Campus Network Operations Optimizing for NREN Connectivity

CRNC 2017 Conference
Bishkek, Kyrgyzstan

These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license (http://creativecommons.org/licenses/by-nc/4.0/)

Research and Education Networks

Some Terminology

- **R&E**: Research and Education
- **REN**: Research and Education Networks
- **NREN**: National REN
- **RREN**: Regional REN

Globally, REN connectivity is complex

REN Characteristics

High bandwidth networks

- 10G backbones with 40G and 100G coming
- Research typically needs uncongested networks
  - Which means many RENs are lightly used with lots of unused capacity (we call it headroom)

Low latency

- Terrestrial fiber

Open Networks with no filtering

- Firewalls can make it hard for ad-hoc activities

Why a REN?

- **Enable research or services that could not be accomplished otherwise**
- Cost Savings (buyers club)
  - Aggregate demand from multiple parties
- Vision of building alliances
- Successful RENs find that there are unanticipated benefits

Why Are We Doing This?

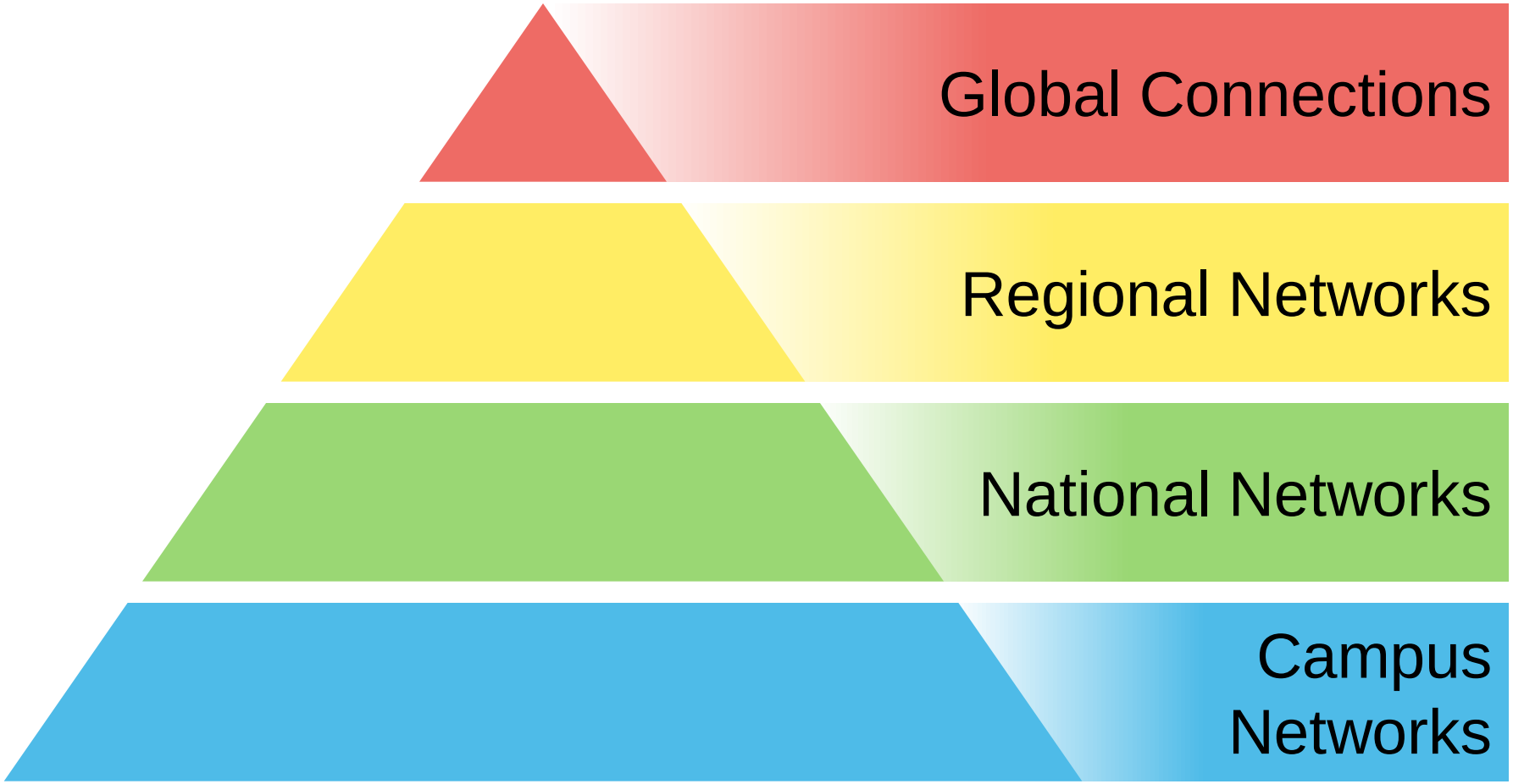
- Our goal is to build networking capacity to support Research and Education
  - Remember: University = Research & Education
- Buying all service from your local ISP is a losing game – you will spend more money and not have control of the network
- The pattern around the world is to build regional, national, and larger Research and Education Networks (RENs)

REN Ecosystem

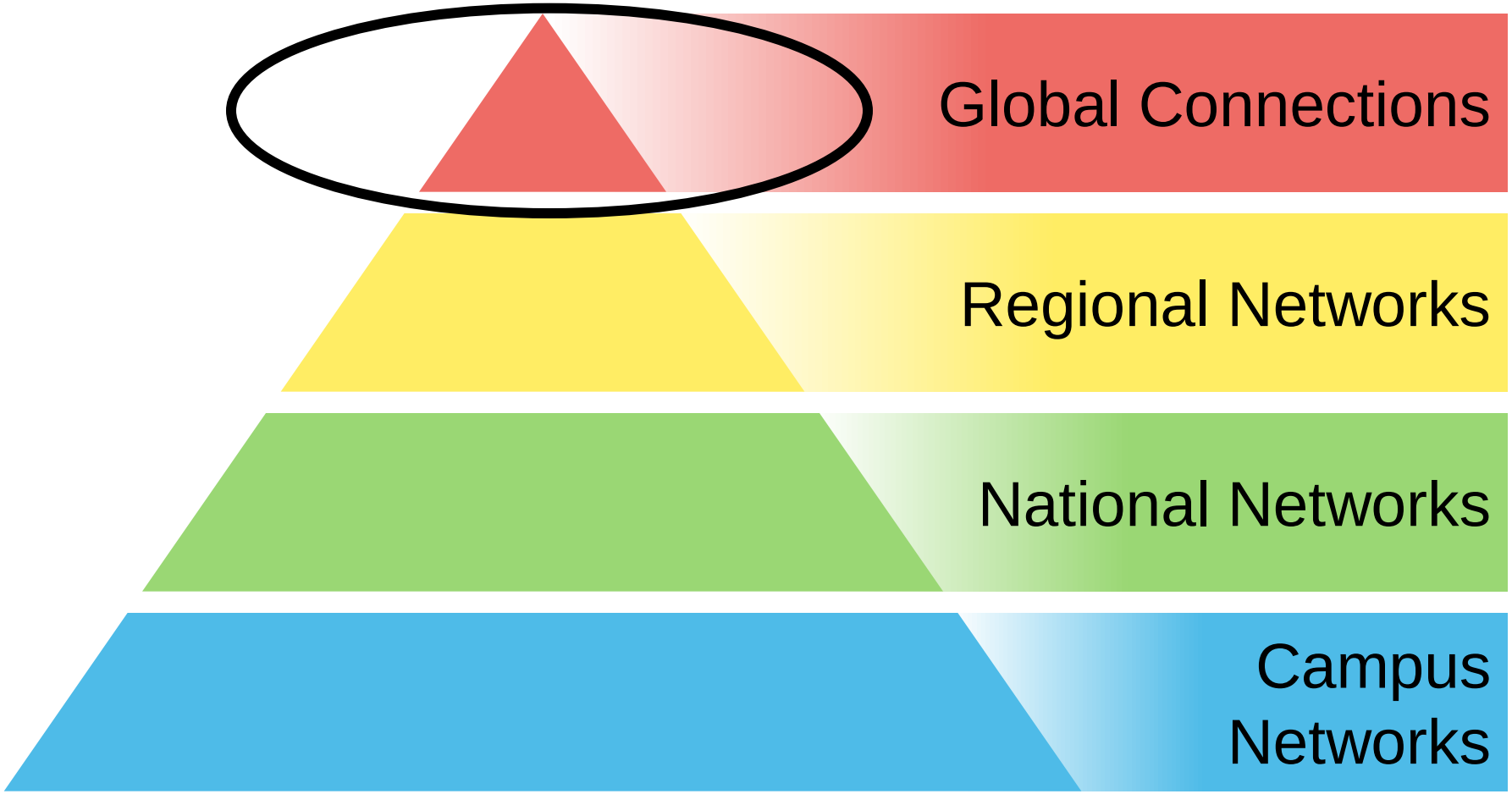
A layered model

- Global Connectivity
- Regional RENs
- National Research and Education Networks
- Campus network
  - This is the network that provides service to the actual users we care about

NREN EcoSystem



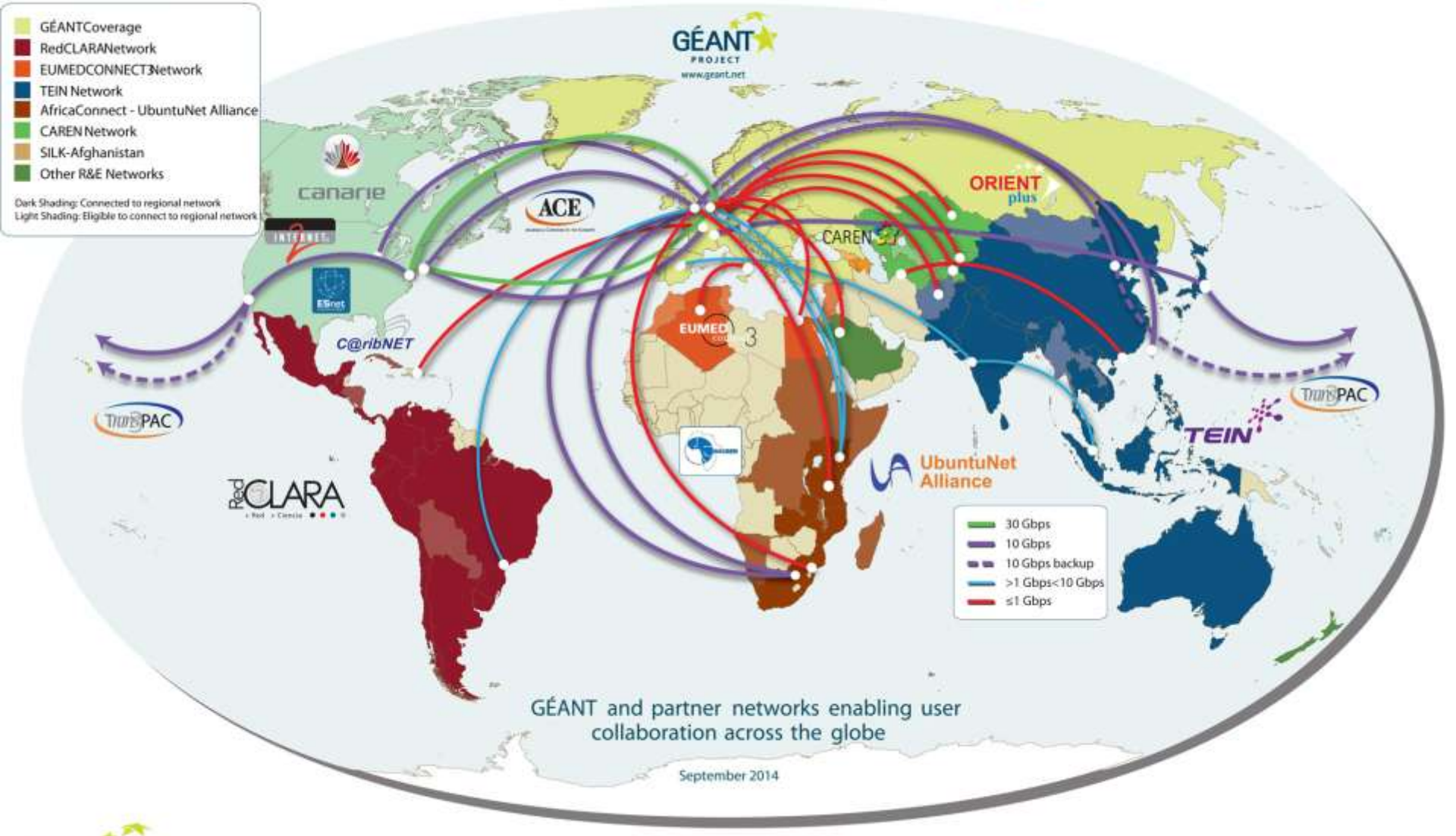
NREN EcoSystem



Global REN Connections

- Connect Regional or National networks together
- Tend to be longer, more expensive circuits
- Not always well coordinated
- Routing policies often inconsistent

At the Heart of Global Research and Education Networking



GÉANT and partner networks enabling user collaboration across the globe

September 2014

GÉANT PROJECT
www.geant.net

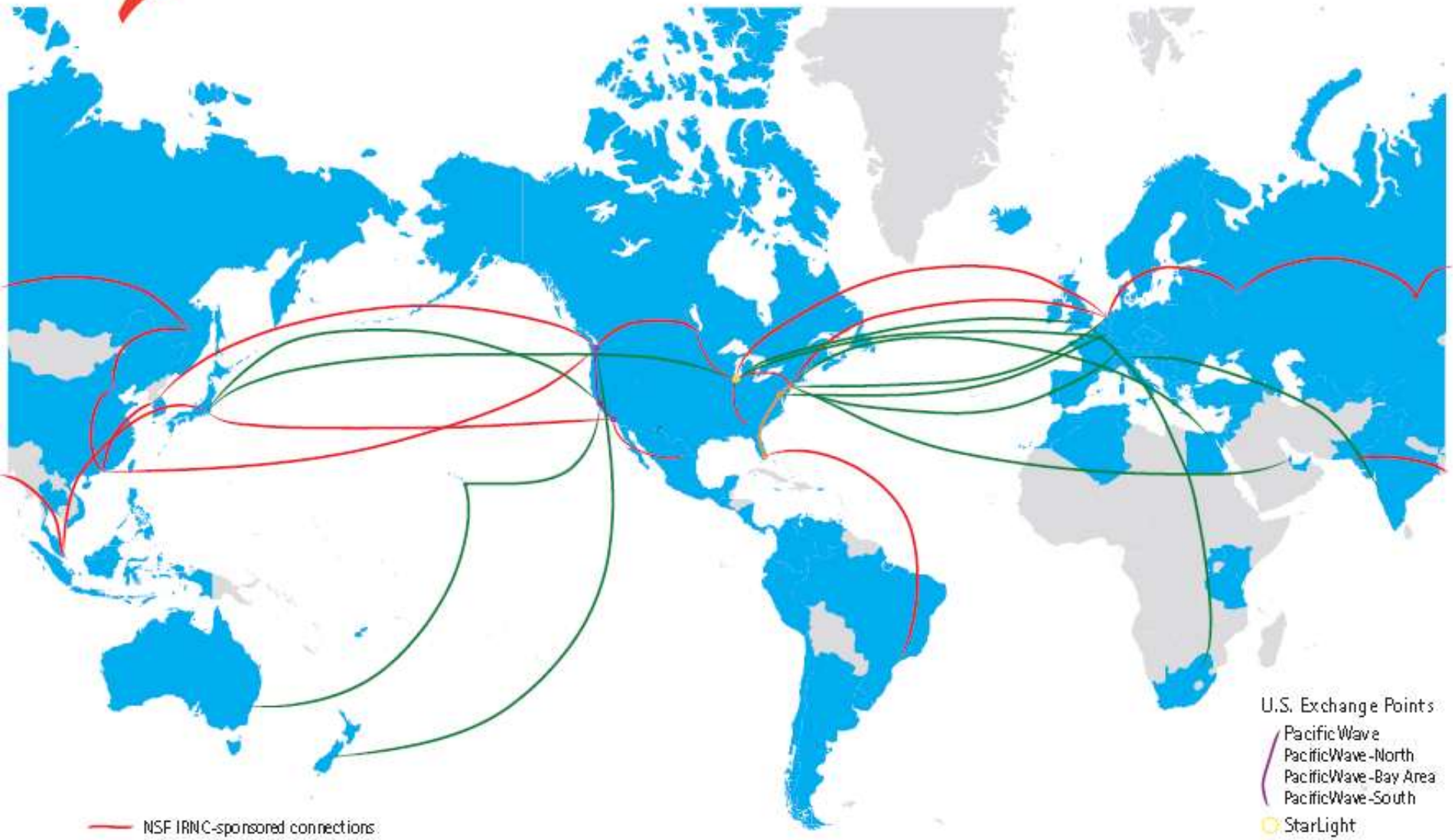
connect • communicate • collaborate

GÉANT is co-funded by the European Union within its 7th R&D Framework Programme.

Co-funded by the European Union

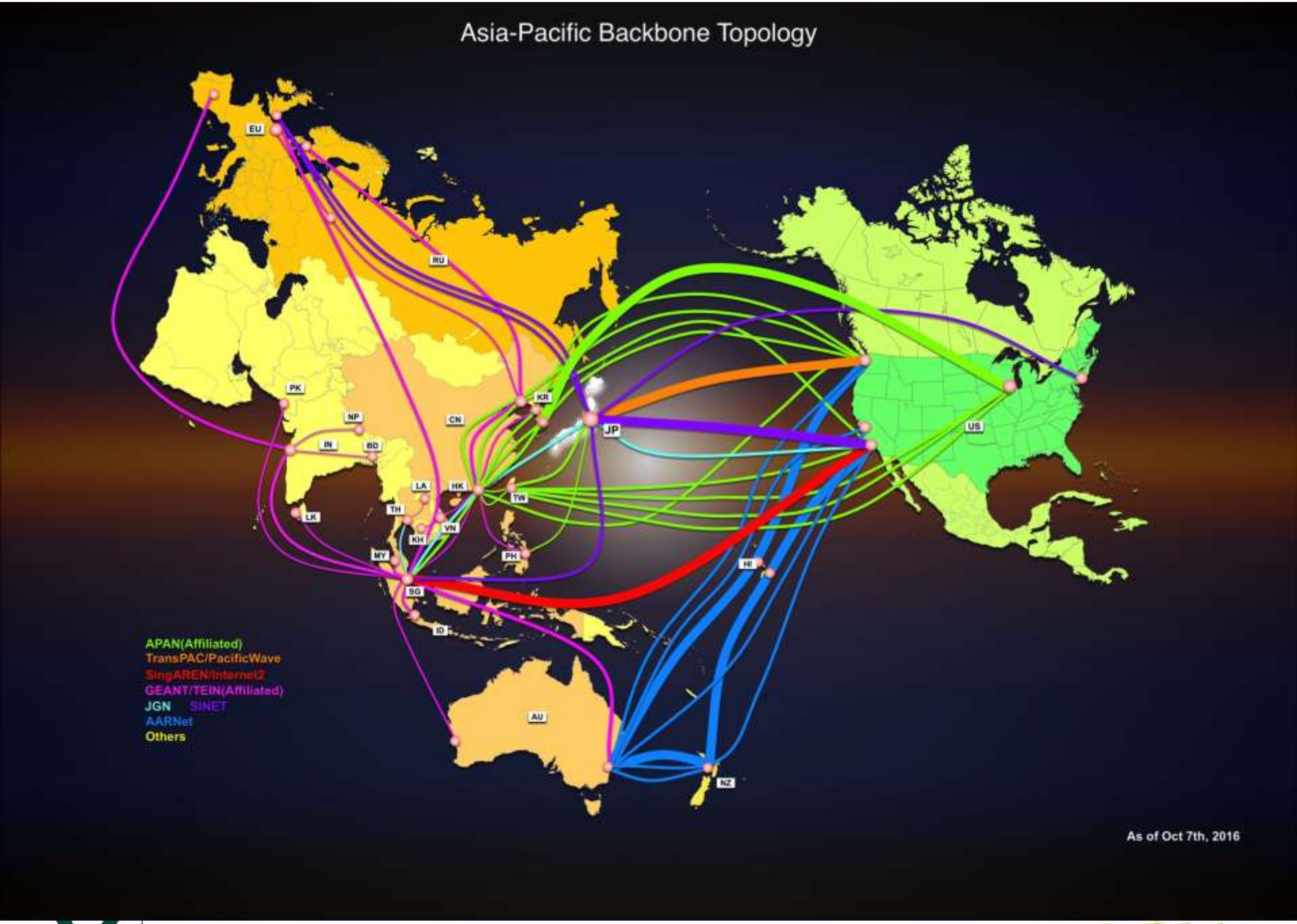
INTERNET2® www.internet.edu

THE INTERNATIONAL REACH OF THE INTERNET2 NETWORK

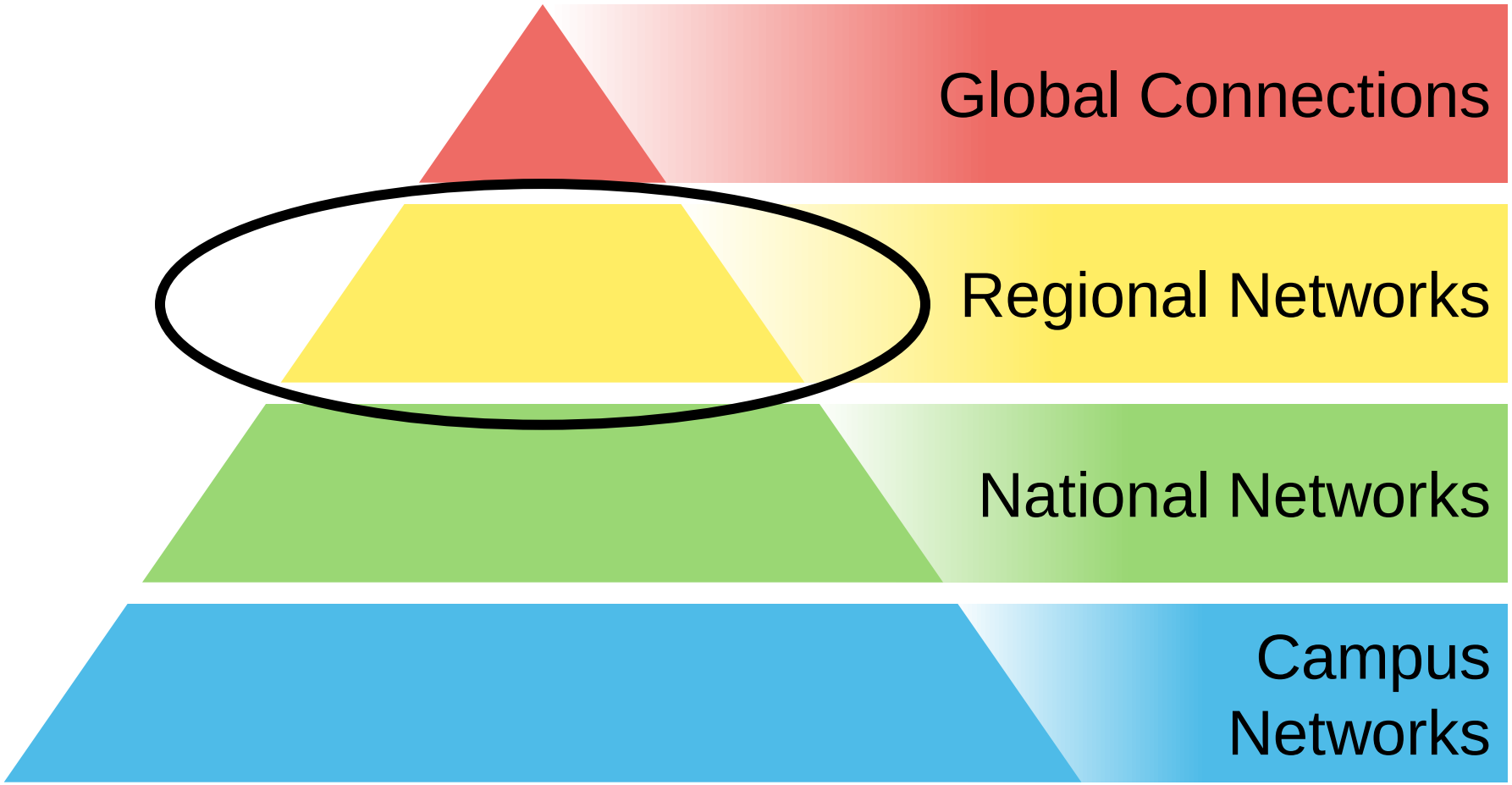


For further information regarding the international programs of Internet2, visit http://internet2.edu/international or contact Heather Boyles, International Relations Director, international@internet2.edu.

A listing of networks reachable via the Internet2 Network is found on the back of this page.


Asia-Pacific Backbone Topology
EU
RU
PK
NP
IN
BD
CN
KR
JP
US
LA
HK
TW
TH
VN
KH
LK
MY
PH
HI
SG
ID
AU
NZ
APAN(Affiliated)
TransPAC/PacificWave
SingAREN/Internet2
GEANT/TEIN(Affiliated)
JGN
SINET
AARNet
Others
As of Oct 7th, 2016

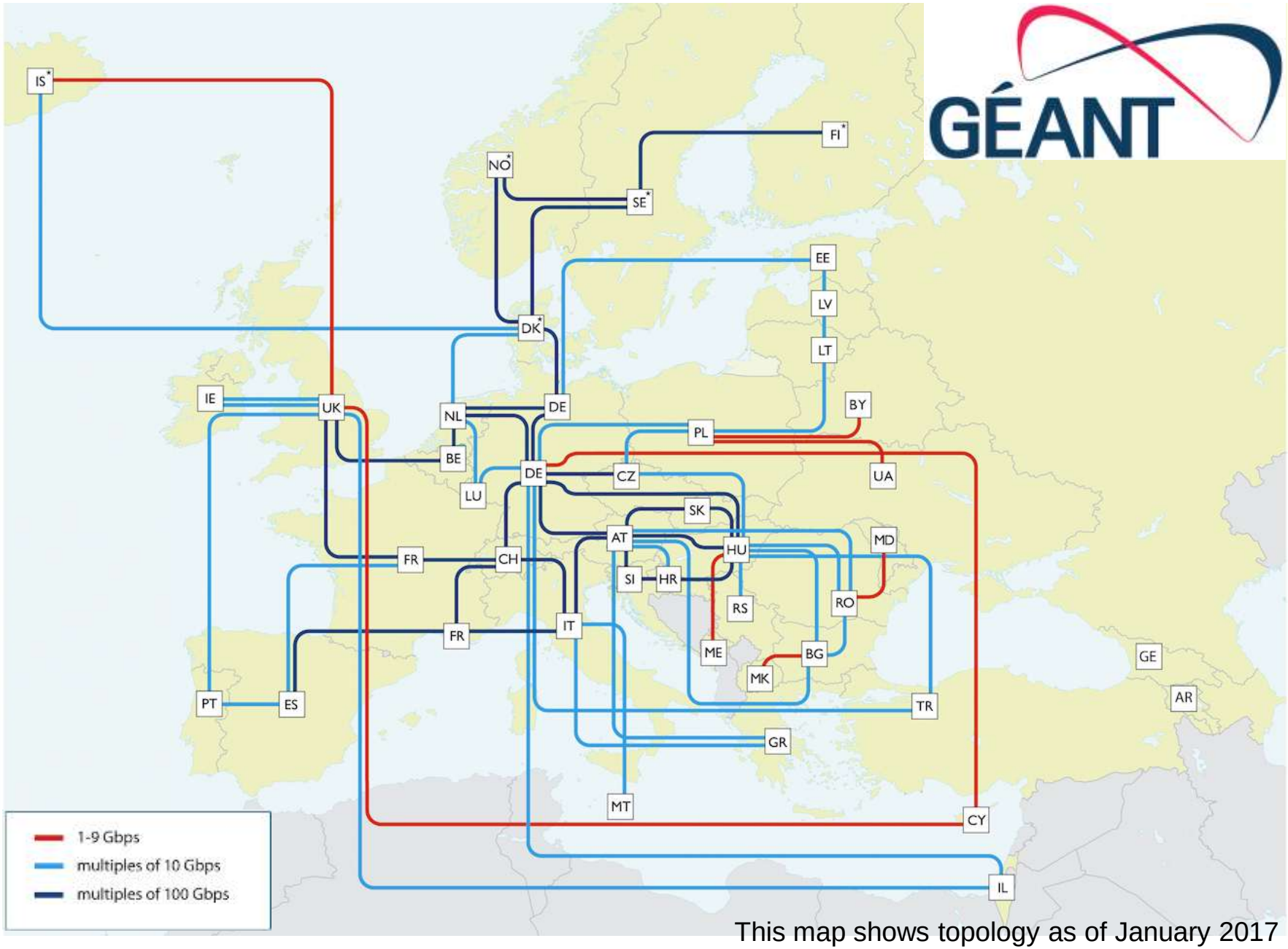
NREN EcoSystem



Regional REN Connections

- Regional RENs connect REN of individual countries within a geographic region
- Many regional networks have funding from European Union
  - CAREN, GEANT, ASREN, TEIN5/Asi@Connect, ALICE/ALICE2 (RedCLARA), Ubuntunet, WACREN, and ASREN


GÉANT
CAREN
Frankfurt
622 Mbps
600 Mbps
155 Mbps
Kazakhstan
Turkmenistan
Kyrgyzstan
Tajikistan
TEIN
TAR ENA
155 Mbps
Hong Kong
CAREN
CAREN
National R&E networks
Regional R&E networks
PoP
CAREN topology map
October 2014

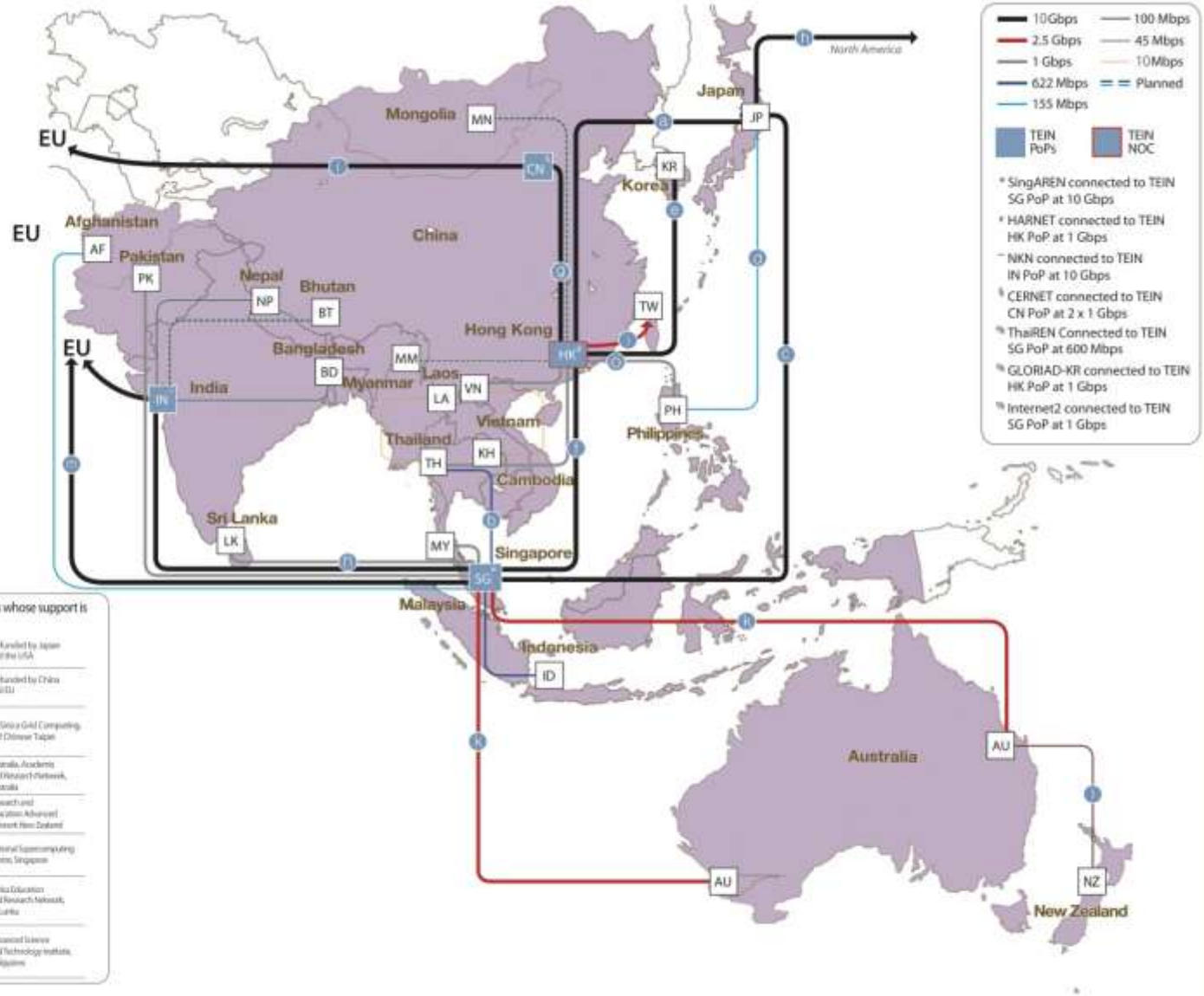


This map shows topology as of January 2017

TEIN

Connecting
Asia and Europe's
Research and Education
Communities

www.tein.asia



TEIN Project Partners

AF Afghanistan	ID Indonesia	NZ New Zealand
AU Australia	JP Japan	PK Pakistan
BD Bangladesh	KR Korea	PH Philippines
BT Bhutan	LA Laos	SG Singapore
KH Cambodia	MM Myanmar	LK Sri Lanka
CN China	MN Mongolia	TH Thailand
HK Hong Kong	MY Malaysia	TW Taiwan
IN India	NP Nepal	VN Vietnam

The following links are fully financed/co-financed by the link owners whose support is gratefully acknowledged

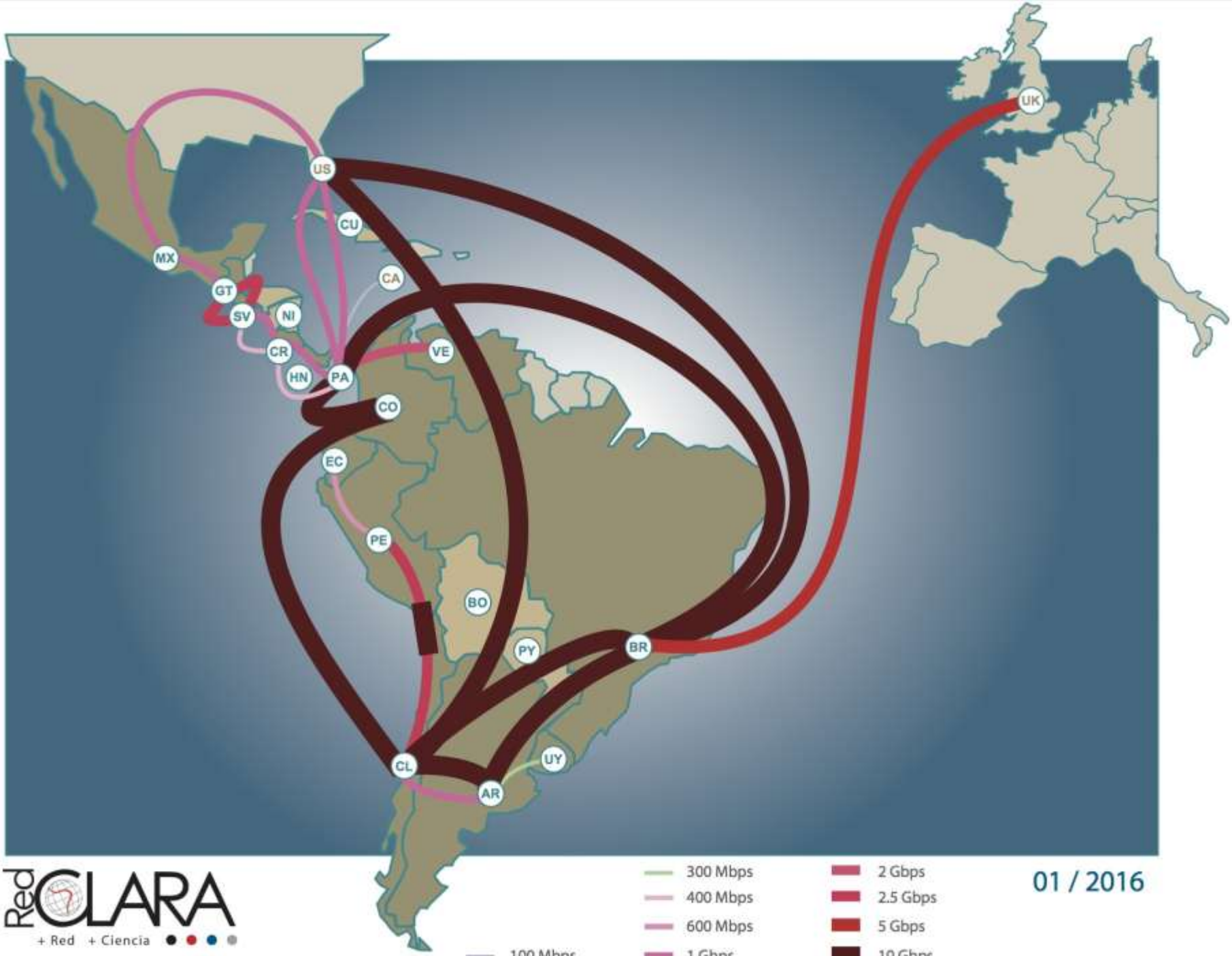
a NICT — National Institute of Information and Communications, Japan
b NICT — National Institute of Information and Communications, Japan; Thailand Research and Education Network, Thailand
c NII — National Institute of Informatics, Japan
d MAFFIN — Ministry of Agriculture, Forestry and Fisheries Research Network, Japan
e f NIA — National Information Society Agency, South Korea
g China Education and Research Network, China; China Science & Technology Network, China
h TransPAC — co-funded by Japan and the USA
i ORIENTplus — co-funded by China and EU
j ASGC — Academia Sinica Grid Computing, Republic of Chinese Taipei
k aarnet — Australia, Academic and Research Network, Australia
l REANNZ — Research and Education Advanced Network New Zealand
m National Supercomputing Centre, Singapore
n LEARN — Lanka Education and Research Network, Sri Lanka
o Advanced Science and Technology Institute, Philippines

As of December 2016

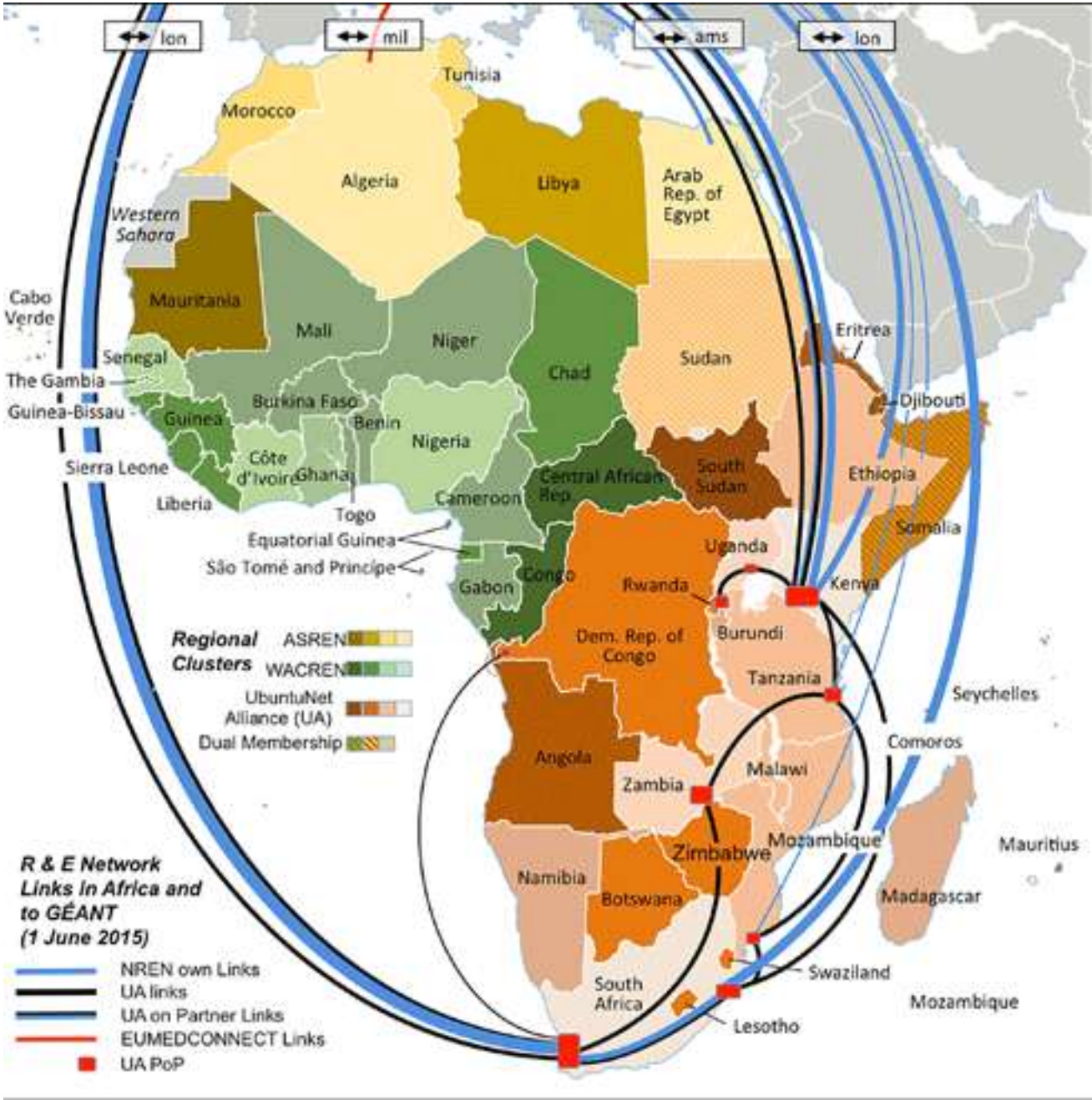
TEIN*CC COOPERATION CENTER
www.teincc.org

TEIN is co-funded by the European Commission through the Directorate-General for Development and Cooperation-EuropeAid

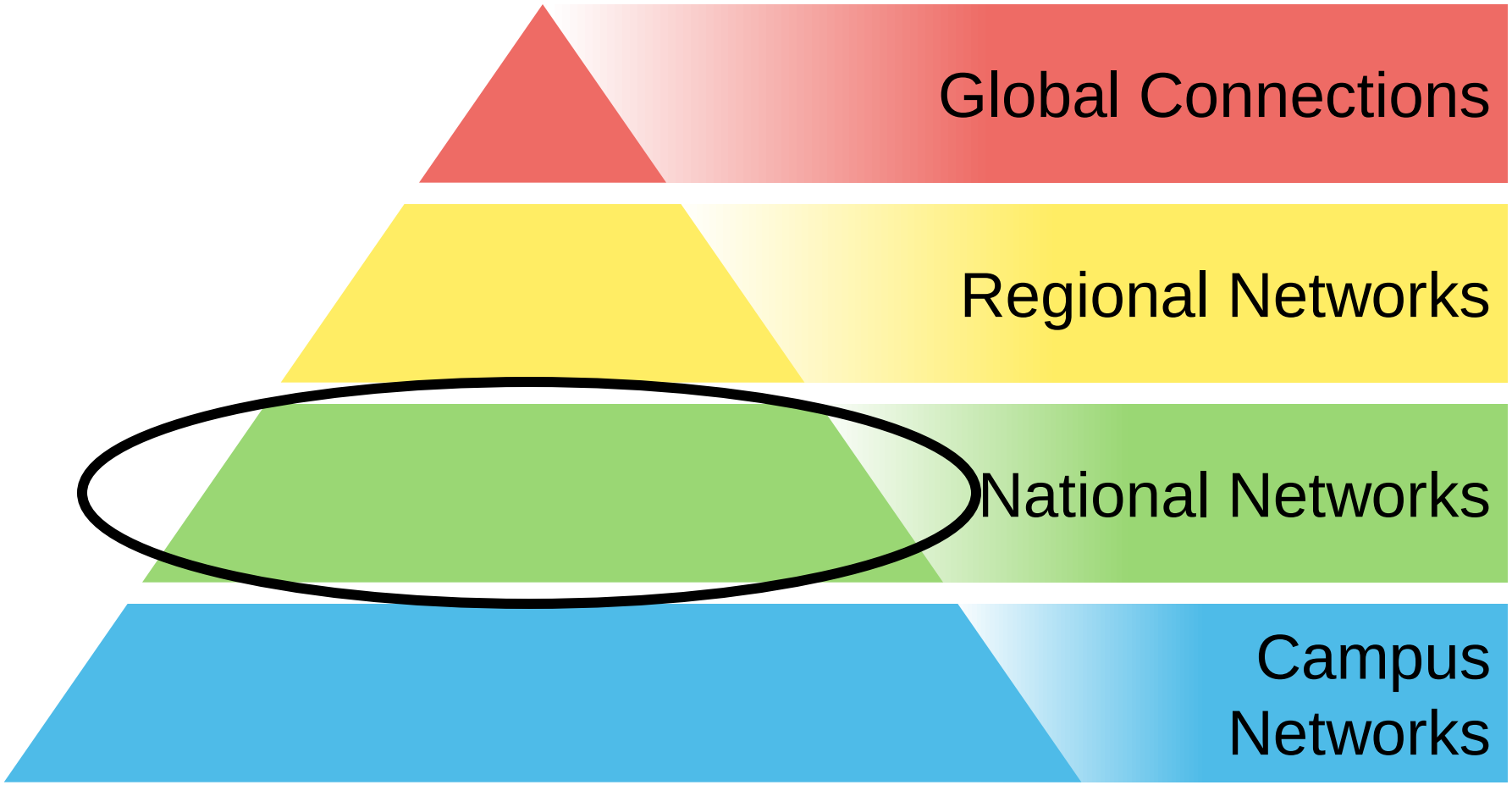
This map has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of TEIN*CC and can under no circumstances be regarded as reflecting the position of the European Union.


US
CU
MX
CA
GT
SV
NI
CR
HN
PA
VE
CO
EC
PE
BO
PY
BR
CL
UY
AR
UK
Red CLARA
+ Red + Ciencia
100 Mbps
300 Mbps
400 Mbps
600 Mbps
1 Gbps
2 Gbps
2.5 Gbps
5 Gbps
10 Gbps
01 / 2016

AfricaConnect2: UbuntuNet and WACREN



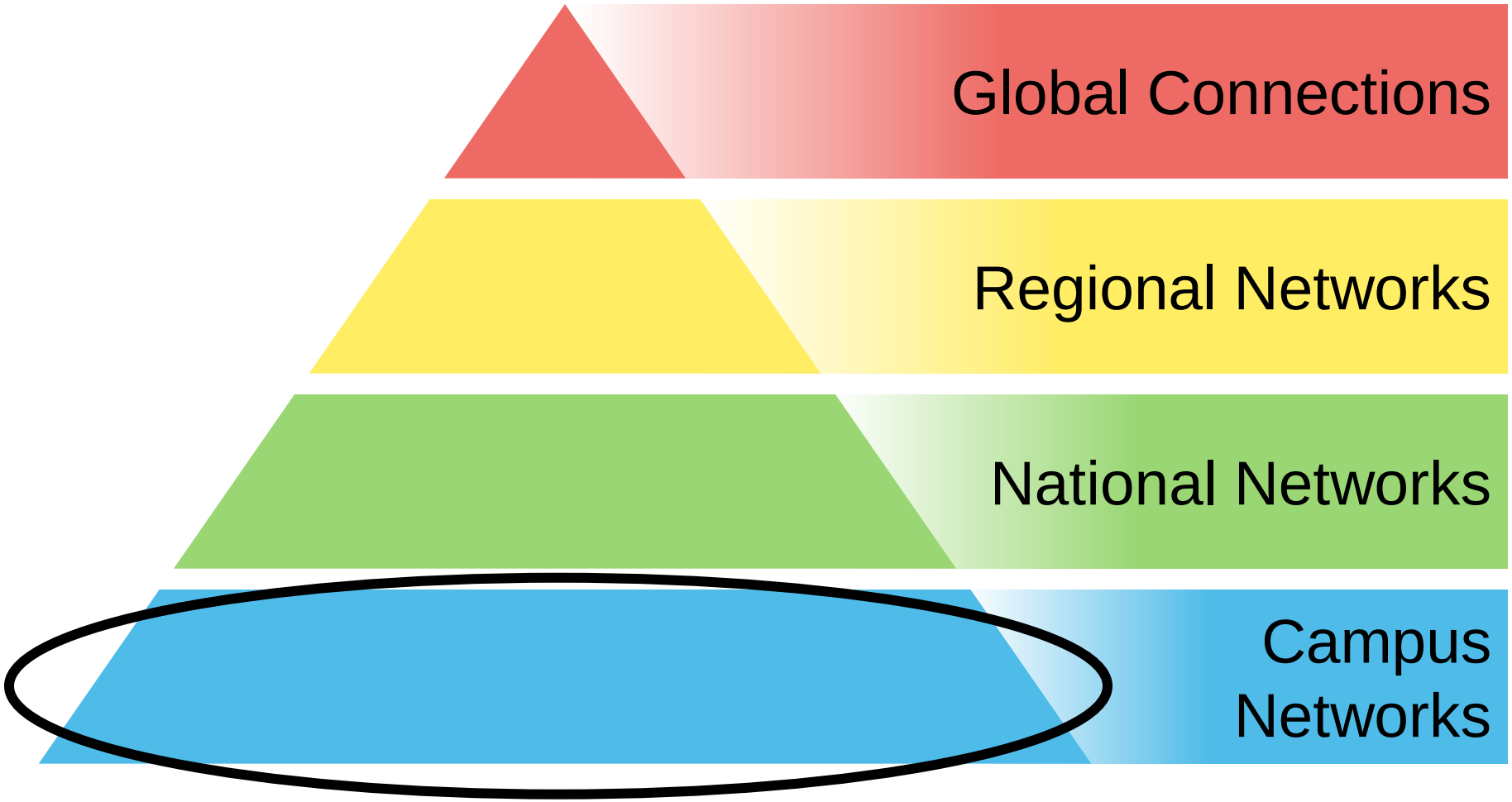
NREN EcoSystem



National RENs (NRENs)

- Provides service to Universities, Colleges, research labs, and others in an entire country
- Often hosted and operated by a prestigious university in the country
- Often provides “value add” services to members
  - Video conferencing, e-learning, web hosting, data center space for disaster recovery, etc.

NREN EcoSystem



Campus Network Role

- No student, researcher, or faculty member is connected directly to a Global, National, or Regional Network.
  - They are all connected to a campus network
- Without a good campus network, the entire ecosystem is affected
  - You can have a 100-gigabit connection to your Regional Network and a 100-gigabit backbone in your national network, but if the users have a poor connections on campus, the entire investment is wasted
- The campus network is the foundation that the entire REN ecosystem is built upon

Foundation Failures

Foundation Failures

Campus Network Challenges

- Many campus networks are not structured properly and can't effectively utilize high bandwidth connections
- Many make heavy use of NAT and firewalls that limit performance
- Many are built with unmanaged network equipment that provide no ability for monitoring or tuning the network
- Some NRENs force campus to dual home

Campus Network Structure

- Campus networks have often grown organically over time without thought to proper architecture
- Campus networks are often built with outdated fiber optic cabling that can't support high speeds
  - Multi mode fiber is bad

Campus Network Challenges

- Many are not structured properly and can't effectively utilize high bandwidth connections
- Many make heavy use of NAT and firewalls that limit performance
- Many are built with unmanaged network equipment that provide no ability for monitoring or tuning the network

How to Best Support R & E

- Research and Education needs flexible and open networks
- Things to consider
  - NAT makes some things hard (H.323 video conferencing)
  - Filtering makes it hard for researchers, teachers, and students to do interesting things
  - Your campus network must not be the bottleneck
- Make a plan for improvement – without a plan, how will you get there.

Campus Network Rules

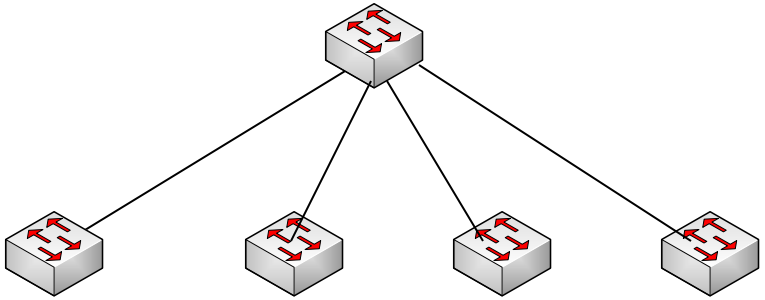
- Minimize number of network devices in any path
- Use standard solutions for common situations
- Build Separate Core and Edge Networks
- Provide services near the core
- Separate border routers from core
- Provide opportunities to firewall and shape network traffic

Core versus Edge

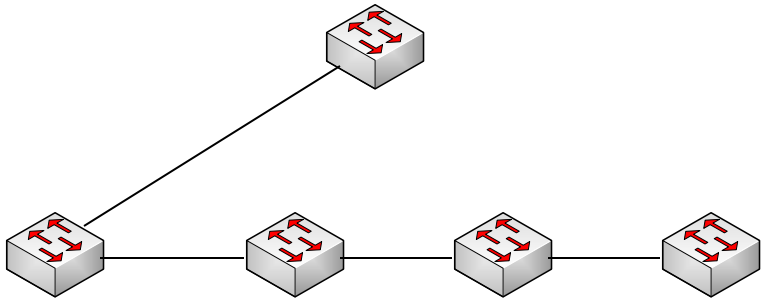
- Core network is the “core” of your network
  - Needs to have reliable power and air conditioning
  - May have multiple cores
  - Always route in the core
- Edge is toward the edges of your network
  - Provide service inside of individual buildings to individual computers
  - Always switch at the edge

Minimize Number of Network Devices in the Path

- Build star networks



- Not daisy chained networks

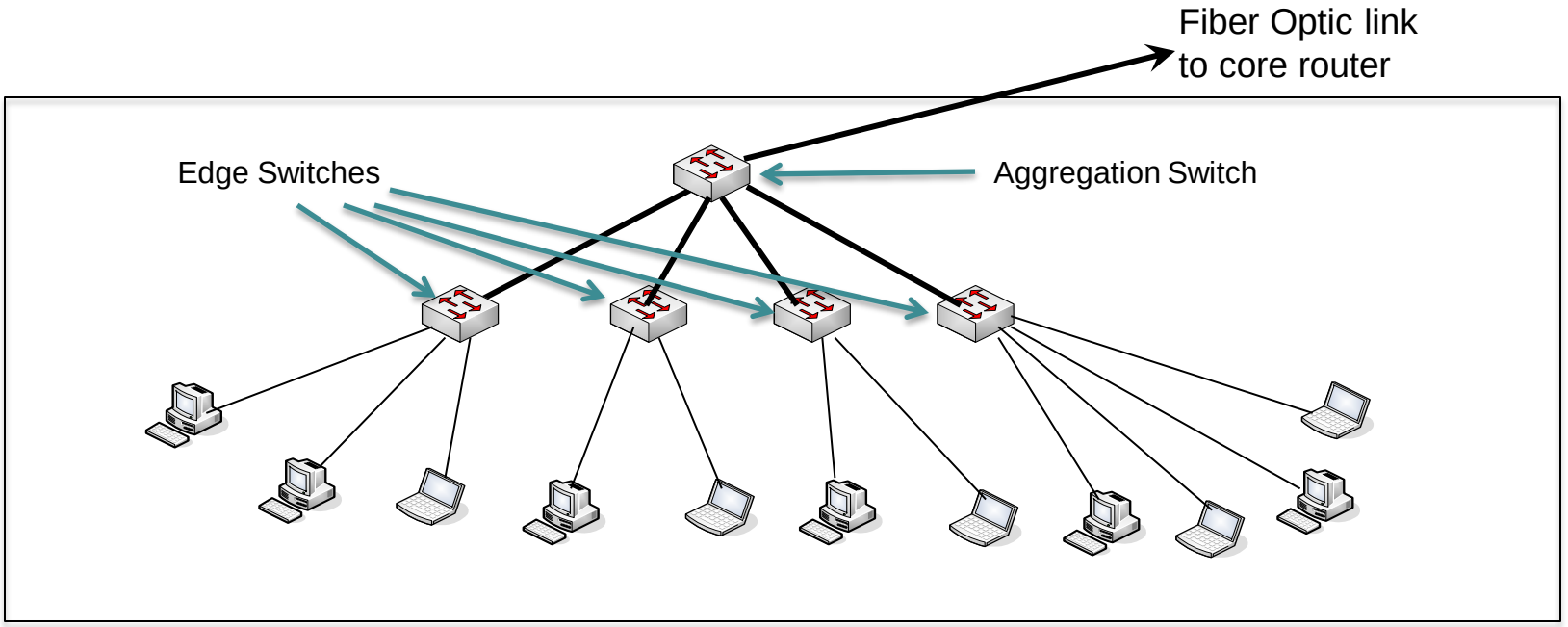


Edge Networks (Layer 2 LANs)

- Provides Service to end users
- Each of these networks will be an IP subnet
- Plan for no more than 250 Computers at maximum
- Should be one of these for every reasonable sized building
- This network should only be switched
- Always buy switches that are managed – no unmanaged switches!

Edge Networks

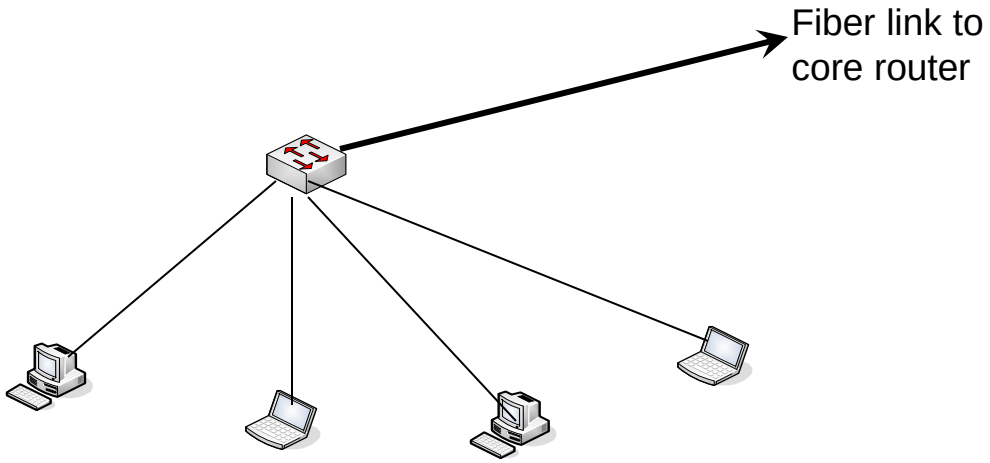
- Make every network in every building look like this:



One Building

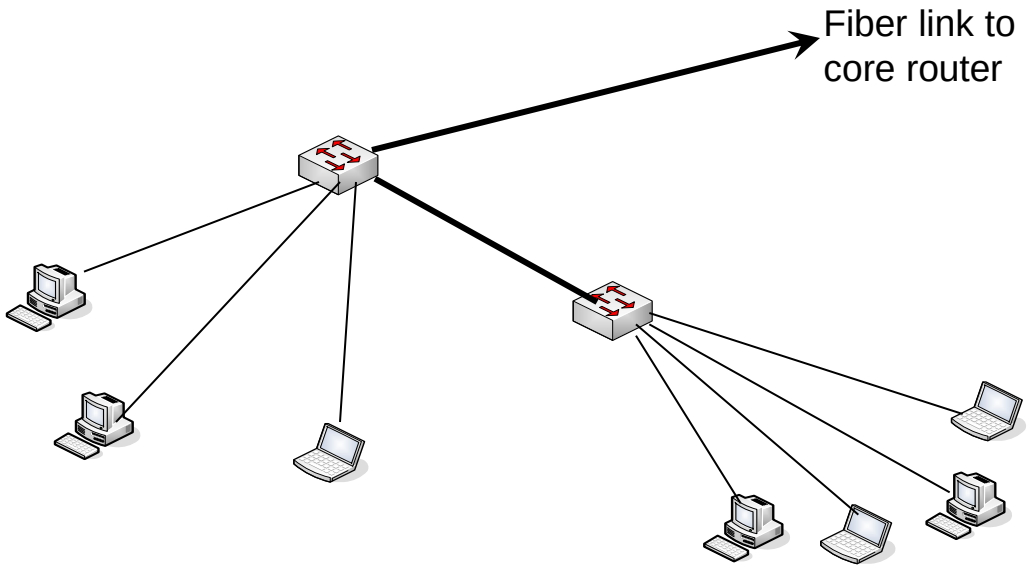
Edge Networks Continued

- Build Edge network incrementally as you have demand and money
- Start Small:



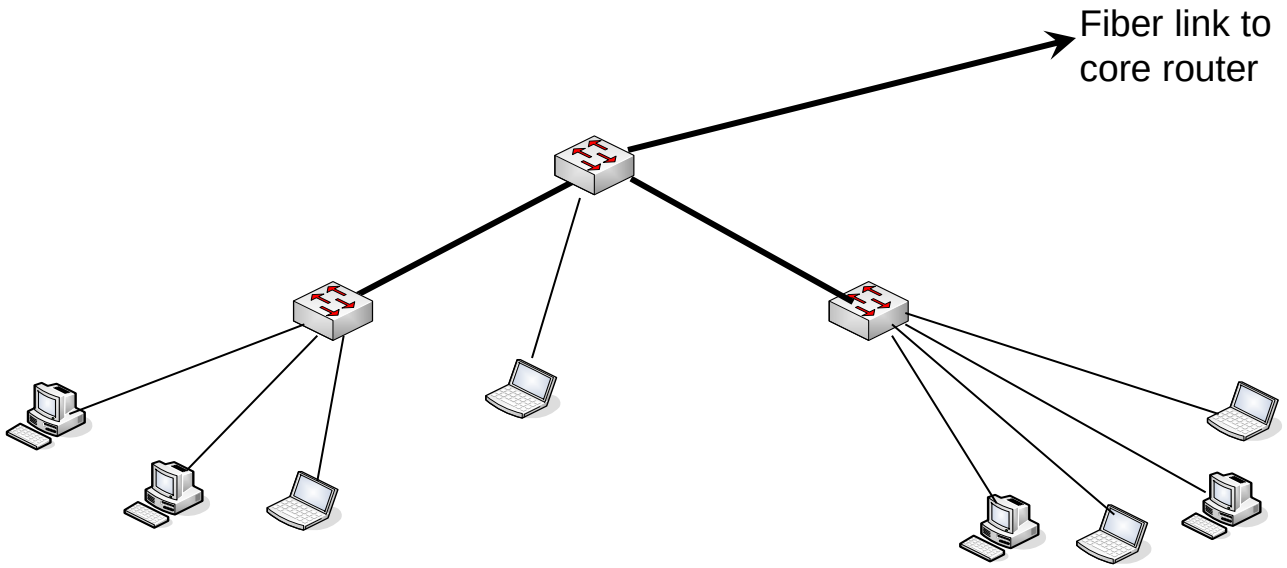
Edge Networks Continued

- Then as you need to add machines to the network, add a switch to get this:



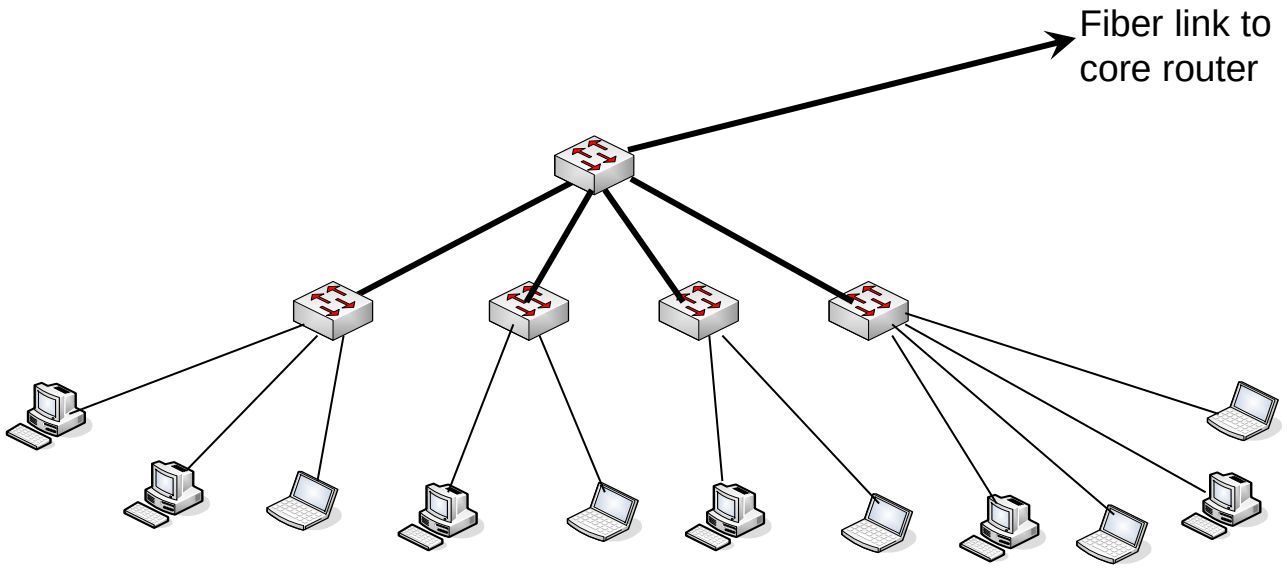
Edge Networks Continued

- And keep adding switches to get to the final configuration



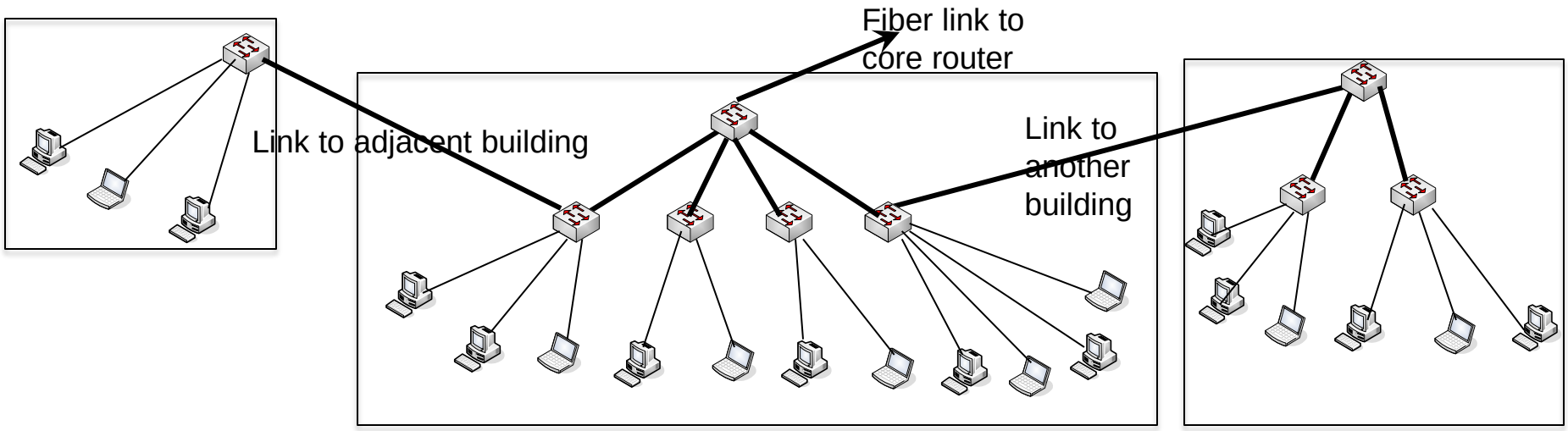
Edge Networks Continued

- And keep adding switches to get to the final configuration



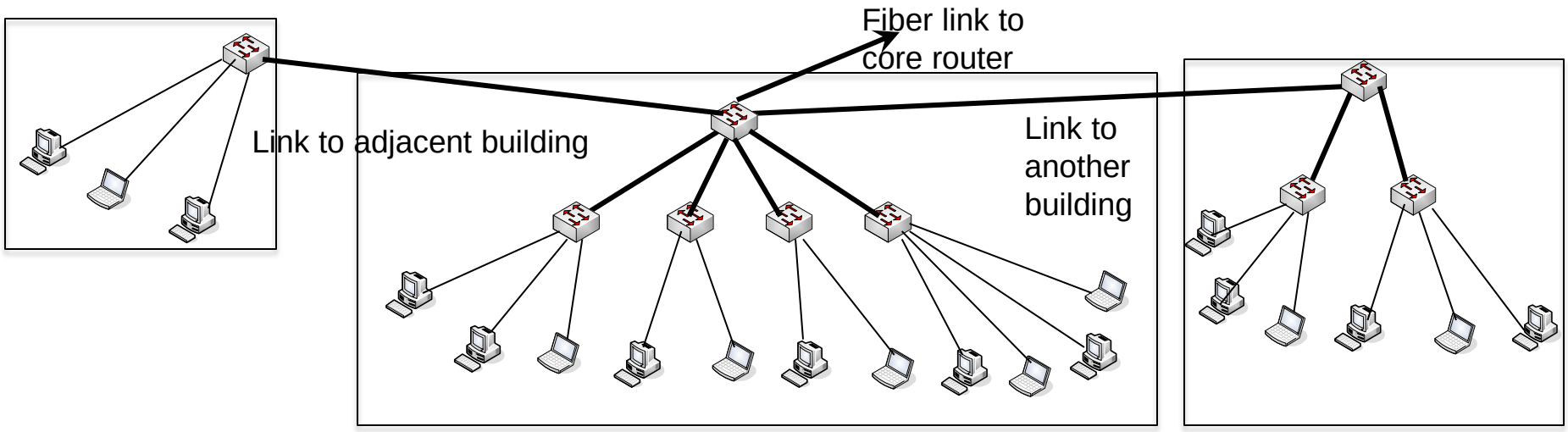
Edge Networks Continued

- Resist the urge to save money by breaking this model and daisy chaining networks or buildings together
- Try hard not to do this:



Edge Networks Continued

- There are cases where you can serve multiple small buildings with one subnet.
- Do it carefully.



Core Network

Routing versus Switching
Layer 3 versus Layer 2

- Routers provide more isolation between devices (they stop broadcasts)
- Routing is more complicated, but also more sophisticated and can make more efficient use of the network, particularly if there are redundancy elements such as loops

Layer 3 Switches

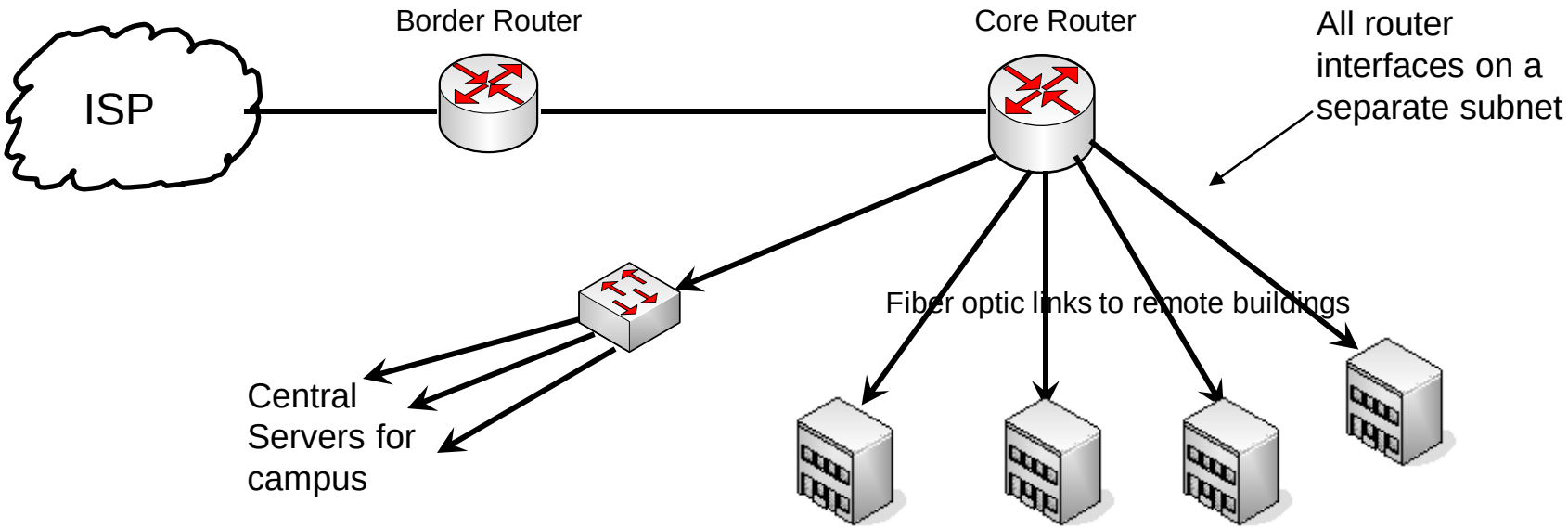
- Many vendors use the term “Layer 3 Switch”.
- These are contradictory terms
  - Layer 3 = Routing
  - Switch = Layer 2
- What vendors mean is that it is a device that can be configured as a router or a switch or possibly both at the same time.

Core Network

- Reliability is the key
  - Remember many users and possibly your whole network relies on the core
- May have one or more network core locations
- Core location must have reliable power
  - UPS battery backup (redundant UPS as your network evolves)
  - Generator
  - Grounding and bonding
- Core location must have reliable air conditioning

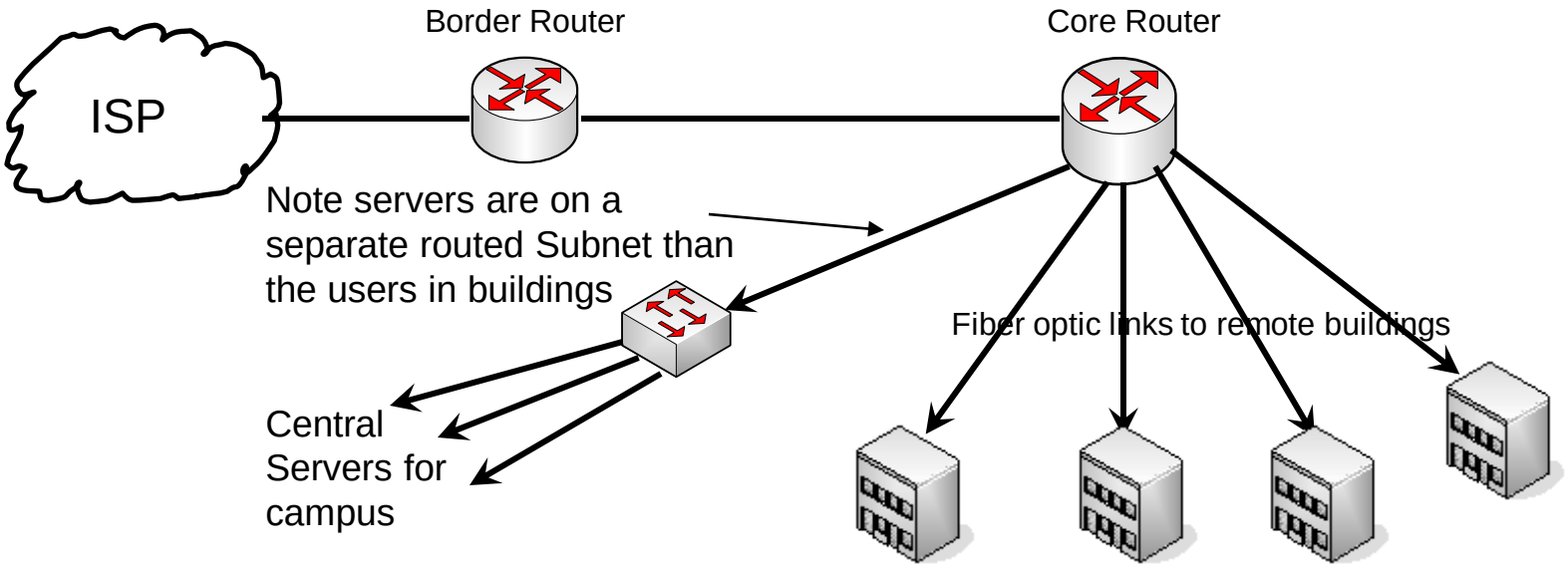
Core Network

- At the core of your network should be routers – you must route, not switch.
- Routers give isolation between subnets
- A simple core:



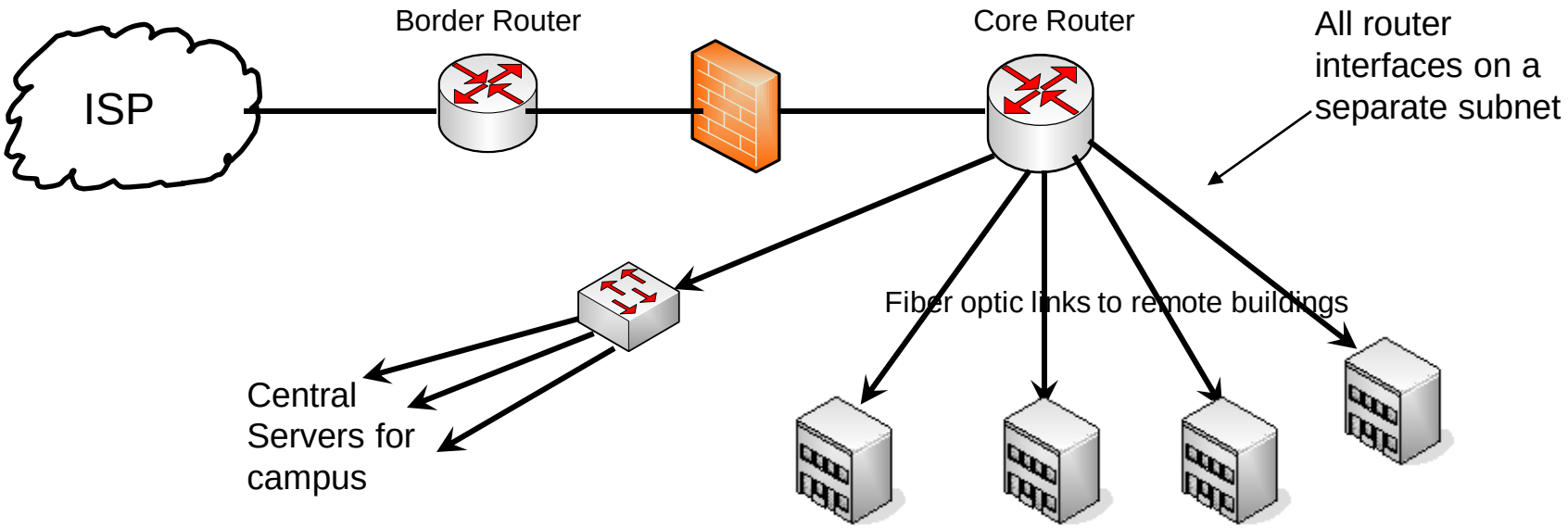
Where to put Servers?

- Servers should never be on the same subnet as users
- Should be on a separate subnet off of the core router
- Servers should be at your core location where there is good power and air conditioning



Where to put Firewalls

- Security devices are often placed “in line”
- Campuses often take a corporate strategy to firewall all of their campus
- This is a typical design:

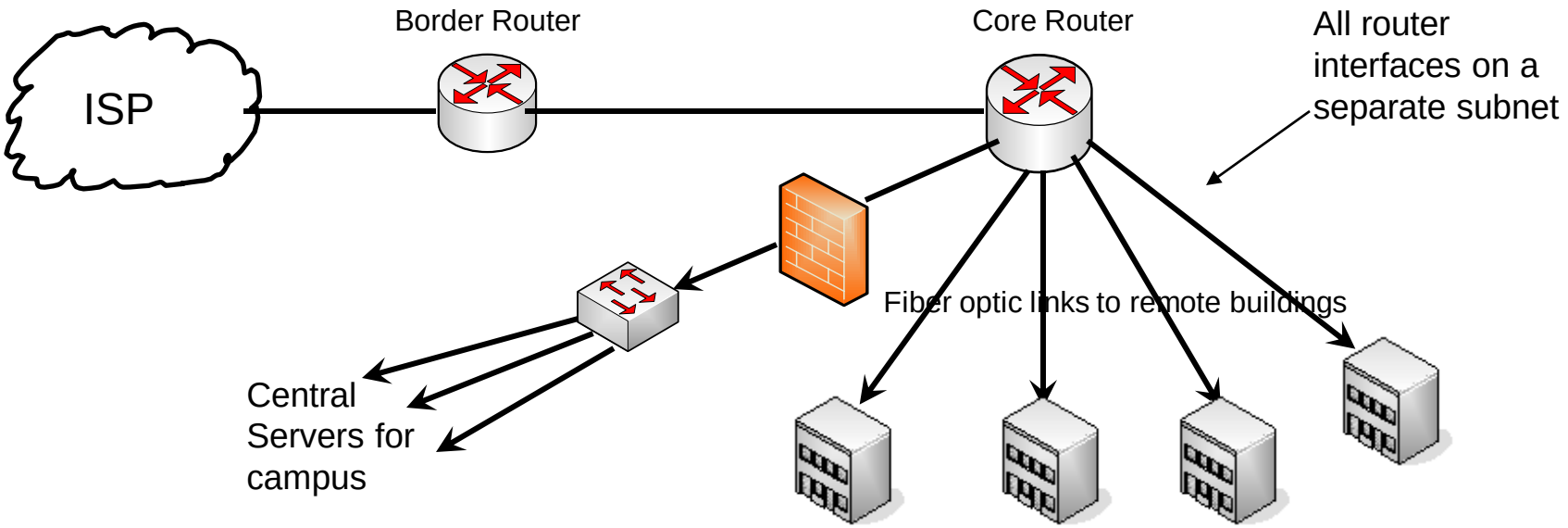


Firewall Placement

- Campuses are not corporate environments
- Firewalls don't protect users from getting viruses that come via two mechanisms
  - "clicked links" while web browsing
  - Email attachments
  - Both are encrypted and firewalls won't help
- As bandwidth increases, in-line firewalls limit performance for all users. This gets to be a bigger problem at higher speeds.

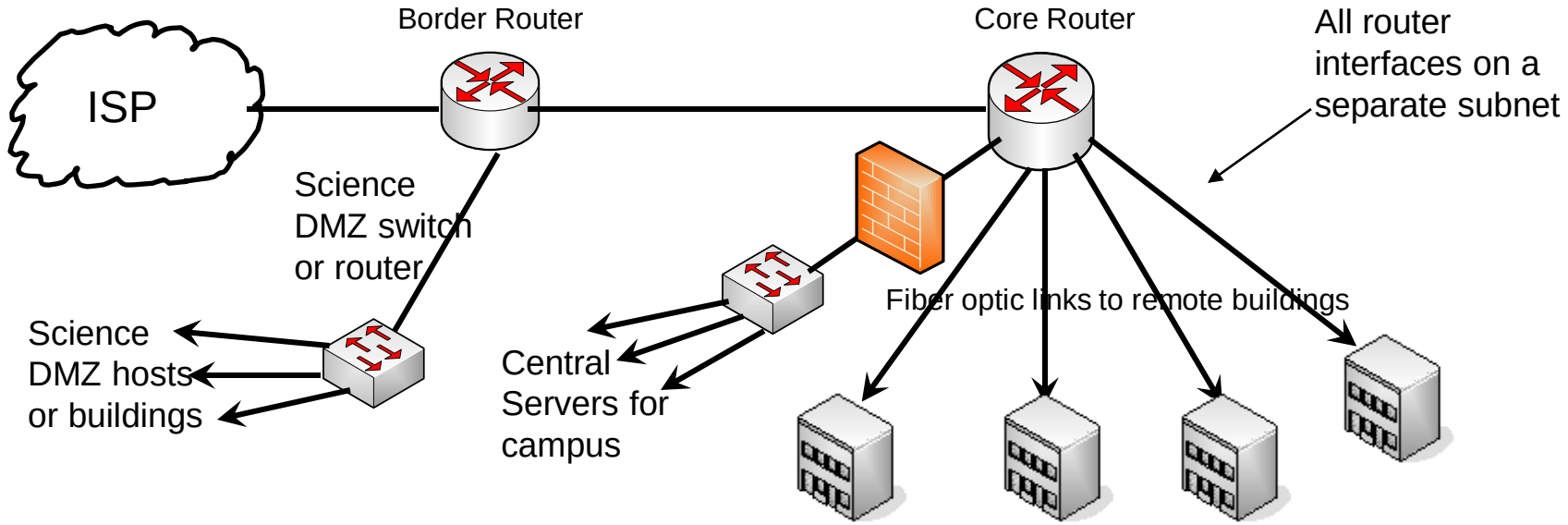
Alternative Suggestion

- Since Firewalls don't really protect users from viruses, let's just think about protecting critical server assets
- This is a typical/better design:



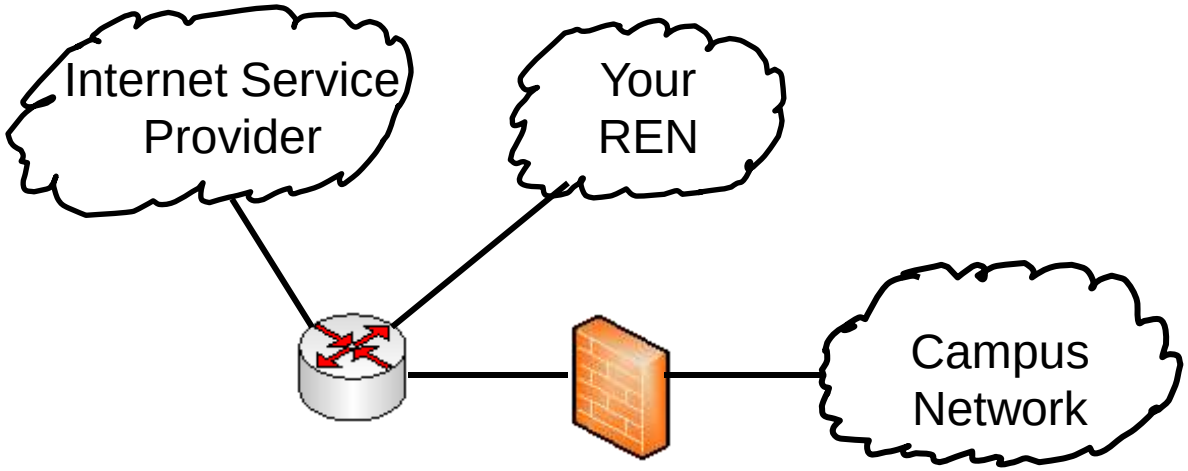
Science DMZ

- Some campuses can't develop the political backing to remove firewalls for the majority of the campus
- Consider moving high bandwidth devices from behind firewall (this is sometimes called the Science DMZ)
- Recommended Configuration:

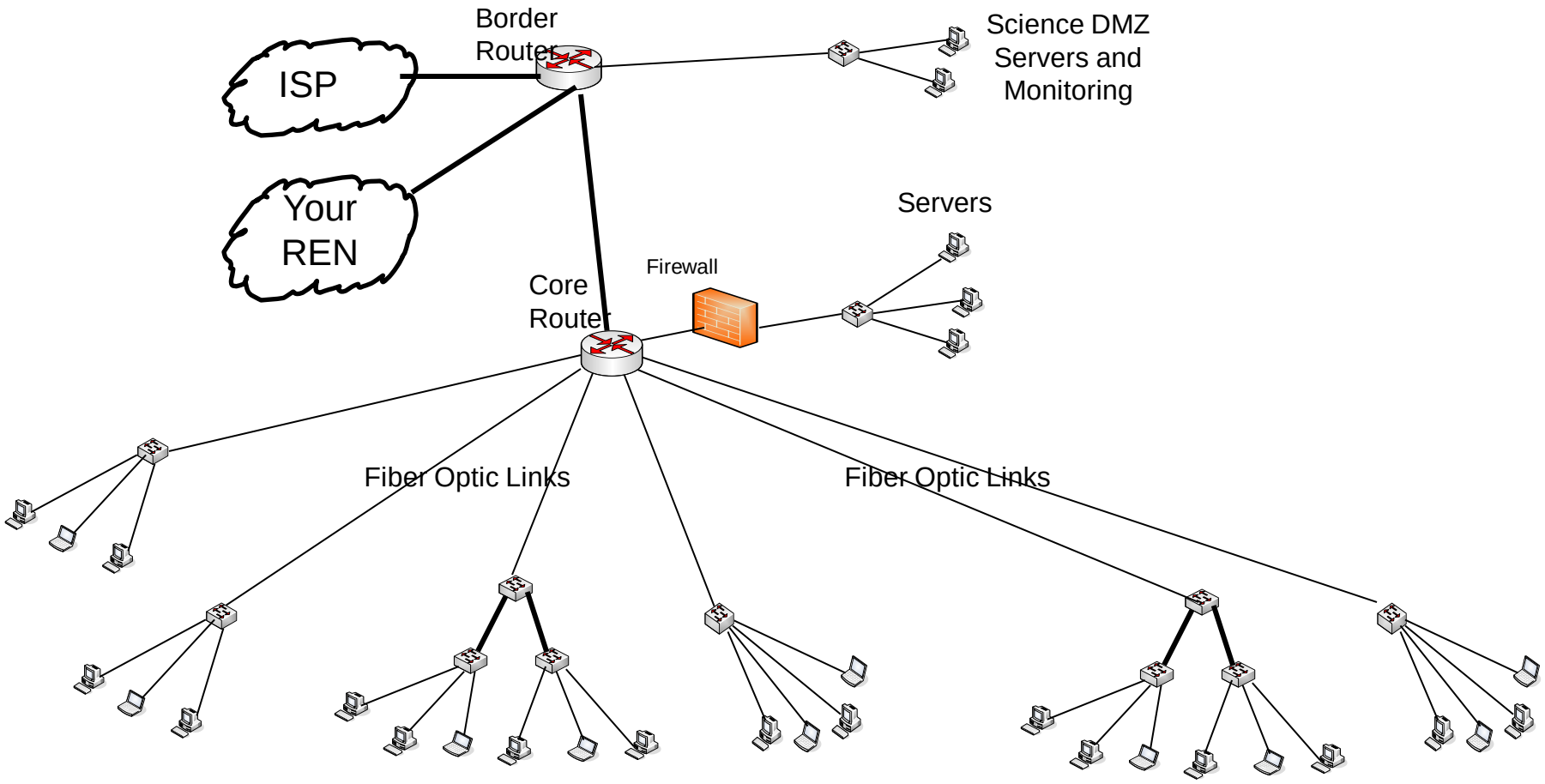


Border Router

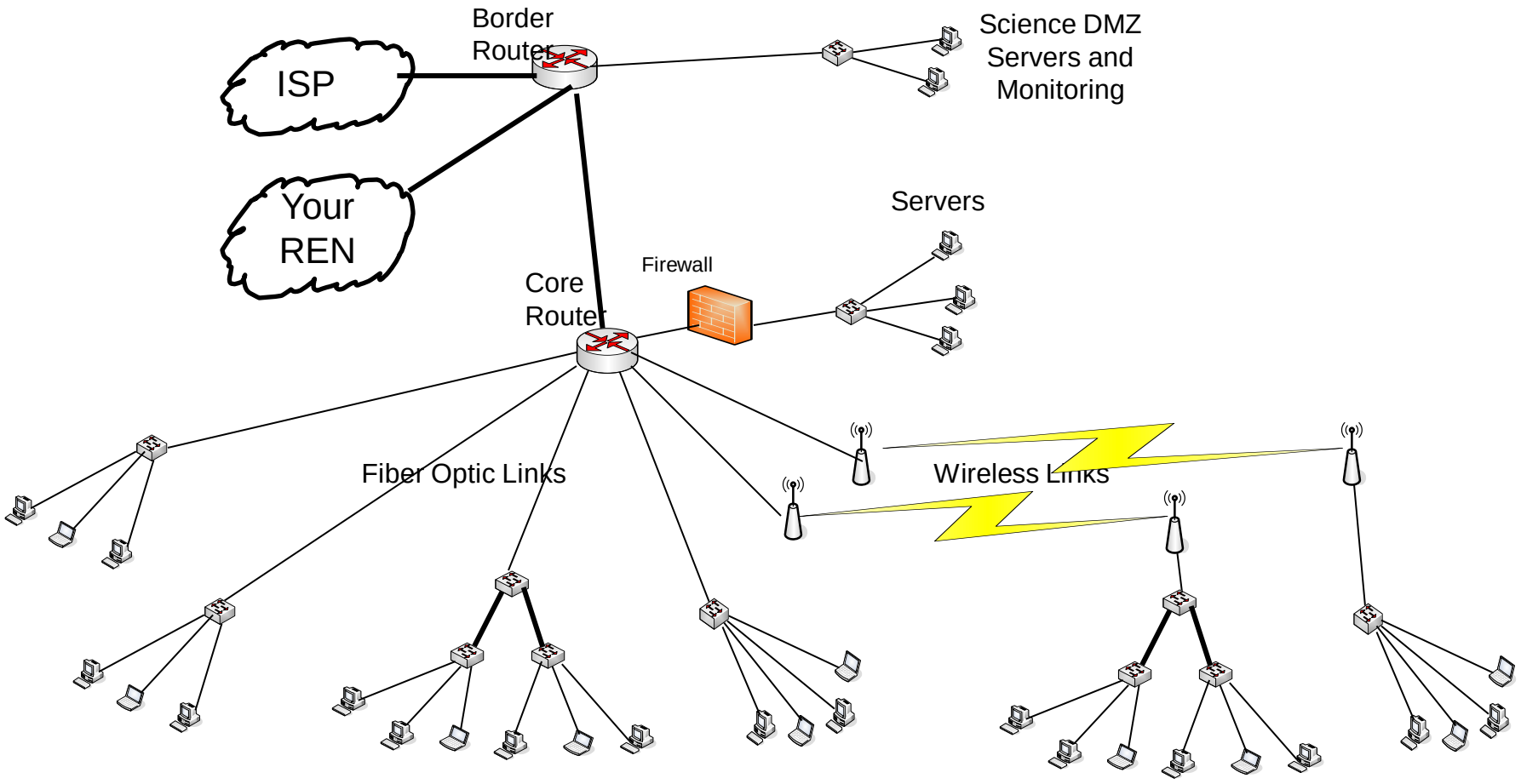
- Connects to outside world
- Many campuses in emerging regions will do NAT on these border routers.
- If you are dual home, you **must** have a border router (dual homing is hard to make it work right)



Putting it all Together



Wireless Links Instead of Fiber



Layer 2 and 3 Summary

- Route in the core
- Switch at the edge
- Build star networks – don’t daisy chain
- Buy only managed switches – re-purpose your old unmanaged switches for labs

Questions?