Packet Clearing House

National & Regional Cyber-Defense: an Integrated Caribbean Strategy

CTU Ministerial

May 30, 2012

Bill Woodcock

Packet Clearing House

Packet Clearing House

The short version:

Know and control your borders

Be self-reliant within your borders

Establish trust relationships with your peers

PCH
Packet Clearing House

Know and Control your Borders

In the Internet, your border is your perimeter of control.

This is not a simple shape, like your physical border.

It’s a complex set of circuits and devices with multiple kinds and layers of access.

Within your perimeter, you have ultimate control of the circuits and devices; outside, your adversaries may.

Accurately knowing where the border of your control lies is the first step in controlling its interior.

PCH
Packet Clearing House

Know and Control your Borders

Your perimeter of control will expand as a function of your strength, and contract in response to threats.

At a minimum, when you are in the time of greatest distress, planning and forethought will give you a redoubt, a minimum perimeter of absolute control beyond which you cannot be compressed, and within which you have the set of tools you need to begin pressing your perimeter outwards again.

Packet Clearing House

Know and Control your Borders

Establishing and maintaining control requires complete knowledge of the terrain. In cybersecurity, your adversary dwells in crannies of your systems that are unknown to you.

Circuits, routers, and servers are each specific and comprehensible devices.

Your knowledge of the terrain they define must be direct and literal, not by abstraction or analogy, as the differences between models and reality form those crannies in which an adversary takes control.

Packet Clearing House

Be Self-Reliant Within your Borders

Internet Exchange Points, IXPs, are the sources of Internet bandwidth.

Most Caribbean bandwidth flows through NOTA, the NAP of the Americas, here in Miami, or Equinix Ashburn, near Washington D.C.

Increasingly, Caribbean countries are establishing their own IXPs, so they are no longer entirely dependent upon their connection to Miami.

Packet Clearing House

Be Self-Reliant Within your Borders

Domain name resolution, people's ability to find things on the Internet, depends upon a hierarchy of domain name servers.

In order to find and communicate with a server sitting right next to you, you still need to be able to first talk to a root nameserver, and a TLD nameserver.

Increasingly, Caribbean countries are moving to host their own root and TLD nameservers on-island, allowing them autonomy from international fiber.

PCH
Packet Clearing House

Be Self-Reliant Within your Borders

Build human and infrastructural capacity domestically.

“Direct foreign investment” means export of capital; that investment demands its return. Debt and the export of capital are strategic weaknesses.

Law enforcement dependence upon foreign-owned carriers for intercept capability means that law enforcement leaks information internationally, and may be the last to gain access to intercepted intelligence.

Packet Clearing House

Establish Trust Relationships

CERTs are the hub of trust relationships

Law-enforcement to ISP

Defense to CERT

Government to government

“Culture of Security”

Packet Clearing House

Critical Infrastructure Checklist

- ✓ Domestic IXP on-island. Redundant pair eventually.
- ✓ Your own ccTLD nameservers on-island and at major IXPs on the other side of your international circuits.
- ✓ Root nameserver on-island. Multiple when possible.
- ✓ DNSSEC sign your national ccTLD.
- ✓ Use DANE to bootstrap a national Certificate Authority.
- ✓ Neighbors' ccTLDs and other TLD nameservers of interest on-island, at your IXP, connected to your ISPs.
- ✓ Datacenters adjacent to your IXP.
- ✓ DDoS sinks on both sides of your international circuits.
- ✓ Redundant fiber paths both on-island and to major IXPs bordering the region.

Packet Clearing House

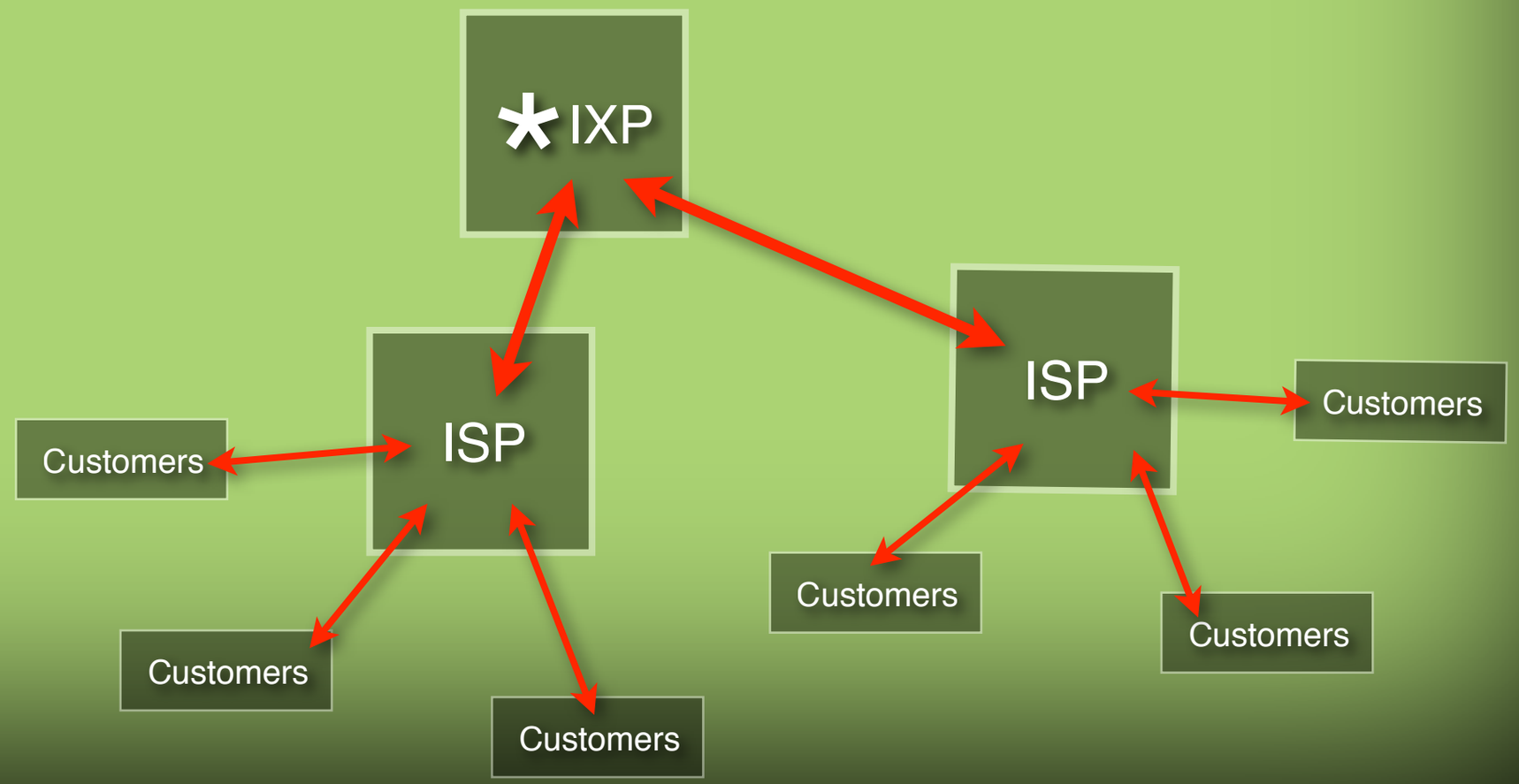
Policy & Regulatory Checklist

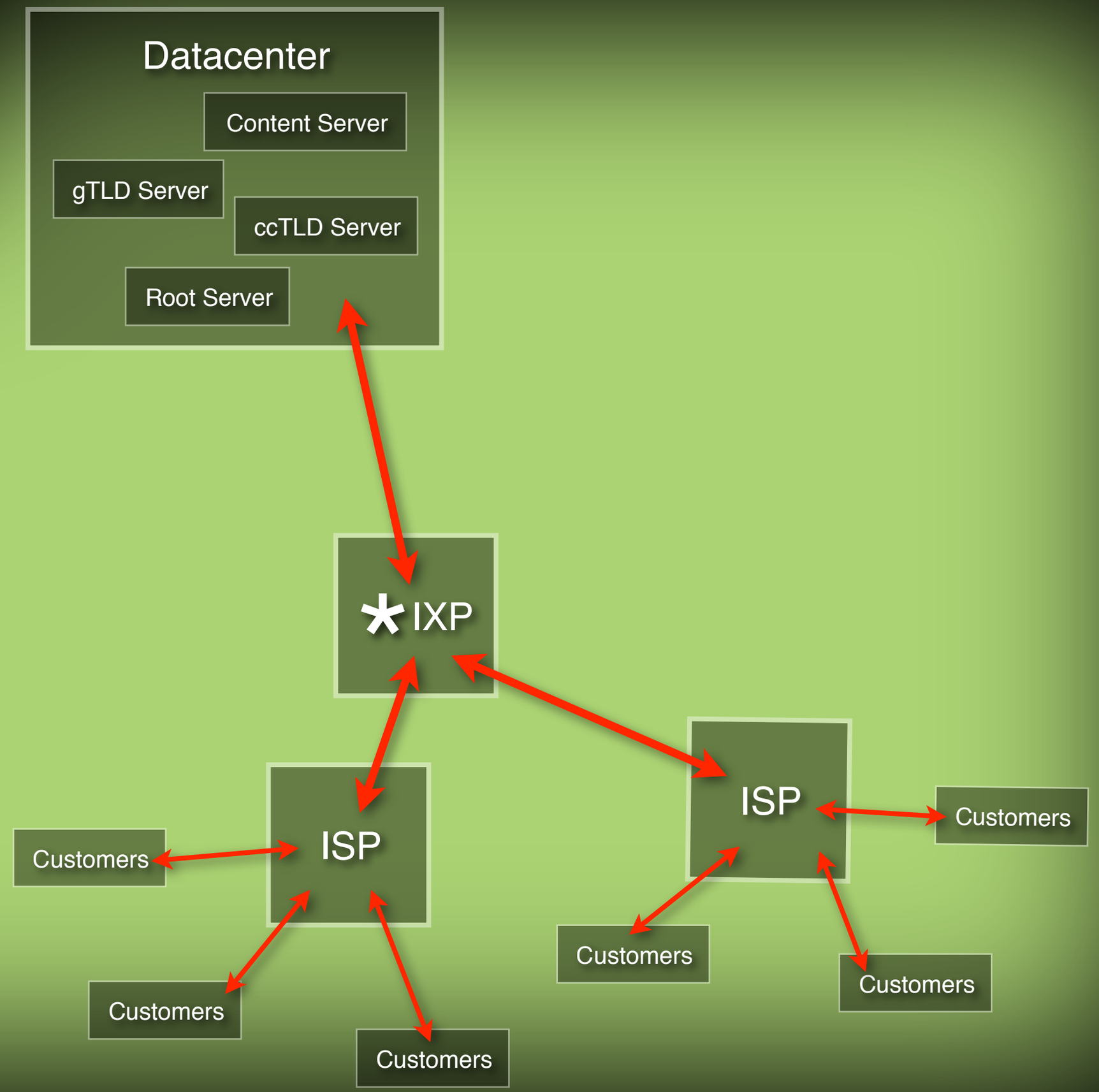
- ✓ Avoid over-spending and gold-plating.
- ✓ Encourage international content to mirror at your IXP.
- ✓ Maintain a competitive domestic marketplace in all services. Regulate only constrained common goods. Use class licenses rather than individual licenses by default.
- ✓ Encourage your ISPs to do business in neighboring countries, and welcome their ISPs to do business in yours. Together you'll boot-strap into larger markets.
- ✓ Adopt or ratify the Council of Europe Convention on Cybercrime.
- ✓ Be aware of and participate in Internet governance, don't let others speak in your stead, and don't get used as a disposable pawn in other people's fights.

PCH
Packet Clearing House

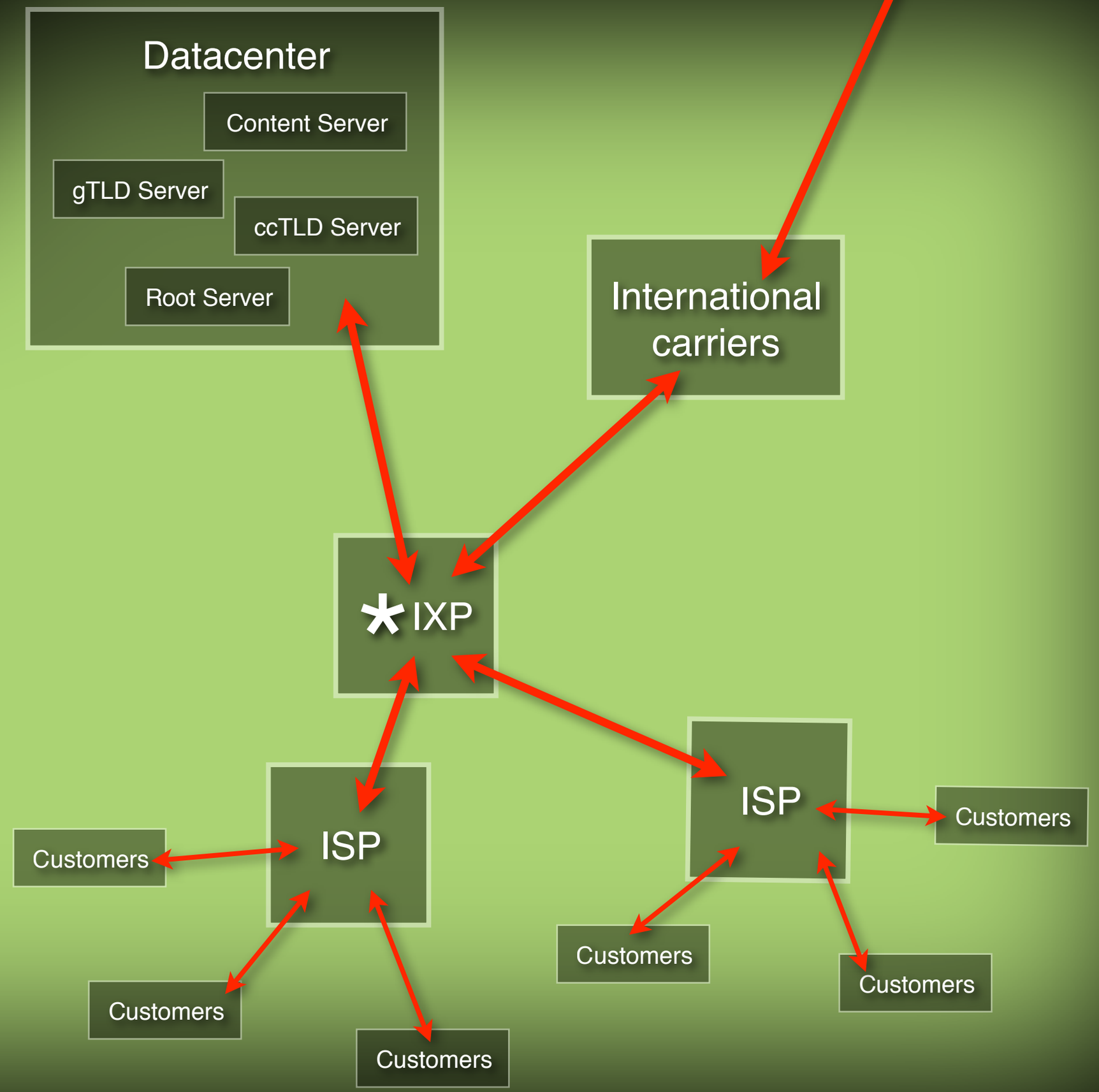
*IXP

PCH
Packet Clearing House




Datacenter
Content Server
gTLD Server
ccTLD Server
Root Server
*IXP
ISP
ISP
Customers
Customers
Customers
Customers
Customers
Customers

PCH
Packet Clearing House



PCH
Packet Clearing House

Datacenter

Content Server

gTLD Server

ccTLD Server

Root Server

International carriers

*IXP

Academia

Government

Ministries

Customers

ISP

Customers

Customers

Customers

ISP

Customers

Customers

Customers

PCH
Packet Clearing House

Datacenter

Content Server

gTLD Server

ccTLD Server

Root Server

International carriers

Outbound DDoS sink

*IXP

Academia

Government

Ministries

ISP

Customers

Customers

ISP

Customers

Customers

Customers

Customers

Packet Clearing House

Datacenter

Content Server

gTLD Server

ccTLD Server

Root Server

International carriers

Law enforcement intercept facility

Outbound DDoS sink

*IXP

Academia

Government

Ministries

ISP

Customers

Customers

ISP

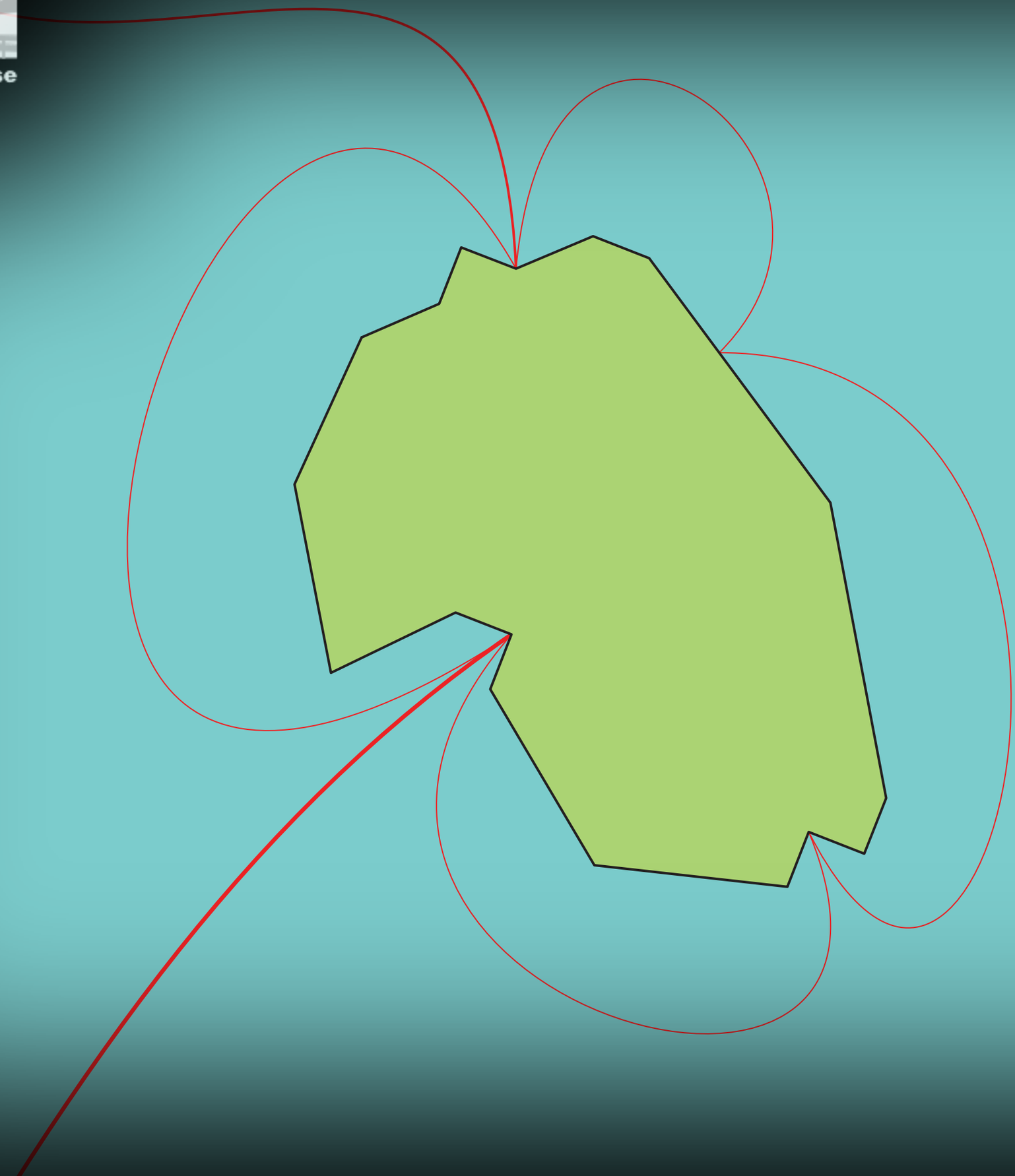
Customers

Customers

Customers

Customers

PCH
Packet Clearing House



PCH
Packet Clearing House

Regional cable

Cable landing

Cable landing

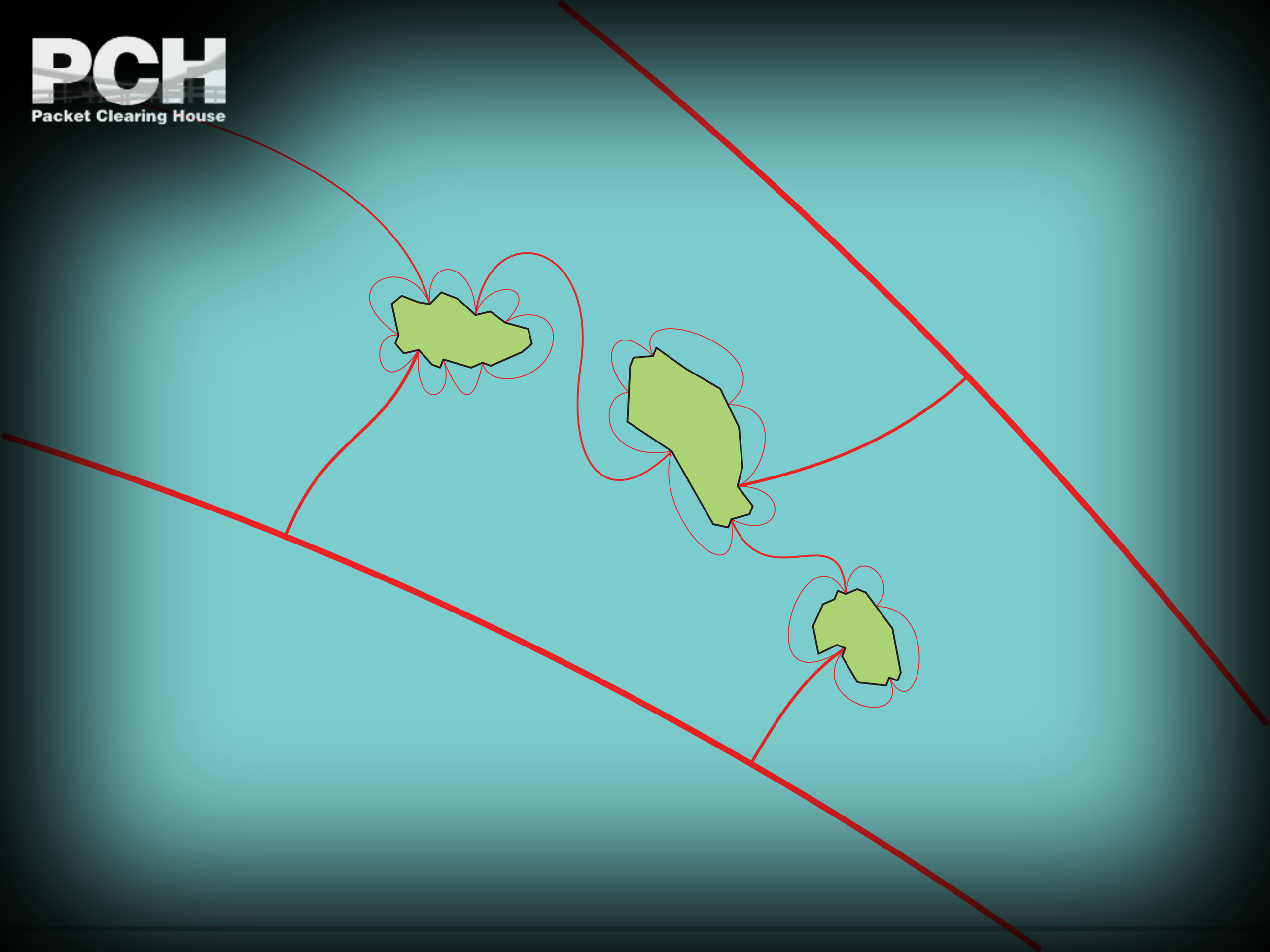
Domestic festoon cable

IXP

Cable landing

Branch from international cable

PCH
Packet Clearing House



PCH
Packet Clearing House

International cable

Regional cable

Festoon cable

IXP

Festoon cable

IXP

Branching unit

Regional cable

Branching unit

Regional cable

Festoon cable

IXP

Branching unit

International cable

PCH
Packet Clearing House

PCH
Packet Clearing House

To the eastern seaboard

To Europe

NOTA
Miami

IXP

IXP

IXP

IXP

IXP

IXP

IXP

To Brazil

PCH
Packet Clearing House

To the eastern seaboard

To Europe

NOTA
Miami

DDoS Mitigation
Mainland anycast hosting

IXP

IXP

IXP

IXP

IXP

IXP

IXP

To Brazil

Packet Clearing House

Announcement

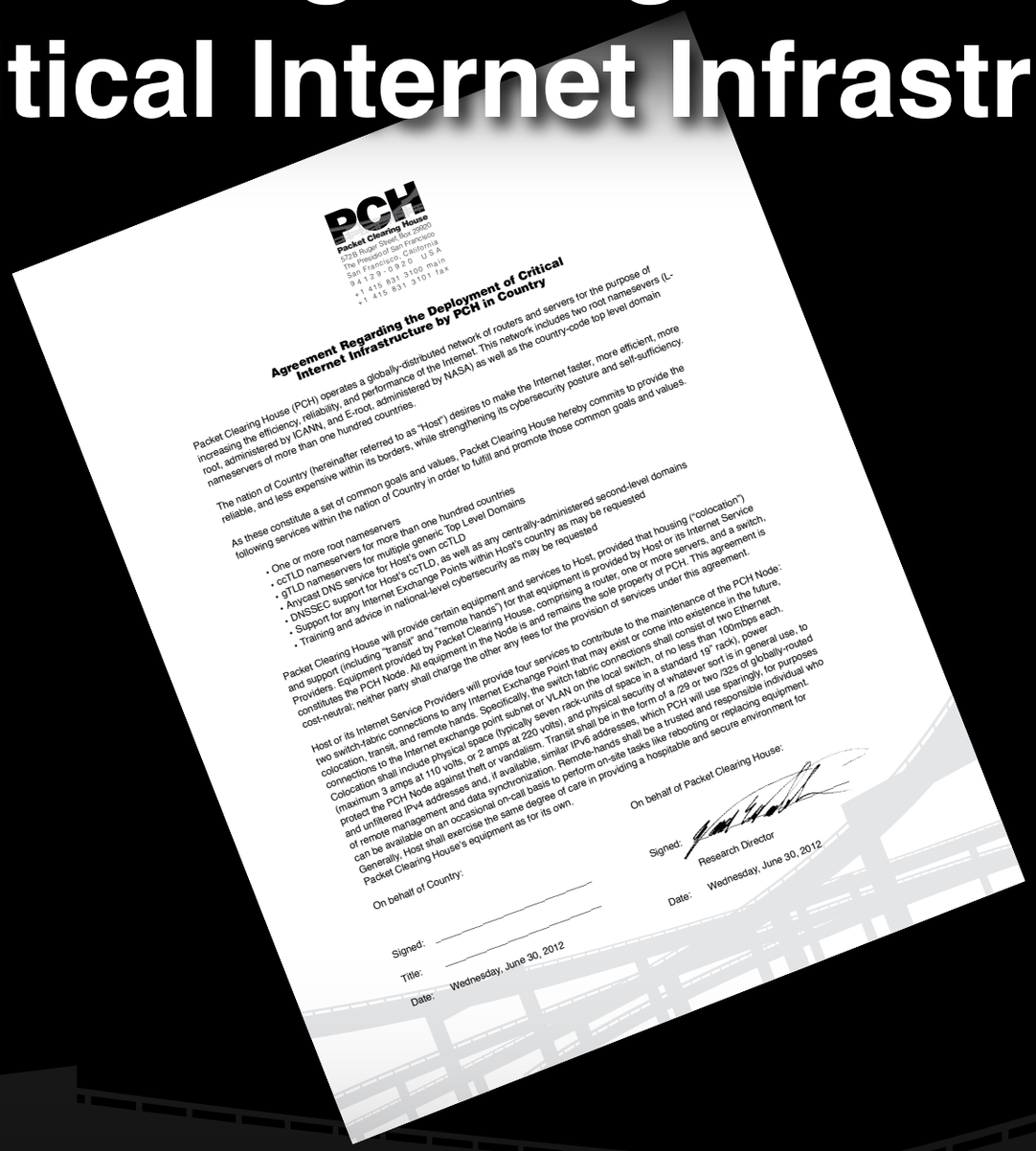
with Rodrigo de la Parra

Vice President for Latin America

ICANN

PCH
Packet Clearing House

Agreement Regarding the Deployment of Critical Internet Infrastructure



PCH
Packet Clearing House
2728 Ruger Street, Box 29920
The Presidio of San Francisco
San Francisco, California
94129-0920 USA
+1 415 831 3100 main
+1 415 831 3101 fax

Agreement Regarding the Deployment of Critical Internet Infrastructure by PCH in Country

Packet Clearing House (PCH) operates a globally-distributed network of routers and servers for the purpose of increasing the efficiency, reliability, and performance of the Internet. This network includes two root nameservers (L-root, administered by ICANN, and E-root, administered by NASA) as well as the country-code top level domain nameservers of more than one hundred countries.

The nation of Country (hereinafter referred to as "Host") desires to make the Internet faster, more efficient, more reliable, and less expensive within its borders; while strengthening its cybersecurity posture and self-sufficiency.

As these constitute a set of common goals and values, Packet Clearing House hereby commits to provide the following services within the nation of Country in order to fulfill and promote those common goals and values.

- One or more root nameservers
- ccTLD nameservers for more than one hundred countries
- gTLD nameservers for multiple generic Top Level Domains
- Anycast DNS service for Host's own ccTLD
- DNSSEC support for Host's ccTLD, as well as any centrally-administered second-level domains
- Support for any Internet Exchange Points within Host's country as may be requested
- Training and advice in national-level cybersecurity as may be requested

Packet Clearing House will provide certain equipment and services to Host, provided that housing ("colocation") and support (including "transit" and "remote hands") for that equipment is provided by Host or its Internet Service Providers. Equipment provided by Packet Clearing House, comprising a router, one or more servers, and a switch, constitutes the PCH Node. All equipment in the Node is and remains the sole property of PCH. This agreement is cost-neutral, neither party shall charge the other any fees for the provision of services under this agreement.

Host or its Internet Service Providers will provide four services to contribute to the maintenance of the PCH Node: two switch-fabric connections to any Internet Exchange Point that may exist or come into existence in the future, colocation, transit, and remote hands. Specifically, the switch fabric connections shall consist of two Ethernet connections to the Internet exchange point subnet or VLAN on the local switch, of no less than 100mbps each. Colocation shall include physical space (typically seven rack-units of space in a standard 19" rack), power (maximum 3 amps at 110 volts, or 2 amps at 220 volts), and physical security of whatever sort is in general use, to protect the PCH Node against theft or vandalism. Transit shall be in the form of a /29 or two /32s of globally-routed and unfiltered IPv4 addresses and, if available, similar IPv6 addresses, which PCH will use sparingly, for purposes of remote management and data synchronization. Remote-hands shall be a trusted and responsible individual who can be available on an occasional on-call basis to perform on-site tasks like rebooting or replacing equipment. Generally, Host shall exercise the same degree of care in providing a hospitable and secure environment for Packet Clearing House's equipment as for its own.

On behalf of Country:

Signed: _____

Title: _____

Date: Wednesday, June 30, 2012

On behalf of Packet Clearing House:

Signed:

Research Director

Date: Wednesday, June 30, 2012

Agreement Regarding the Deployment of Critical Internet Infrastructure

nameservers of more than one hundred countries.

The nation of Country (hereinafter referred to as “Host”) desires to make the Internet faster, more efficient, more reliable, and less expensive within its borders, while strengthening its cybersecurity posture and self-sufficiency.

As these constitute a set of common goals and values, Packet Clearing House hereby commits to provide the following services within the nation of Country in order to fulfill and promote those common goals and values.

- One or more root nameservers
- ccTLD nameservers for more than one hundred countries
- gTLD nameservers for multiple generic Top Level Domains
- Anycast DNS service for Host’s own ccTLD
- DNSSEC support for Host’s ccTLD, as well as any centrally-administered second-level domains
- Support for any Internet Exchange Points within Host’s country as may be requested
- Training and advice in national-level cybersecurity as may be requested

Packet Clearing House will provide certain equipment and services to Host, provided that housing (“colocation”) and support (including “transit” and “remote hands”) for that equipment is provided by Host or its Internet Service Providers. Equipment provided by Packet Clearing House, comprising a router, one or more servers, and a switch, constitutes the PCH Node. All equipment in the Node is and remains the sole property of PCH. This agreement is cost-neutral; neither party shall charge the other any fees for the provision of services under this agreement.

Thanks, and Questions?

Copies of this presentation can be found
in Keynote and PDF formats at:

http:// www.pch.net / resources / papers

Bill Woodcock
Research Director
Packet Clearing House
woody@pch.net