Practical Network Defense

Master's degree in Cybersecurity 2018-19

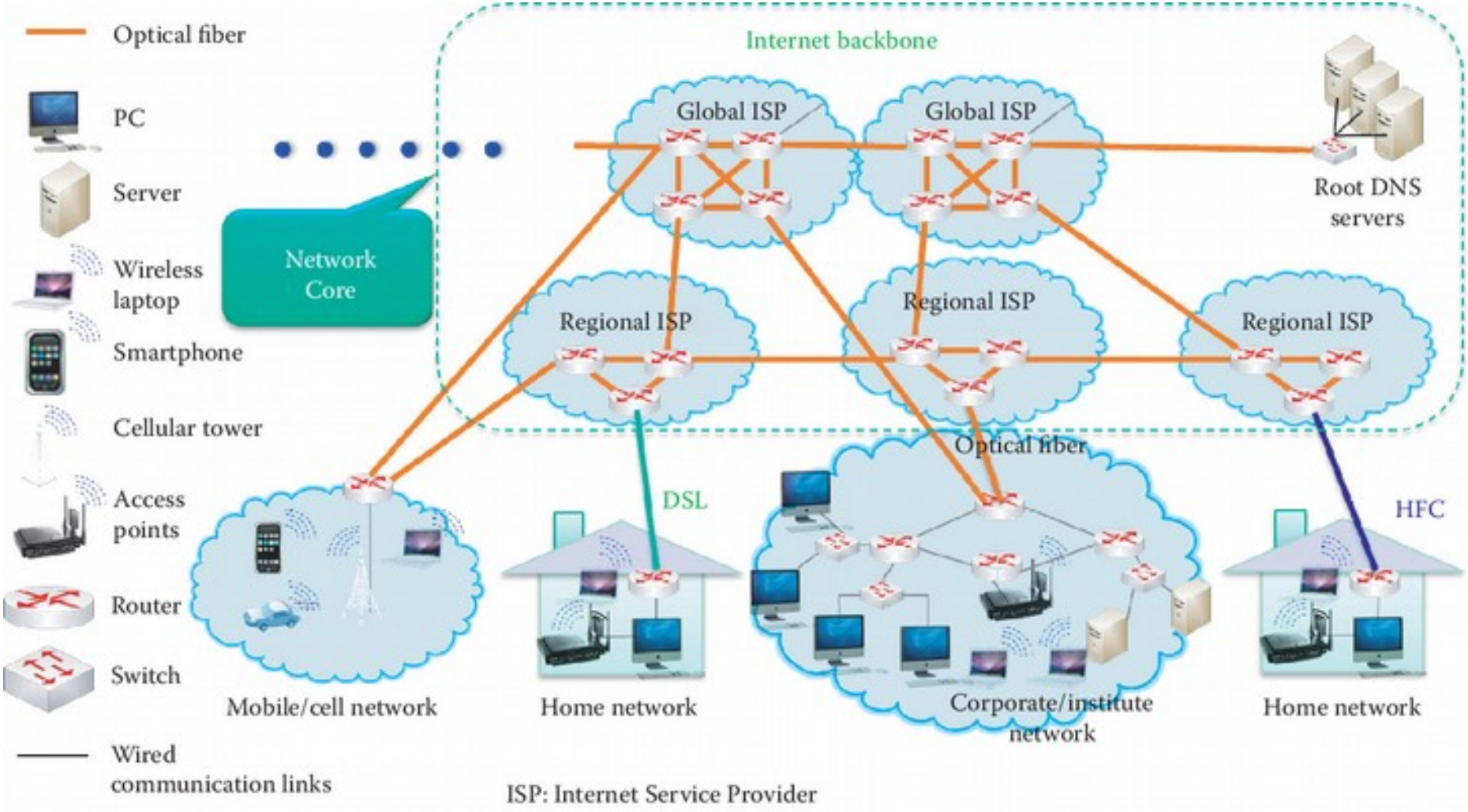
Networking refresh

Angelo Spognardi
spognardi@di.uniroma1.it
Dipartimento di Informatica
Sapienza Università di Roma

What is Internet

- Internet: an interconnected network of networks
  - Hierarchical networks:
    - Internet backbone: connecting the ISPs' backbones
    - ISP backbone: connecting organizations' backbones
    - Organization backbone connects local area networks (LANs)
    - LAN connects end systems
  - Public Internet versus private intranet
- Internet standards
  - RFC: Request for comments
  - IETF: Internet Engineering Task Force
  - Free download of RFCs at rfc-editor.org

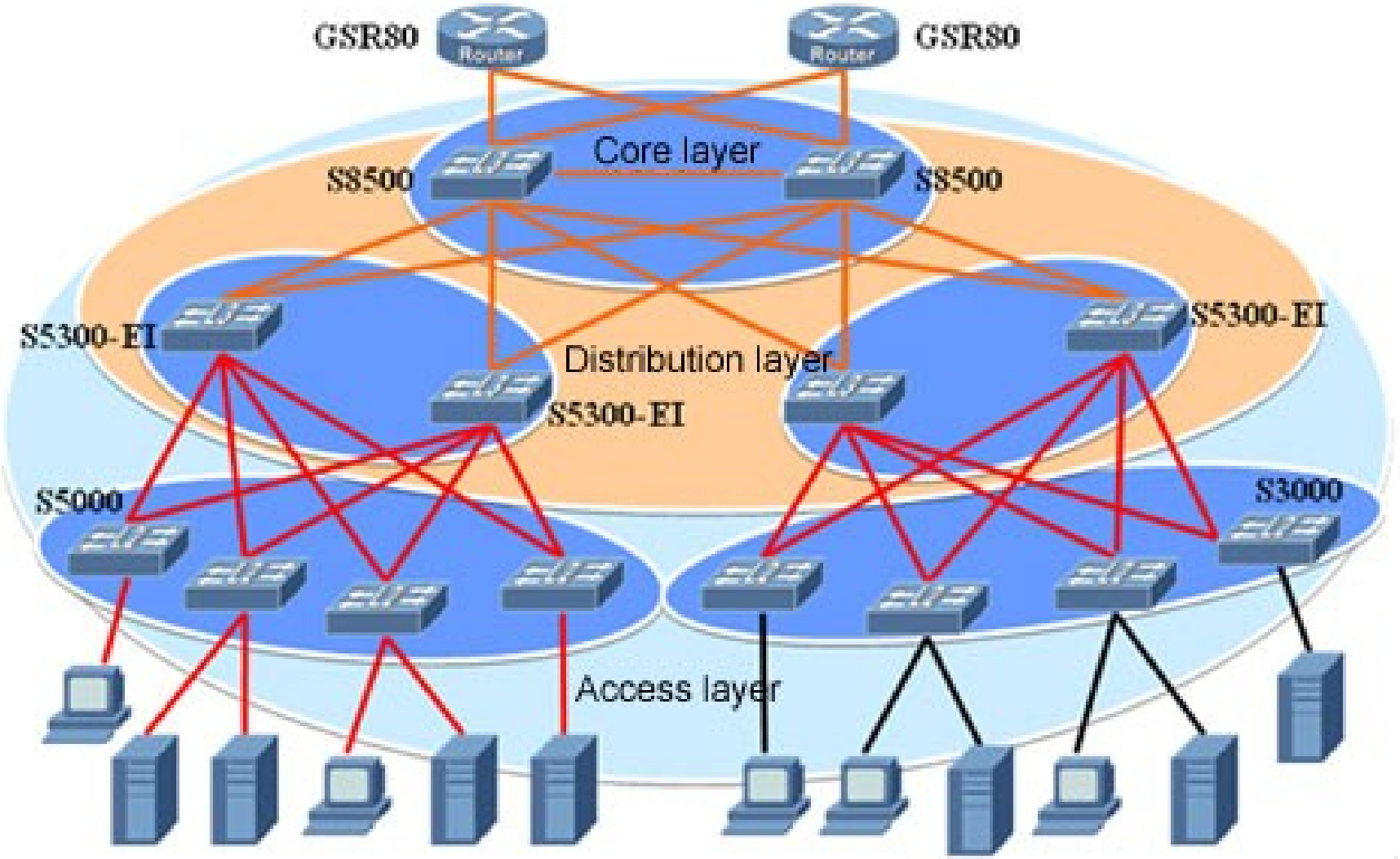
Internet architecture



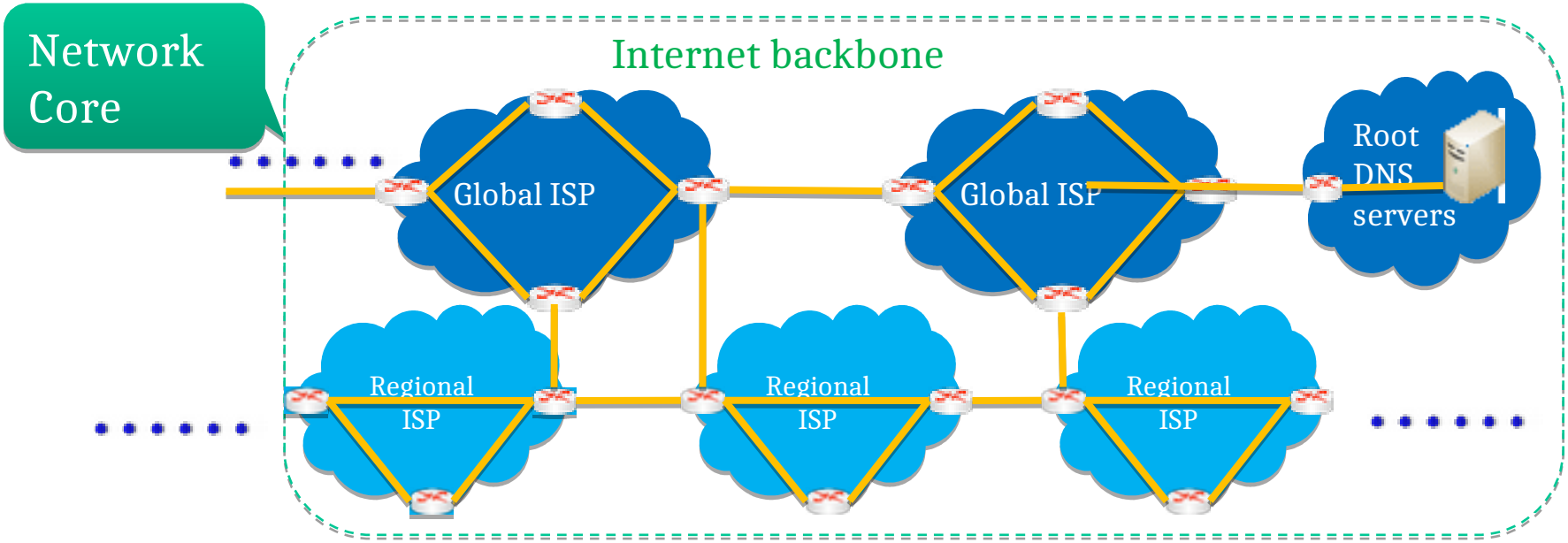
Internet hierarchy

- Network edge
  - Hosts: server, client, P2P
  - Applications: http, mail, Facebook, Twitter
- Network core
  - Edge router: connecting an organization/ISP to the Internet
  - Interconnection of routers using fiber
  - Naming services
- Access networks
  - Wired, or wireless communication links

Internet, hierarchical approach

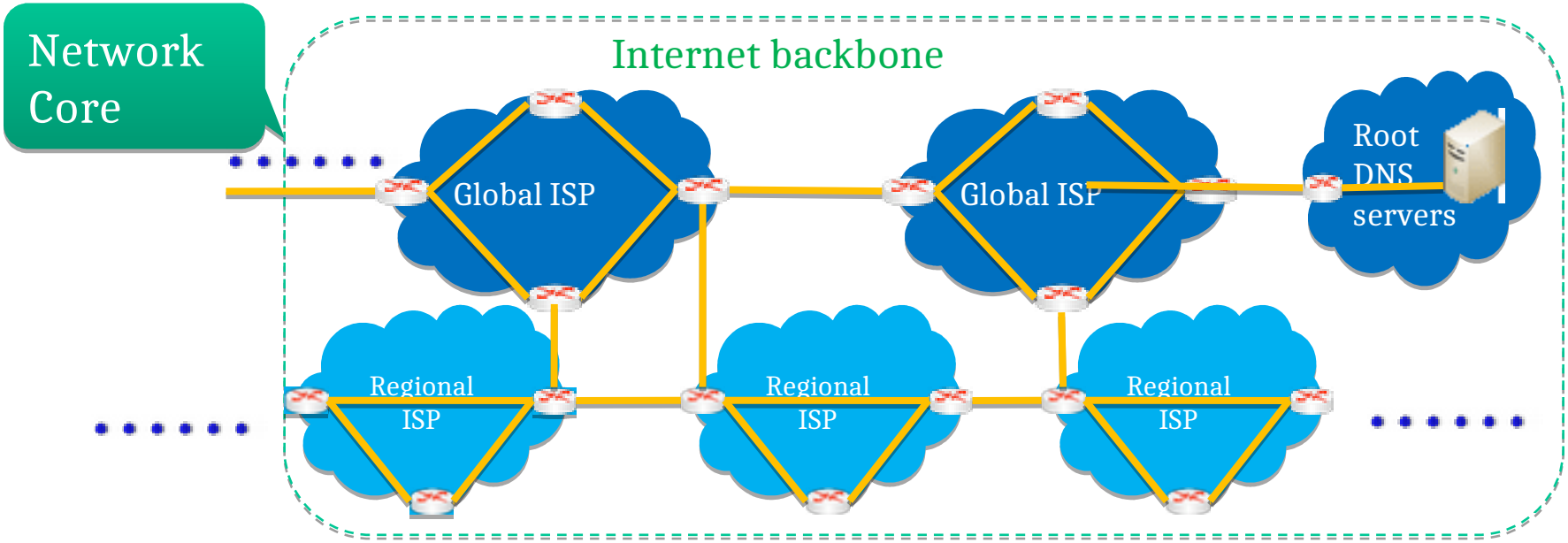


Internet Core



- Routers and fiber links (in orange) form the Internet core
- Routers work together to figure out the most efficient path for routing a packet from source to destination host
  - A distributed algorithm can adapt to changing Internet conditions
    - Great idea during the cold war
  - Routing tables are generated and maintained in real time

Internet core management: ISPs

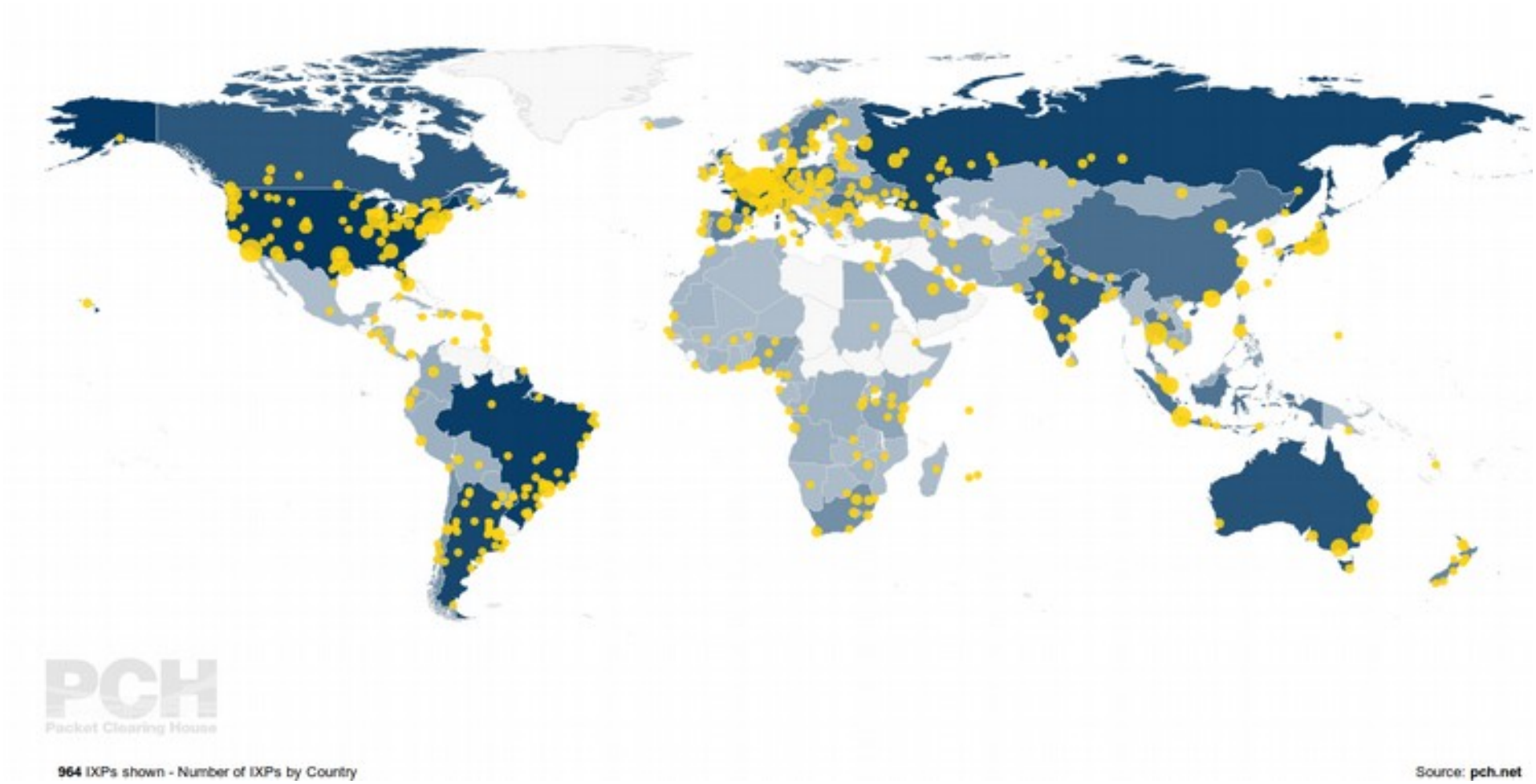


- The core is provided by ISPs that interconnect multiple continents
- ISPs
  - Global ISPs or Tier-1 ISPs
  - Regional ISPs or Tier-2 ISPs

Internet: network of networks

- Internet Backbone connects tier-1 ISPs
  - e.g., Verizon, Sprint, AT&T, Qwest, Level 3 Communications
- The backbones of tier-1 ISPs are interconnected at various access points called Internet eXchange Points (IXP)
- The number of IXPs around the world is continually growing
  - to date more than 1000
- Interactive (probably not exhaustive) map: https://www.pch.net

Global map of Internet eXchange Points



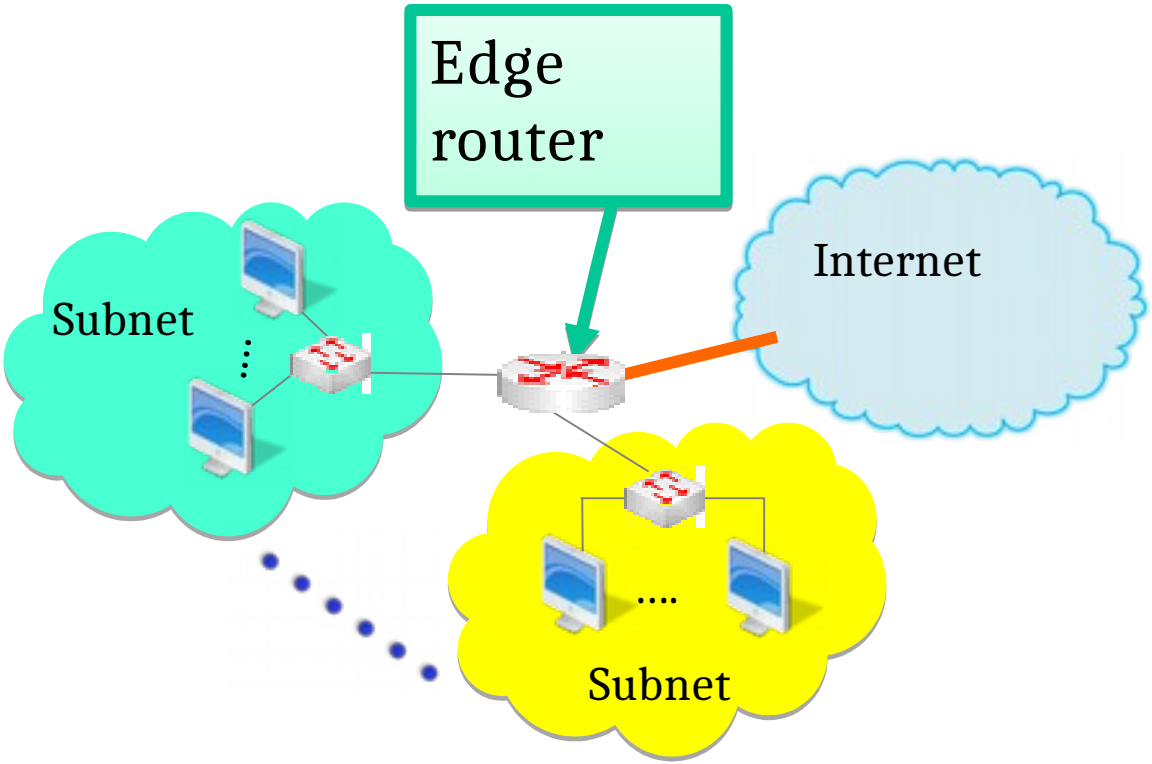
Protocols

- Specify rules about the desired service
  - Procedure Rules
    - Types and sequences of messages exchanged
      - Syntax and semantics
    - Actions to take with respect to messages and events
  - Message Format: format, size and coding of messages.
  - Timing: the time to wait between any event.
    - Access to medium
    - Flow control
    - Timeouts

Protocol specification examples

- Modularization → Many protocols for each layer
  - Hides implementation details
  - Layers can change without disturbing other layers
    - Development (one company can tackle one module)
    - Maintenance
    - Updating the system
- Packet switching
  - Best effort delivery
  - Better for resource sharing
- Network congestion and flow control

Router and subnet



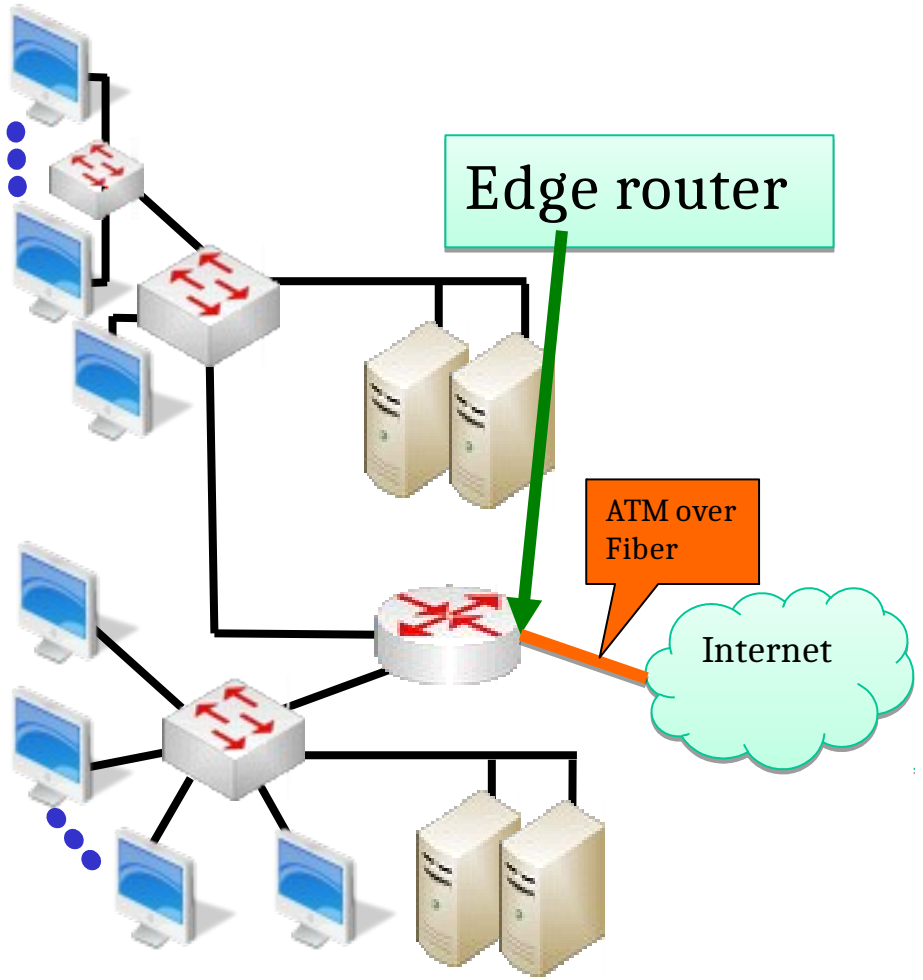
- Internet uses a gateway (edge router) to connect a Local Area Network (LAN) or a subnet to the hierarchical network

Residential Internet access overview

- Point to point protocol (PPP) for access to an ISP
- Dialup via modem
- DSL: digital subscriber line
- Cable modem
- Fiber In The Loop
- Broadband over a power line
- Broadband wireless: such as WiMAX
- Satellite

Local area network connected to Internet

- Organization/home local area network (LAN) or subnet connects hosts to edge router
- Edge router connects LANs to Internet
  - Telco uses ATM over fiber
- Ethernet LAN
  - Hosts connect into Ethernet switch
  - 10Mbps, 100Mbps, 1Gbps, 10Gbps Ethernet
- ATM: asynchronous transfer mode



Access layer

- Constituted by networks with end-points of the same local management
- Provides connectivity among stations on the same network
- Nodes in the same network can directly communicate among them
  - Used protocol: Ethernet family

Ethernet (IEEE 802.3) networks

- Each host in a Ethernet network has a NIC (Network Internet Card) with a (generally) fixed address
- MAC addresses are 48 bits (6 bytes) long and UNIQUELY ideintify hosts in the network
- Each host only processes packets intended for it
- Each Ethernet packet ("frame") has a fixed format

How to build a Ethernet network

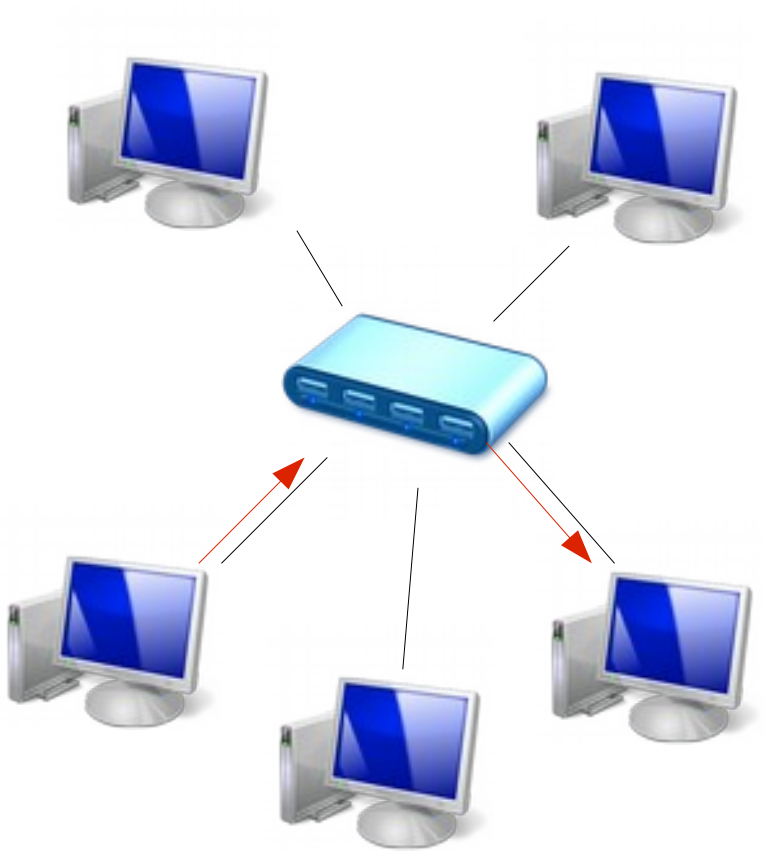
- All the hosts connected together with a shared "transmission system" based on Ethernet are a network, as if they were connected to the same medium
  - Two computer with a single Ethernet cable
  - Many computer connected with several Ethernet cables to a single device (generally a **switch,** but also **repeater, hubs** or **bridges**)
  - Many computer connected with several Ethernet cables to several devices (generally **switches**)

Ethernet and its broadcast domains

- An Ethernet network constitutes a **broadcast domain**
  - For historical reasons there also exist collision domains, but full-duplex and switches have made them obsolete
- Ideally frames sent in a broadcast domain are potentially received by all the hosts in the network
  - All the host receive all the frames and only read some
- Actually, switches segment the network to limit the explosion of packets in the network
- Only broadcast messages are "replicated"

How switches segment the network

- Switches remembers the source MAC addresses on the different ports
- They only replicate the frame on the segment where the destination MAC address replies
  - Tables of MAC are
    - ARP tables for hosts
    - CAM tables for switches

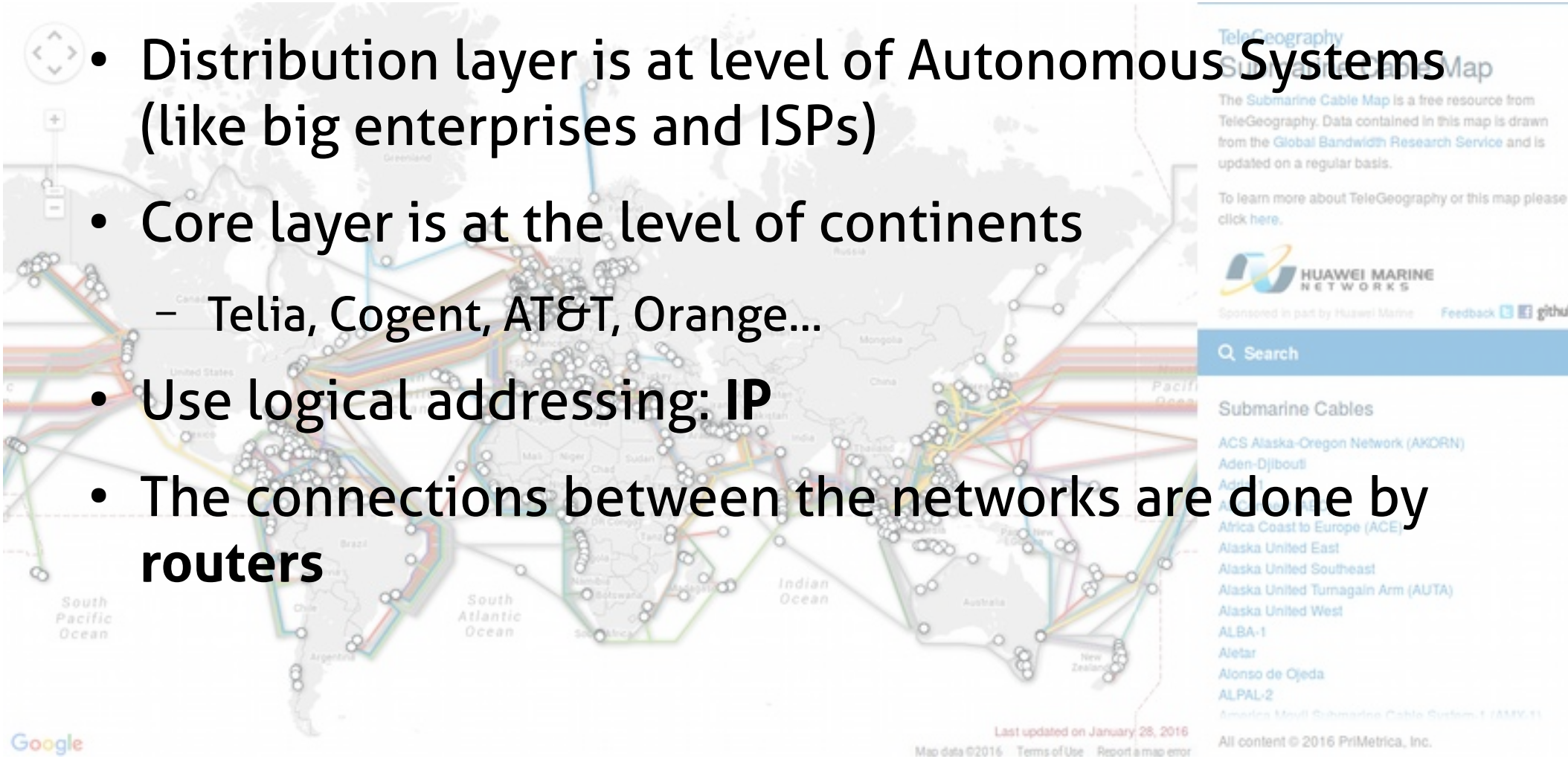


Why Internet is not a large Ethernet net?

- Ethernet makes high use of broadcast packets
  - Inefficient for large networks
- Large networks are split in order to reduce the broadcast domain
- There is the need of a LOGICAL division of the networks: Ethernet is the Access layer, but wee need a Distribution layer
- Hosts in a local network use a Default Gateway to go out and have access to the Distribution layer
- Distribution layer is based on IP, the Internet Protocol

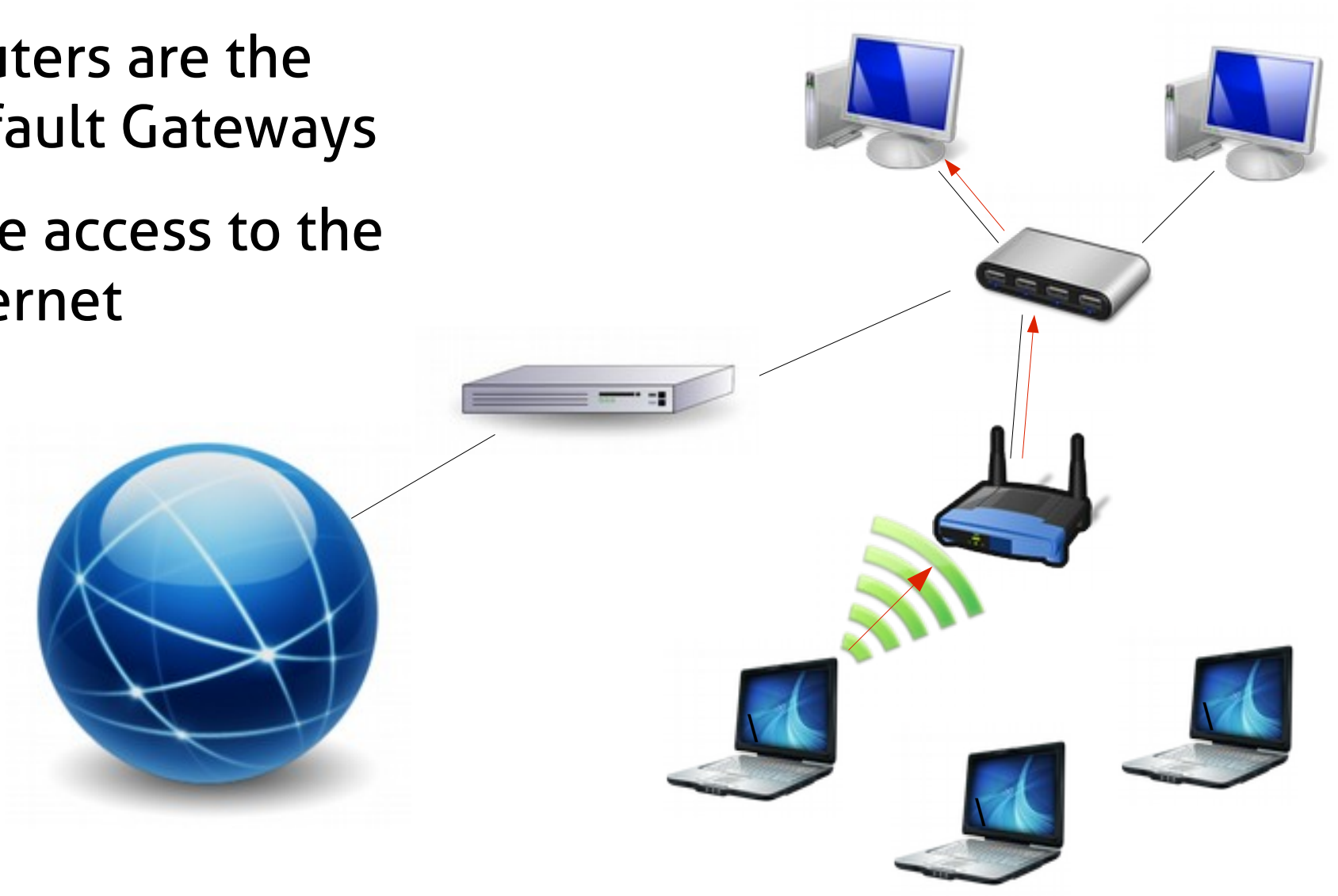
Distribution and core layers

- Interconnect local networks among them
- Distribution layer is at level of Autonomous Systems (like big enterprises and ISPs)
- Core layer is at the level of continents
  - Telia, Cogent, AT&T, Orange…
- Use logical addressing: **IP**
- The connections between the networks are done by **routers**



Router and switches

- Routers are the Default Gateways
- Give access to the Internet



Ethernet vs IP addresses

- Ethernet has **physical** addresses
  - You can not(*) change the MAC address of your NICs
    - It is like your **name**: it goes wherever you go
  - An Ethernet address tells WHO you are, but does not tell anything on WHERE you are
- IP has **logical** addresses
  - You can change IP address of your NIC
    - It is like your **home address:** it changes if you go somewhere
  - IP addresses are used to identify and reach networks and hosts

Local addresses and remote addresses

- Analogy: if you want to say something to somebody
  - If both of you are in the same room, you can simply call his/her name and he/she will answer
    - Directly connected → Local address
  - If you are NOT in the same room, you have to know where he/she is, before sending the message AND the message has to LEAVE the room through the door
    - Remote address
- How to know if one IP is the same network than you?
  - Subnet mask

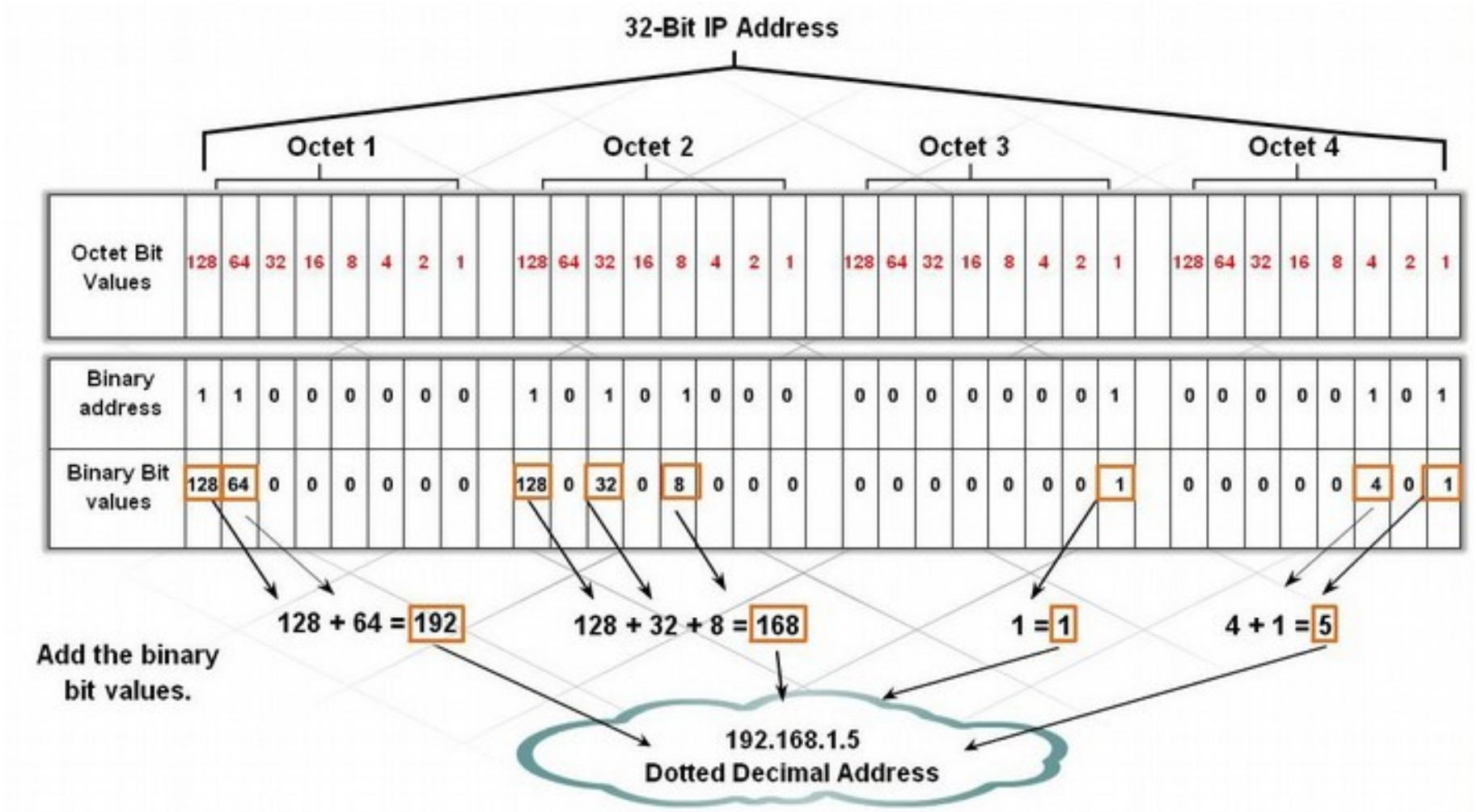
IP Addresses

Two versions of IP addresses: IPv4 and IPv6.

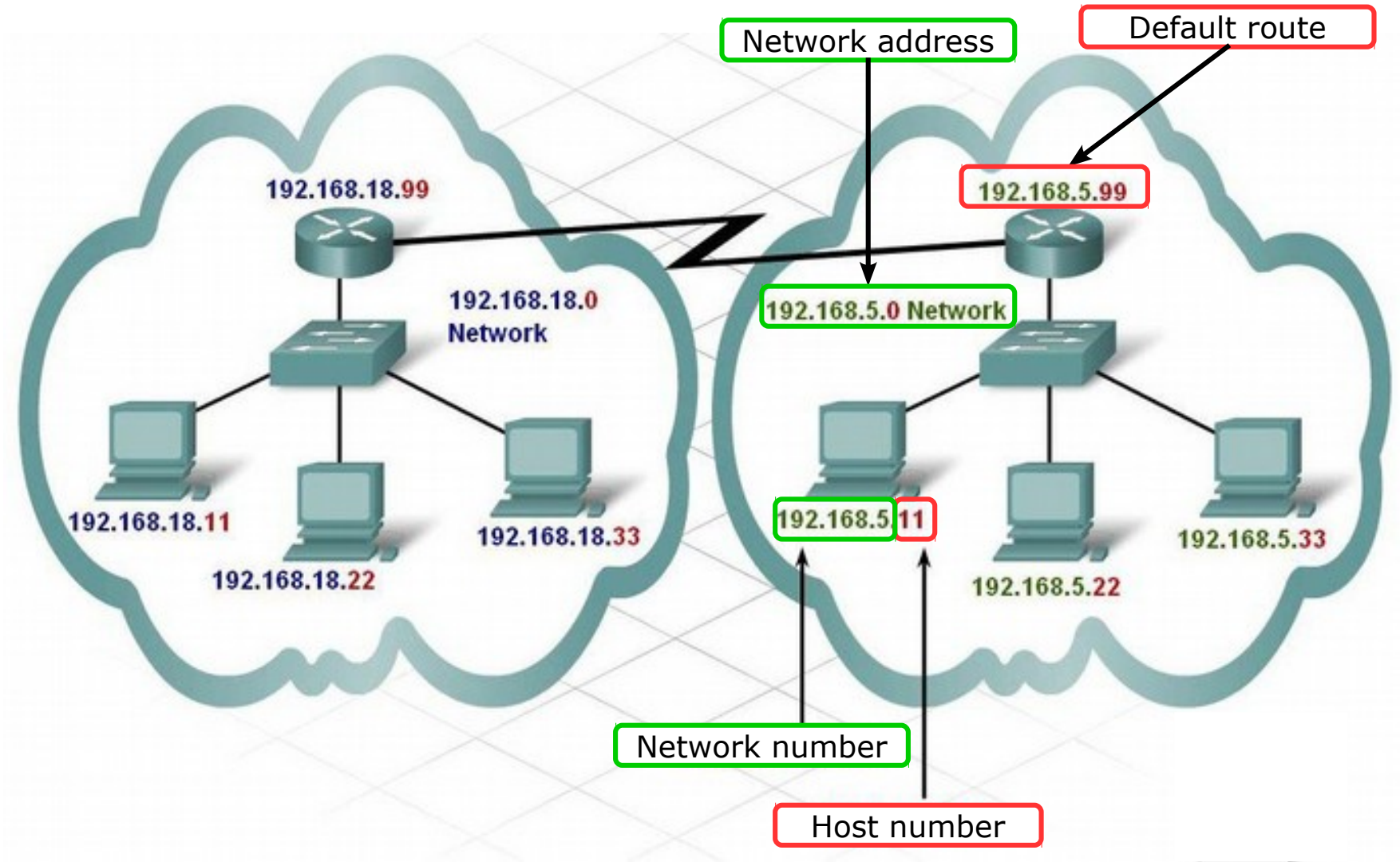
- IPv4 defines IP address with 32 bits organized in four octets (8 bits in each).
- IPv6 (version 6) has 128 bits.

- For human readability, the bits in each octet are separated by dots while writing an IPv4 address (colons in IPv6).
  - E.g. 69.58.201.25 and fe80::250:56ff:fec0:1
- Certain bits from the left correspond to the network address (69.58.201) and the remaining correspond to define the computer (host) on the network (25).
- Subnet mask defines boundary between network portion and the host portion of the IP address.

Dotted decimal IP Address



Network address and Host address



Types of IP Addressing

There are three types of IP addresses

- **Unicast (one to one)**
  - These refer to a single destination host
- **Broadcast (one to all)**
  - These refer to every host on a network or subnet
- **Multicast (one to many)**
  - Refers to a group of IP addresses in a network, not necessarily all of them
    - http://www.firewall.cx/networking-topics/general-networking/107-network-multicast.html

IP Addressing, Classful

Allocation classes of IP addresses

- **Class A** (24 bits for host addresses, or /8)
  - 0.0.0.0 to 127.255.255.255
- **Class B** (16 bits for hst addresses, or /16)
  - 128.0.0.0 to 191.255.255.255
- **Class C** (8 bits for host addresses, or /24)
  - 192.0.0.0 to 223.255.255.255
- **Class D** (Multicast)
  - 224.0.0.0 to 239.255.255.255
- **Class E** (Reserved)
  - 240.0.0.0 to 255.255.255.255

IP Addressing

- There are routable and non-routable address ranges
- Routable addresses need to be unique on the Internet
- Non-routable address ranges are defined in RFC1918
  - Distinction between "private" and "public" IP
  - 10.0.0.0 - 10.255.255.255 (10/8 prefix)
  - 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
  - 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

IP Addressing, example

192.168.8.0/24

- The last eight (32 minus 24) bits of 32 total will be used for host addresses
- The first address reserved for the **network address**
- The last adress reserved for the **broadcast address**
  - Then, we have **2^(32-netmask) – 2** hosts in any CIDR specified network
- So, if we are given **192.168.8.0/24**, 192.168.8.0 is the network address, 192.168.8.255 is the broadcast address, and .1 to .254 are host addresses

IP Addressing, Classless

- Each set of 8-bits (octet) can hold values from 0-255
  - Poor flexibility!
- Idea: let's use a Variable Length Subnet Mask (VLSM)
- Introduced by CIDR (Classless Inter-Domain Routing), a new notation for the netmask:
  - specify how many bits of the 32-bit total will specify the network address
  - The remaining bits specify the host addresses
- Ex: 10.10.10.0/26
  - the netmask can also be specified in dotted-quad notation, as in 10.10.10.0/255.255.255.192

IP Addressing, other example

192.168.1.248/30

- **2^(32-30) – 2 = 2^2 – 2 = 4 -2 = 2** hosts (2 usable addresses)
  - 192.168.1.248 is the network address
  - 192.168.1.251 is the broadcast address
- Large networks can be subnetted:
  - We say things like "There are 64 /30 **subnets** in a /24 network"
- Many smaller networks can be "supernetted" for routing reasons → "summarization"

Notes about IP addresses

- In Point-to-Point links, using a 30 bit netmask is a waste…
  - If A sends a broadcast, only B will receive it…
- There is the proposal of RFC 3021:
  - *Using 31-Bit prefixes on IPv4 Point-to-Point Links*
    - https://tools.ietf.org/rfc/rfc3021.txt
- Reduce the waste of IP addresses in a subnet
  - Other ways to reduce it?
    - NAT
    - IPv6

Exercises

- Determine the network part, the host part, the network size (number of hosts), the network address, the broadcast address and the type of the following IP addresses:
  - 10.11.12.1 netmask 255.255.255.128
  - 192.168.4.32 netmask 255.255.255.224
  - 172.17.17.17 netmask 255.255.240.0
  - 10.11.12.0/21
  - 192.168.4.32/27
  - 172.17.17.17/29

Exercises 2

- Determine whether the destination IP address is local or remote
  - Namely, if it belongs to the same network than the Host
    - It is plenty of tools online for this job, but try to put your pen to paper

Host IP address	Host subnet mask	Destination IP address
210.145.149.123	255.255.255.0	210.145.253.199
192.168.4.189	255.255.255.224	192.168.1.107
10.154.187.89	255.192.0.0	10.152.179.88
132.100.45.5	255.255.252.0	132.100.45.45
151.251.100.101	255.255.0.0	166.200.110.10
172.32.9.82	255.255.255.240	172.32.9.79

Summary

- Internet: a mess!
  - Networks connected by other networks that meet in IXP
- Hierarchical structure: to make Internet admins to survive!
  - Core and distribution layers managed by ISPs
- Protocols: the Internet manuals!
  - Describe rules and formats to exchange data and make services to be well defined
- Ethernet and IP: who you are and where you are
  - Addresses with two different meanings, for two different purposes
- Networks and subnet masks: to train with math!

Lab preparation

To do the assignment

- Kathará (formerly known as netkit)
  - A container-based framework for experimenting computer networking: http://www.kathara.org/
- Please install it in your laptop
- Three exercises to complete about network configuration

That's all for today

- **Questions?**
- See you next lecture!
- Bonus reference to get used to Linux CLI and tools:

  http://overthewire.org/wargames/bandit/bandit0.html

  - Go to bandit and try to reach level 34!!
    - 33 is also good :-)
  - Take notes of the passwords and how you obtained them
  - Try to learn as much as you can solving each level

Lab useful commands

Assigning IP addresses

- Blocks of public addresses are allocated by IANA (Internet Assigned Numbers Authority) and RIRs (regional Internet registries)
  - To companies, institutions, universities and so on
- Private addresses can be used by anyone
  - Manually
  - Automatically (via DHCP Dynamic Host Configuration Protocol)

Properly configure a host

- In order to (properly) use Internet a host has to receive 3 main pieces of information
  - The complete IP address (IP and netmask)
  - The IP address of its default gateway
    - Namely the host of its local network able to access to the distribution layer
  - The IP address of a DNS (Domain Name Server)
    - Namely a remote host able to translate human intelligible names to IP addresses
- Automatically provided by DHCP

DHCP

- Client-server mechanism
- Server has a pool of IP addresses to distribute, together with the network configuration
- Client requesting a new IP address receive a proposal and accept it
- Once accepted, the IP is reserved for a "leasing time"
- Observations?

Manual network configuration (linux)

- **ifconfig** to assign the IP address
  - This command is used to configure network interfaces, or to display their current configuration. In addition to activating and deactivating interfaces with the “up” and “down” settings
- **route** to define the default gateway
  - The route command is the tool used to display or modify the routing table
- **/etc/resolv.conf** to specify the DNS server(s)

Manual network configuration using ip

- **ip addr** to assign the IP address
  - This command is used to configure network interfaces, or to display their current configuration. In addition to activating and deactivating interfaces with the “up” and “down” settings
- **ip route** to define the default gateway
  - The route command is the tool used to display or modify the routing table
- **/etc/resolv.conf** to specify the DNS server(s)

Other details about ip command

- Show interfaces
  - `ip link show`
- Bringing interface up/down
  - `ip link set eth0 (up|down)`
- Set MAC address
  - `ip link set eth0 address 00:11:22:33:44:55`
- Show IP address
  - `ip address show [dev eth0]`
- Add/remove IP address
  - `ip address (add|del) 10.0.0.1/8 dev eth0`
- Flush any IP address (remove the assigned address/es)
  - `ip address flush [dev eth0]`

ip for routing purposes

- List/flush routing table
  - ip route (list|flush)
- Add/del routes
  - next hop
    - ip route (add|del) 100.0.0.0/8 via 10.0.0.1
  - default
    - ip route (add|del) default via 10.0.0.1
  - direct forwarding
    - ip route (add|del) 10.0.0.0/24 dev eth0

ip for ARP and more

- Show ARP cache
  - ip neigh show [dev eth0]
- Flush ARP cache
  - ip neigh flush dev eth0
- Add/del/change/replace ARP cache entry
  - ip neigh (add|del|change|replace) to 10.0.0.2 lladdr 00:11:22:33:44:55 dev eth0 nud "state_name"
    - (state_name: permanent, stale, noarp, reachable…)
- IP tunneling (IPinIP, IPinGRE, IPv6 tunneling)
  - ip tunnel