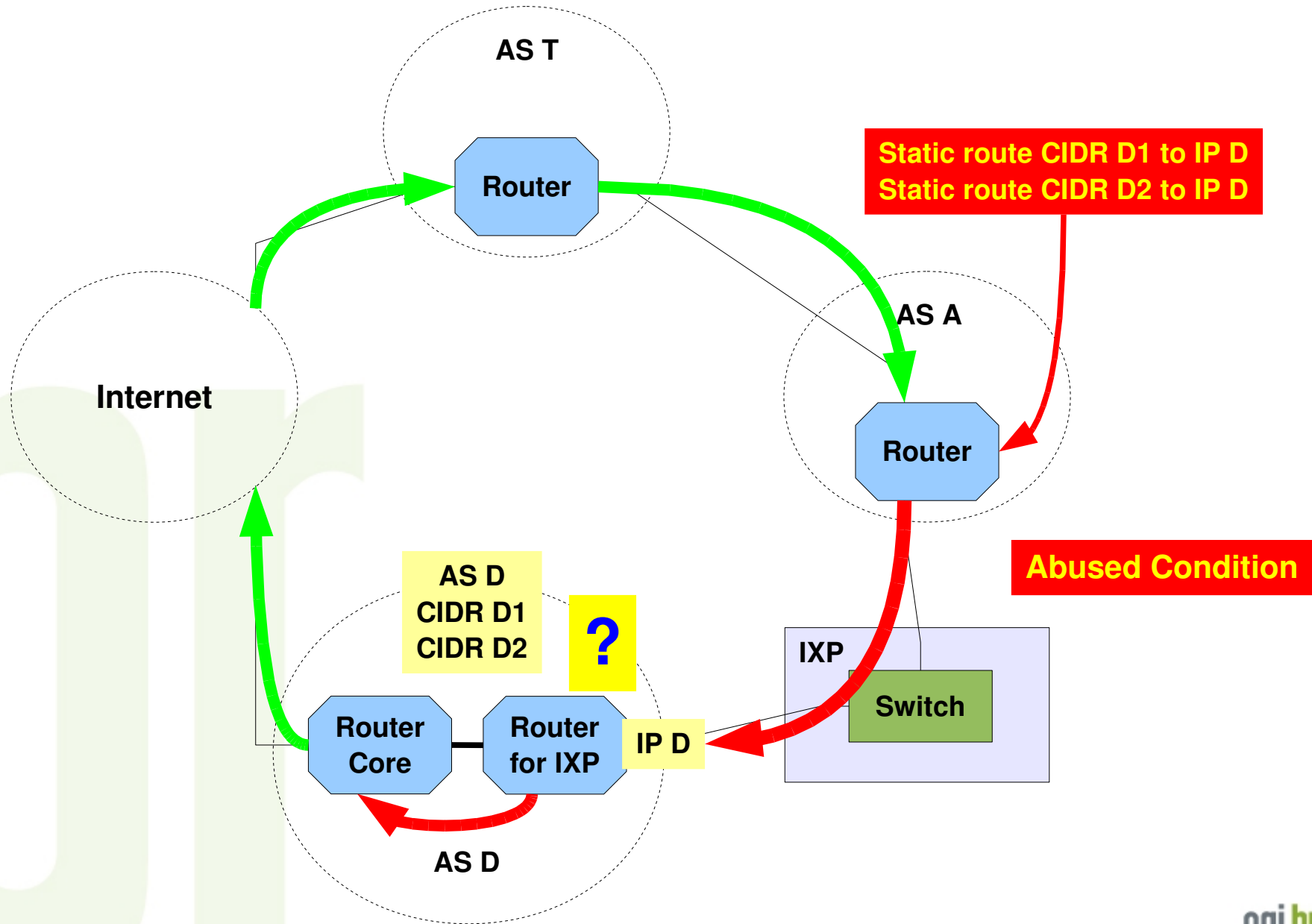




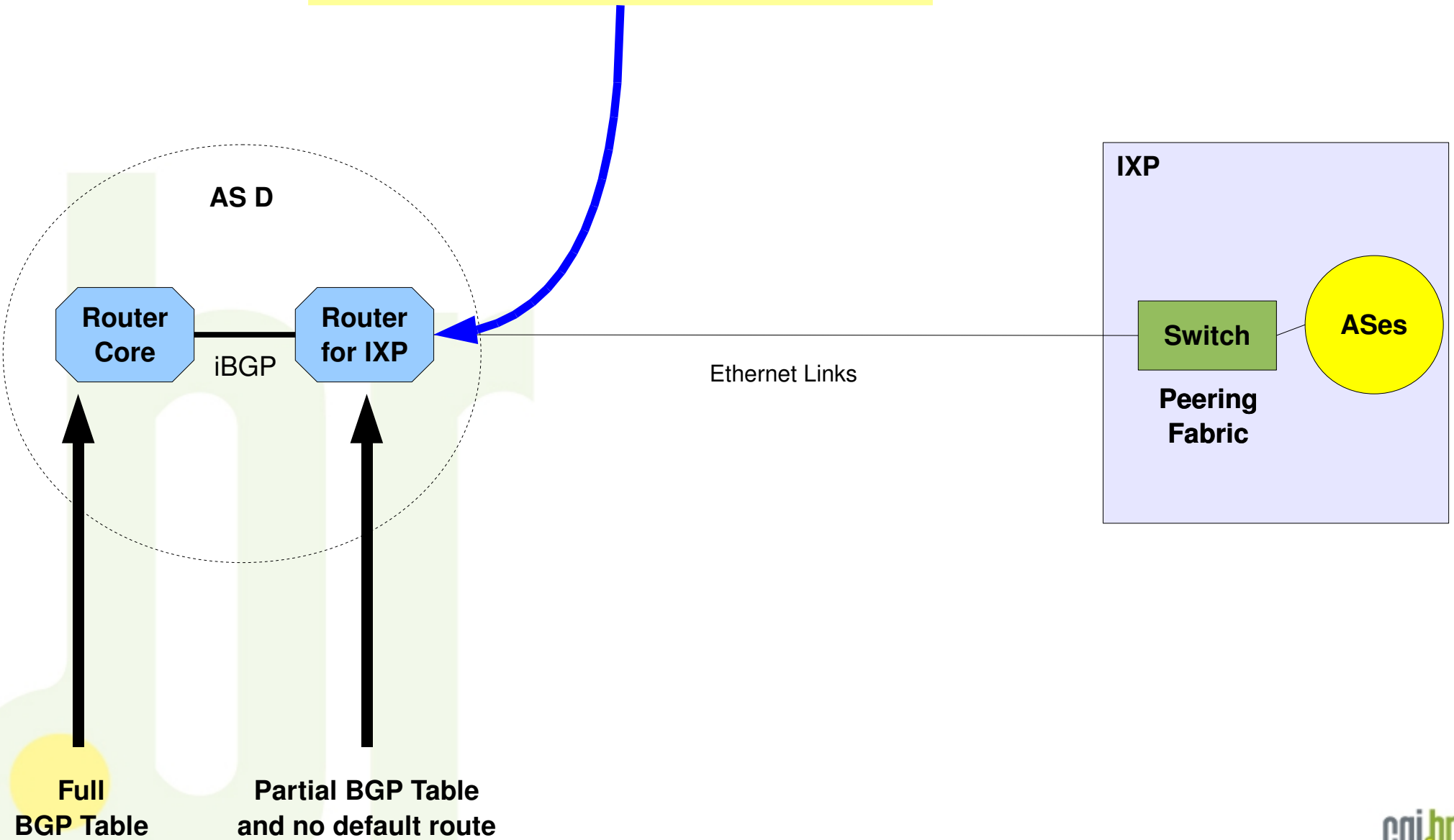


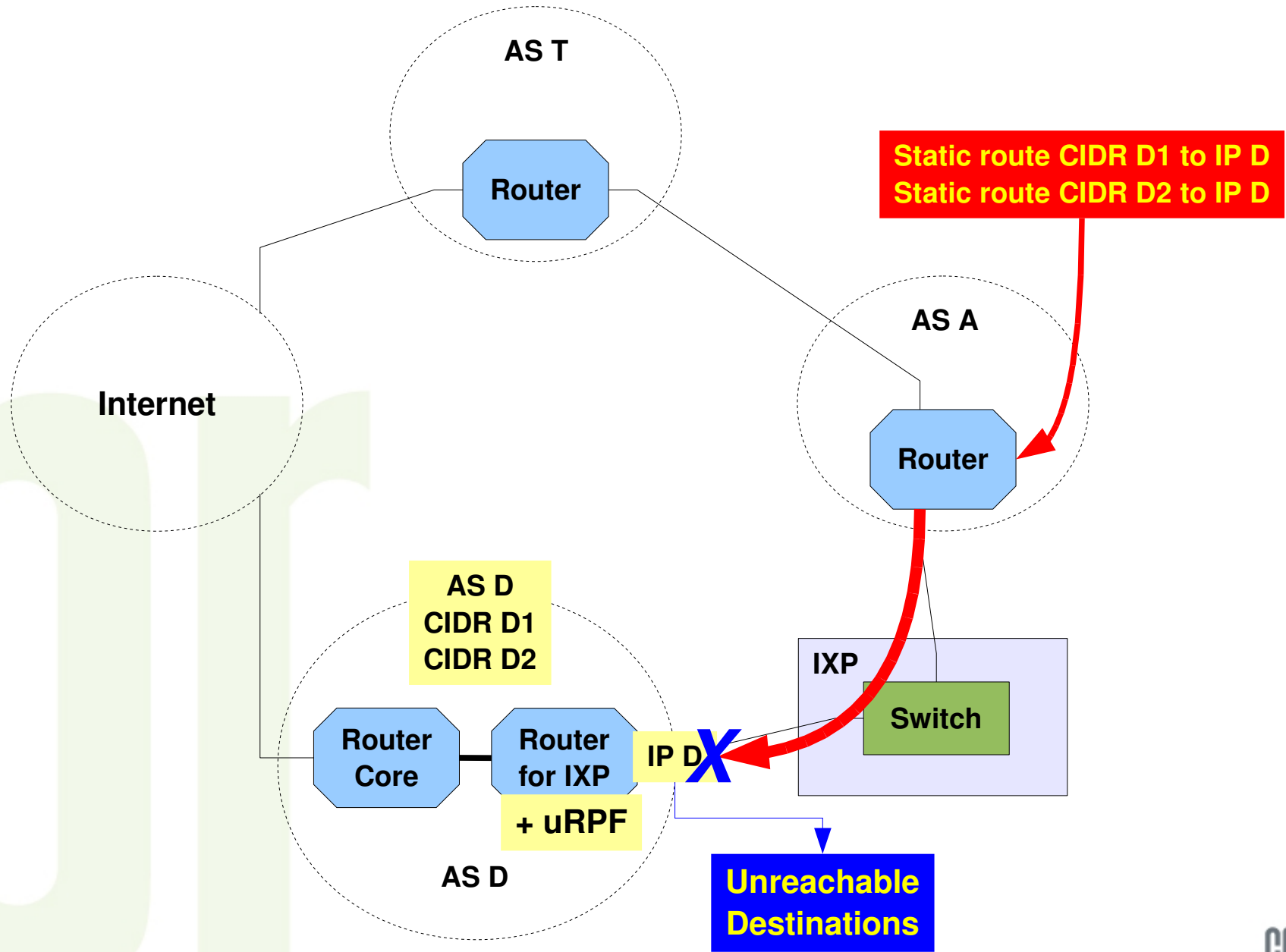






Unicast Reverse Path Forwarding (uRPF)





Thanks

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