Internet Blocking: Part I – A Technical Review

Prof. Dr. Burkhard Stiller, Dr. Thomas Bocek
Communication Systems Group CSG, Department of Informatics IfI
University of Zürich UZH
[stiller¦bocek]@ifi.uzh.ch

in collaboration with ***Prof. Dr. Florent Thouvenin, Kento Reutimann***
Rechtswissenschaftliches Institut der UZH
Lehrstuhl für Informations- und Kommunikationsrecht

Universität Zürich[UZH]

The Internet 1

Blocking and Bypassing 2

Conclusions 3

CSG Communication Systems Group

© 2016 UZH, CSG@IfI

ifi

The Internet – Key Components

- Hosts
  - Wired end-systems

© 2016 UZH, CSG@IfI

The Internet – Key Components

- Hosts
  - Wired end-systems
  - Wireless devices

© 2016 UZH, CSG@IfI

The Internet – Key Components

- Hosts
  - Wired end-systems
  - Wireless devices

- Router
  - Private intermediate systems

The Internet – Key Components

- Hosts
  - Wired end-systems
  - Wireless devices

- Router
  - Private intermediate systems
  - Provider intermediate systems

The Internet – Key Components

- Hosts
  - Wired end-systems
  - Wireless devices

- Router
  - Private intermediate systems
  - Provider intermediate systems

- Links
  - Access

The Internet – Key Components

- Hosts
  - Wired end-systems
  - Wireless devices

- Router
  - Private intermediate systems
  - Provider intermediate systems

- Links
  - Access
  - Radio

© 2016 UZH, CSG@IfI

The Internet – Key Components

- Hosts
  - Wired end-systems
  - Wireless devices

- Router
  - Private intermediate systems
  - Provider intermediate systems

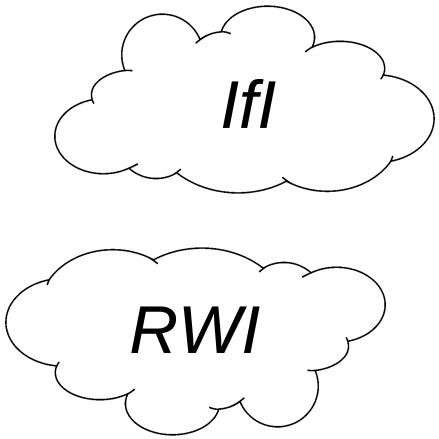
- Links
  - Access
  - Radio
  - Backbone

© 2016 UZH, CSG@IfI

The Internet – Main Structure

Simplified View

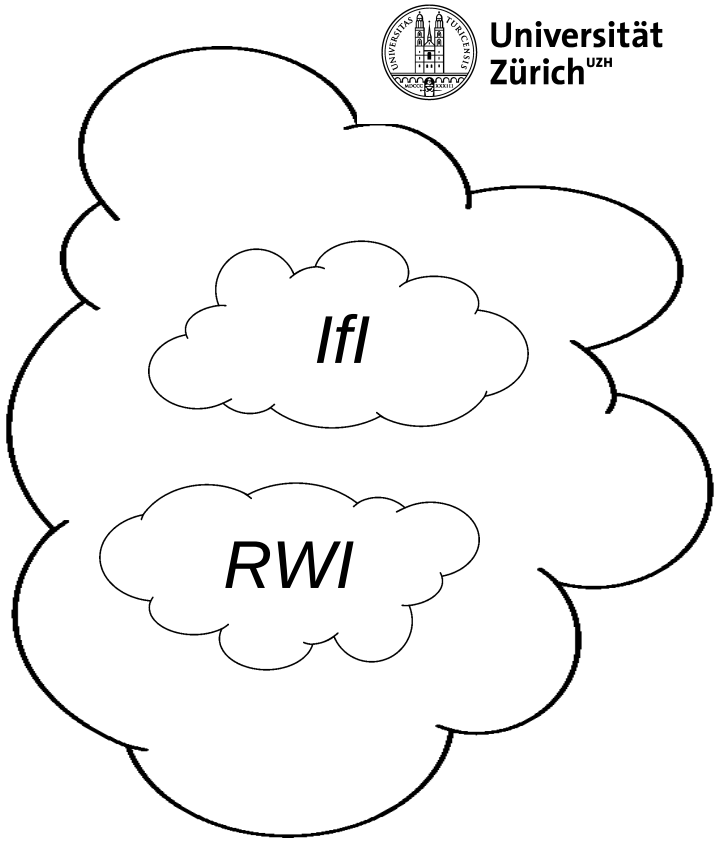
- A network of networks, consisting of subnetworks



The Internet – Main Structure

Simplified View

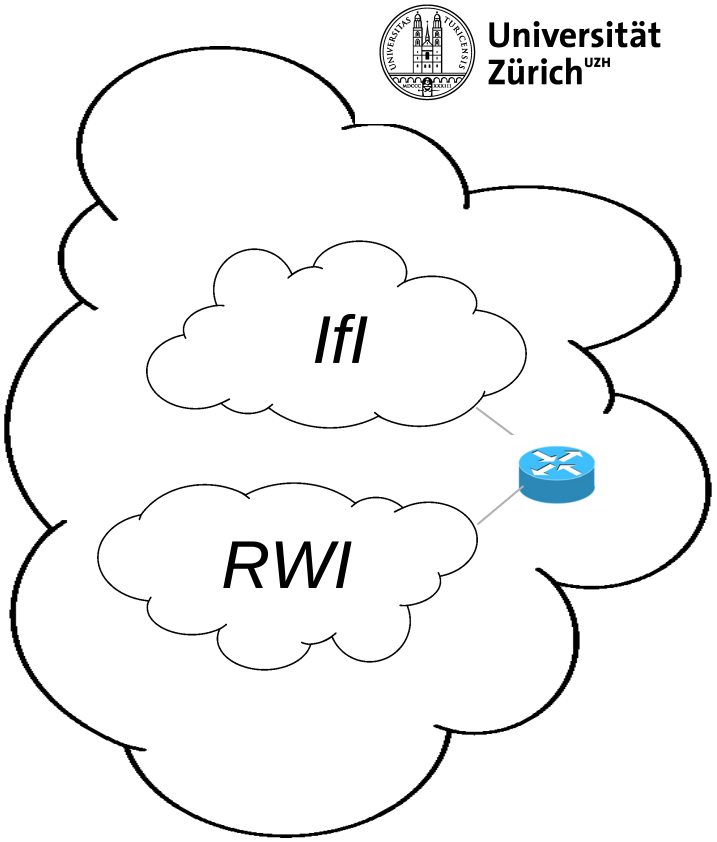
- A network of networks, consisting of subnetworks



The Internet – Main Structure

Simplified View

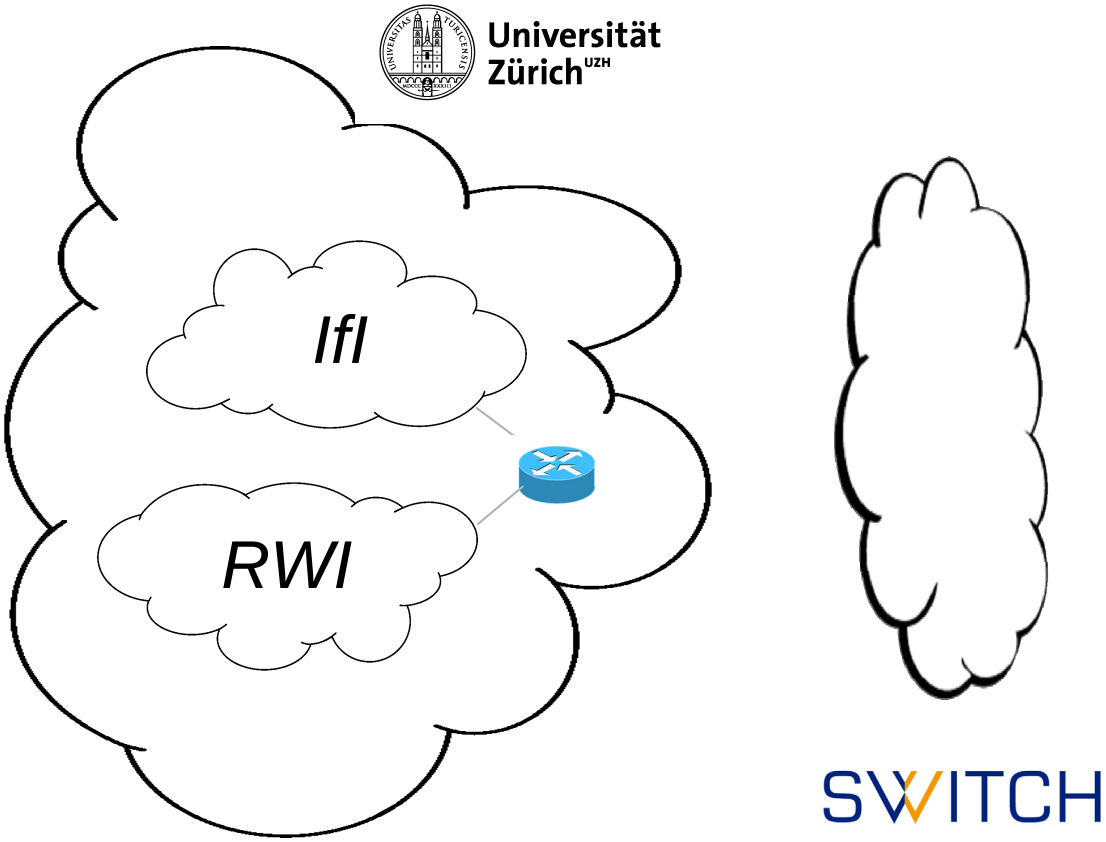
- A network of networks, consisting of subnetworks



The Internet – Main Structure

Simplified View

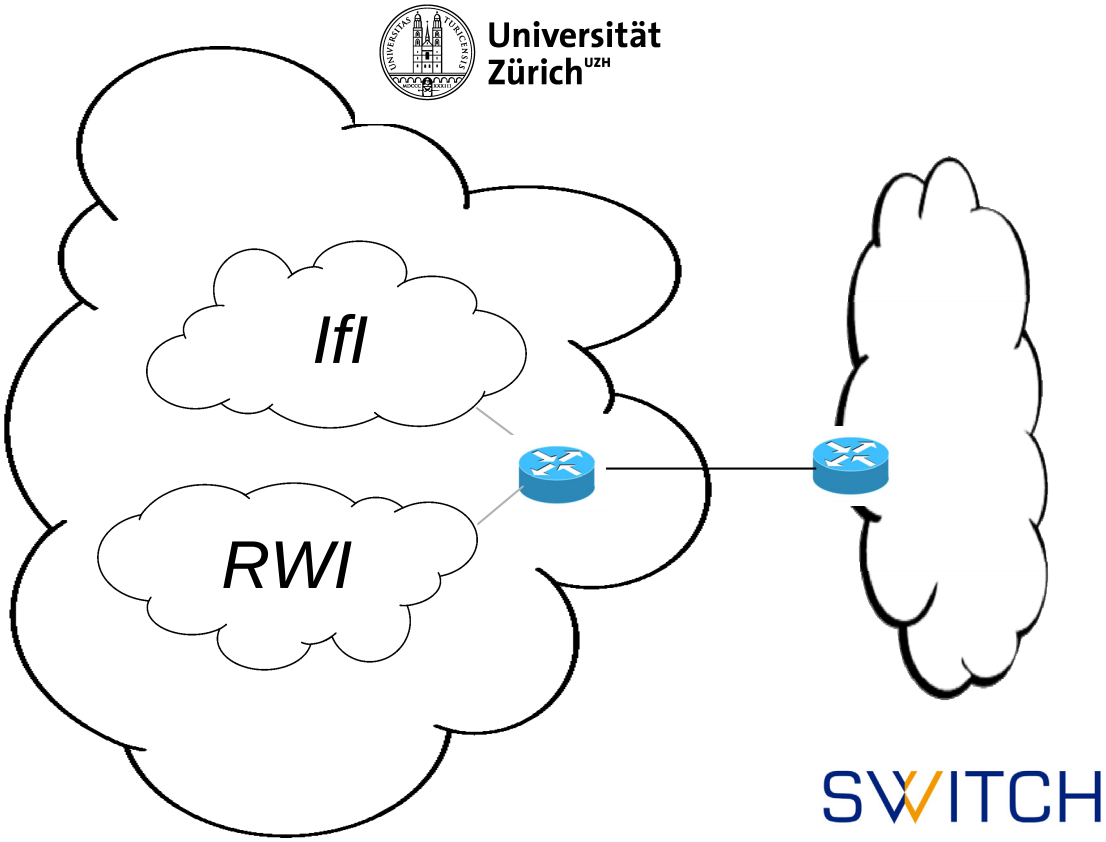
- A network of networks, consisting of subnetworks



The Internet – Main Structure

Simplified View

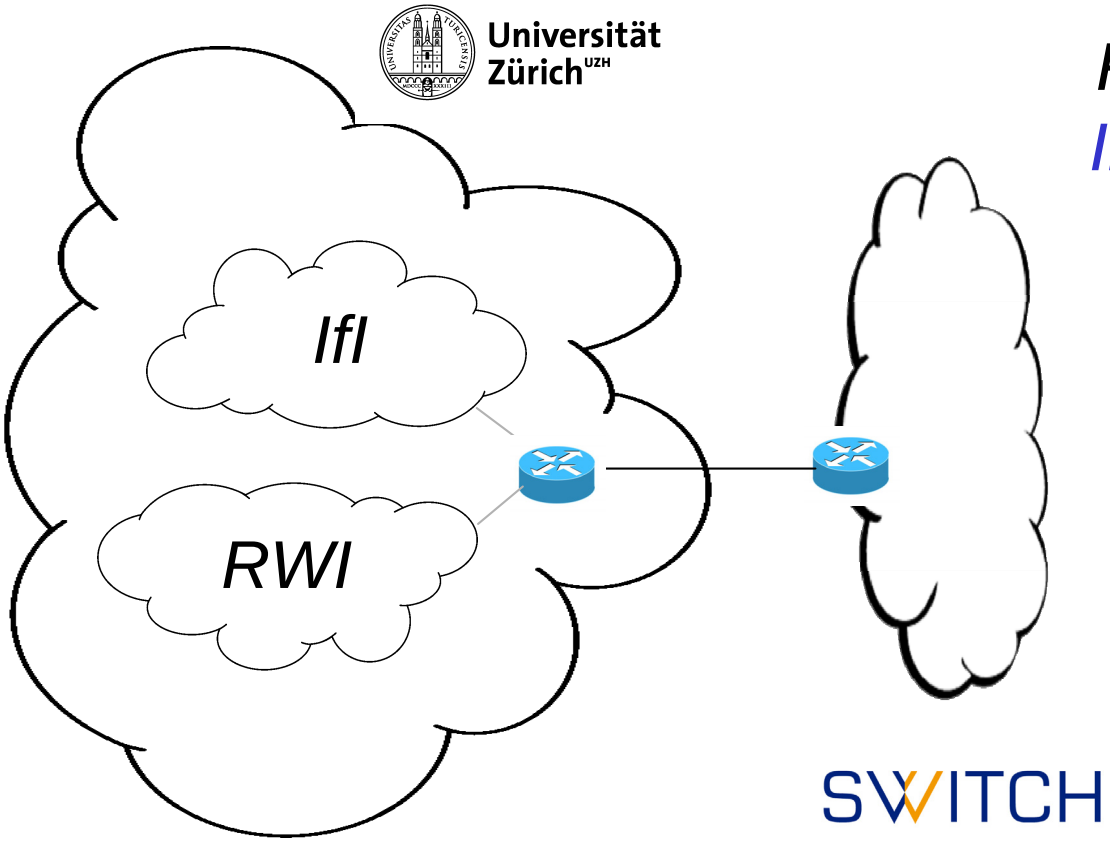
- A network of networks, consisting of subnetworks



The Internet – Main Structure

Simplified View

- A network of networks, consisting of subnetworks

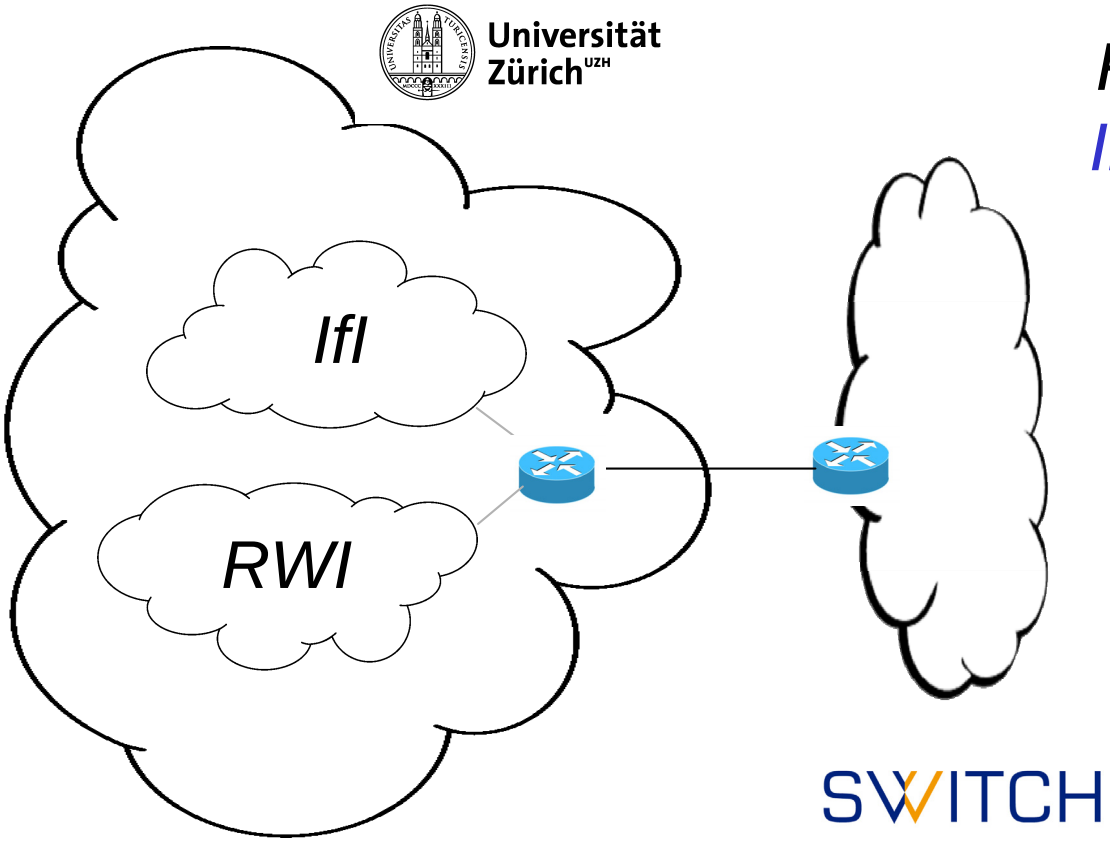


Regional, national, world-wide
Internet Service Provider (ISP)

The Internet – Main Structure

Simplified View

- A network of networks, consisting of subnetworks

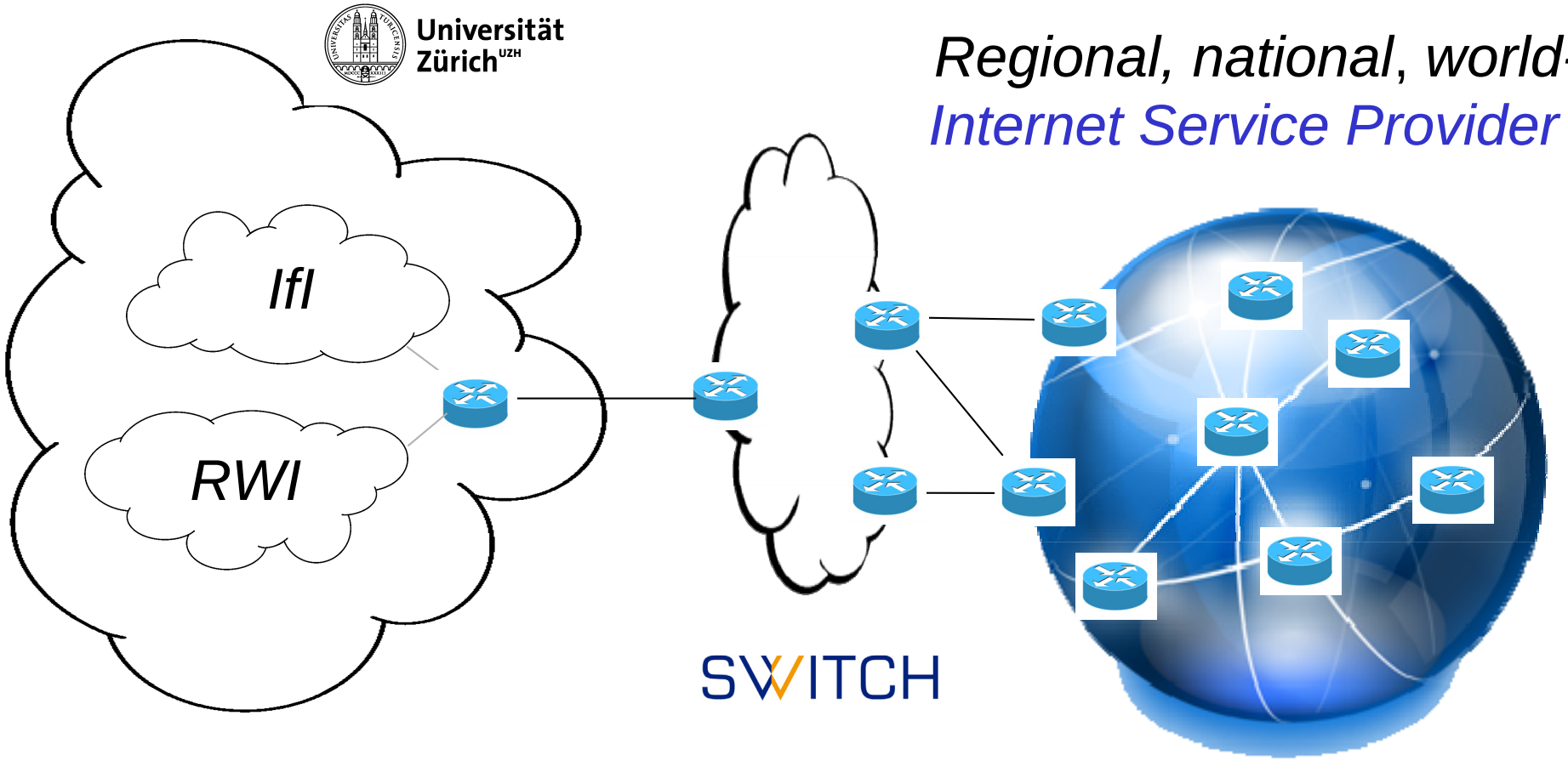


Regional, national, world-wide
Internet Service Provider (ISP)

The Internet – Main Structure

Simplified View

- A network of networks, consisting of subnetworks

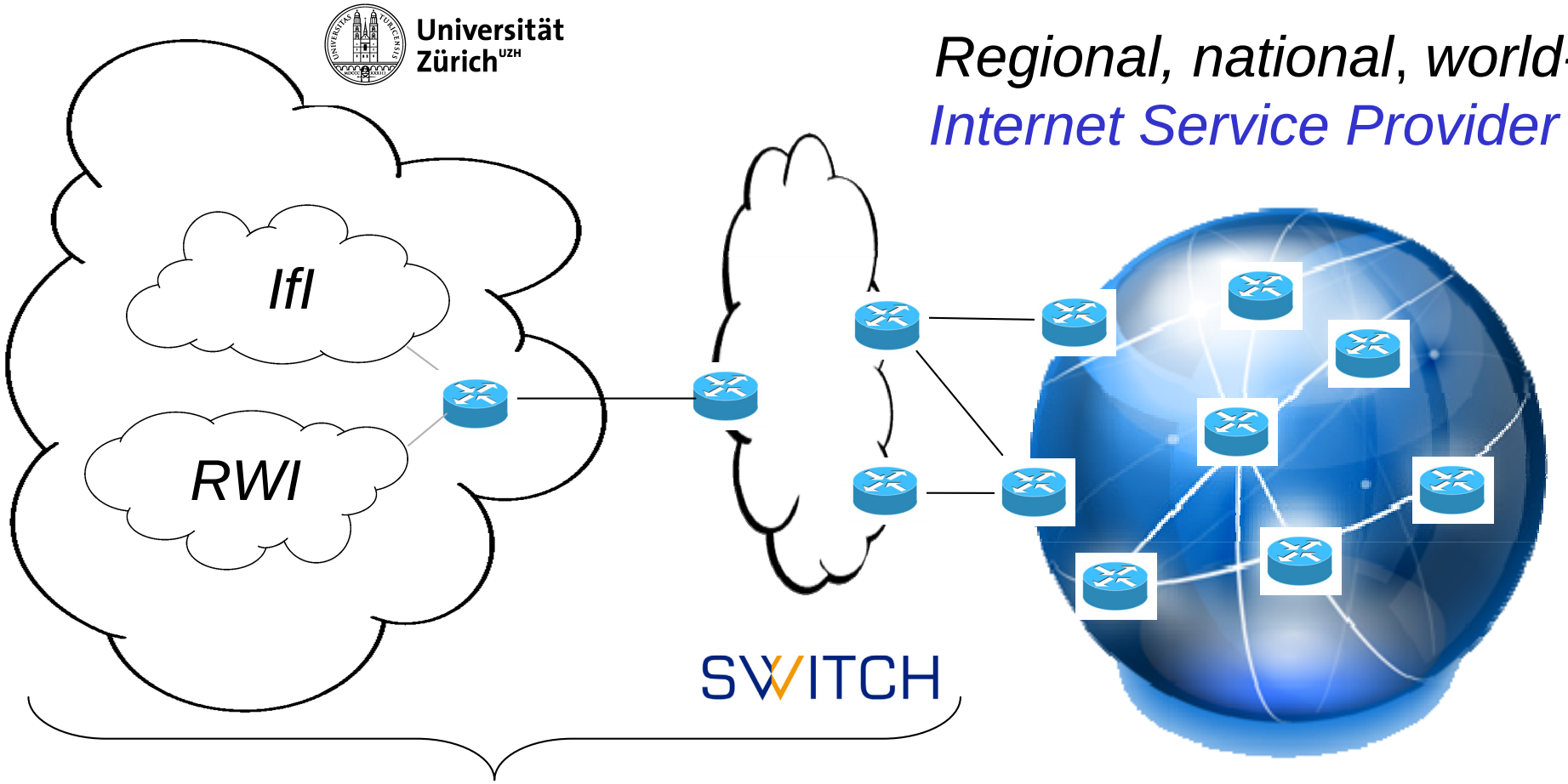


Regional, national, world-wide
Internet Service Provider (ISP)

The Internet – Main Structure

Simplified View

- A network of networks, consisting of subnetworks



Regional, national, world-wide
Internet Service Provider (ISP)

Autonomous System (AS) with ID AS559

© 2016 UZH, CSG@IfI

Addresses and Names

- IP (Internet Protocol) addresses identify hosts & routers
  - Public addresses (example): 130.60.205.7
  - Private addresses (example): 192.168.1.5

© 2016 UZH, CSG@IfI

Addresses and Names

- IP (Internet Protocol) addresses identify hosts & routers
  - Public addresses (example): 130.60.205.7
  - Private addresses (example): 192.168.1.5
- Subnets in same network with common address prefix:
  - Subnetworks: 130.60.0.0/16 (SWITCH's UNIZH assignment)

Addresses and Names

- IP (Internet Protocol) addresses identify hosts & routers
  - Public addresses (example): 130.60.205.7
  - Private addresses (example): 192.168.1.5
- Subnets in same network with common address prefix:
  - Subnetworks: 130.60.0.0/16 (SWITCH's UNIZH assignment)
- Domain names are human-readable identifiers
  - Example: ns1.uzh.ch (for 130.60.205.7) UZH's Name Server 1

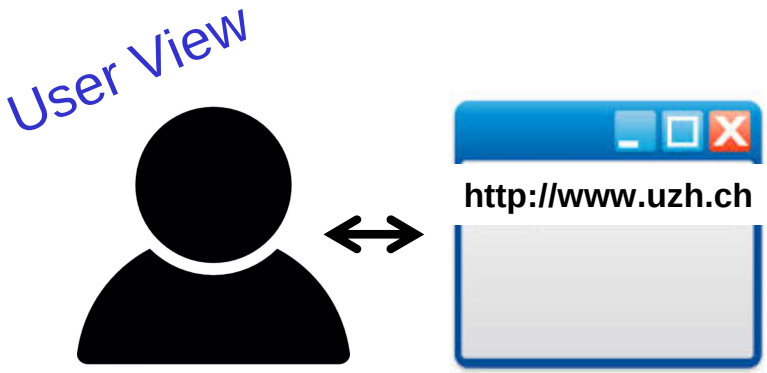
Addresses and Names

- IP (Internet Protocol) addresses identify hosts & routers
  - Public addresses (example): 130.60.205.7
  - Private addresses (example): 192.168.1.5
- Subnets in same network with common address prefix:
  - Subnetworks: 130.60.0.0/16 (SWITCH's UNIZH assignment)

- Domain names are human-readable identifiers
  - Example: ns1.uzh.ch (for 130.60.205.7) UZH's Name Server 1
- Domain Name System (DNS) hierarchically organizes world-wide and assigns locally names to IP addresses
  - ".ch" Swiss Name Registrar; ".uzh" UZH; "ns1" local machine

© 2016 UZH, CSG@IfI

Accessing Information/Services



Uniform Resource Locator (URL)

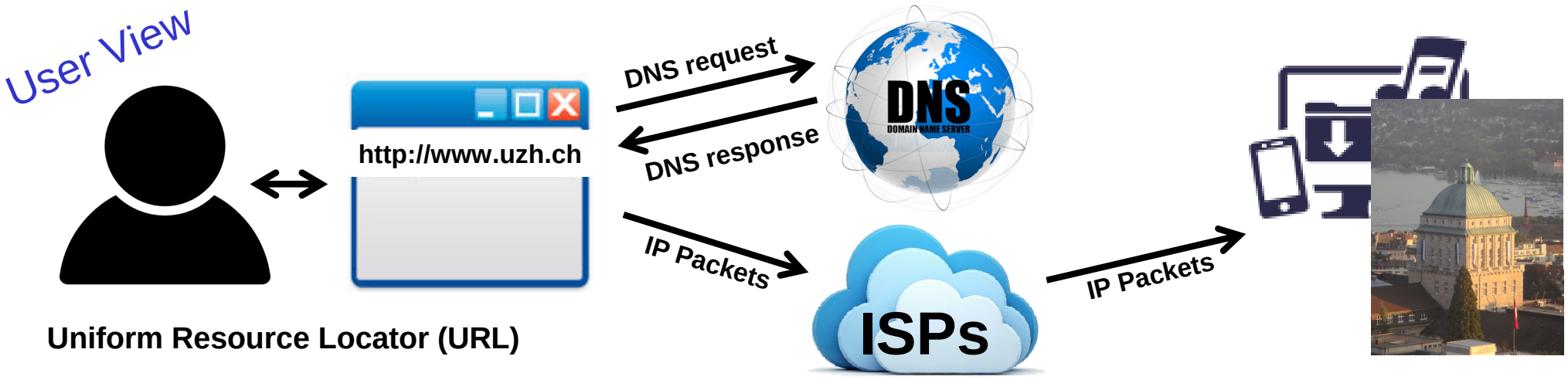
Accessing Information/Services

Uniform Resource Locator (URL)

Accessing Information/Services

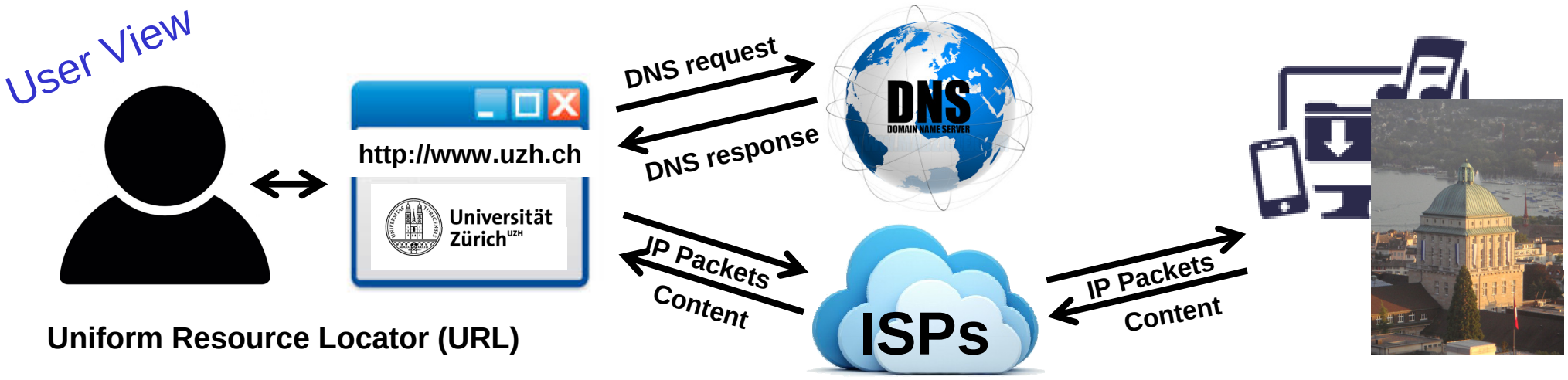
Uniform Resource Locator (URL)

Accessing Information/Services



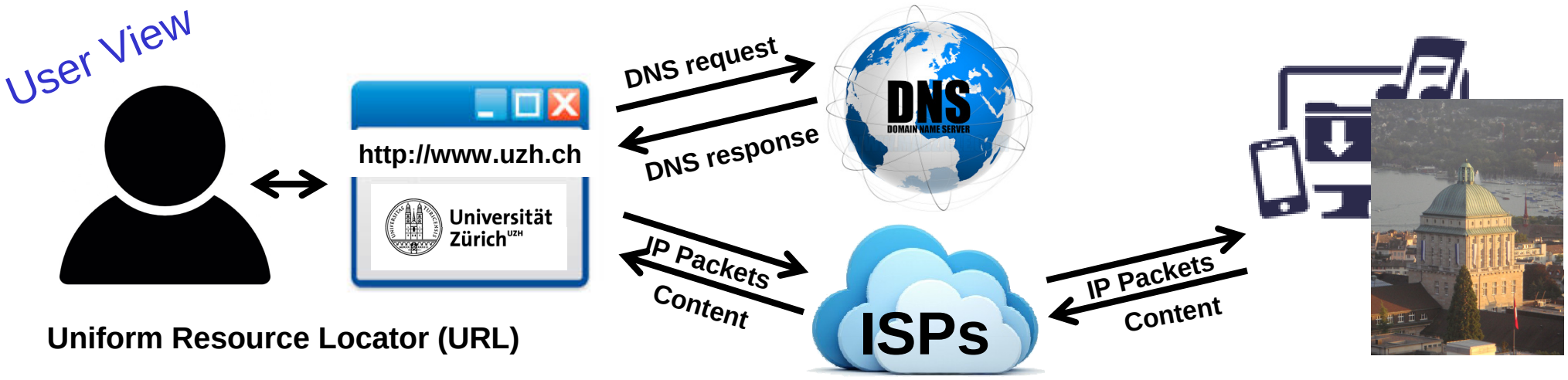
Uniform Resource Locator (URL)

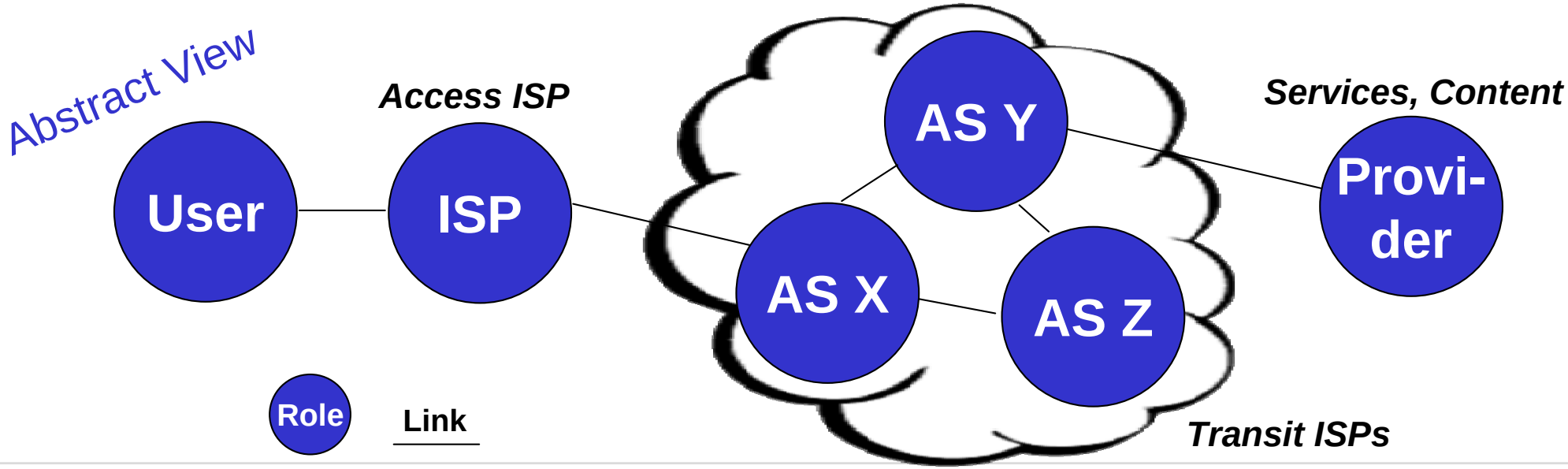
Accessing Information/Services



Uniform Resource Locator (URL)

Accessing Information/Services

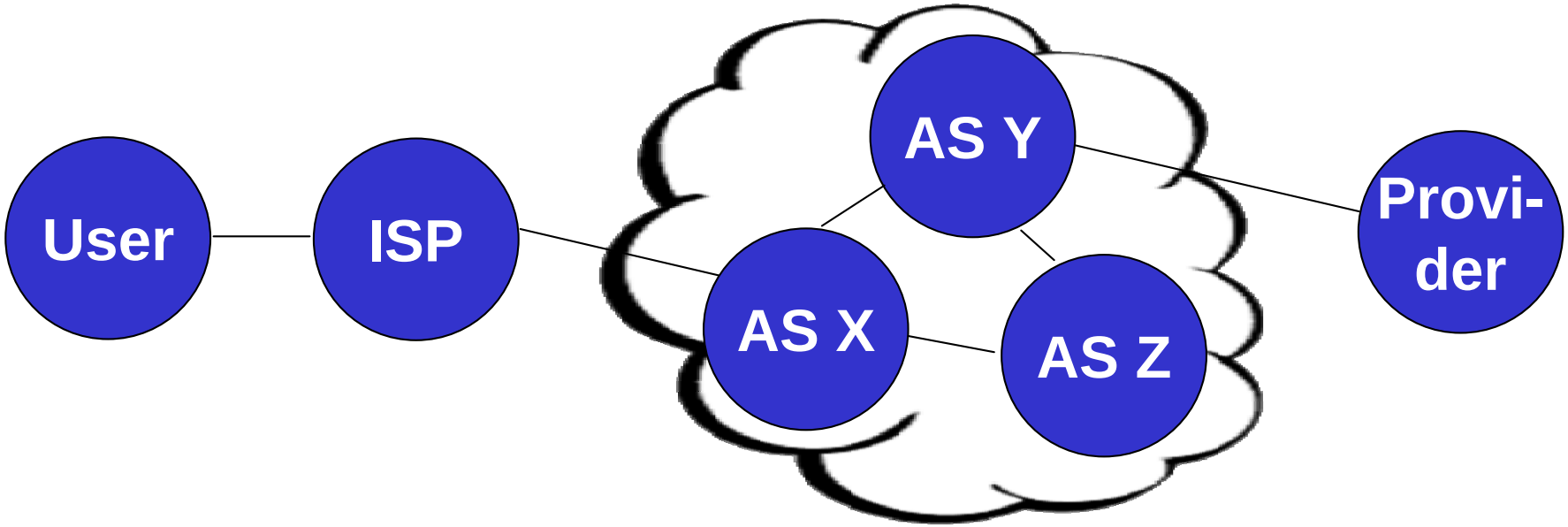




© 2016 UZH, CSG@IfI

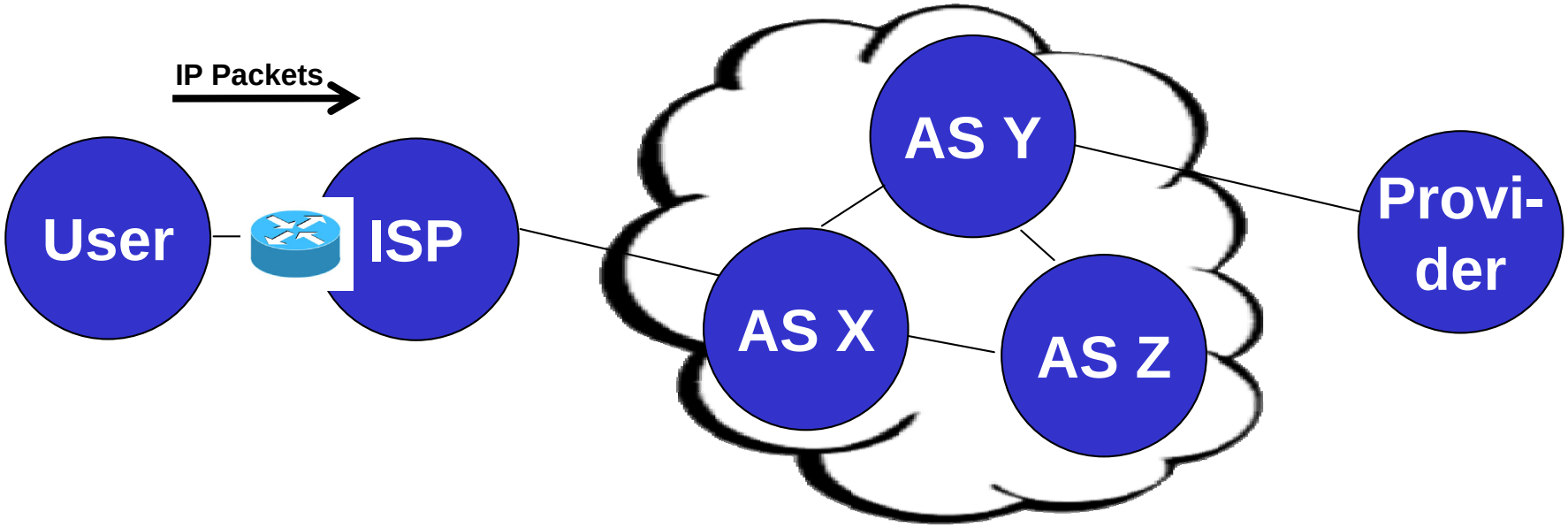
Blocking and Bypassing

ISP-based IP Address Blocking



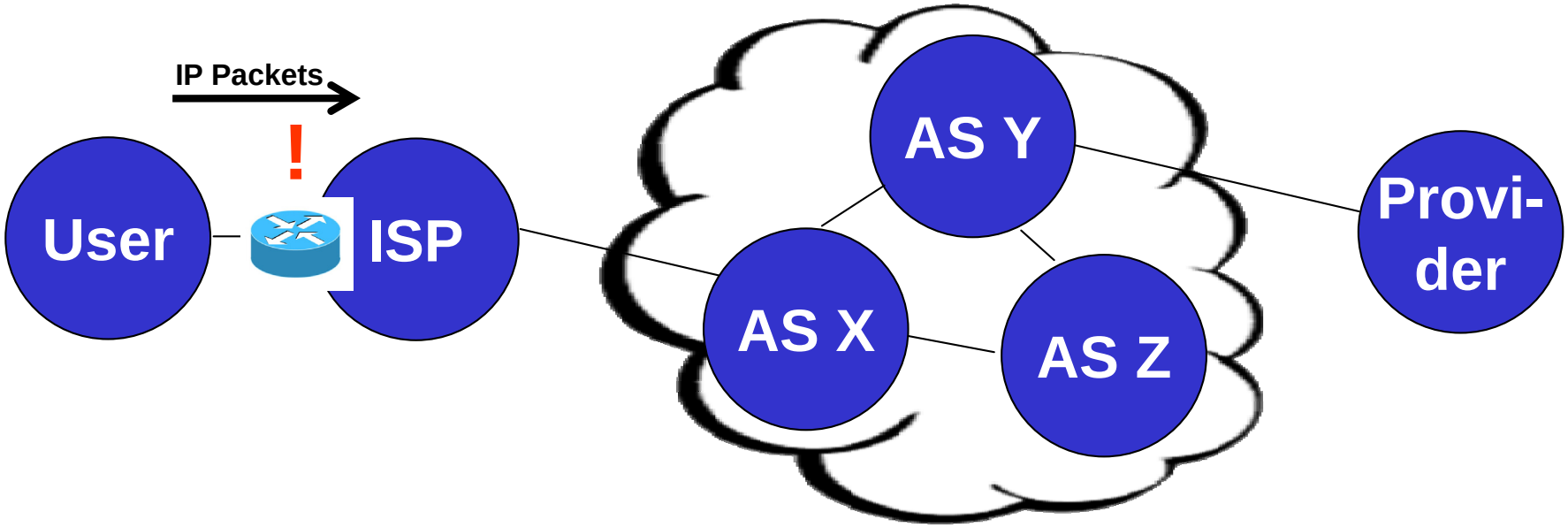
© 2016 UZH, CSG@IfI

ISP-based IP Address Blocking



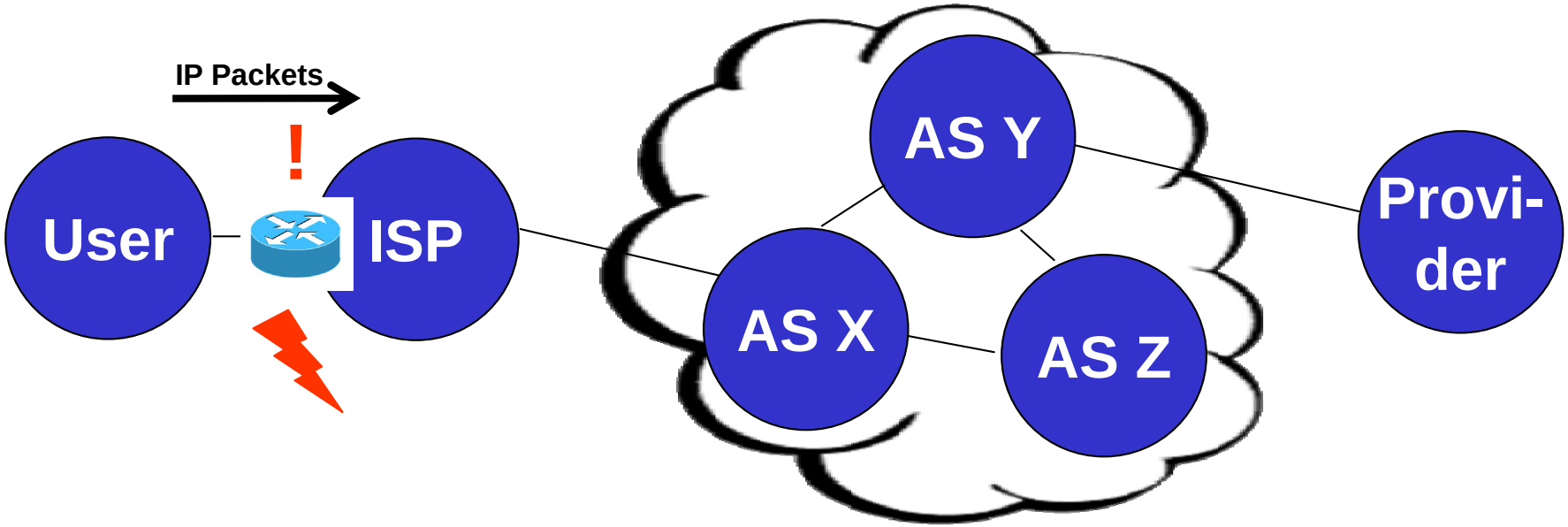
- Upon sending IP packets, at one ISP's router

ISP-based IP Address Blocking



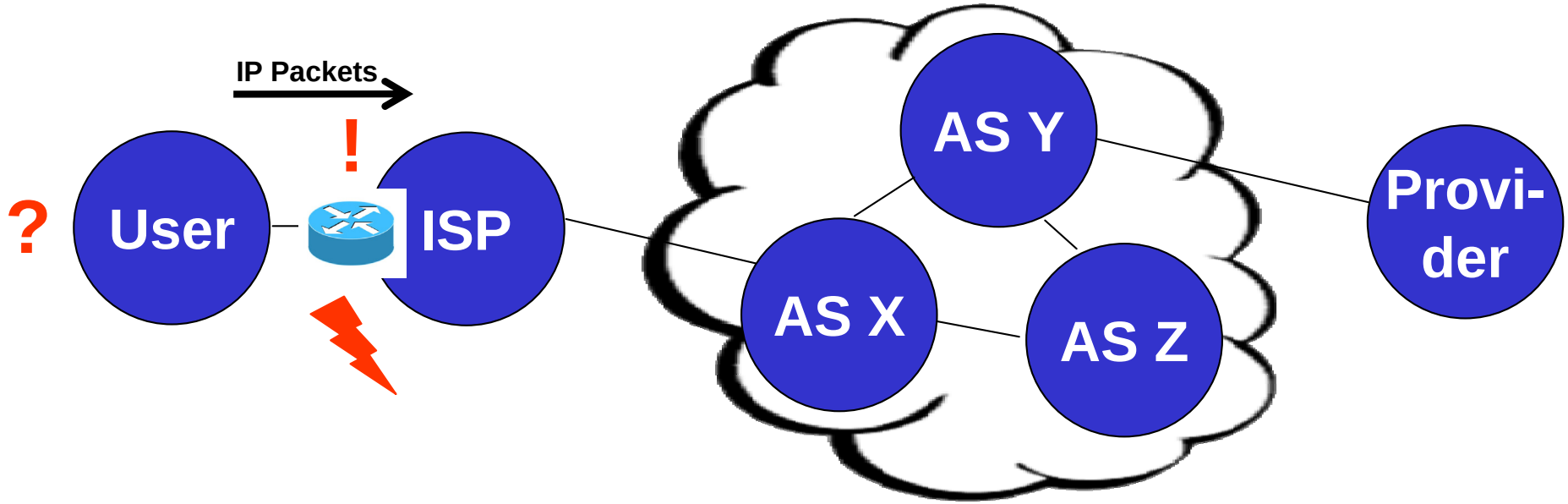
- Upon sending IP packets, at one ISP's router
  - User's IP packet address recognized at ISP to be blocked

ISP-based IP Address Blocking



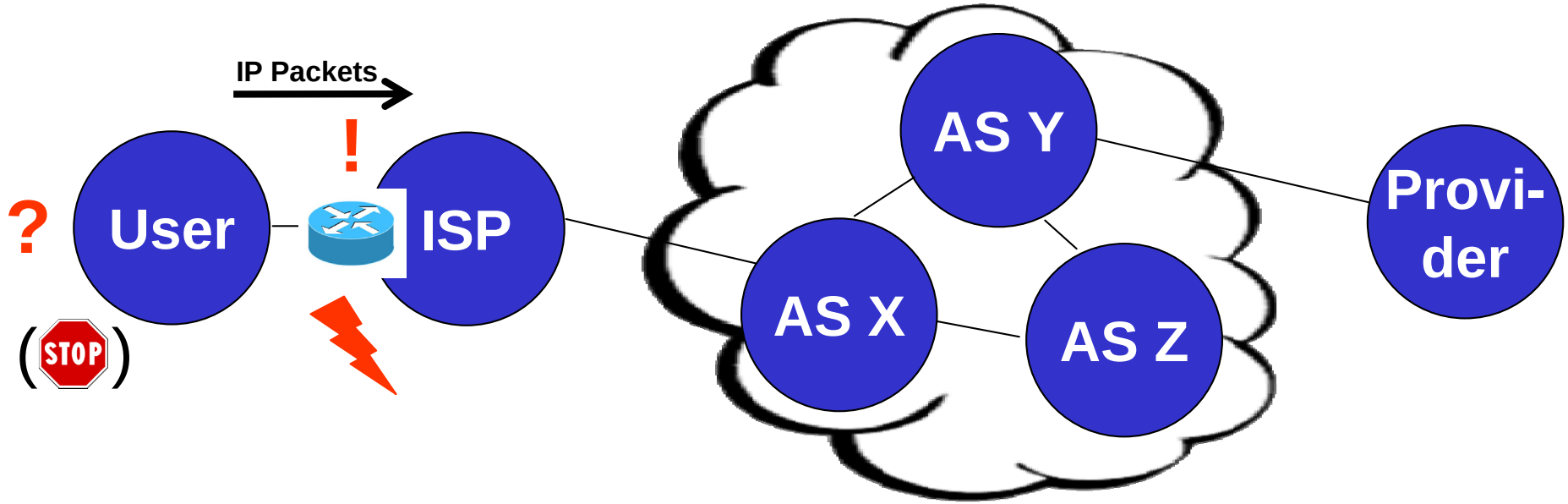
- Upon sending IP packets, at one ISP's router
  - User's IP packet address recognized at ISP to be blocked
  - IP packet with blocked IP address discarded or re-routed

ISP-based IP Address Blocking



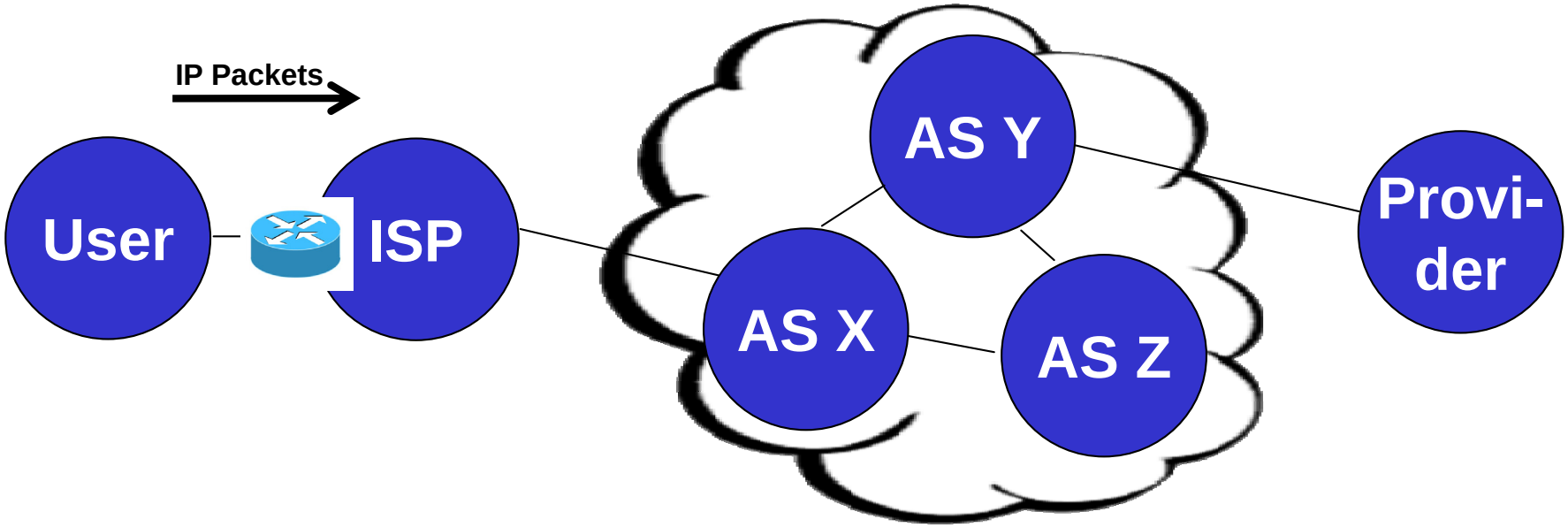
- Upon sending IP packets, at one ISP's router
  - User's IP packet address recognized at ISP to be blocked
  - IP packet with blocked IP address discarded or re-routed
  - Typically no information of user

ISP-based IP Address Blocking



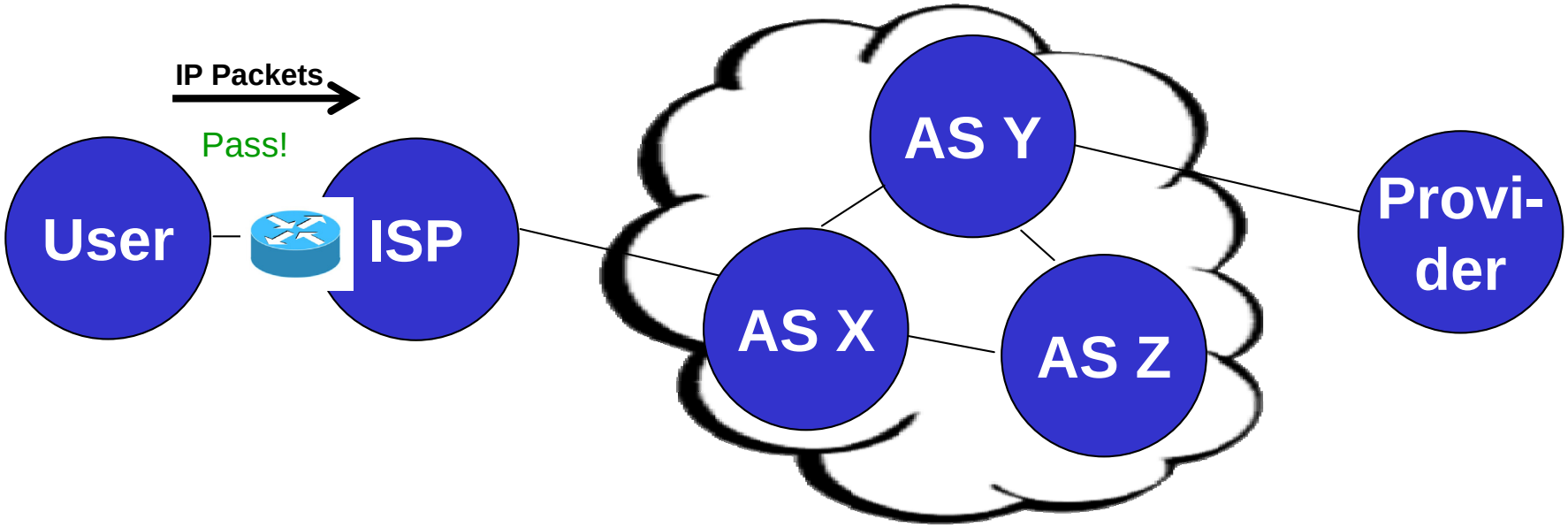
- Upon sending IP packets, at one ISP's router
  - User's IP packet address recognized at ISP to be blocked
  - IP packet with blocked IP address discarded or re-routed
  - Typically no information of user
  - "Stop Page" display to user technically feasible
    - Large effort for ISPs (IP vs. Browser traffic)

Bypassing ISP-based IP Address Checks



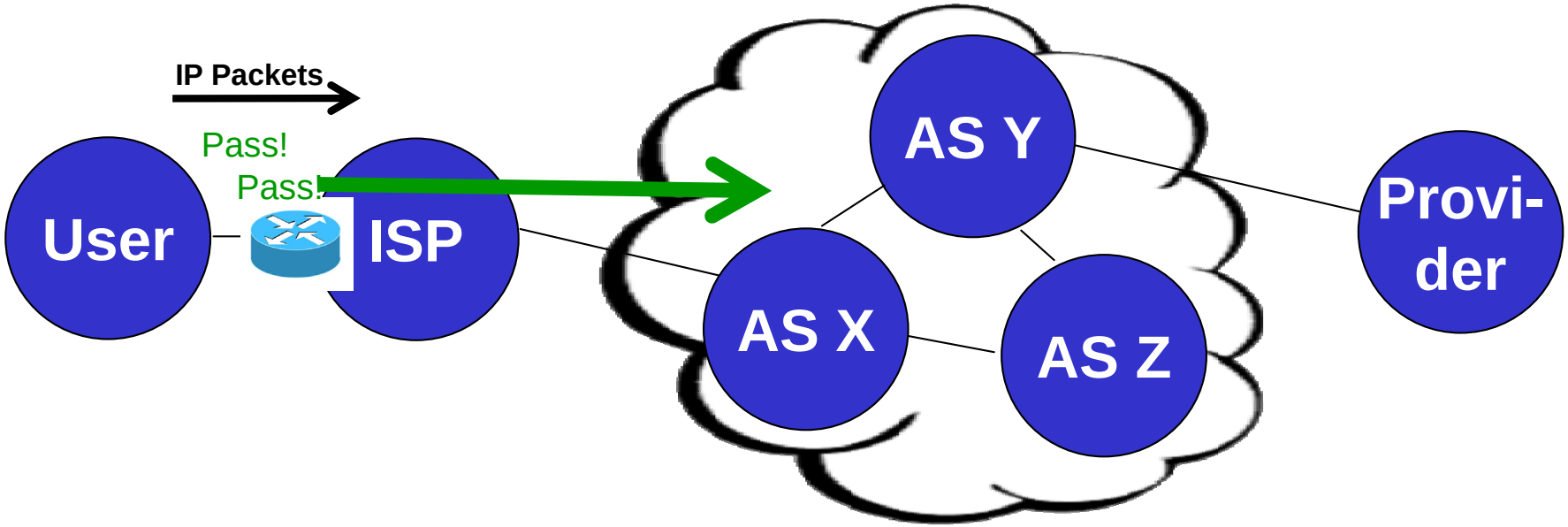
- Technical options to hide original destination IP from ISP

Bypassing ISP-based IP Address Checks



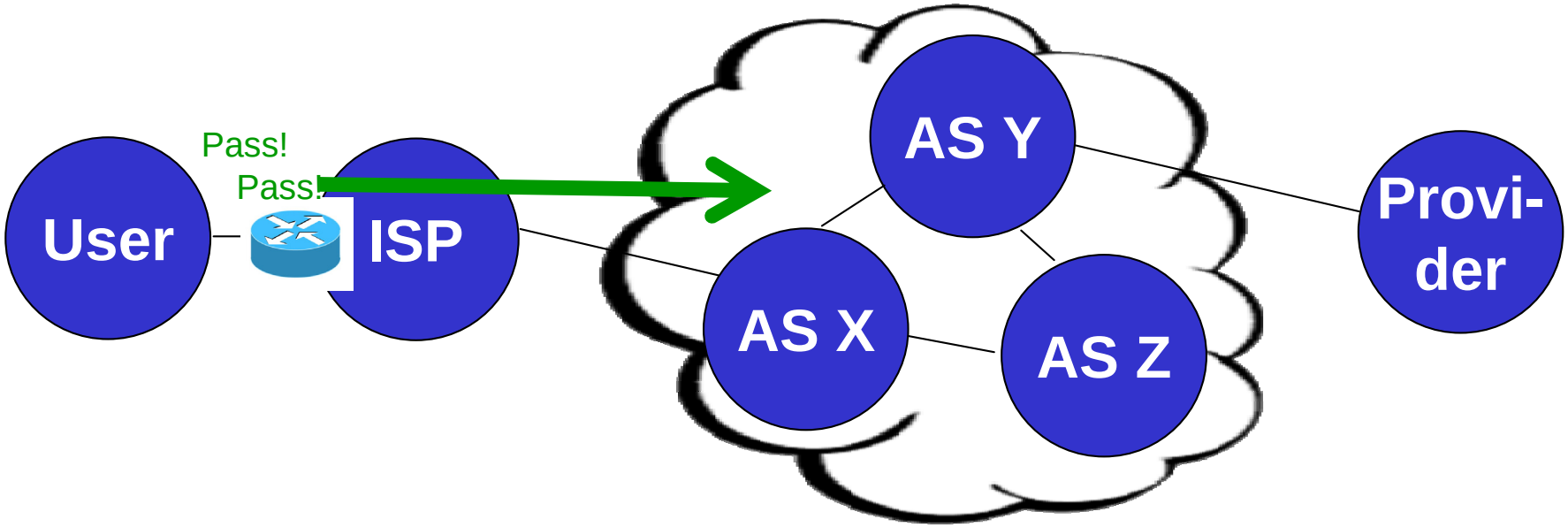
- Technical options to hide original destination IP from ISP
  - Anonymization of user traffic, *e.g.*, via Tor

Bypassing ISP-based IP Address Checks



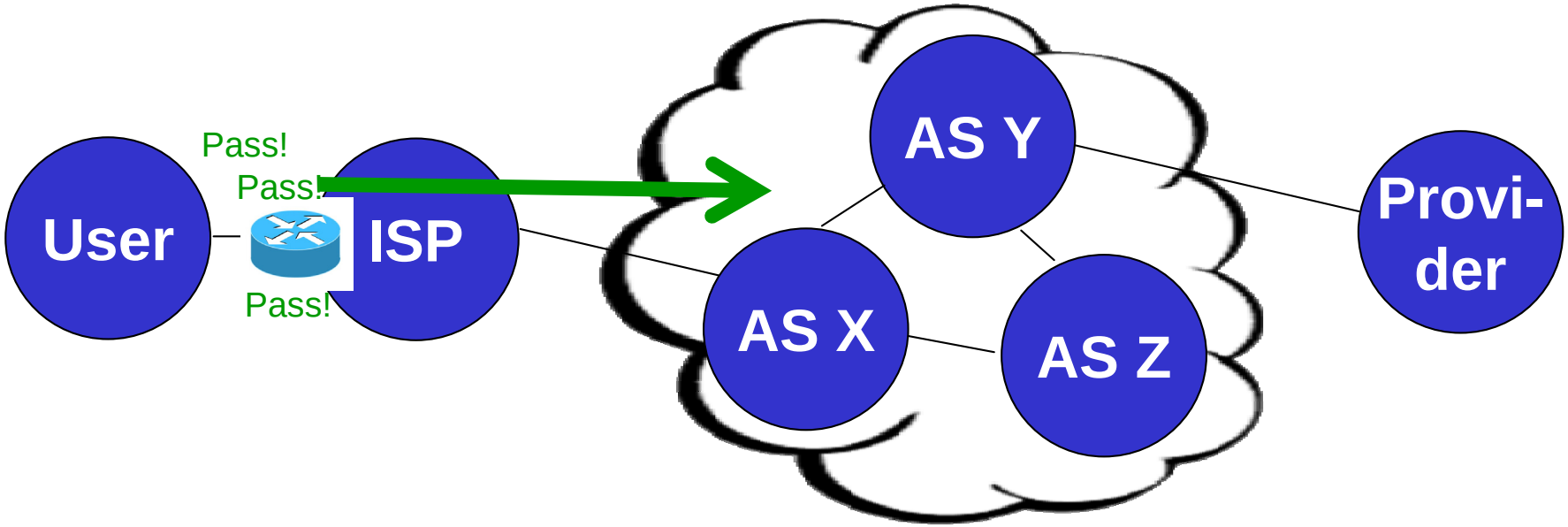
- Technical options to hide original destination IP from ISP
  - Anonymization of user traffic, *e.g.*, via Tor
  - Virtual Private Network (VPN)

Bypassing ISP-based IP Address Checks



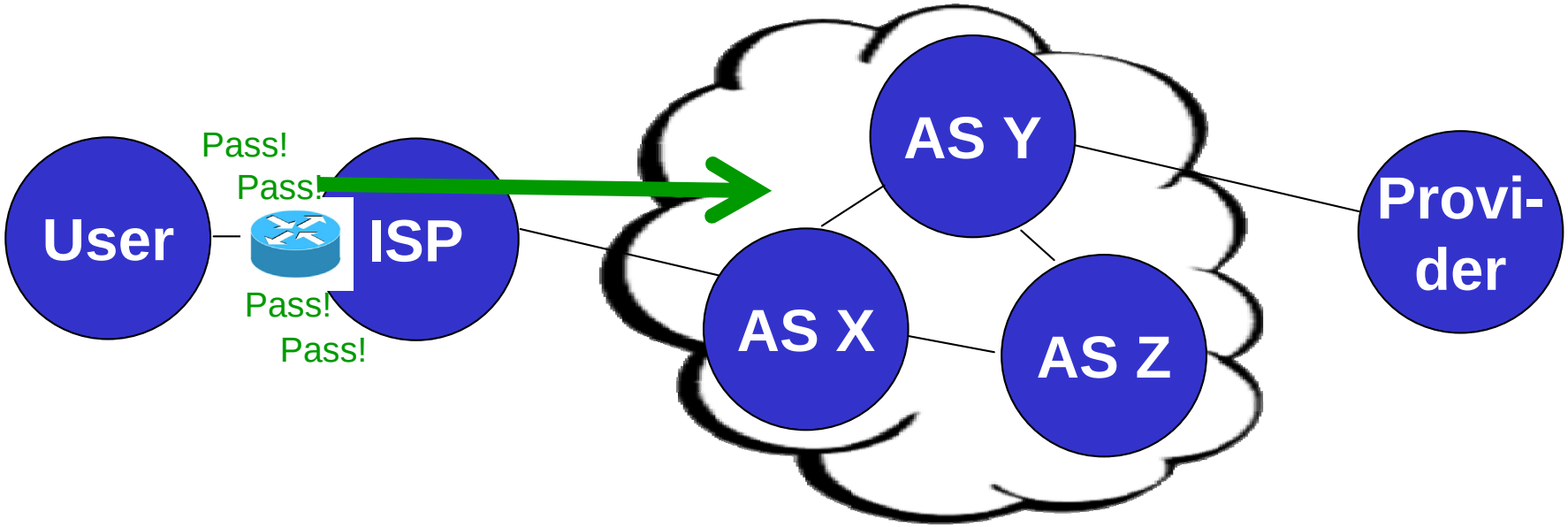
- Technical options to hide original destination IP from ISP
  - Anonymization of user traffic, *e.g.*, via Tor
  - Virtual Private Network (VPN)

Bypassing ISP-based IP Address Checks



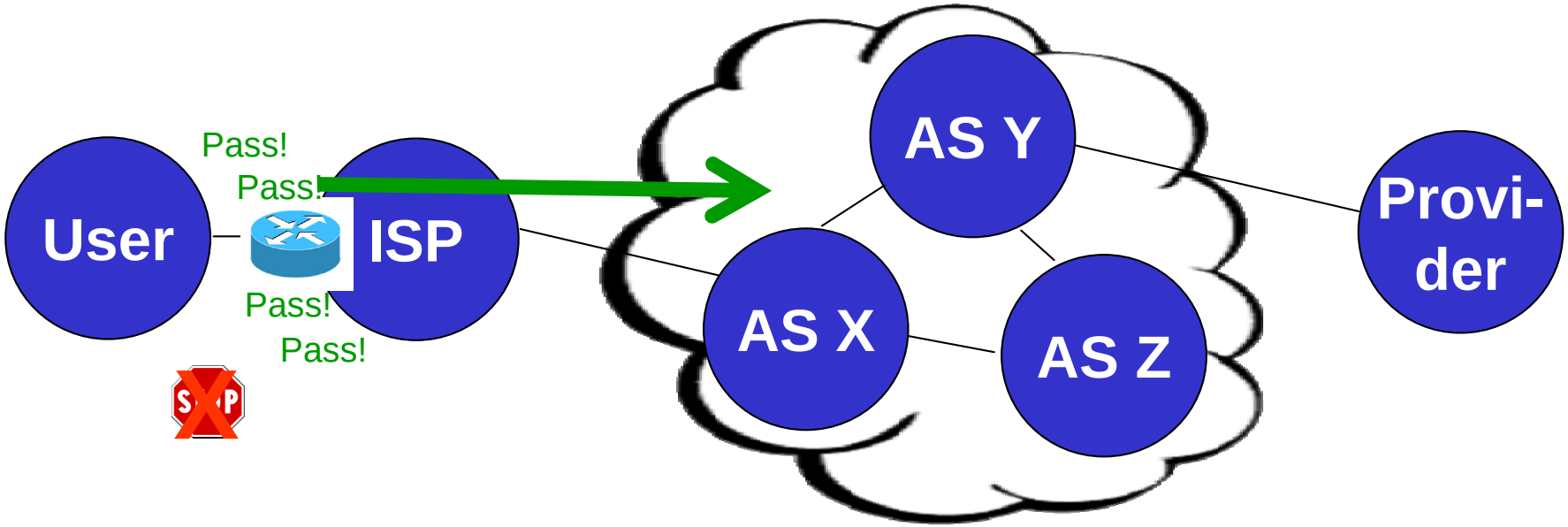
- Technical options to hide original destination IP from ISP
  - Anonymization of user traffic, *e.g.*, via Tor
  - Virtual Private Network (VPN)
  - Web Real-Time Communication (WebRTC)

Bypassing ISP-based IP Address Checks



- Technical options to hide original destination IP from ISP
  - Anonymization of user traffic, *e.g.*, via Tor
  - Virtual Private Network (VPN)
  - Web Real-Time Communication (WebRTC)
  - Content Distribution Network (CDN)

Bypassing ISP-based IP Address Checks

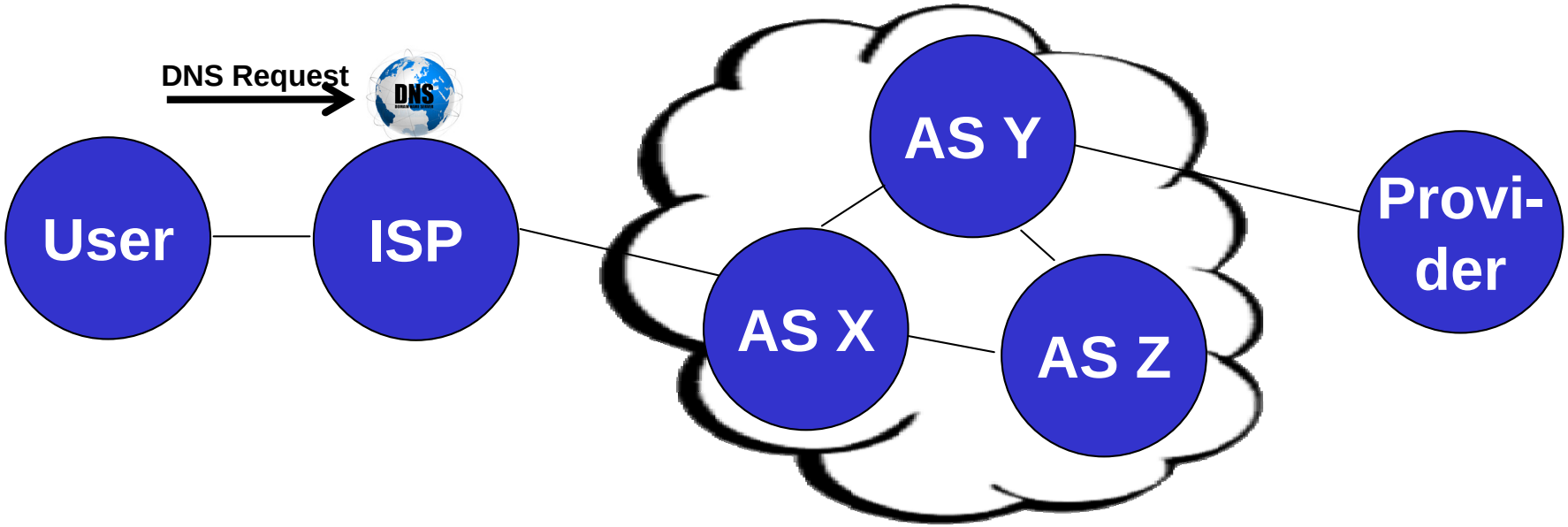


- Technical options to hide original destination IP from ISP
  - Anonymization of user traffic, *e.g.*, via Tor
  - Virtual Private Network (VPN)
  - Web Real-Time Communication (WebRTC)
  - Content Distribution Network (CDN)

→ All traffic NOT detectable by ISP's router, no stopping

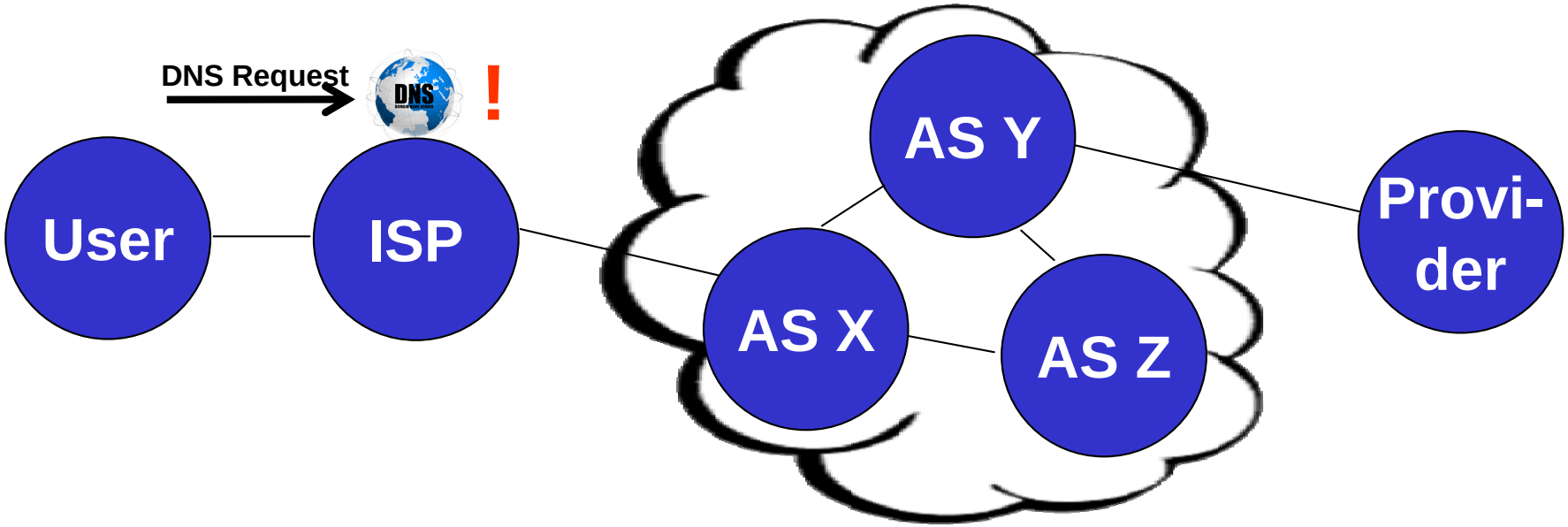
© 2016 UZH, CSG@IfI

ISP-based DNS Blocking



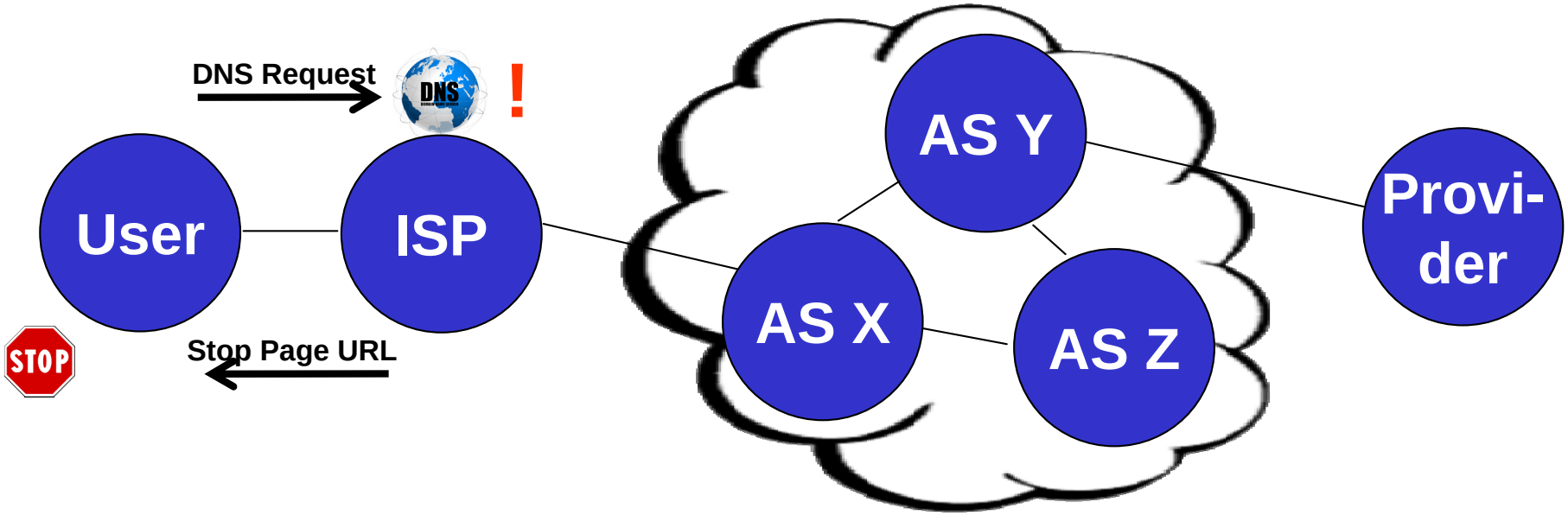
- Upon sending a DNS request, at the ISP's DNS server
  - DNS Hijacking is performed

ISP-based DNS Blocking



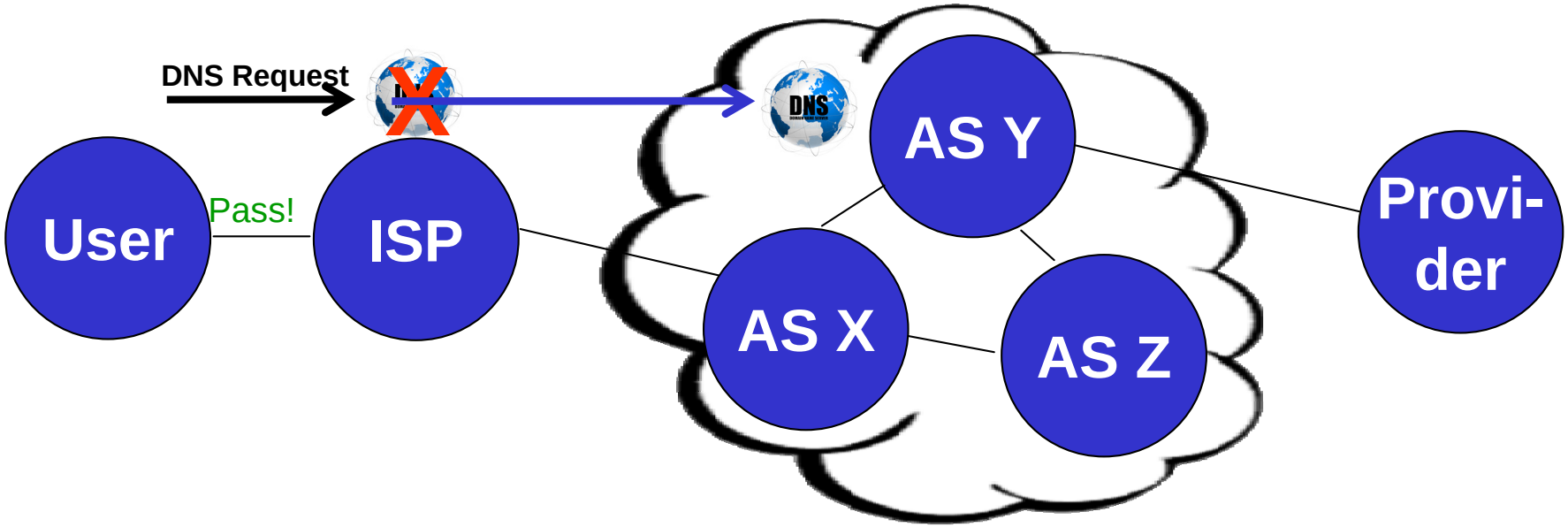
- Upon sending a DNS request, at the ISP's DNS server
  - DNS Hijacking is performed
  - User's DNS request recognized at ISP's DNS to be blocked

ISP-based DNS Blocking



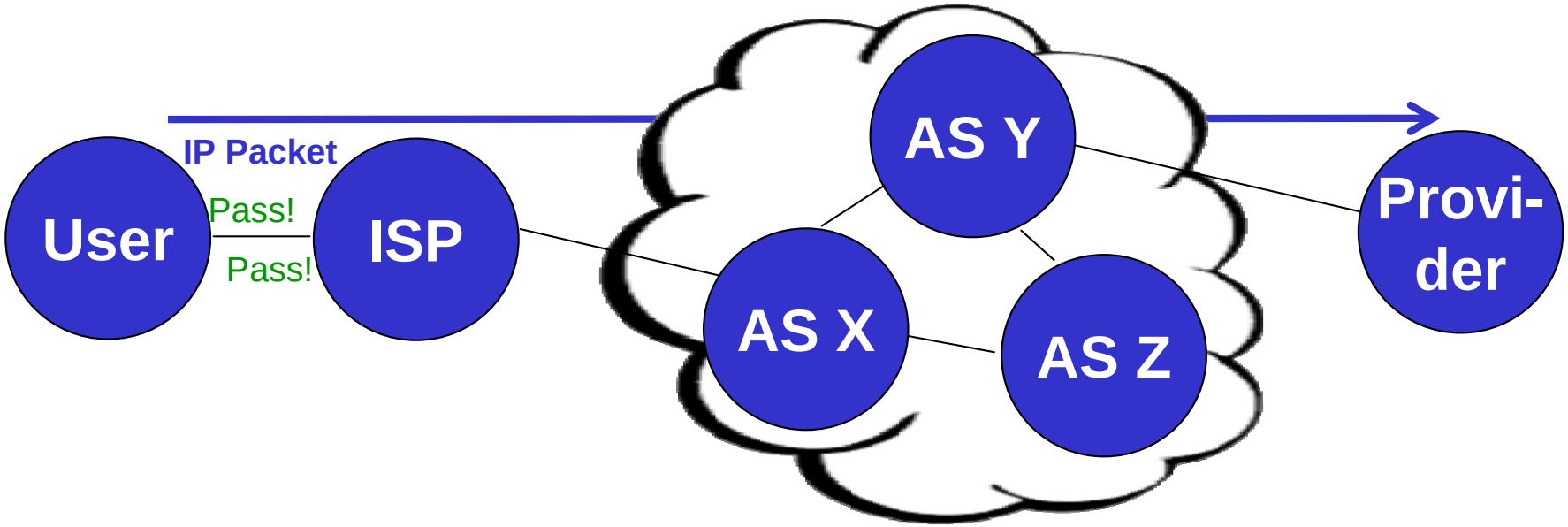
- Upon sending a DNS request, at the ISP's DNS server
  - DNS Hijacking is performed
  - User's DNS request recognized at ISP's DNS to be blocked
  - Resulting in "Stop Page" display to user in Browser
    - Special page hosted at ISP with respective legal advise
    - Less effort for ISPs (DNS request → Browser traffic)

Bypassing ISP-based DNS Blocking



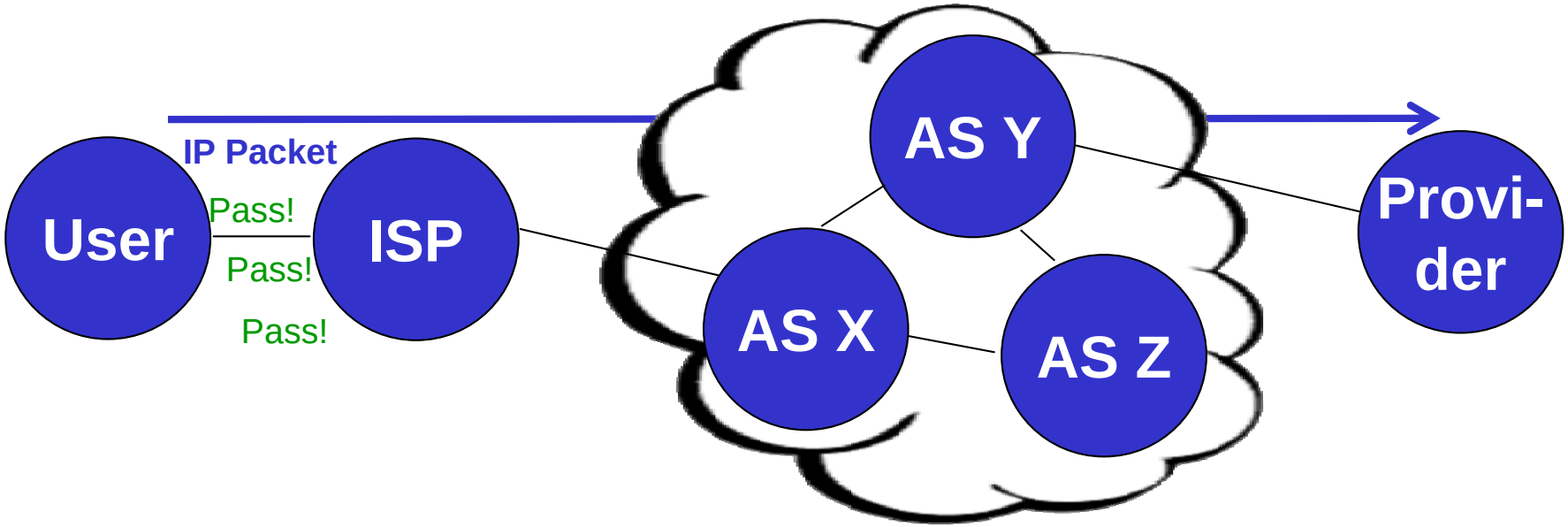
- Upon sending a DNS request
  - User configures and uses a "public" or a root DNS server

Bypassing ISP-based DNS Blocking



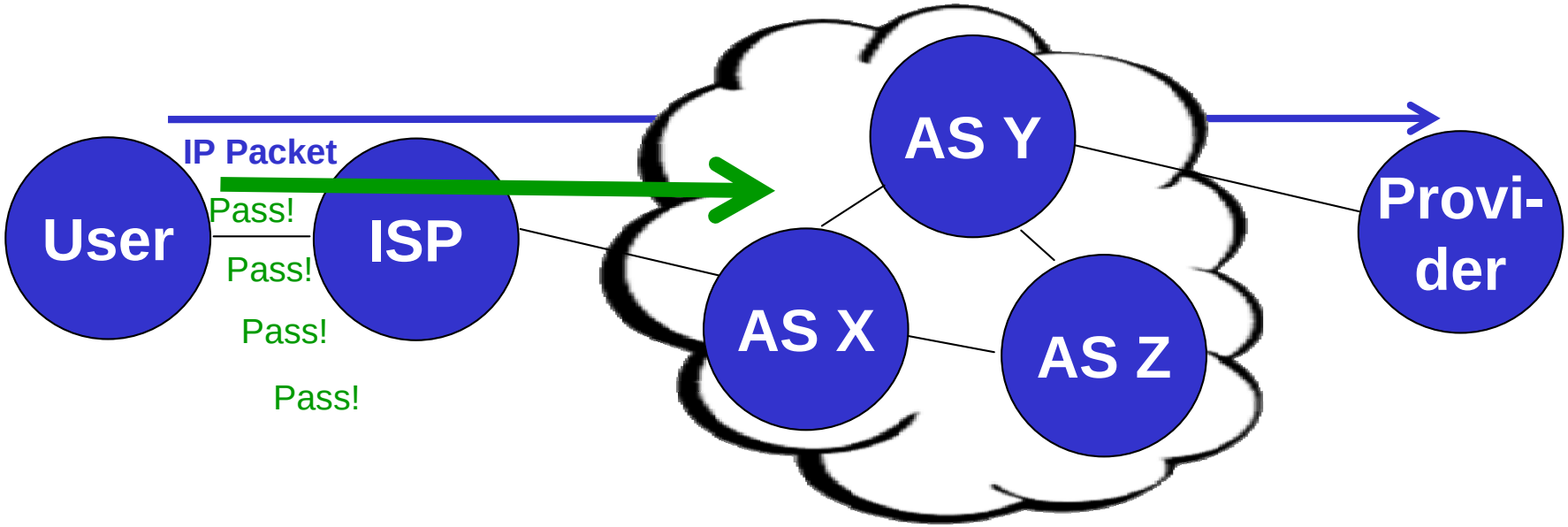
- Upon sending a DNS request
  - User configures and uses a "public" or a root DNS server
  - User applies known IP address of provider directly

Bypassing ISP-based DNS Blocking



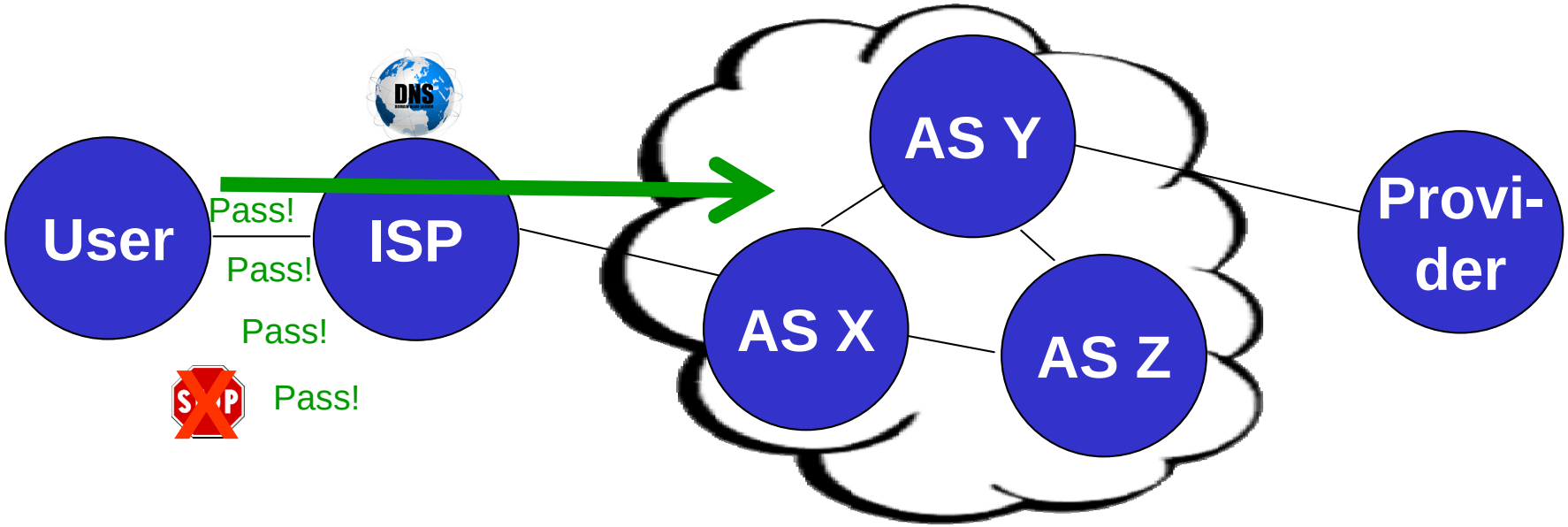
- Upon sending a DNS request or an IP packet
  - User configures and uses a "public" or a root DNS server
  - User applies known IP address of provider directly
  - Anonymization of user traffic, *e.g.*, via Tor

Bypassing ISP-based DNS Blocking



- Upon sending a DNS request or an IP packet
  - User configures and uses a "public" or a root DNS server
  - User applies known IP address of provider directly
  - Anonymization of user traffic, *e.g.*, via Tor
  - Virtual Private Network (VPN)

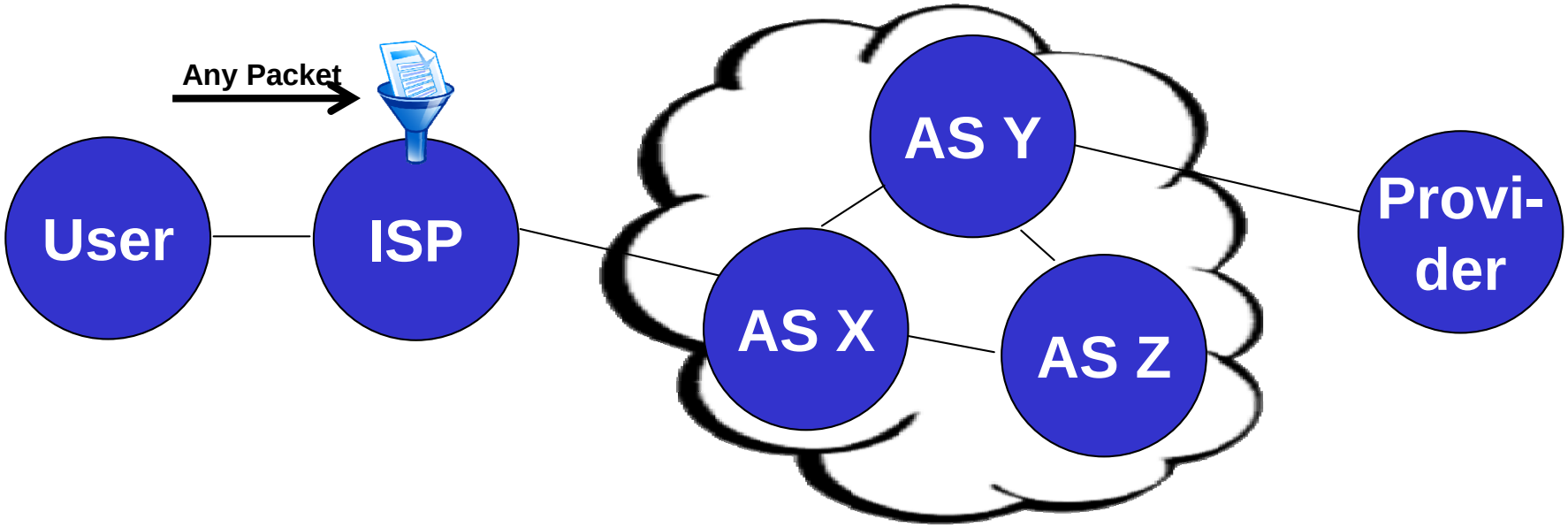
Bypassing ISP-based DNS Blocking



- Upon sending a DNS request or an IP packet
  - User configures and uses a "public" or a root DNS server
  - User applies known IP address of provider directly
  - Anonymization of user traffic, *e.g.*, via Tor
  - Virtual Private Network (VPN)

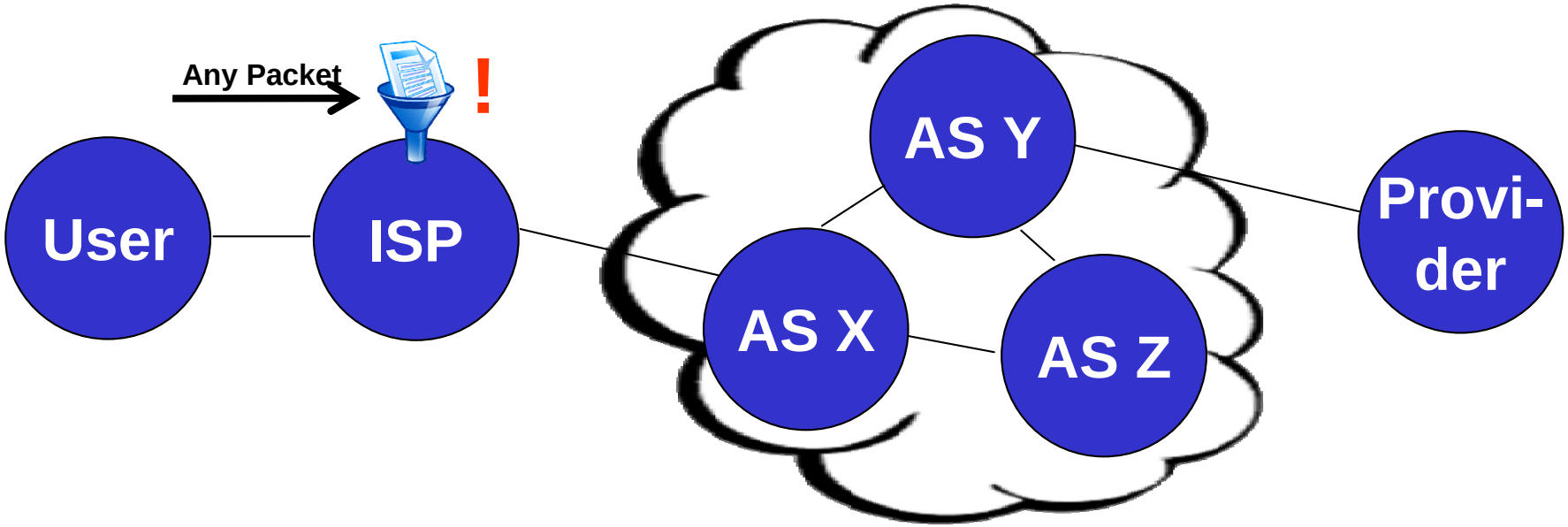
→ All traffic NOT detectable by ISP's DNS, no stopping

ISP Application Filters/Proxy Servers



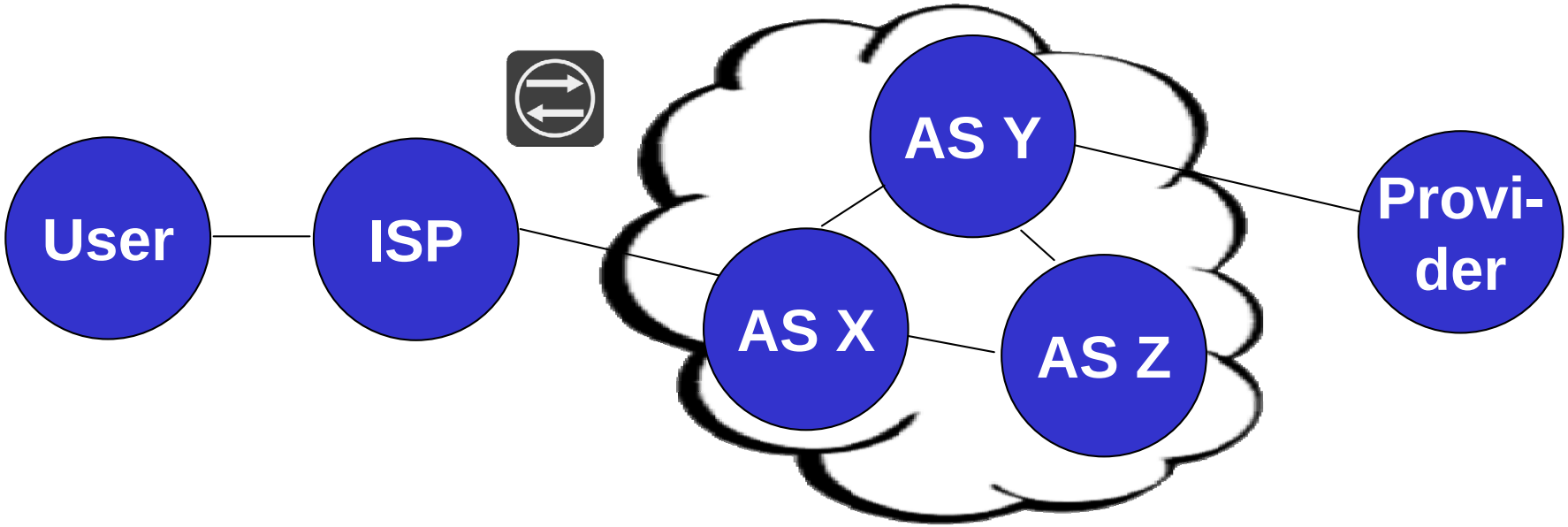
- ISP Application Filters
  - Many IP control and meta data, plus payload "interpreted"

ISP Application Filters/Proxy Servers



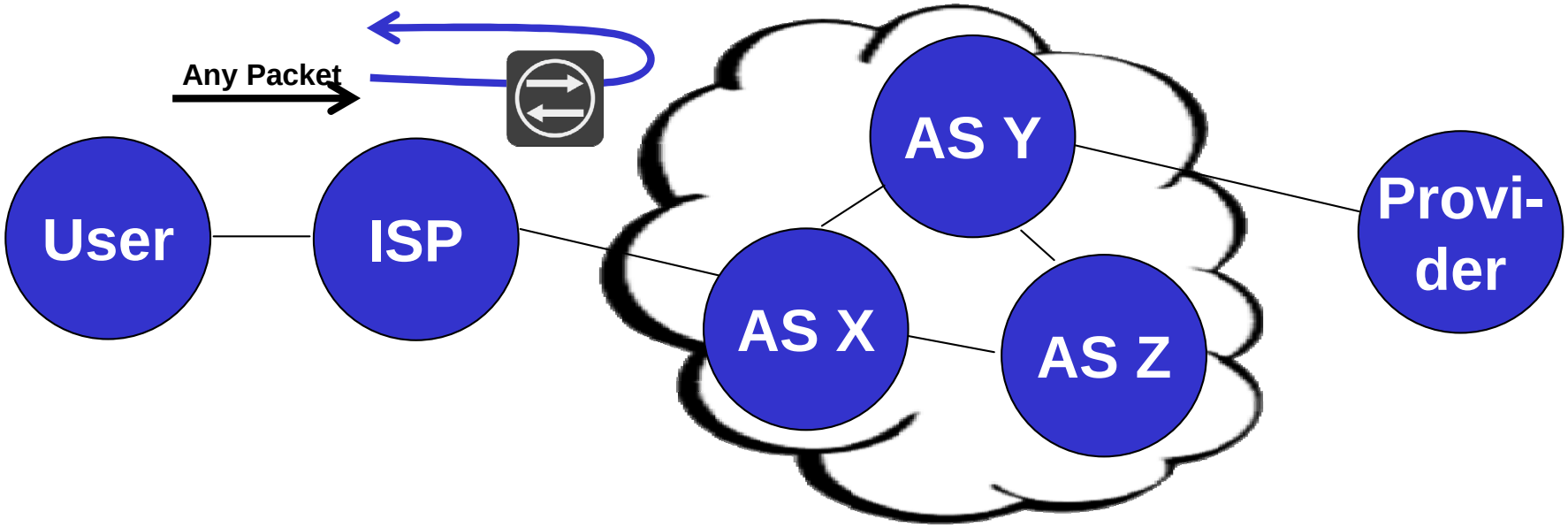
- ISP Application Filters
  - Many IP control and meta data, plus payload "interpreted"
  - Different violations of "rules" detectable

ISP Application Filters/Proxy Servers



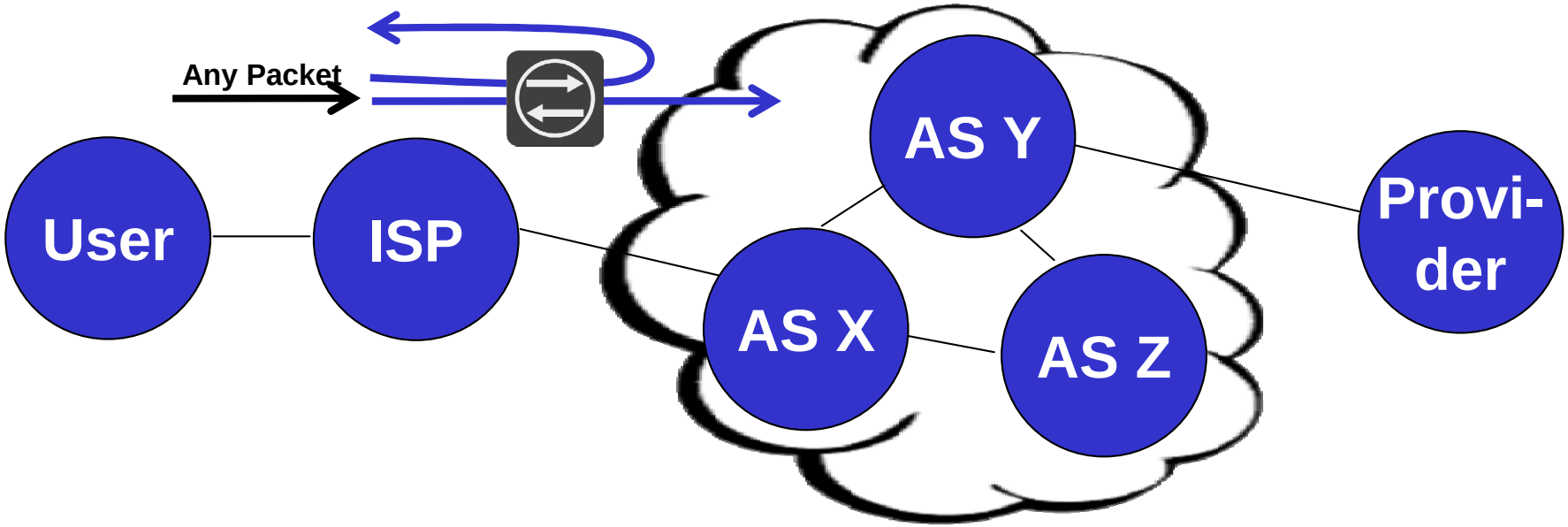
- ISP Application Filters
  - Many IP control and meta data, plus payload "interpreted"
  - Different violations of "rules" detectable
- Proxy Servers (intermediary)
  - A forwarding service for rule-based packet/content handling

ISP Application Filters/Proxy Servers



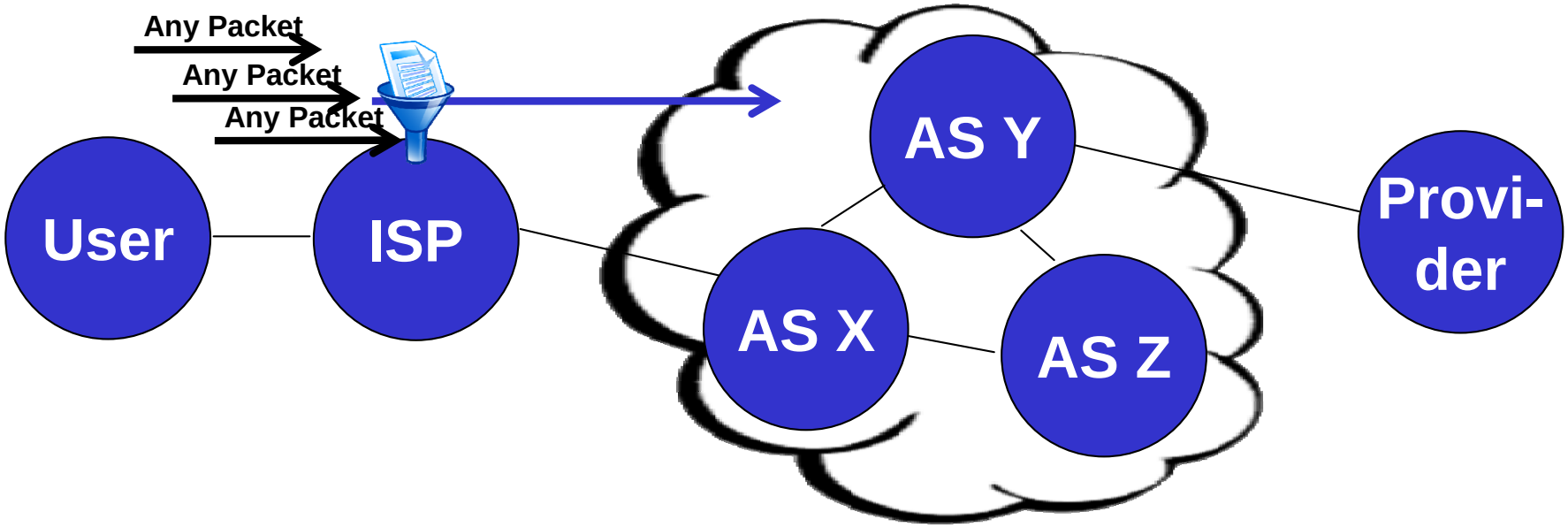
- ISP Application Filters
  - Many IP control and meta data, plus payload "interpreted"
  - Different violations of "rules" detectable
- Proxy Servers (intermediary)
  - A forwarding service for rule-based packet/content handling
  - Different destinations of forwards possible

ISP Application Filters/Proxy Servers



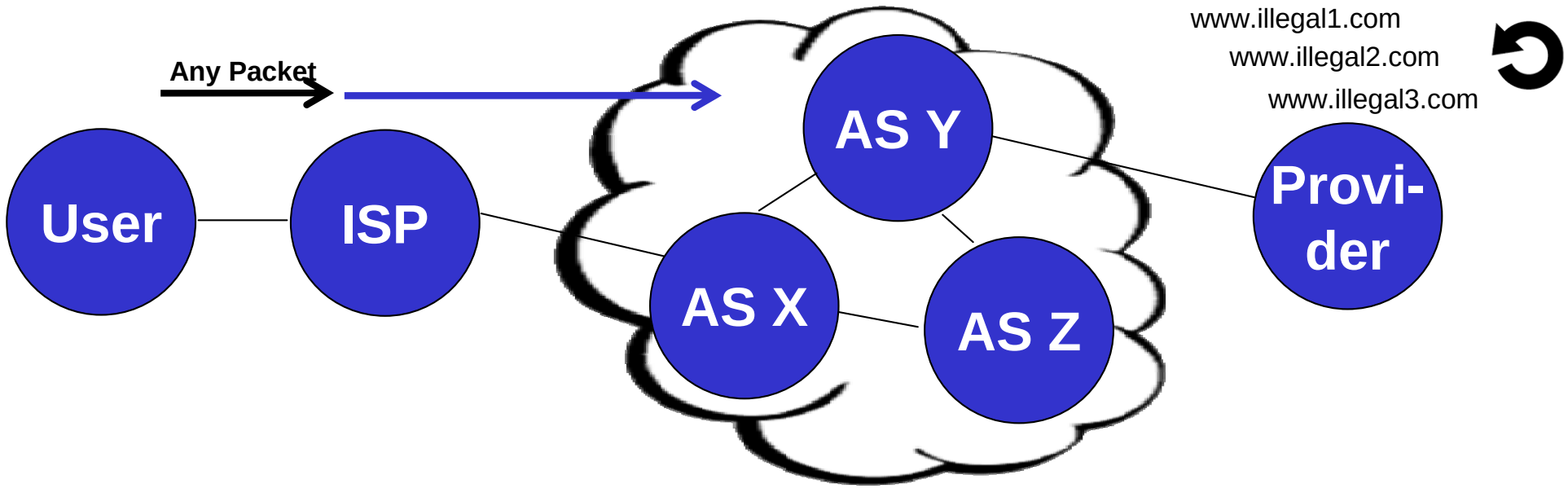
- ISP Application Filters
  - Many IP control and meta data, plus payload "interpreted"
  - Different violations of "rules" detectable
- Proxy Servers (intermediary)
  - A forwarding service for rule-based packet/content handling
  - Different destinations of forwards possible

Bypassing ISP Application Filters



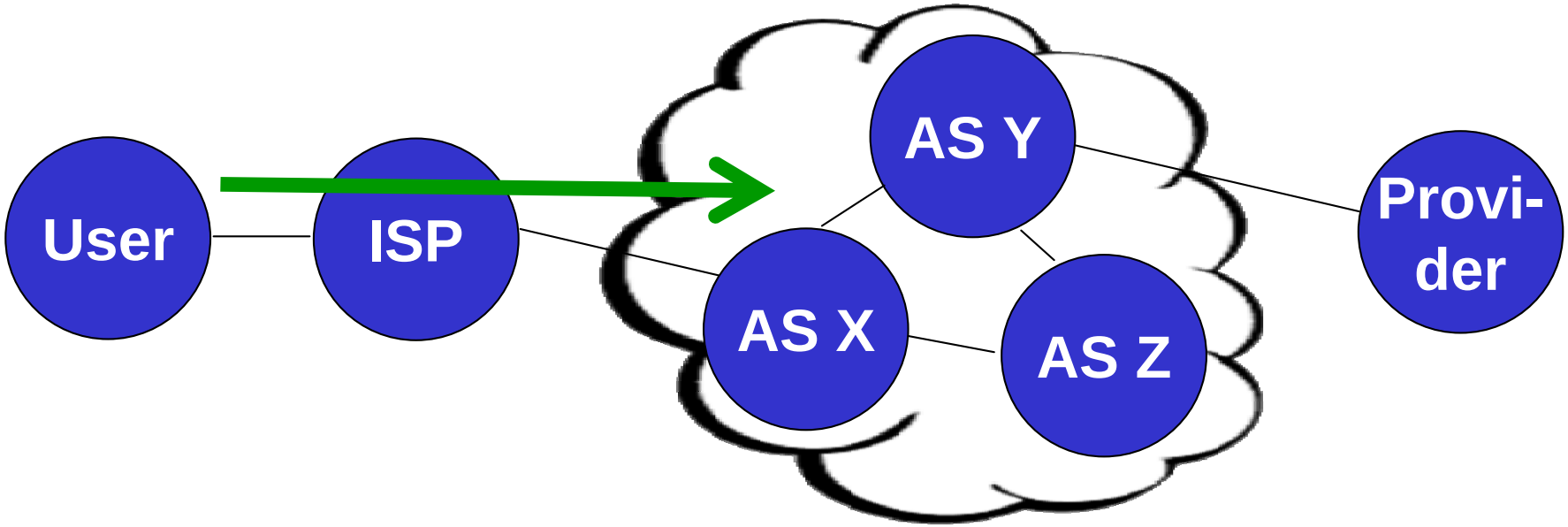
- Frequent adaptation of user's sending behavior
  - Change of file names, content, addresses
  - Testing ISP filter behavior

Bypassing ISP Application Filters



- Frequent adaptation of user's sending behavior
  - Change of file names, content, addresses
  - Testing ISP filter behavior
- Provider changes DNS names/IP addresses irregularly

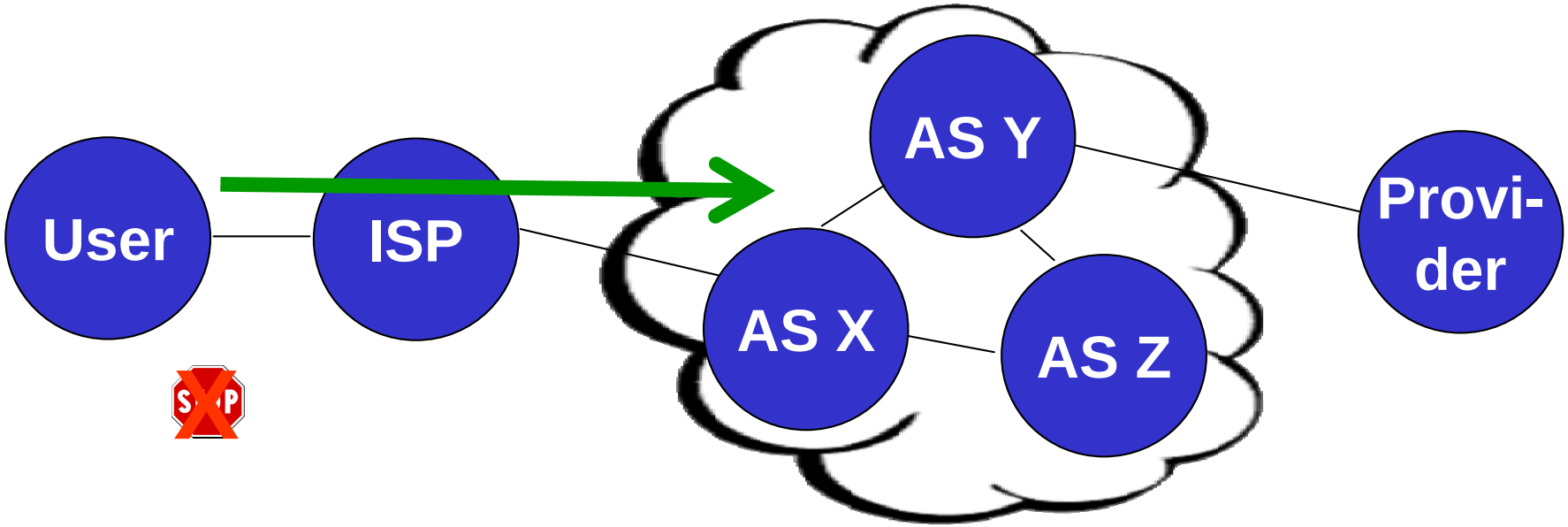
Bypassing ISP Application Filters



- Frequent adaptation of user's sending behavior
  - Change of file names, content, addresses
  - Testing ISP filter behavior
- Provider changes DNS names/IP addresses irregularly
- Encrypted transmission (*e.g.*, VPNs, SSL, or TLS)

SSL: Secure Socket Layer, TLS: Transport Layer Security

Bypassing ISP Application Filters



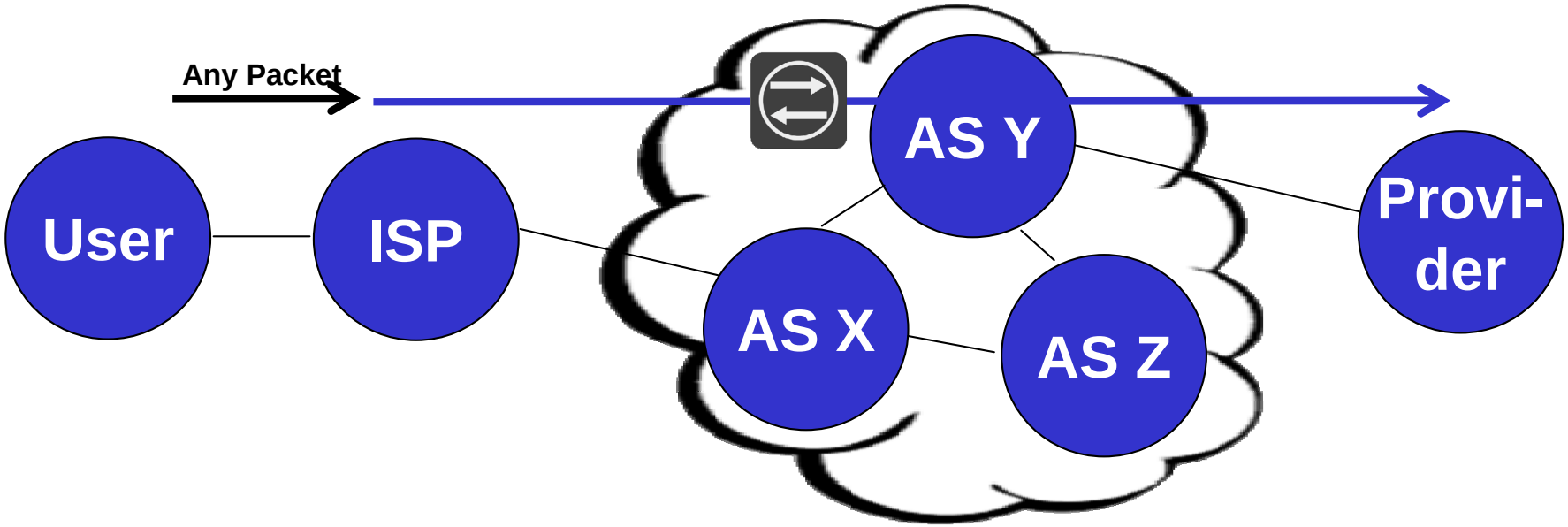
- Frequent adaptation of user's sending behavior
  - Change of file names, content, addresses
  - Testing ISP filter behavior
- Provider changes DNS names/IP addresses irregularly
- Encrypted transmission (*e.g.*, VPNs, SSL, or TLS)

SSL: Secure Socket Layer, TLS: Transport Layer Security

→ All traffic finally NOT detectable by ISP filters, no stopping

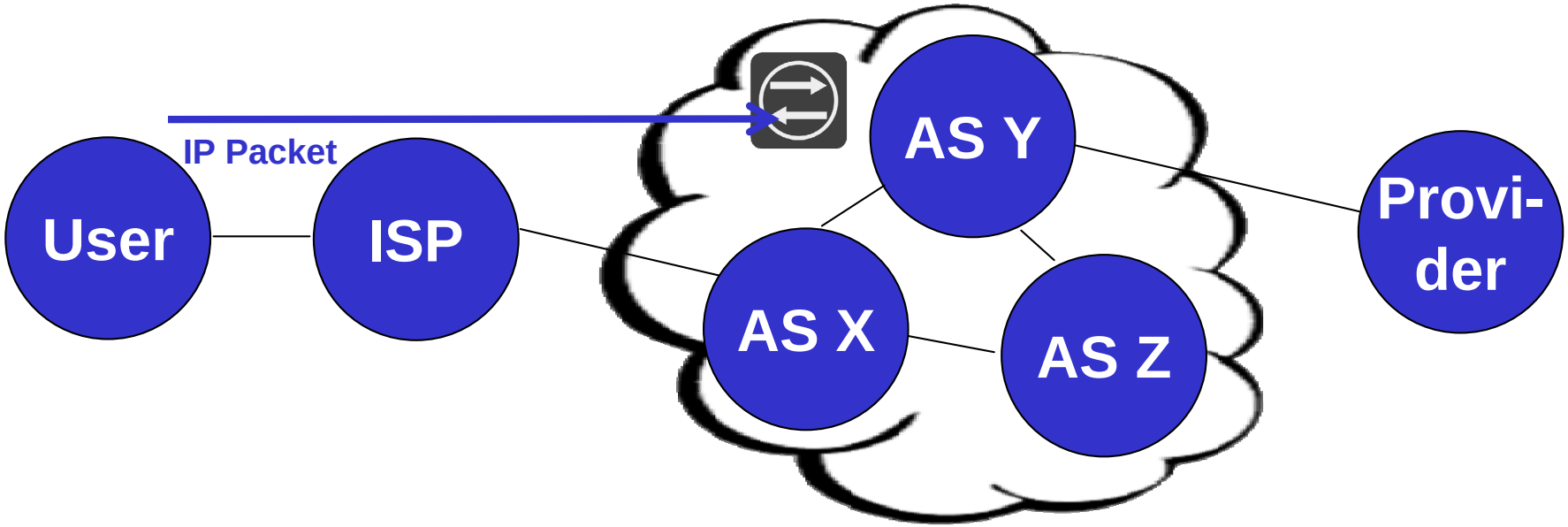
© 2016 UZH, CSG@IfI

Bypassing Proxy Servers



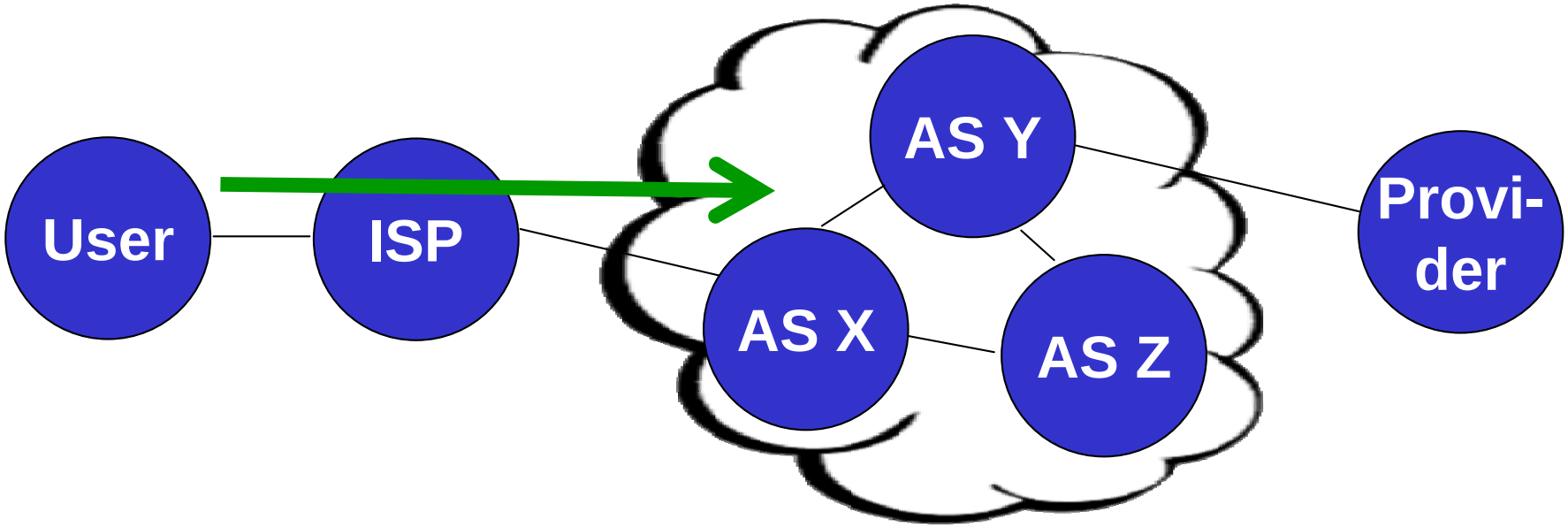
- Set-up of own proxy servers outside “local” ISP

Bypassing Proxy Servers



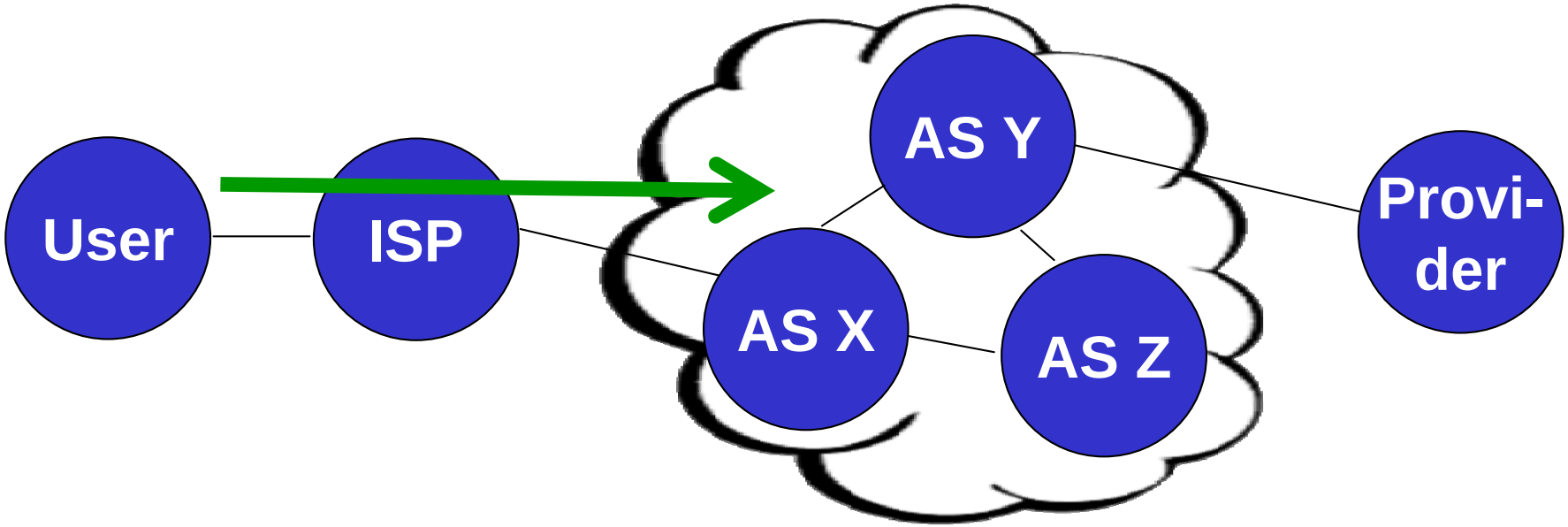
- Set-up of own proxy servers outside “local” ISP
- Anonymization of user traffic, *e.g.*, via Tor

Bypassing Proxy Servers



- Set-up of own proxy servers outside “local” ISP
- Anonymization of user traffic, *e.g.*, via Tor
- Virtual Private Network (VPN)

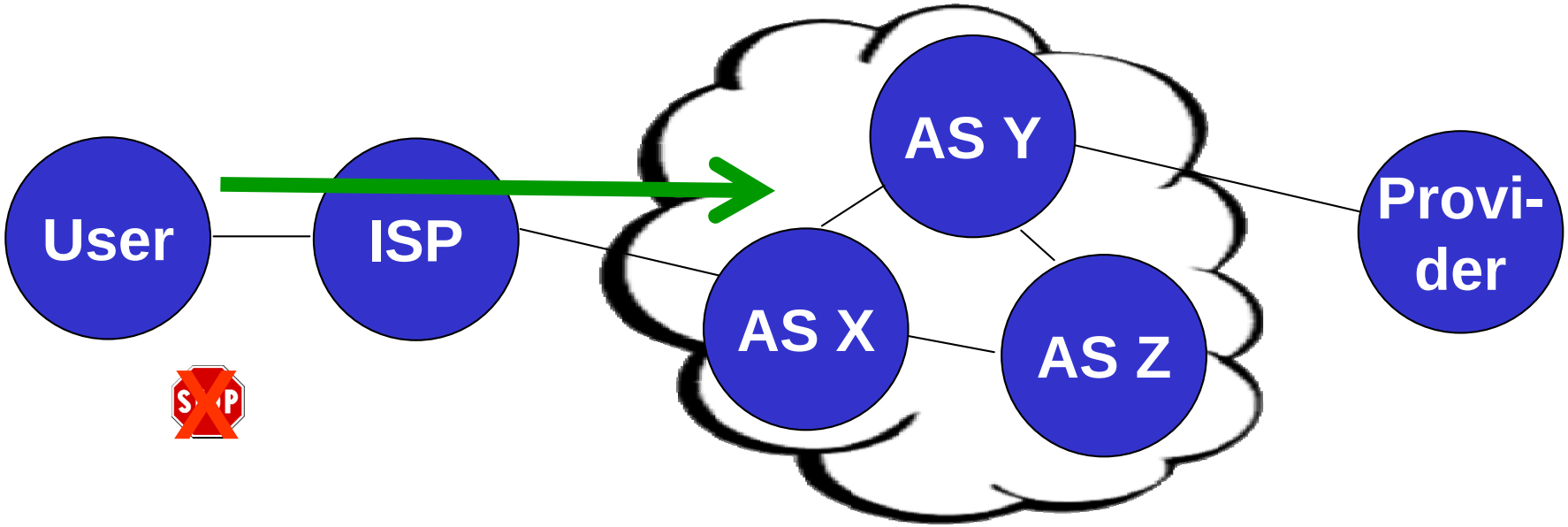
Bypassing Proxy Servers



- Set-up of own proxy servers outside “local” ISP
- Anonymization of user traffic, *e.g.*, via Tor
- Virtual Private Network (VPN)
- Encrypted transmission (*e.g.*, SSL or TLS)

© 2016 UZH, CSG@IfI

Bypassing Proxy Servers



- Set-up of own proxy servers outside “local” ISP
- Anonymization of user traffic, *e.g.*, via Tor
- Virtual Private Network (VPN)
- Encrypted transmission (*e.g.*, SSL or TLS)

→ All traffic NOT detectable by local ISP, no stopping

Conclusions

Major Obervations

- The Internet is operated
  - Via local domains (most liklely of different jurisdictions) and
  - Globally, interconnected by ASes (technically guided);
  - But decentrally managed (according to local rules)

Major Obervations

- The Internet is operated
  - Via local domains (most liklely of different jurisdictions) and
  - Globally, interconnected by ASes (technically guided);
  - But decentrally managed (according to local rules)
- As an example network operations component, DNS is
  - Hierarchically organized;
  - But redundantly accessible (guided by different jurisdictions)

© 2016 UZH, CSG@IfI

Major Obervations

- The Internet is operated
  - Via local domains (most liklely of different jurisdictions) and
  - Globally, interconnected by ASes (technically guided);
  - But decentrally managed (according to local rules)
- As an example network operations component, DNS is
  - Hierarchically organized;
  - But redundantly accessible (guided by different jurisdictions)
- User-controlled services/tools available world-wide

© 2016 UZH, CSG@IfI

Major Obervations

- The Internet is operated
  - Via local domains (most liklely of different jurisdictions) and
  - Globally, interconnected by ASes (technically guided);
  - But decentrally managed (according to local rules)
- As an example network operations component, DNS is
  - Hierarchically organized;
  - But redundantly accessible (guided by different jurisdictions)
- User-controlled services/tools available world-wide
- Internet traffic is more than DNS and Browser data
  - *E.g.*, Protocols (TCP, RTCP, UDP), Applications (E-mail, FTP, P2P), *Security Services* (HTTPS, SSL, TLS), Signaling

© 2016 UZH, CSG@IfI

Technical Conclusions

- Blocking IP addresses/DNS entries technically possible
  - Browser and DNS traffic considered here as a simpler example
  - Different traffic types need (partially) different handling

© 2016 UZH, CSG@IfI

Technical Conclusions

- Blocking IP addresses/DNS entries technically possible
  - Browser and DNS traffic considered here as a simpler example
  - Different traffic types need (partially) different handling

- Technical ISP efforts differ at large
  - Maintenance of to be blocked IP addresses, DNS entries, URLs
    - Data base? Procedures for entering/deleting/changing? Redressing?
  - During operations: loss of “fast path” router capabilities

© 2016 UZH, CSG@IfI

Technical Conclusions

- Blocking IP addresses/DNS entries technically possible
  - Browser and DNS traffic considered here as a simpler example
  - Different traffic types need (partially) different handling
- Technical ISP efforts differ at large
  - Maintenance of to be blocked IP addresses, DNS entries, URLs
    - Data base? Procedures for entering/deleting/changing? Redressing?
  - During operations: loss of “fast path” router capabilities
- Any such blocking – either installed by subnetwork operators or local ISPs – can be circumvented by even technically lower-skilled users

Thank you for your attention!