Networking Basics

DENOG 13

GERMAN NETWORK OPERATORS GROUP

Wolfgang Tremmel
academy@de-cix.net

Where networks meet

DENOG

GERMAN NETWORK OPERATORS GROUP

Networking Basics

01 - Networks, Packets, and Protocols

Wolfgang Tremmel
academy@de-cix.net

DE CIX

Where networks meet

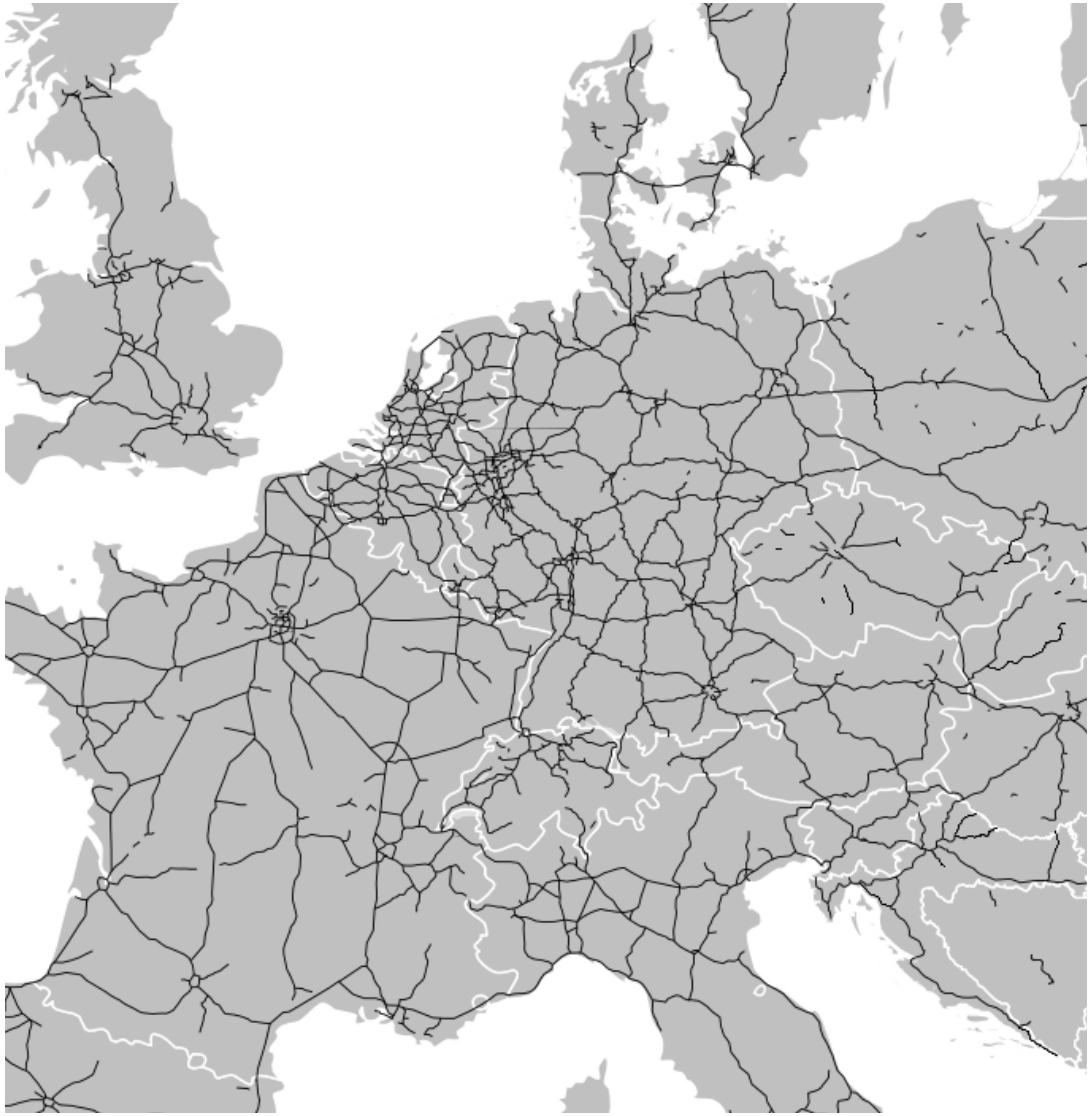
Networking Basics
DE-CIX Academy

Networks

Networks

Networks are everywhere

- You all know and use networks
- I am not talking about the Internet
- Networks are everywhere
- Example: The **road network**
- It connects cities, using roads and cars



Attribution: https://commons.wikimedia.org/wiki/User:Scooter20
https://commons.wikimedia.org/wiki/File:Europe_Completed_Motorways_Dec_2012.png

Networks

Networks are everywhere

- You all know and use networks
- I am not talking about the Internet
- Networks are everywhere
- Example: The **railway network**
- It connects railway stations, using rails and trains

Attribution: Hbf878, OpenStreetMap contributors
https://commons.wikimedia.org/wiki/File:Bahnstrecken_Deutschland_Karte.svg

DE CIX

Networks

Networks are everywhere

- You all know and use networks
- I am not talking about the Internet
- Networks are everywhere
- Example: The **electrical grid**
- It connects producers and consumers of electricity

Attribution: Wolfgang Tremmel

DE CIX

Networks

Networks are everywhere

- You all know and use networks
- I am not talking about the Internet
- Networks are everywhere
- Example: The **postal network**
- It connects senders and receivers of letters and **Packets**

Packets

Just imagine...

Using the postal network

- Lets say you have seen this garden shed in a catalog
- And want to mail order it
- It does not fit into one package
- So the sender dismantles it

Attribution: Concord
https://commons.wikimedia.org/wiki/File:HGW_Gewaechshaeuser_5_2014_017.JPG

DE CIX

Just imagine...

Using the postal network

- So the sender dismantles it
- Packs it into several packages
- And sends them to you
- You unpack the packages
- And put the garden shed together again

Attribution: Concord
https://commons.wikimedia.org/wiki/File:HGW_Gewaechshaeuser_5_2014_017.JPG

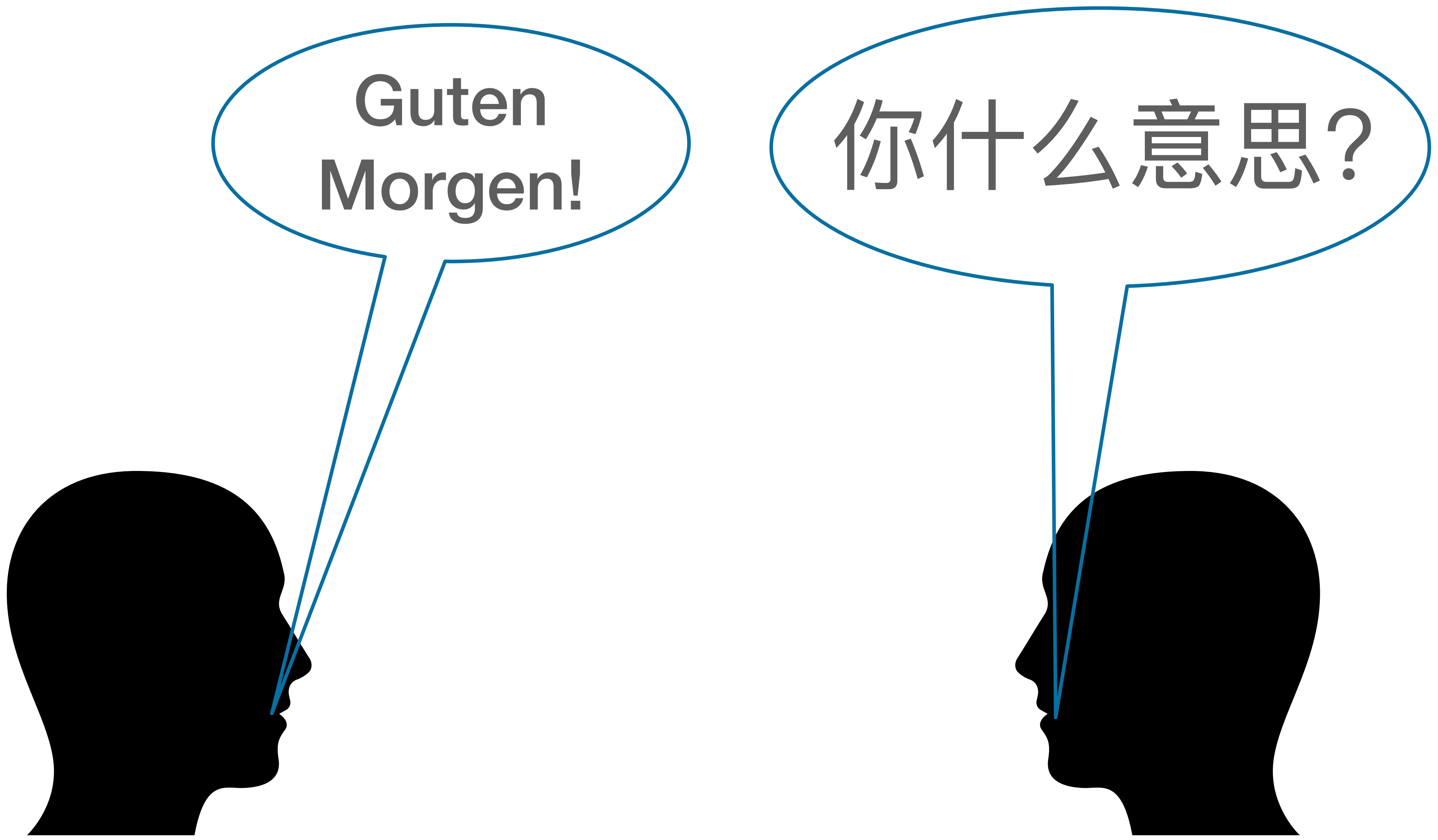
Using a computer network
Data is sent in packets

- Computer networks (and the Internet) work in the same way
- Data is most of the time too big to sent as a whole
- So it is cut into packets by the sender
- And put together by the receiver
- Network Protocols take care that the transmission is successful

Protocols

What is a "Protocol"?

- If you want to communicate, you need to speak a common language
- Otherwise you will not understand each other



PS: I used Google Translate. Hope it says "I do not understand"

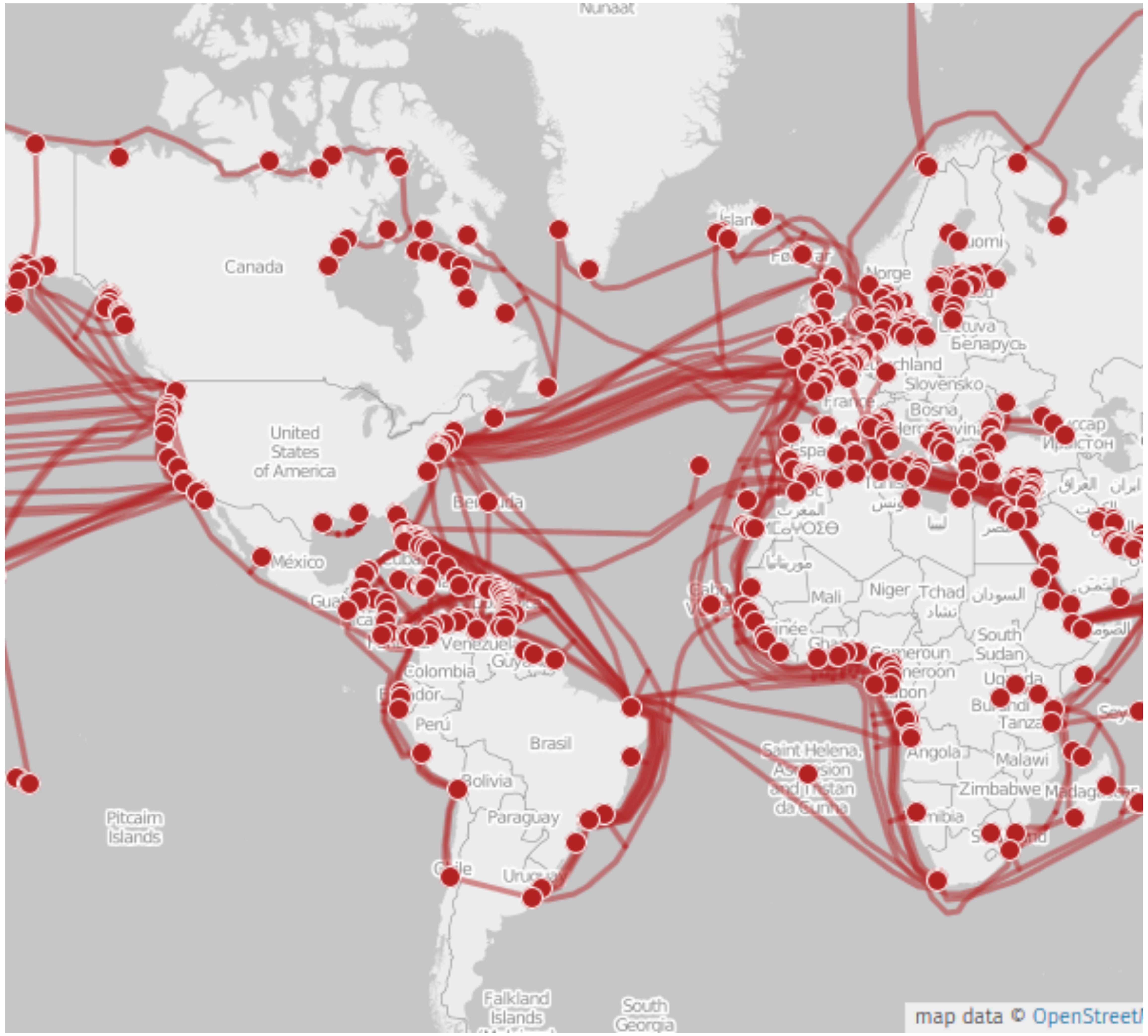
What is a "Protocol"?

- If you want to communicate, you need to speak a common language
- Otherwise you will not understand each other
- The same is true for computers or other network devices

Protocols used

Internet

- The protocol used for the Internet is called "IP"
- IP stands for "Internet Protocol"
  - actually there are two variants of this protocol used
  - IPv4 and IPv6
  - There will be a webinar about IP!



Attribution: cable data by Greg Mahlknecht , map by Openstreetmap contributors
https://commons.wikimedia.org/wiki/File:Submarine_cable_map_umap.png

Protocols used

Local networks

- The protocol used for your local network at home is called "Ethernet"
- But you also use IP!
- Confused?
    - *Multiple* protocols are used
    - This is called a Protocol Stack

Protocol Stack

OSI reference model

The Protocol Stack

OSI reference model

- OSI = Open Systems Interconnection
  - Project at ISO (International Organization for Standardization)
- Defined in the 1970s and 1980s
- Intended as a vendor-independent "real" network model
  - But never took off
  - Still relevant as reference for teaching

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

DE CIX

OSI Model
Relevance

- It was intended as a working network
- It had some good ideas
    - Like the separation of layers
    - And layers building on each other
- While OSI was writing papers, the Internet guys were already implementing
- Despite all money put into OSI, Internet won

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

DE-CIX

OSI Model

Layer	Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Internet Model

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

DE CIX

Internet Model

Also has layers

- The IP protocols do not exactly fit into the OSI model
- There is also no intention of compliance to OSI
- Internet Protocols care more about architecture and optimization than about layering
- "Running code" most important

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

DE CIX

Internet Model

Physical Layer

- Data units are bits or symbols
- via a physical medium
- Like light pulses or electrical signals
- Examples:
    - an optical transceiver
    - an electrical Ethernet port

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

DE CIX

Internet Model

Link Layer

- Data units are called "Frames"
- Provides node-to-node data transfer
- Examples:
  - Point-to-Point Protocol (PPP)
  - Ethernet

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

DE CIX

Internet Model

IP / Internet Layer

- Data units are called "Packets"
- Provides source to destination transport
- Needs addresses for hosts
- Examples:
  - IPv4
  - IPv6

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

Internet Model

Transport Layer

- May provide flow control, reliability, congestion avoidance
- Not all of them in all protocols
- Also contains information about the next layer up
- Examples:
  - TCP (flow control, reliability, congestion avoidance)
  - UDP (none of the above)

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

Internet Model

Application Layer

- no special name for data units, just "Data"
- Contains all application protocols
- Examples:
  - SMTP, HTTP, SSH and all others

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

Conclusion

Conclusion

This is what you should remember

- Networks are everywhere
- Data is sent in **packets** via a network
- A **protocol** is a common language devices speak so they understand each other
- The OSI model defines a network as a number of **layers**
- The Internet does not exactly fit into the OSI model

DE CIX

Networking Basics

02 - Ethernet

DENOG 13

GERMAN NETWORK OPERATORS GROUP

Wolfgang Tremmel
academy@de-cix.net

DE-CIX

Where networks meet

DE-CIX Management GmbH | Lindleystr. 12 | 60314 Frankfurt | Germany
Phone + 49 69 1730 902 0 | sales@de-cix.net | www.de-cix.net

Networking Basics
DE-CIX Academy

01 - Networks, Packets, and Protocols

02 - Ethernet

- 02a - VLANs

03 - The Internet Protocol (IP)

- 03a - IP addresses, prefixes, and routing
- 03b - Global IP routing

04a - UDP

04b - TCP

04c - ICMP

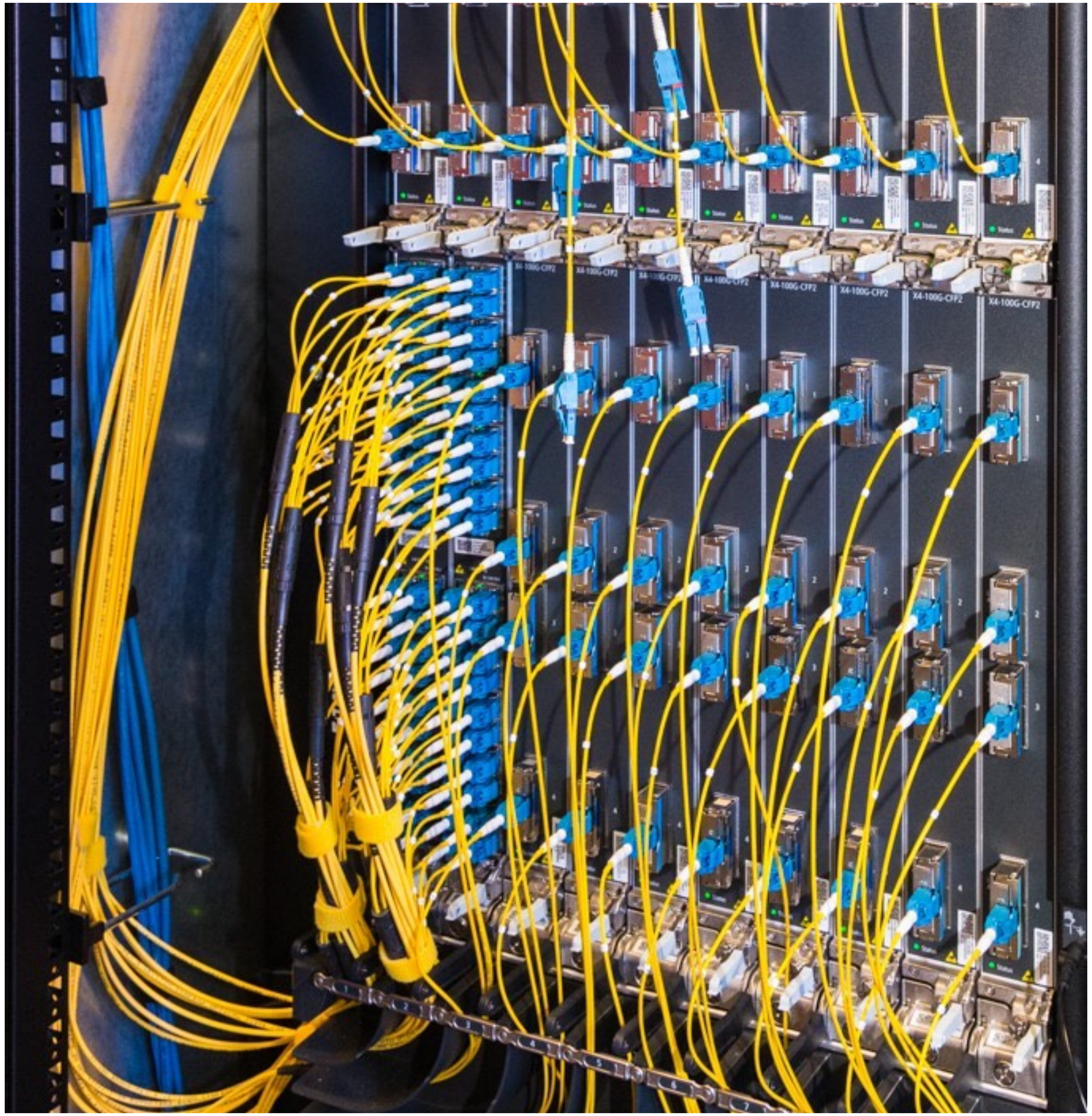
05 - Unicast, Broadcast, Multicast, Anycast

Ethernet

A Modern Ethernet Device

Nokia 7950

- As used by DE-CIX
- Connects 100s of devices
- using optical interfaces
- with speeds up to 400Gbps



Attribution: DE-CIX

Another Modern Ethernet Device

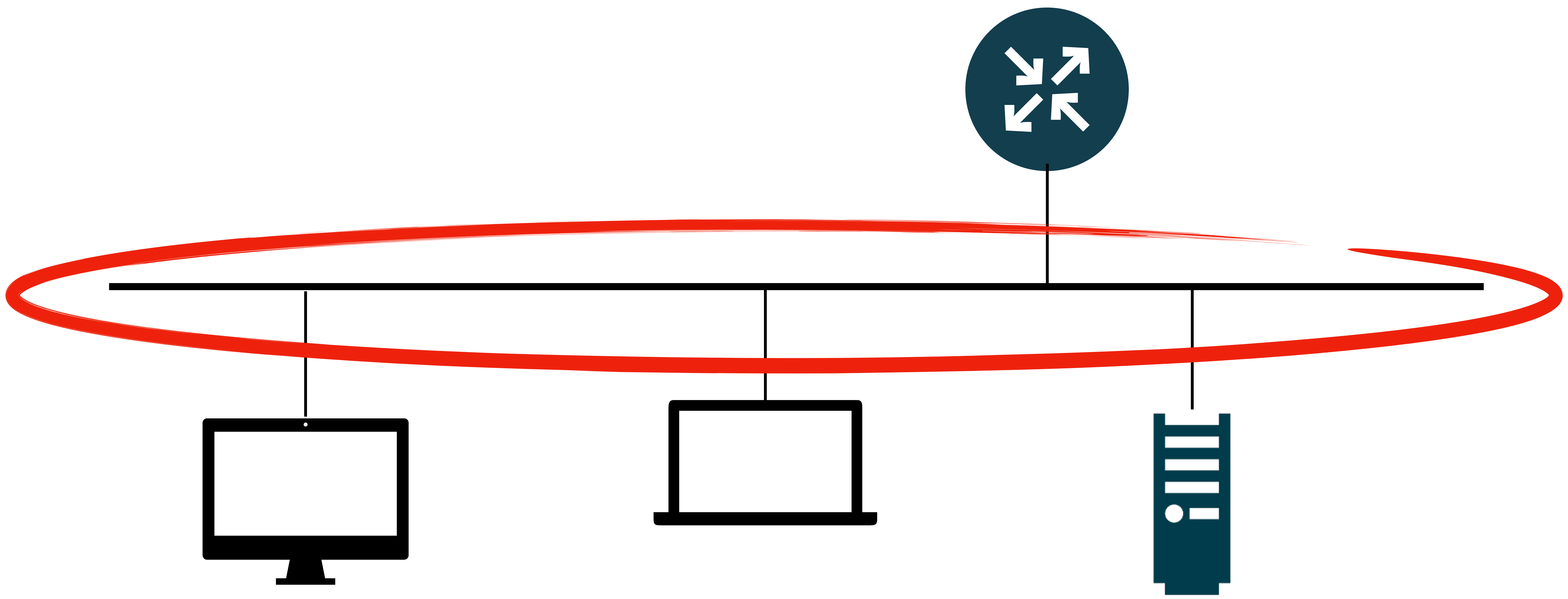
Fritzbox

- as used at home
- connects 4 devices directly
- using copper interfaces
- with speeds up to 1Gbps

Attribution: Wolfgang Tremmel

DE CIX

So why does the symbolic drawing of Ethernet look like this?



1971

It began in Hawaii: ALOHA-Net

ALOHA-Net

University of Hawaii, 1971

- Radio based network
- To interconnect sites
- Simple principle:
  - If you have data to send, send it
  - If you receive something while sending, stop and try again later

1973

Robert Metcalfe - Xerox PARC

Ethernet

Xerox PARC, 1973

- Instead of radio, uses a coax cable
    - For higher bandwidth
    - And more reliability
- Inspired by ALOHAnet
- Standardized in 1980
- Ethernet II in 1982, standardized as IEEE 802.3 in 1983

Attribution: Coolcaesar at the English language Wikipedia
https://commons.wikimedia.org/wiki/File:Parcentrance.jpg

10BASE5

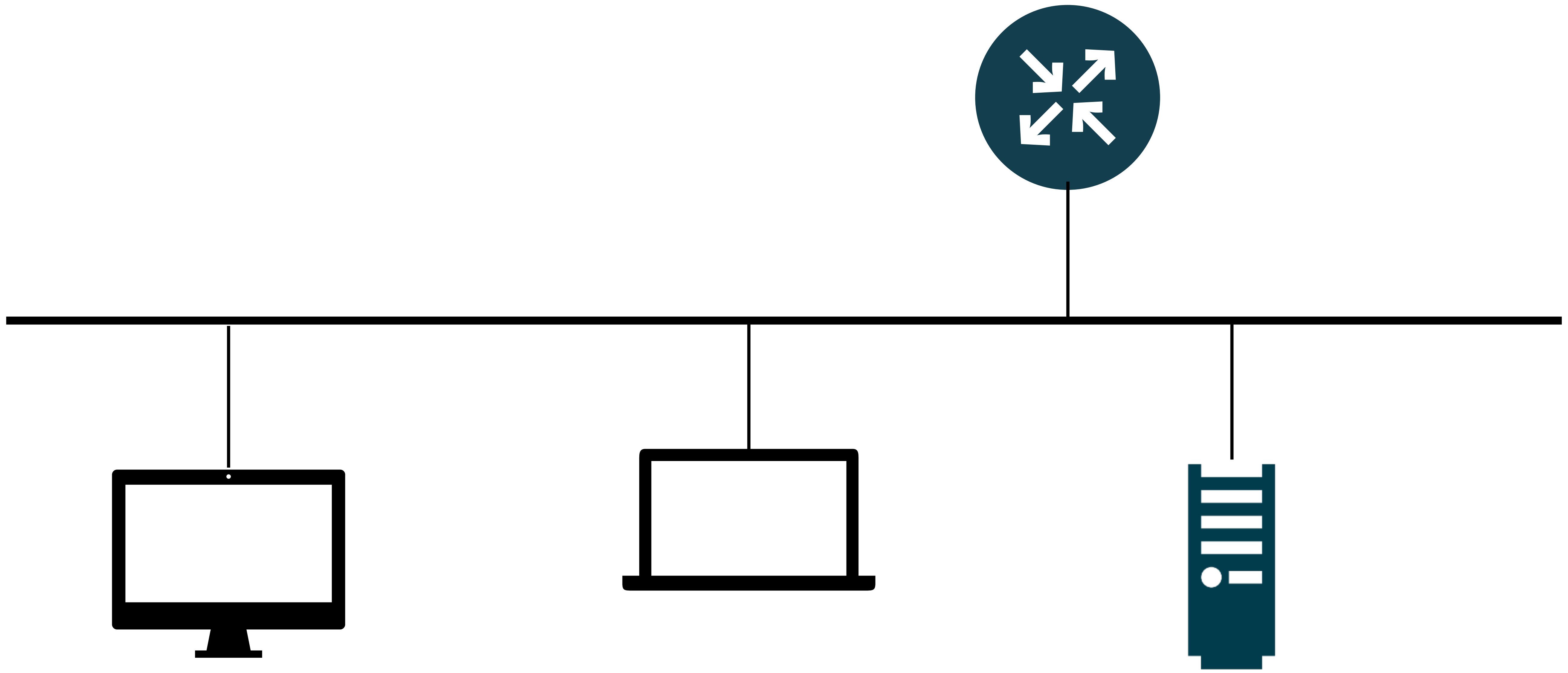
10 Mbit/s Ethernet

- 10 - Mbit/s
- BASE - uses baseband modulation
- 5 - 500m max. segment length
- Hardware:
  - 1cm thick coax cable
  - "Vampire-Tap" Transceivers

Attribution: Robert.Harker at English Wikipedia
https://commons.wikimedia.org/wiki/File:10Base5transcievers.jpg

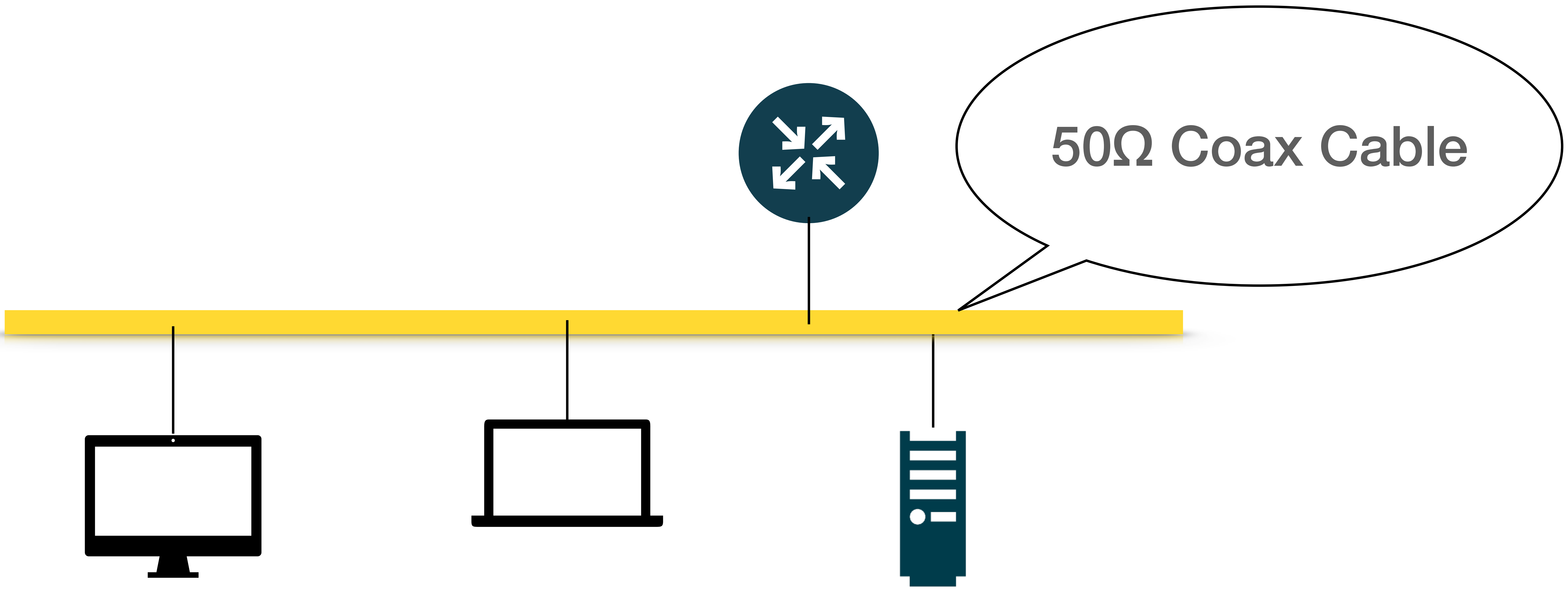
10Base5 Ethernet

Remember the drawing



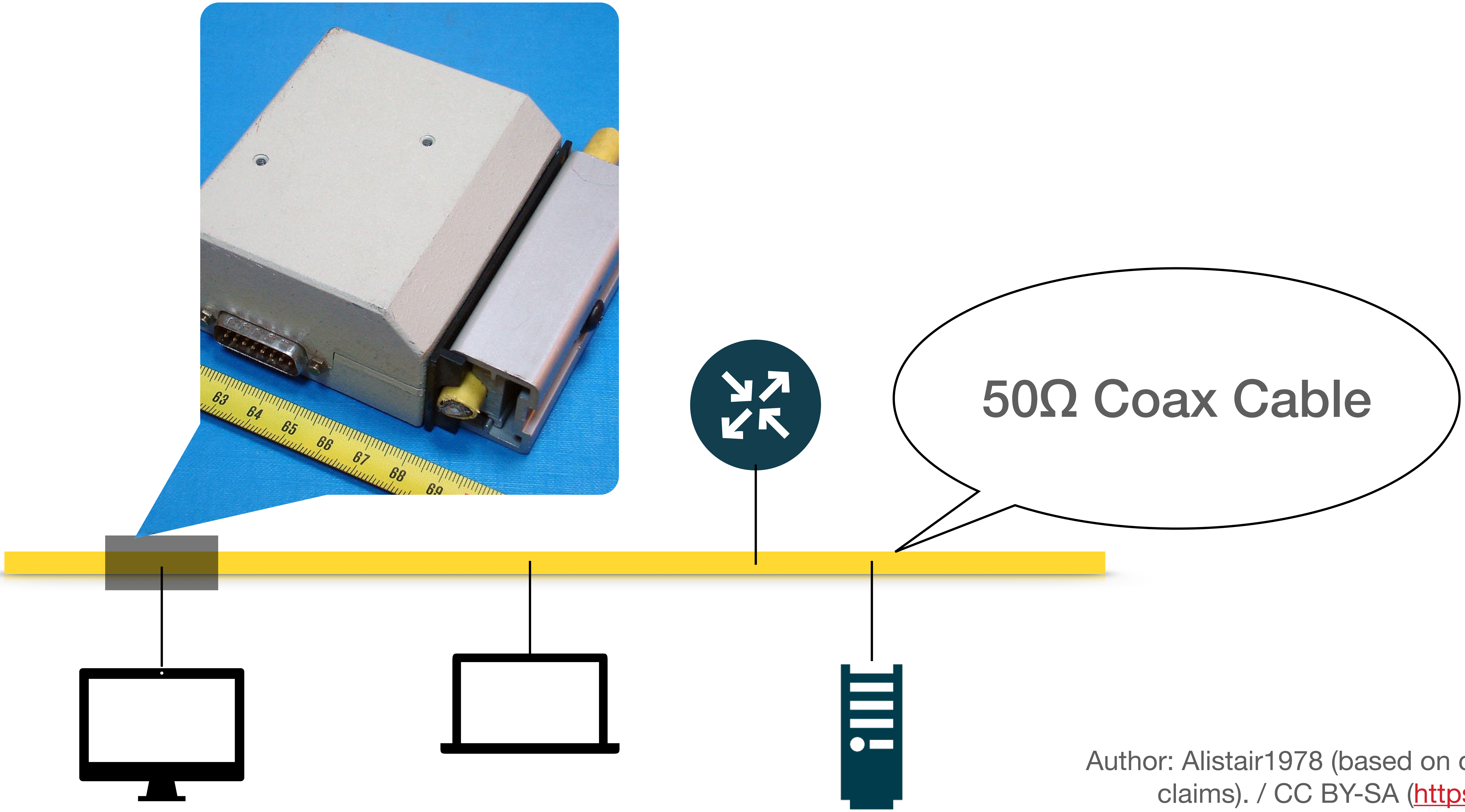
10Base5 Ethernet

Remember the drawing



10Base5 Ethernet

Remember the drawing

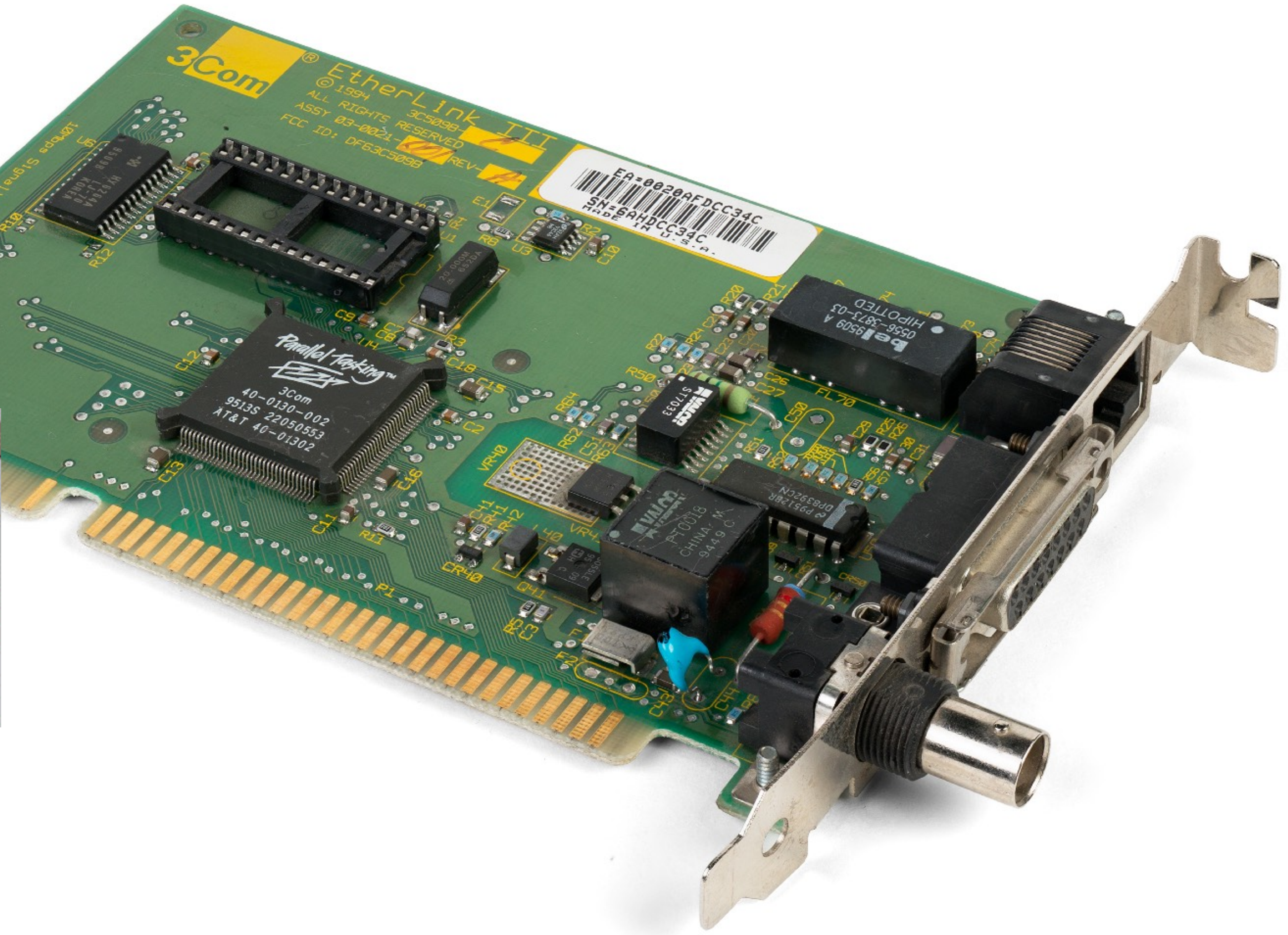


10BASE2

still only 10 Mbit/s Ethernet

- Hardware:
  - thin coax cable
  - BNC-"T"-connectors
- Up to 200m total length
- "Cheapernet"
- mid to late 1980s

Attribution: @the_mutax
https://twitter.com/the_mutax/status/1303700688745226240



Attribution: Dmitry Nosachev
https://commons.wikimedia.org/wiki/File:3Com_3C509BC_Ethernet_NIC.jpg

10Base-T

still only 10 Mbit/s Ethernet

- Hardware:
  - two pairs of twisted copper wires
  - 8P8C (RJ45) plastic connector
- Since 1988
- Needs an active component (hub or switch) to interconnect

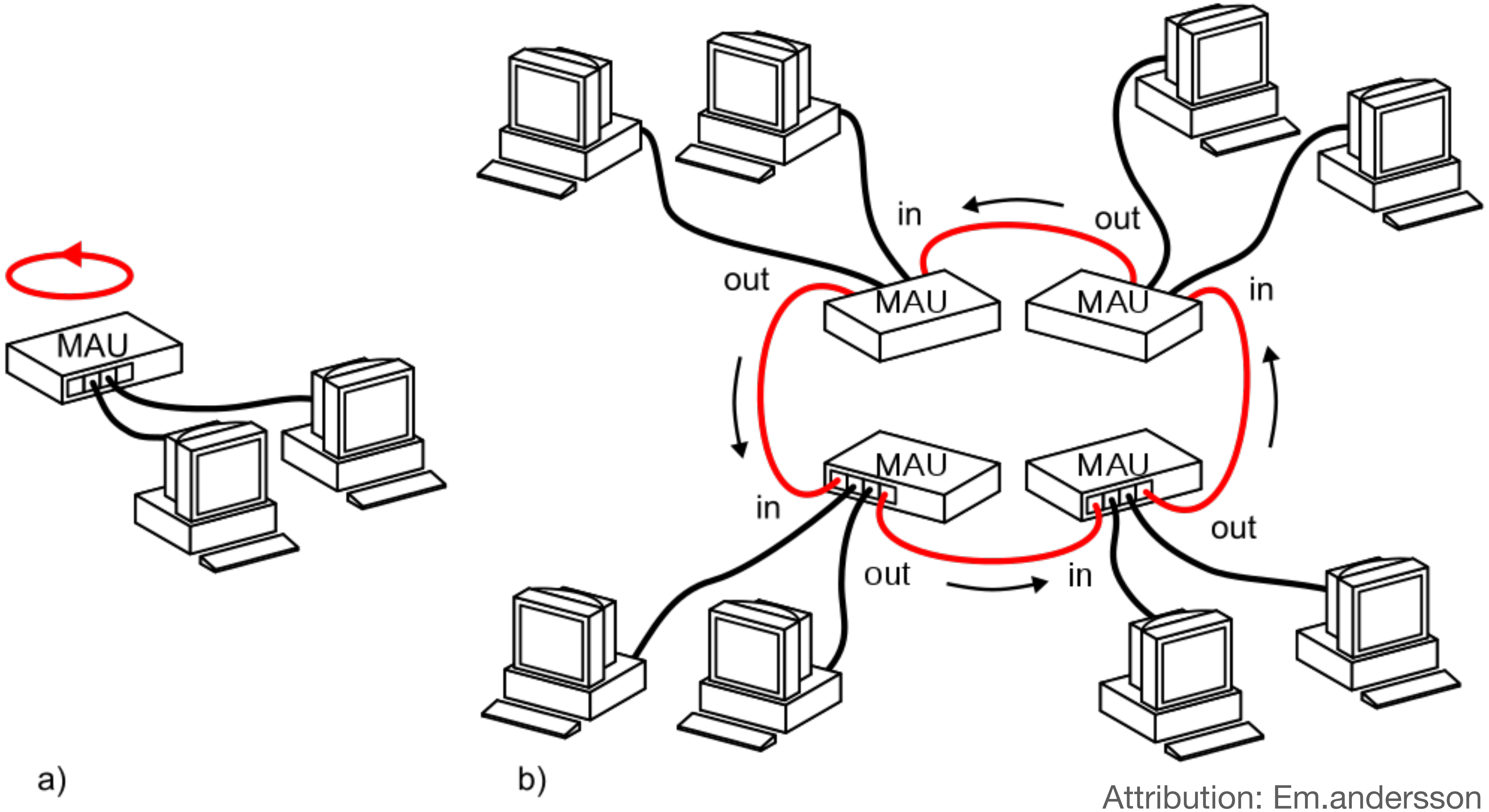
Attribution: Dmitry Nosachev
https://commons.wikimedia.org/wiki/File:3Com_3C509BC_Ethernet_NIC.jpg

Competing standards

Token Ring

1984 - 1990s

- Developed by IBM
- 4Mbit/s, later 16Mbit/s
- Deterministic access
- Needs central Multistation Access Unit
- More complex than Ethernet
- More expensive than Ethernet



Attribution: Em.andersson
https://en.wikipedia.org/wiki/File:Token_ring.png

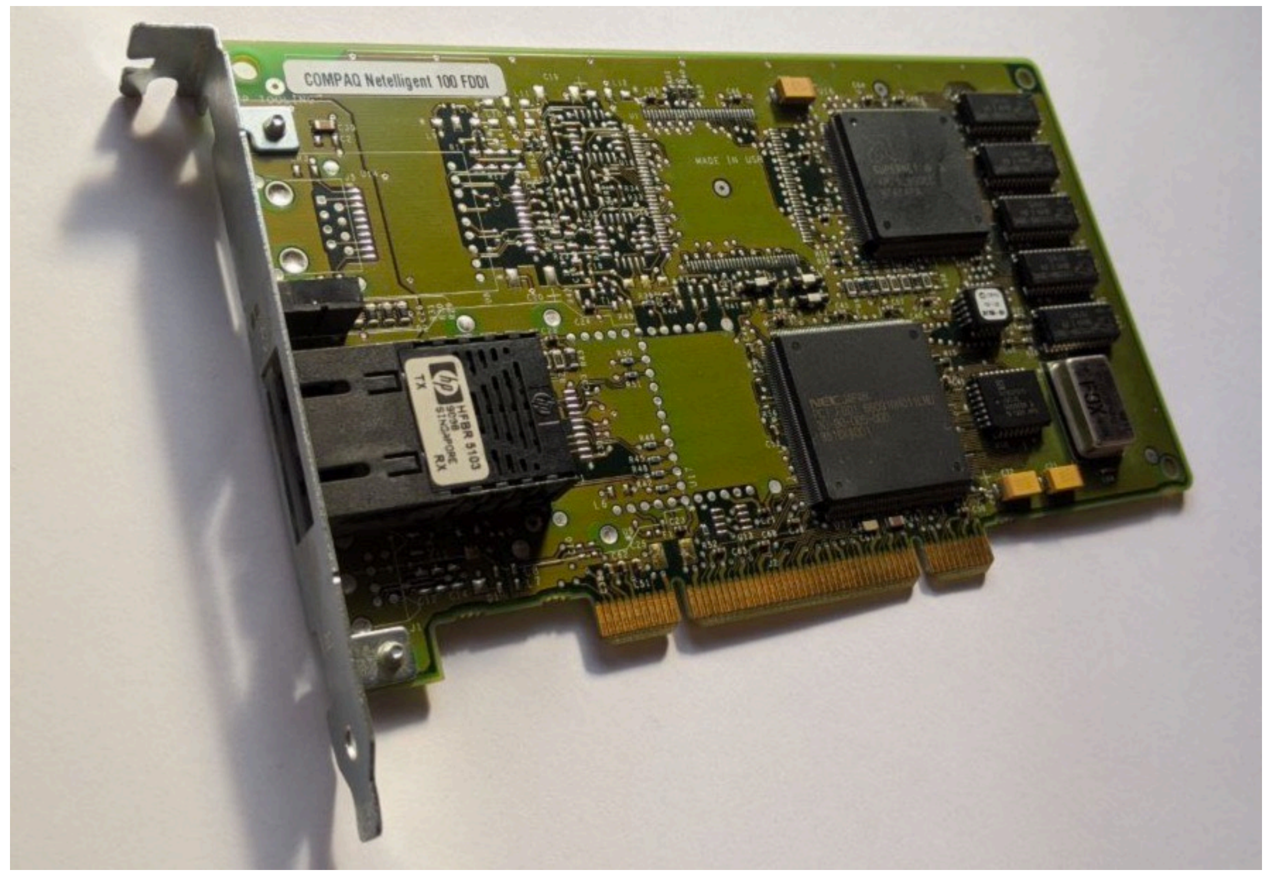
Attribution: Jens Link
https://commons.wikimedia.org/wiki/File:IBM_PCMCIA_Token_Ring_Card.jpg

DE CIX

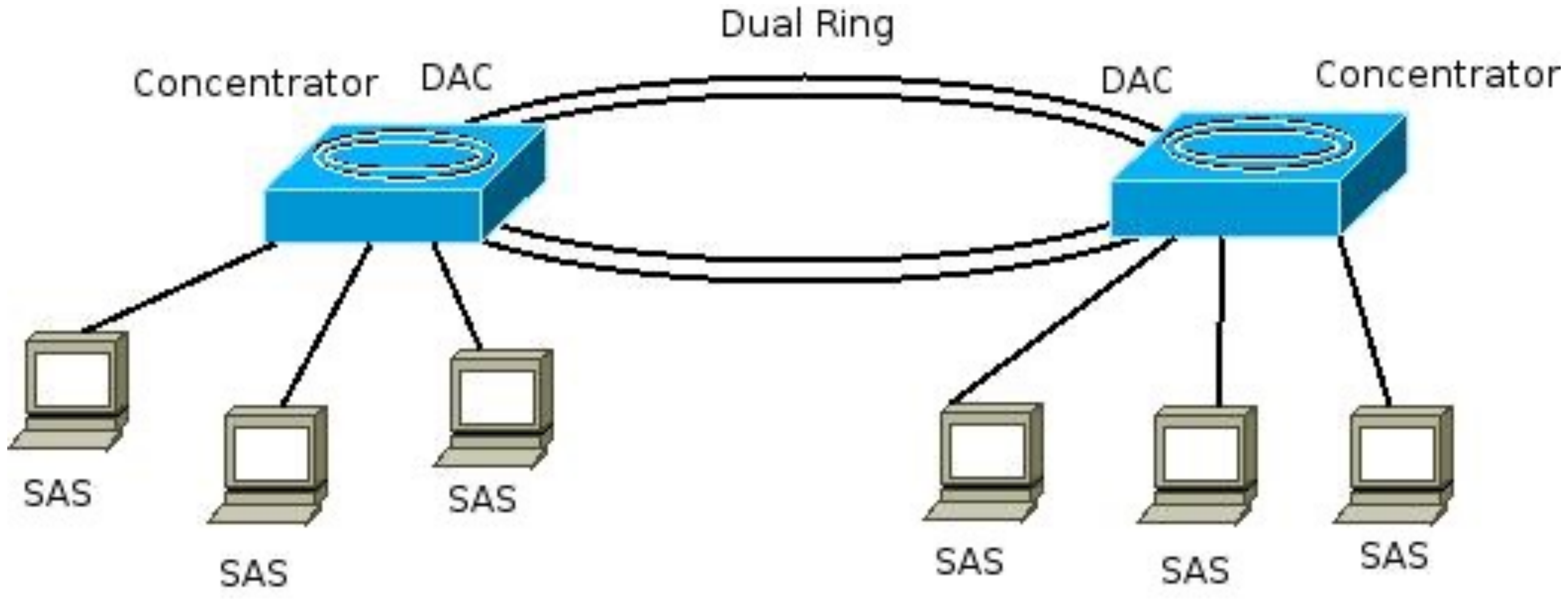
FDDI

late 1980s - 1990s

- Fiber Distributed Data Interface
- Optical network
- 100Mbit/s speed, up to 200km size
- Frame-size of 4352 bytes
- double ring topology
- made obsolete by GigabitEthernet



Attribution: Maximilian Wilhelm



Attribution: Vincent van der kussen at nl.wikibooks
https://commons.wikimedia.org/wiki/File:FDDI_Concentrator.jpeg

Back to Ethernet

Ethernet is a ***broadcast*** network where all devices are connected to a ***shared*** medium

Broadcast network

One is sending, everybody is receiving

- All stations share one medium
- Only one station at a time can send data
- If two stations start sending at the same time, a *collision* occurs
  - Both stop sending, wait for a random time, then retry
  - This was one of the main criticisms (no guaranteed delivery)

DE CIX

Broadcast network

One is sending**, everybody is receiving**

- Everybody is receiving everything
- How to avoid overload / unnecessary processing of data?
  - Each station has a unique 48-Bit address
  - Receivers address is at the beginning of each frame
  - And can be processed by the network card
  - Only frames with matching address or broadcast frames are forwarded to the CPU

Ethernet

Frame Structure

Preamble				SFD	Destination MAC Address	Source MAC Address	Ethertype	Payload	Checksum
10101010	10101010	10101010	10101010	10101011	48 Bits 6 Octets	48 Bits 6 Octets	16 Bits 2 Octets	46 - 1500 Octets	32 Bits 4 Octets

Ethernet
Frame Structure

- Preamble - 56 bits of 10101010....
- Start of frame marker - 8 bits: 10101011
- Destination MAC address
- Source MAC address
- EtherType (or length)
- Payload
- 32 bit checksum

Preamble				SFD	Destination MAC Address	Source MAC Address	Ethertype	Payload	Checksum
10101010	10101010	10101010	10101010	10101011	48 Bits 6 Octets	48 Bits 6 Octets	16 Bits 2 Octets	46 - 1500 Octets	32 Bits 4 Octets

Ethernet

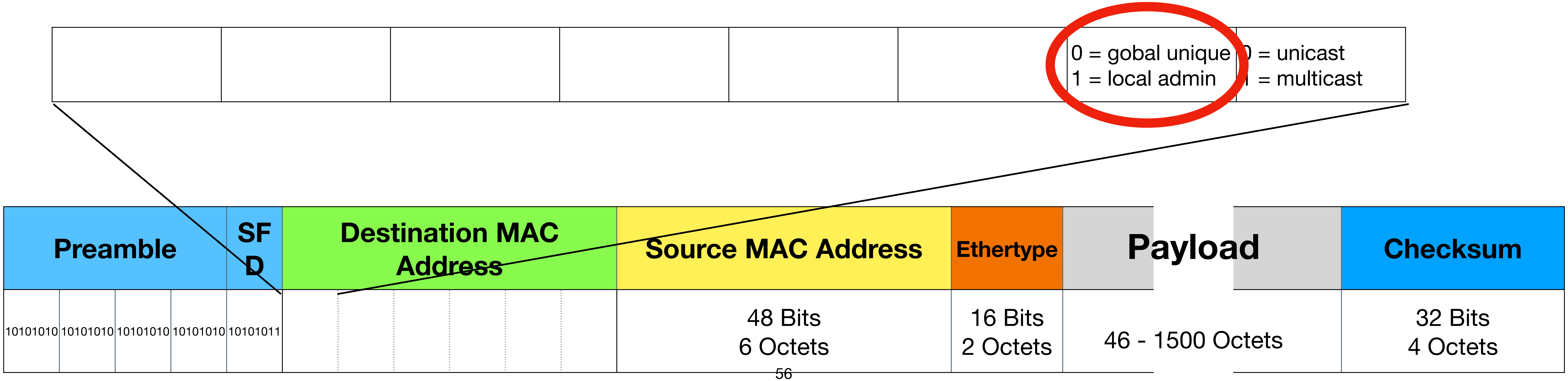
Addressing

- 48 Bit address - 6 octets
- 281 trillion possible addresses
- managed by IEEE
  - you can purchase blocks of addresses
- notation examples:
  - 00:26:b0:d8:3d:8a
  - 0026.b0d8.3d8a
  - 00-26-b0-d8-3c-8a

Preamble				SFD	Destination MAC Address	Source MAC Address	Ethertype	Payload	Checksum
10101010	10101010	10101010	10101010	10101011	48 Bits 6 Octets	48 Bits 6 Octets	16 Bits 2 Octets	46 - 1500 Octets	32 Bits 4 Octets

Ethernet
Addressing

- Two bits in first octect have special meaning
- one for local vs. globally unique addresses
  - unique: usually "burned" into the hardware by manufacturer
- one for unicast vs. multicast



Ethernet

Special Addresses

- **FF:FF:FF:FF:FF:FF**

  The ***broadcast*** address

- Received by all nodes

Preamble	SFD	Destination MAC Address	Source MAC Address	Ethertype	Payload	Checksum
10101010 10101010 10101010 10101010	10101011		48 Bits 6 Octets	16 Bits 2 Octets	46 - 1500 Octets	32 Bits 4 Octets

Ethernet

Ethertype

- Was once used to indicate size of payload
  - Using values up 1500
- → Ethertype values start at 1536
- Some well-known values:

0x0800	IPv4
0x86dd	IPv6
0x0806	ARP
0x8100	VLAN Tagged

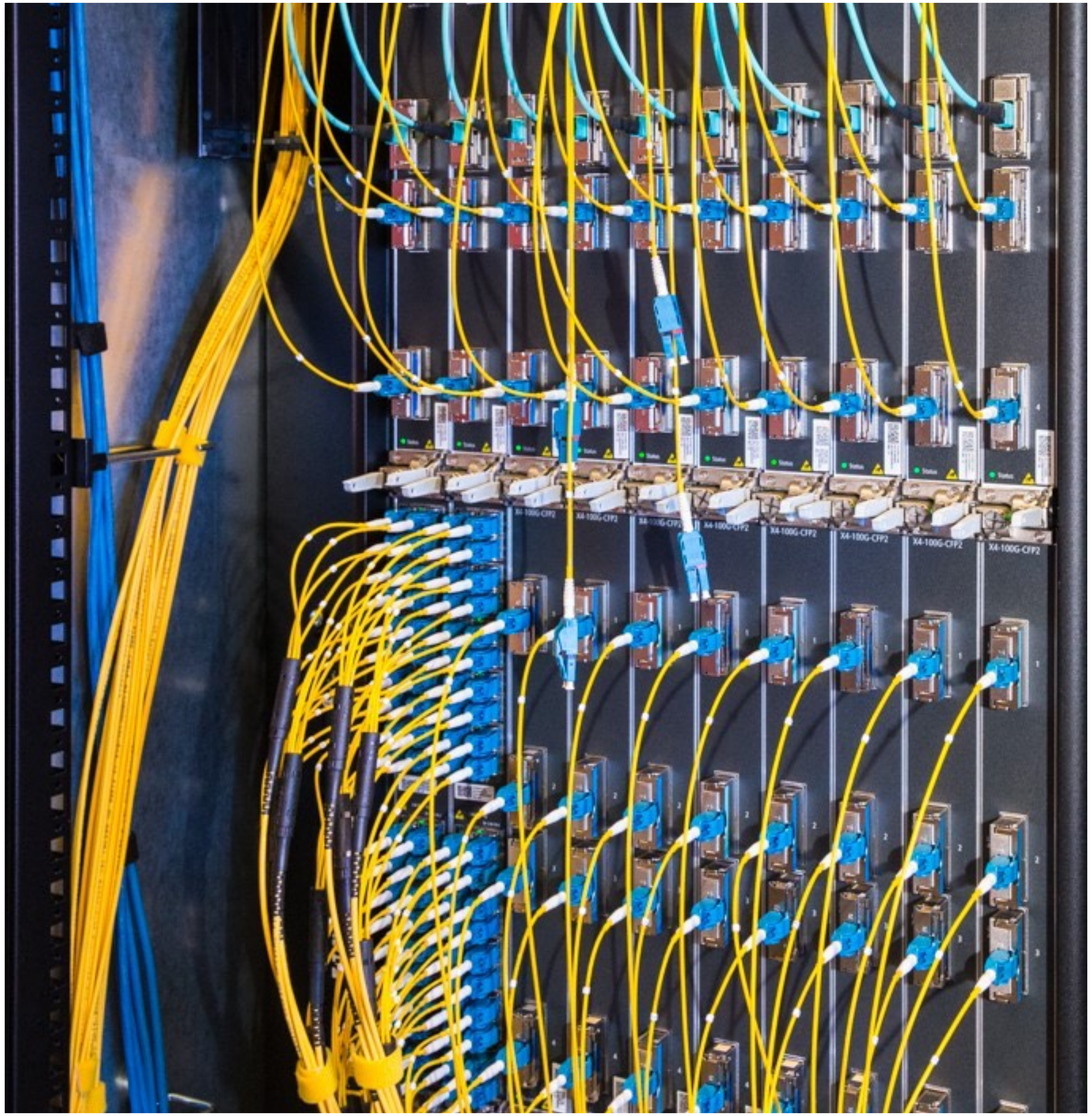
Preamble				SFD	Destination MAC Address	Source MAC Address	Ethertype	Payload	Checksum
10101010	10101010	10101010	10101010	10101011	48 Bits 6 Octets	48 Bits 6 Octets	16 Bits 2 Octets	46 - 1500 Octets	32 Bits 4 Octets

Ethernet Today

Ethernet connections

In data centers

- Usually optical fibres are used
- Various types exist (single mode, multi mode)
- Speeds are 1 GBit/s, 10 GBit/s, 100 GBit/s or 400 GBit/s
- Connections are between a *switch* and an end device



Ethernet at home

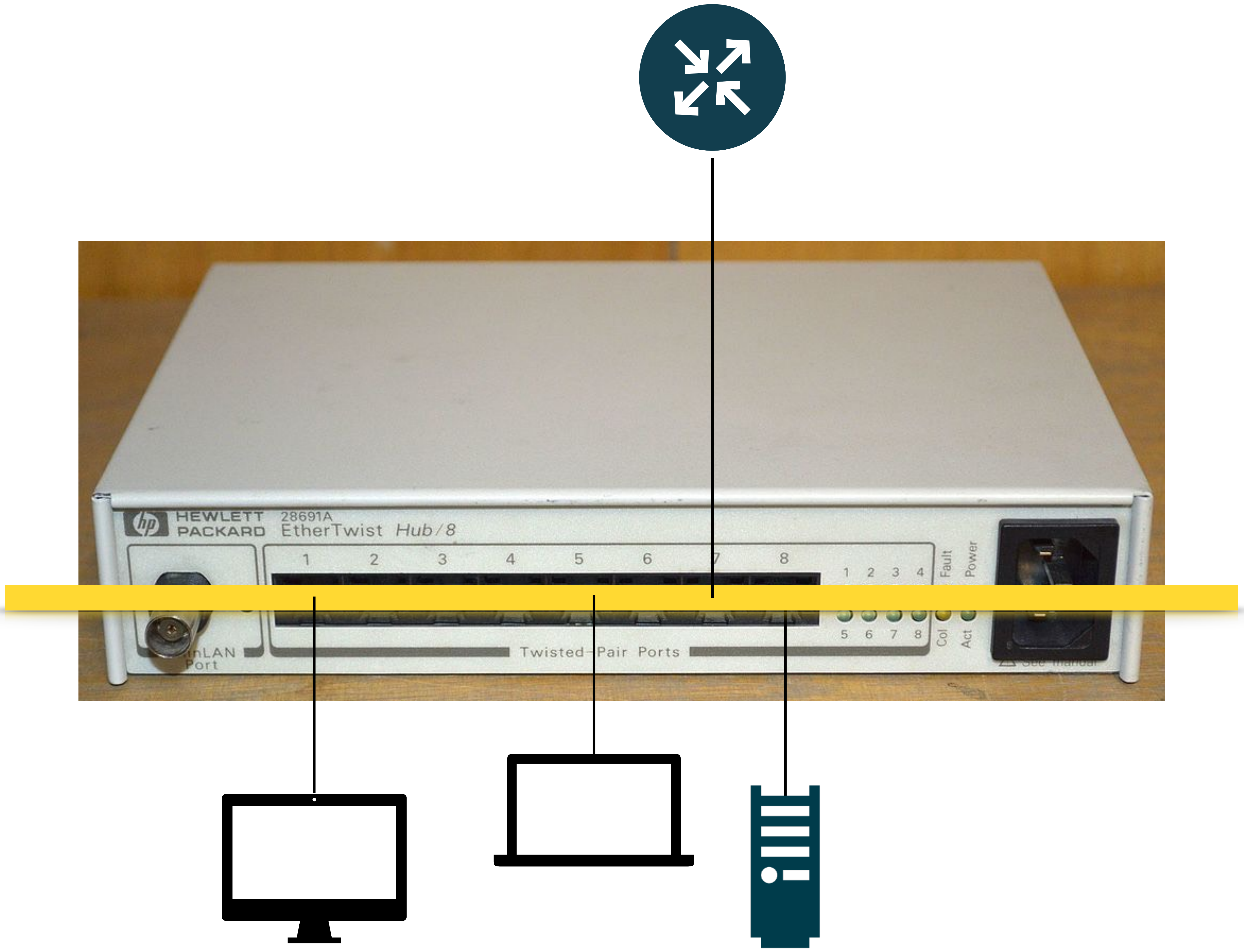
10Base-T

- Only wire-based connections are in use
- Speeds are 100Mbit/s or 1Gbit/s
- With a *switch* as a center
- Wireless Ethernet - WIFI is most common

Ethernet at home

10Base-T

- 10Base-T (twisted pair) requires a central device
- To replace the yellow coax cable
- Early devices: a *hub*
    - Function: What is received on one port is broadcasted out on all other ports
    - Just like the yellow coax cable



Attribution: Zac67
https://commons.wikimedia.org/wiki/File:HP_EtherTwist_Hub8.jpg

Ethernet Switch

Ethernet today

- Instead of a hub, a switch is common today
- Advantage:
  - a switch learns which devices are connected to which port
  - and only sends frames on ports they are destined to
  - fallback: unknown destinations are still broadcasted on all ports

Attribution: Wolfgang Tremmel

DE CIX

But...
Ethernet still....

- ...usually has a max payload size of 1500 octets
  - "jumbo frames" with 9000 octets exist, but are not commonly used
- ...uses 48-bit addresses
- ...is a broadcast medium.
  - but today *switches* are used and connections are point-to-point

DE CIX

Network layers - Internet Model

Ethernet: Link Layer

- Data units are called "Frames"
- Provides node-to-node data transfer
- Examples:
  - Point-to-Point Protocol (PPP)
  - Ethernet

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

Conclusion

Please remember....

Facts about Ethernet

- Ethernet is a **broadcast** network
- It uses **48-Bit** addresses
  - Which are globally **unique**
- Ethernet frames have usually max. 1500 octets **payload**
- Today ***switches*** interconnect devices

DENOG
GERMAN NETWORK OPERATORS GROUP

Networking Basics

02a - Ethernet + VLANs

Wolfgang Tremmel
academy@de-cix.net

Networking Basics
DE-CIX Academy

01 - Networks, Packets, and Protocols

02 - Ethernet

  02a - Ethernet + VLANs

03 - The Internet Protocol (IP)

  03a - IP addresses, prefixes, and routing

  03b - Global IP routing

04a - UDP

04b - TCP

04c - ICMP

05 - Unicast, Broadcast, Multicast, Anycast

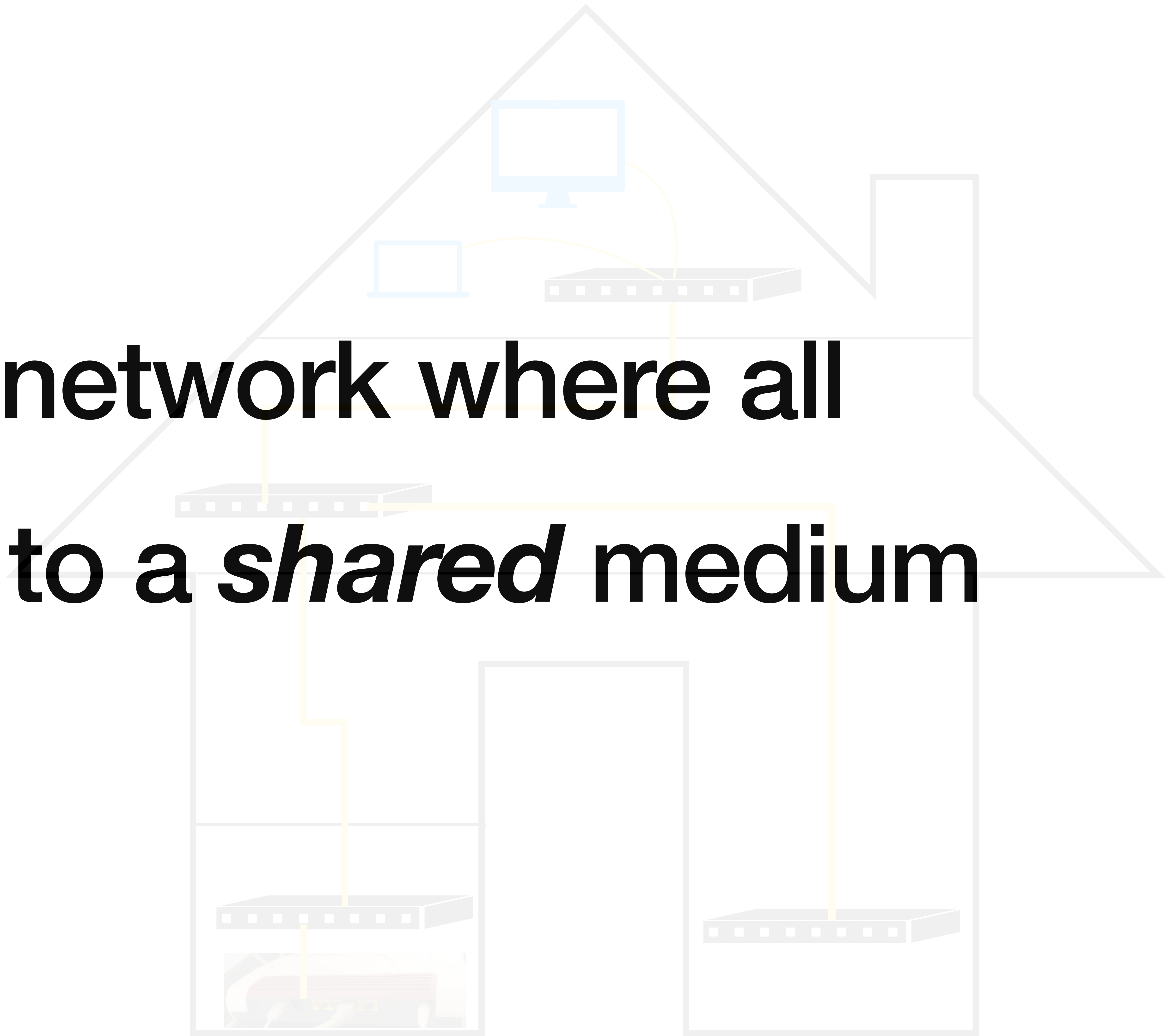
DE-CIX

Ethernet

A typical Ethernet

In an office building or a home

- A router where your Internet comes in
- A switch on each floor
- Multiple switches in larger offices
- End devices (computers) connected to the switches



Ethernet is a ***broadcast*** network where all devices are connected to a ***shared*** medium

Now you want a second network

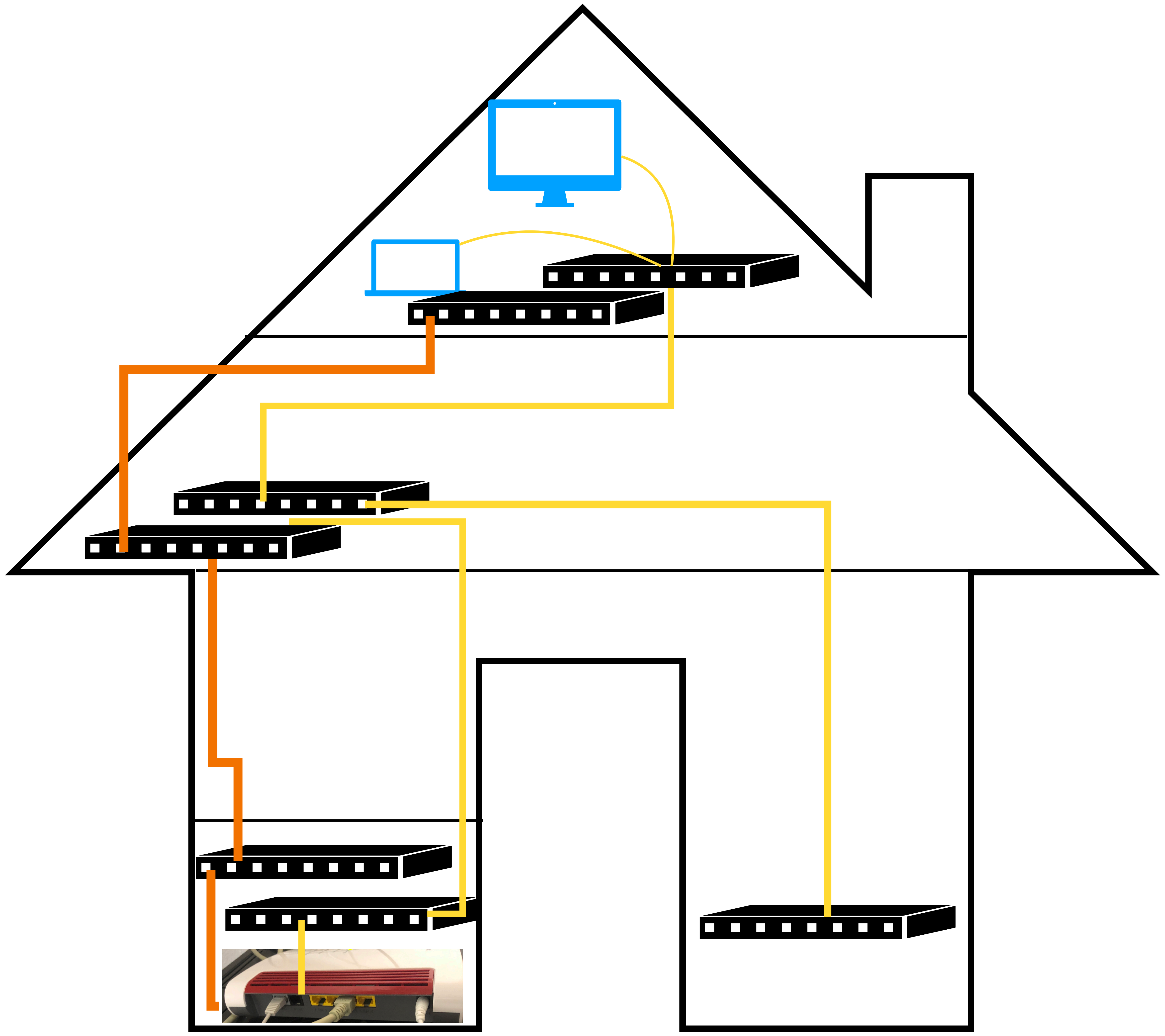
Now you want a second network

- For guests
- Or your telephones
- Or for network connected "things"

Second network

To keep separate things separate

- For example: Guest network
- Duplicate everything?
- No need - it's easier
- **VLANs** to the rescue!



VLANs

Virtual LANs

Ethernet Frame

- Some well-known values:

0x0800	IPv4
0x86dd	IPv6
0x0806	ARP
0x8100	VLAN Tagged

Preamble				SFD	Destination MAC Address	Source MAC Address	Ethertype	Payload	Checksum
10101010	10101010	10101010	10101010	10101011	48 Bits 6 Octets	48 Bits 6 Octets	16 Bits 2 Octets	46-1500 Octets	32 Bits 4 Octets

Ethernet Frame

VLAN tagged

- Some well-known values:

0x0800	IPv4
0x86dd	IPv6
0x0806	ARP
0x8100	VLAN Tagged

Preamble					SFD	Destination MAC Address	Source MAC Address	Ethertype	Payload	Checksum
10101010	10101010	10101010	10101010		10101011	48 Bits 6 Octets	48 Bits 6 Octets	16 Bits 2 Octets	46-1500 Octets	32 Bits 4 Octets

Preamble					SFD	Destination MAC Address	Source MAC Address	VLAN Header (801.1Q)		Ethertype	Payload	Checksum
10101010	10101010	10101010	10101010		10101011	48 Bits 6 Octets	48 Bits 6 Octets	0x8100	VLAN	16 Bits 2 Octets	42 - 1500 Octets	32 Bits 4 Octets

Ethernet

VLAN tagged frame

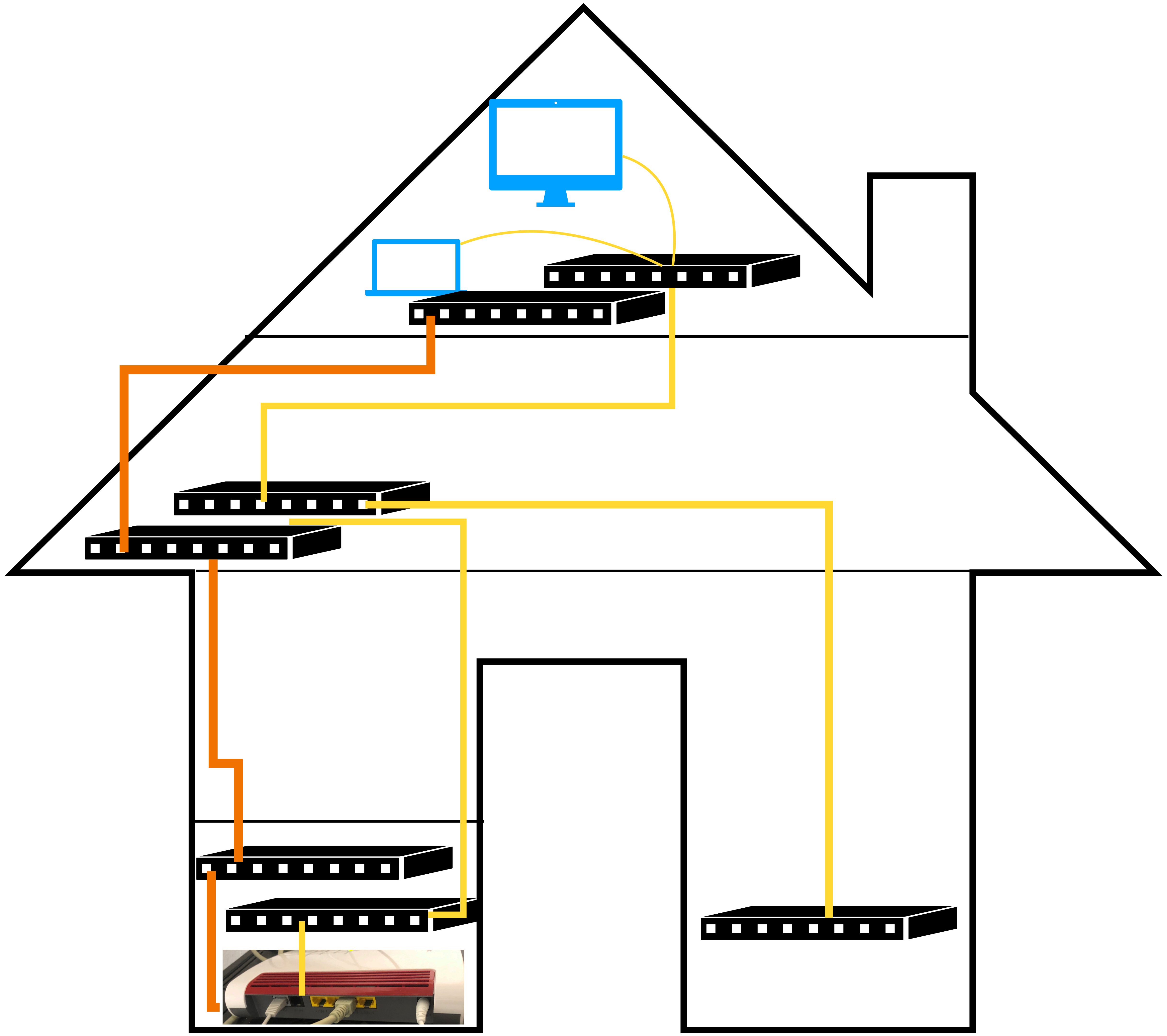
Preamble				SFD	Destination MAC Address	Source MAC Address	VLAN Header (801.1Q)		Ethertype	Payload	Checksum
10101010	10101010	10101010	10101010	10101011	48 Bits 6 Octets	48 Bits 6 Octets	0x8100	VLAN	16 Bits 2 Octets	42 - 1500 Octets	32 Bits 4 Octets

VLAN Header (801.1Q)			
16 Bits	3 Bits	1 Bit	12 Bits
0x8100	Priority	May be dropped?	VLAN ID 1-4094

Multiple networks

Use VLANs to separate

- You can have multiple VLANs on one physical infrastructure

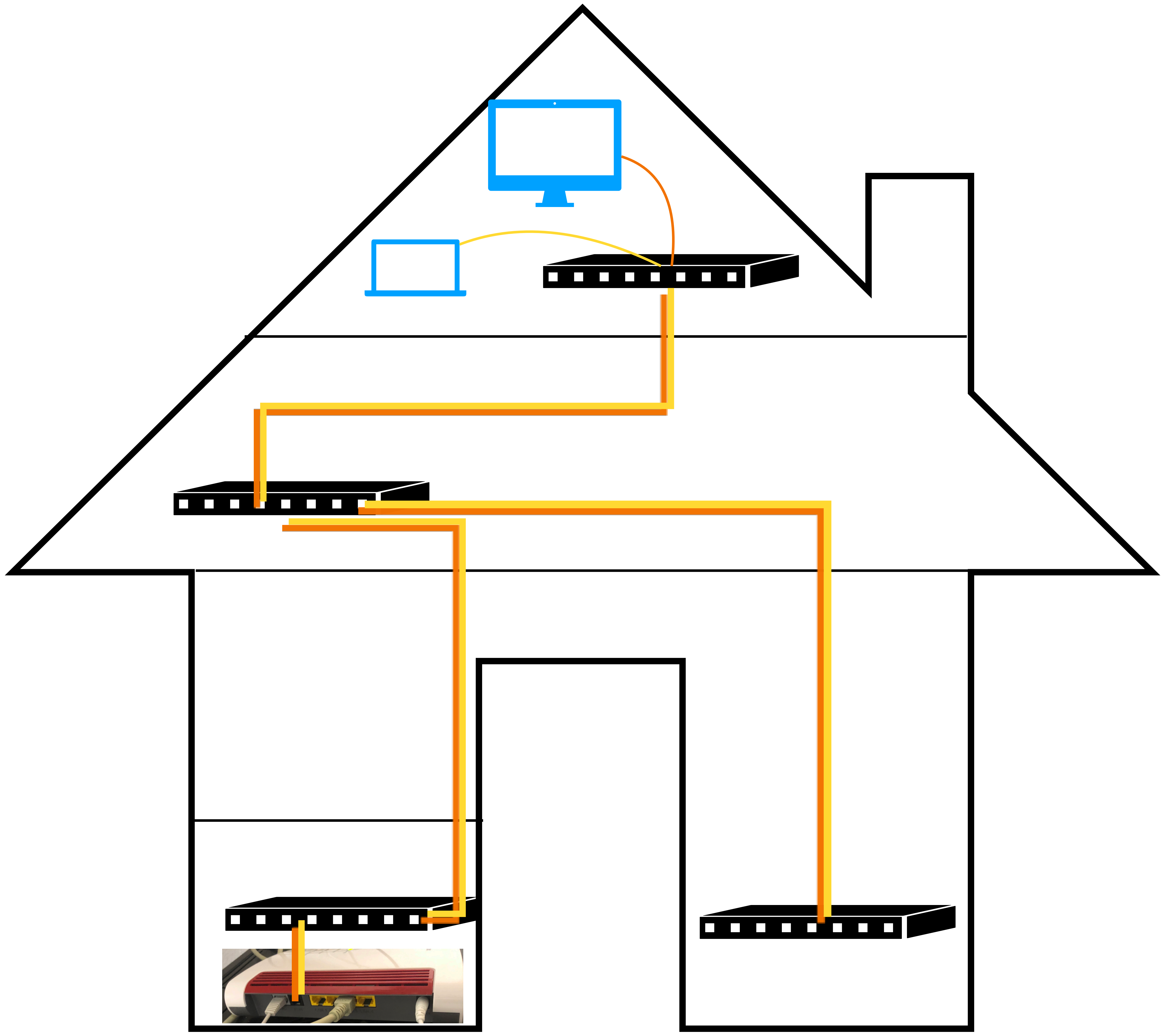


DE CIX

Multiple networks

Use VLANs to separate

- You can have multiple VLANs on one physical infrastructure
- Connections can have one or multiple VLANs on them
- Connections which carry multiple VLANs are called "trunk"



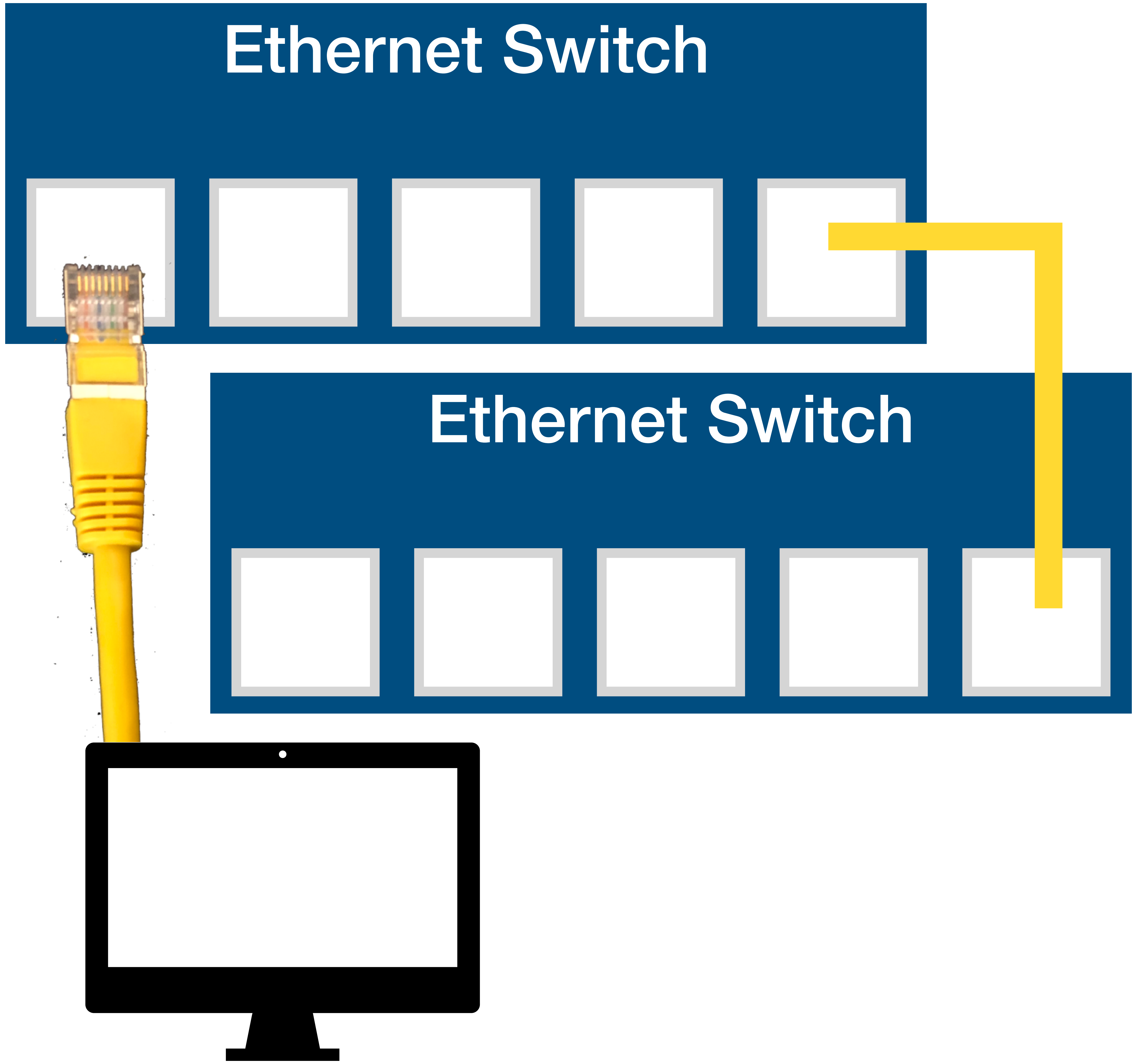
DE CIX

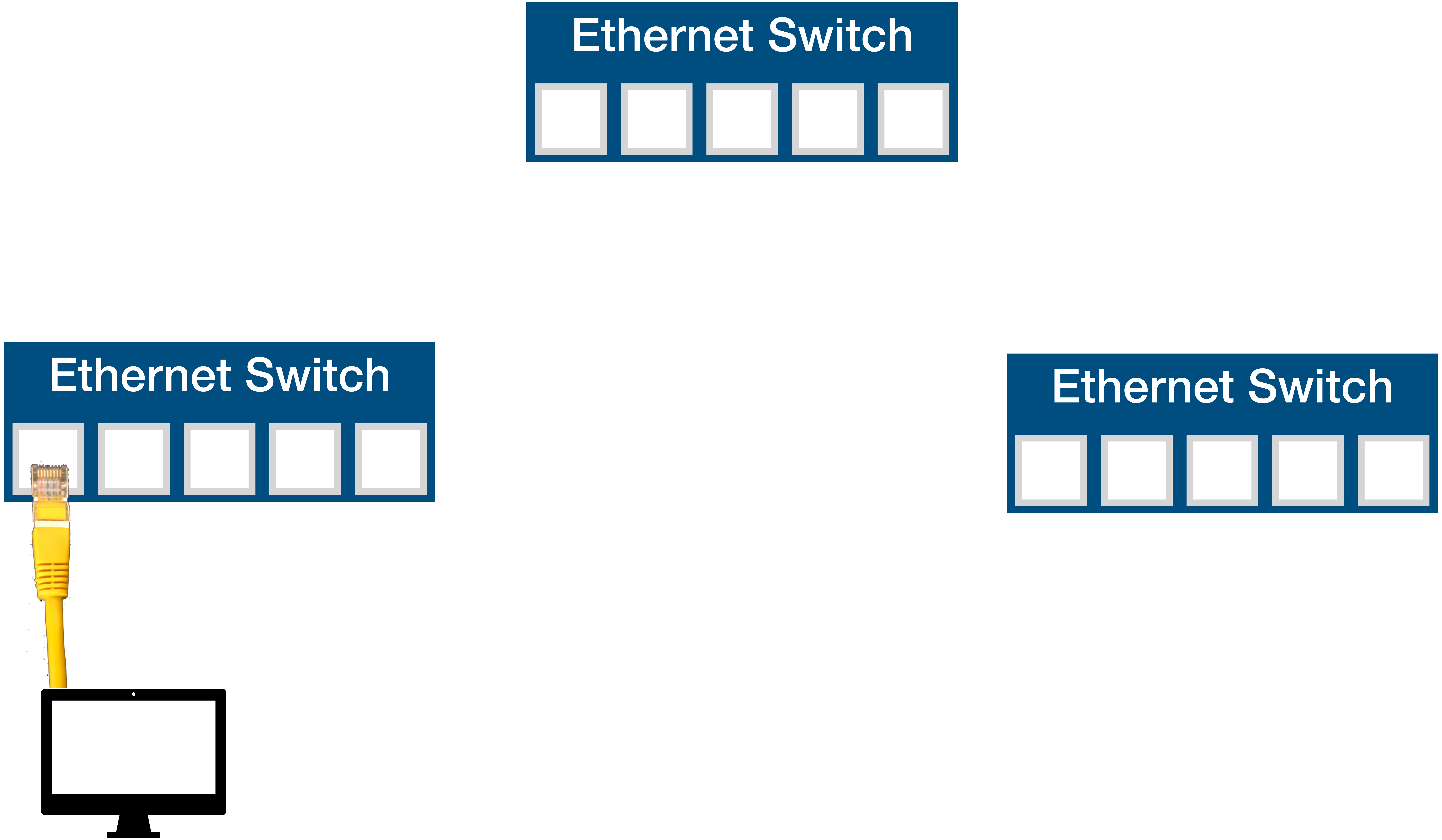
How to set it up?

How to set it up?

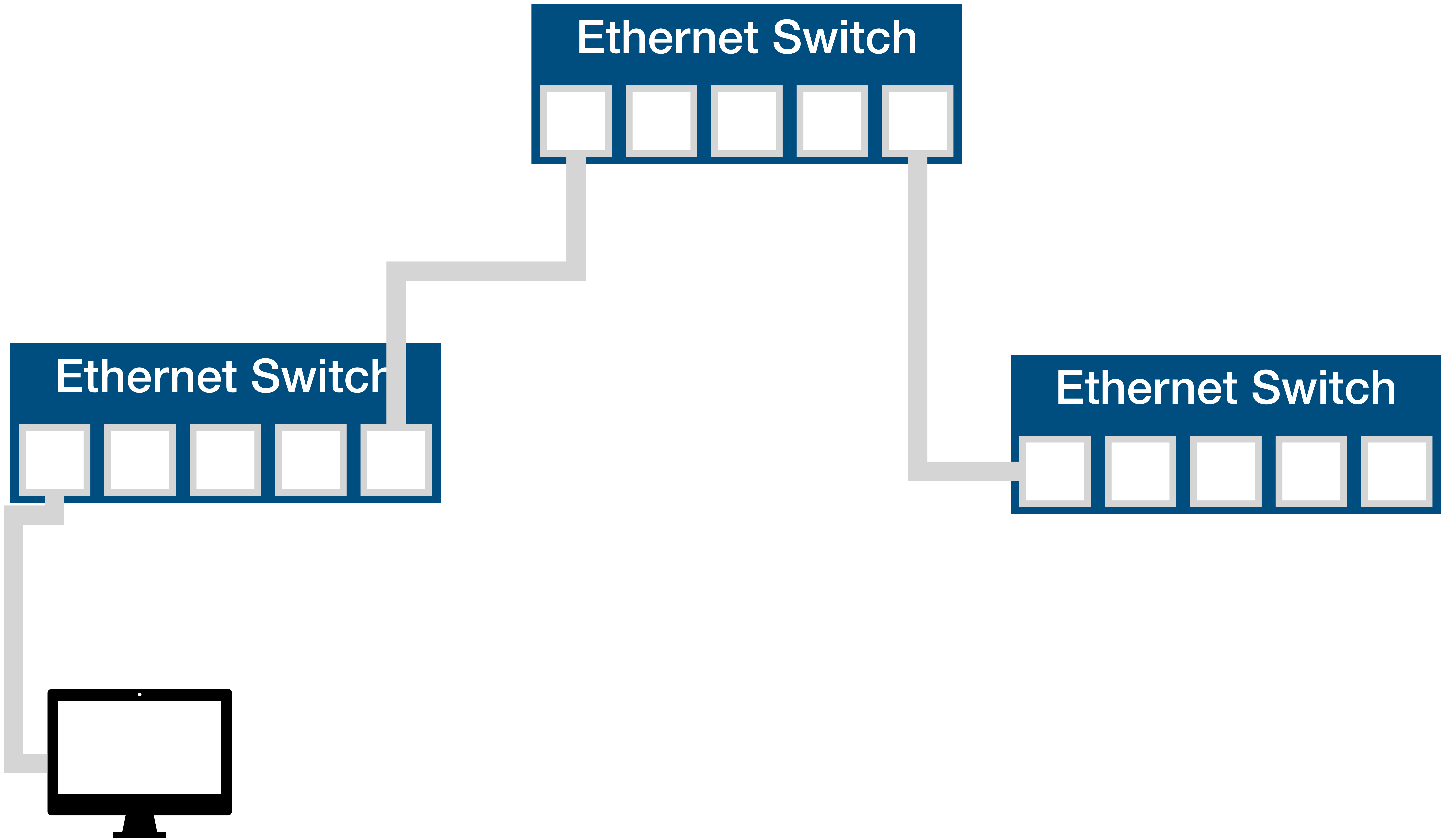
Building an Ethernet with VLANs

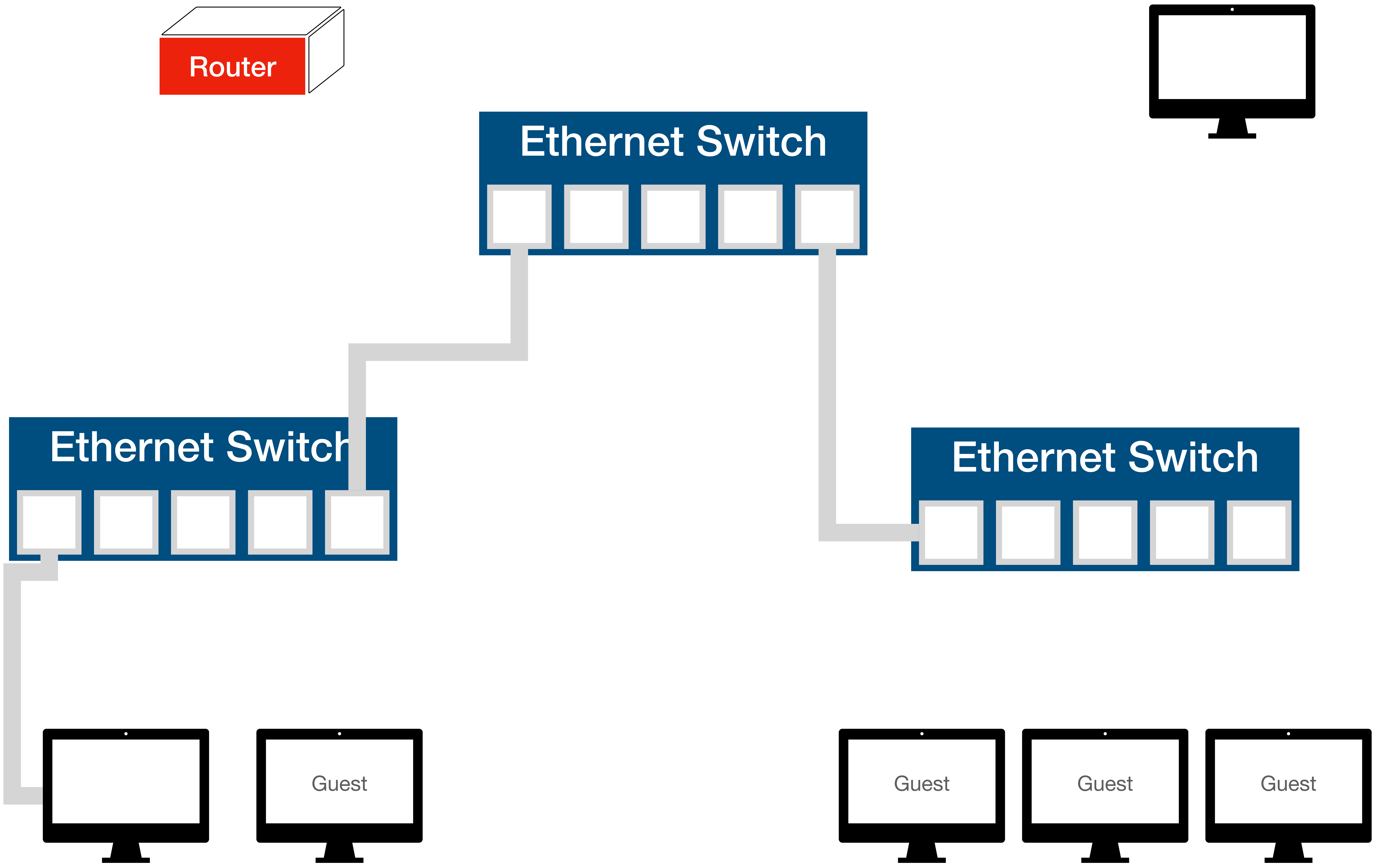
- You remember Ethernet switches?
- You might have one in your basement
- Ethernet switches connect devices to each other
- Ethernet switches also can connect to other switches

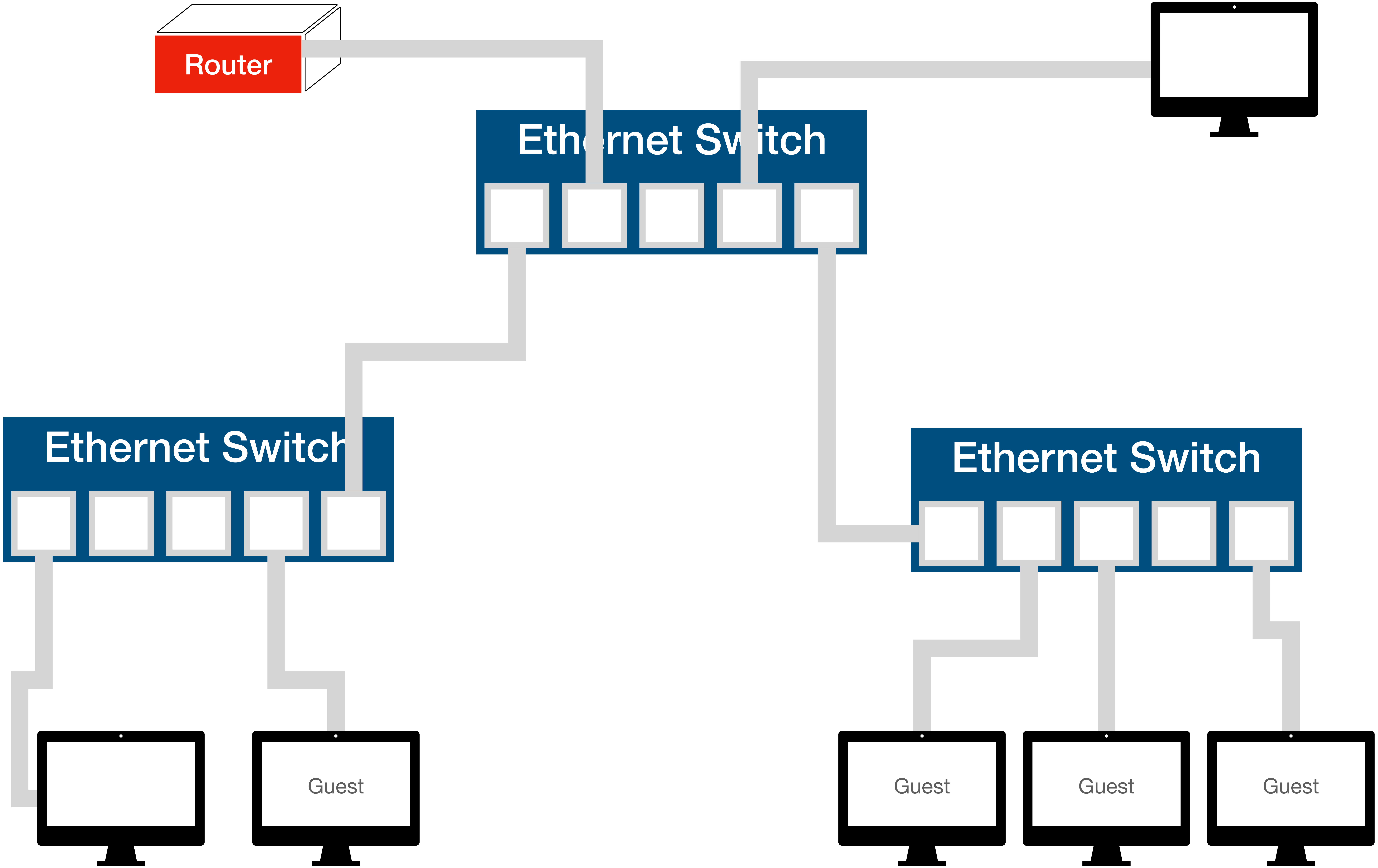




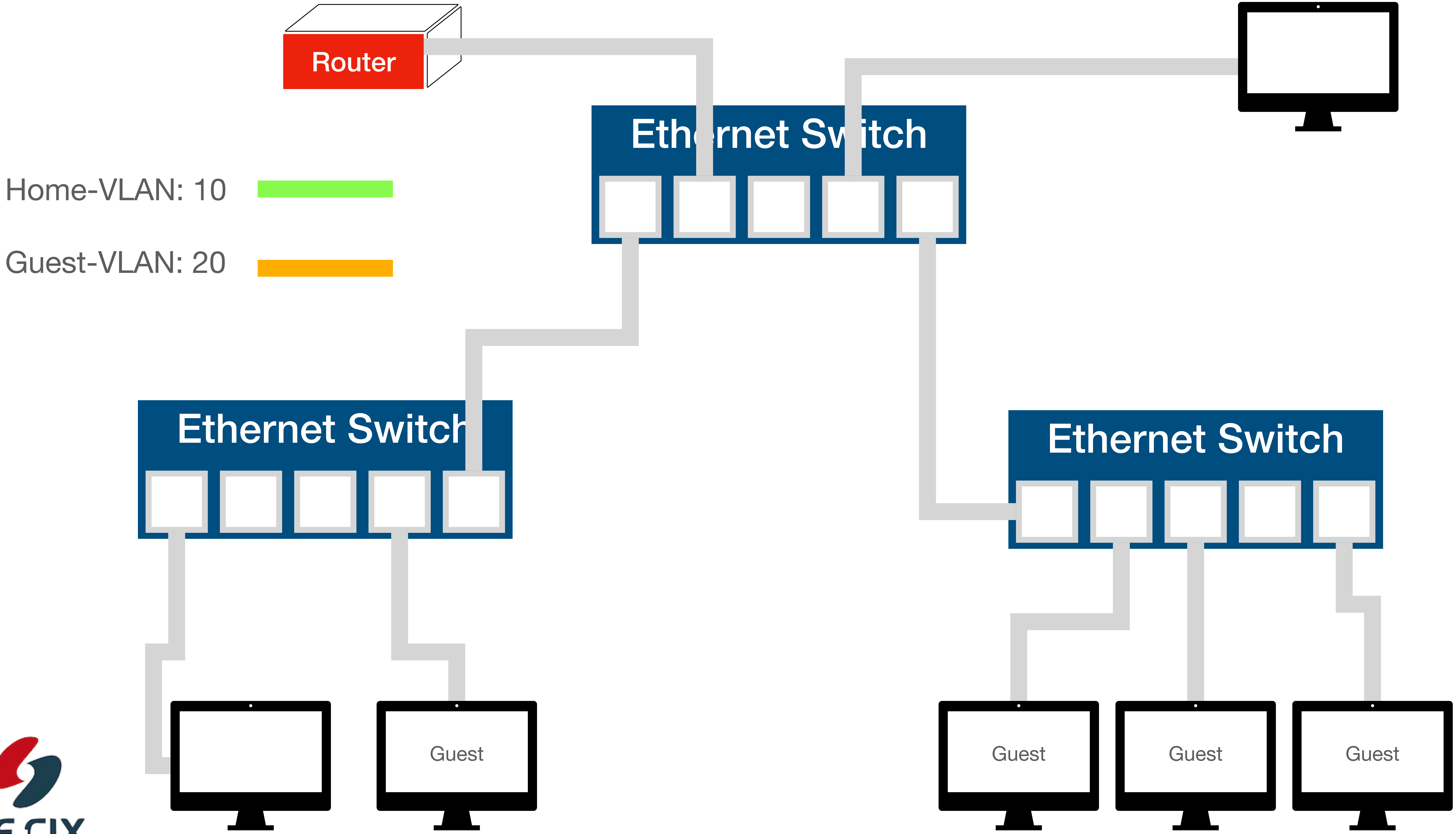
DE CIX

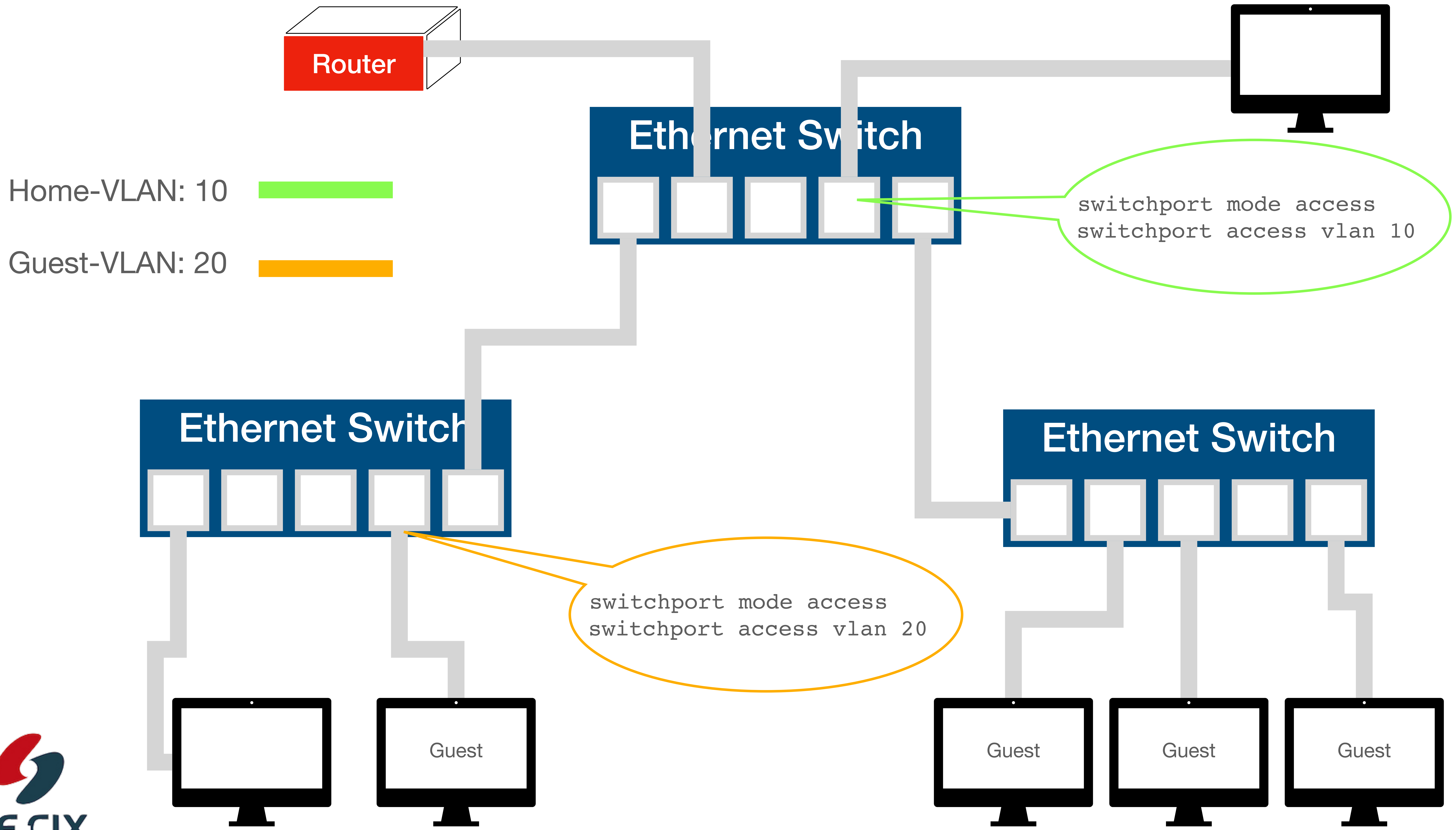

Ethernet Switch
Ethernet Switch
Ethernet Switch

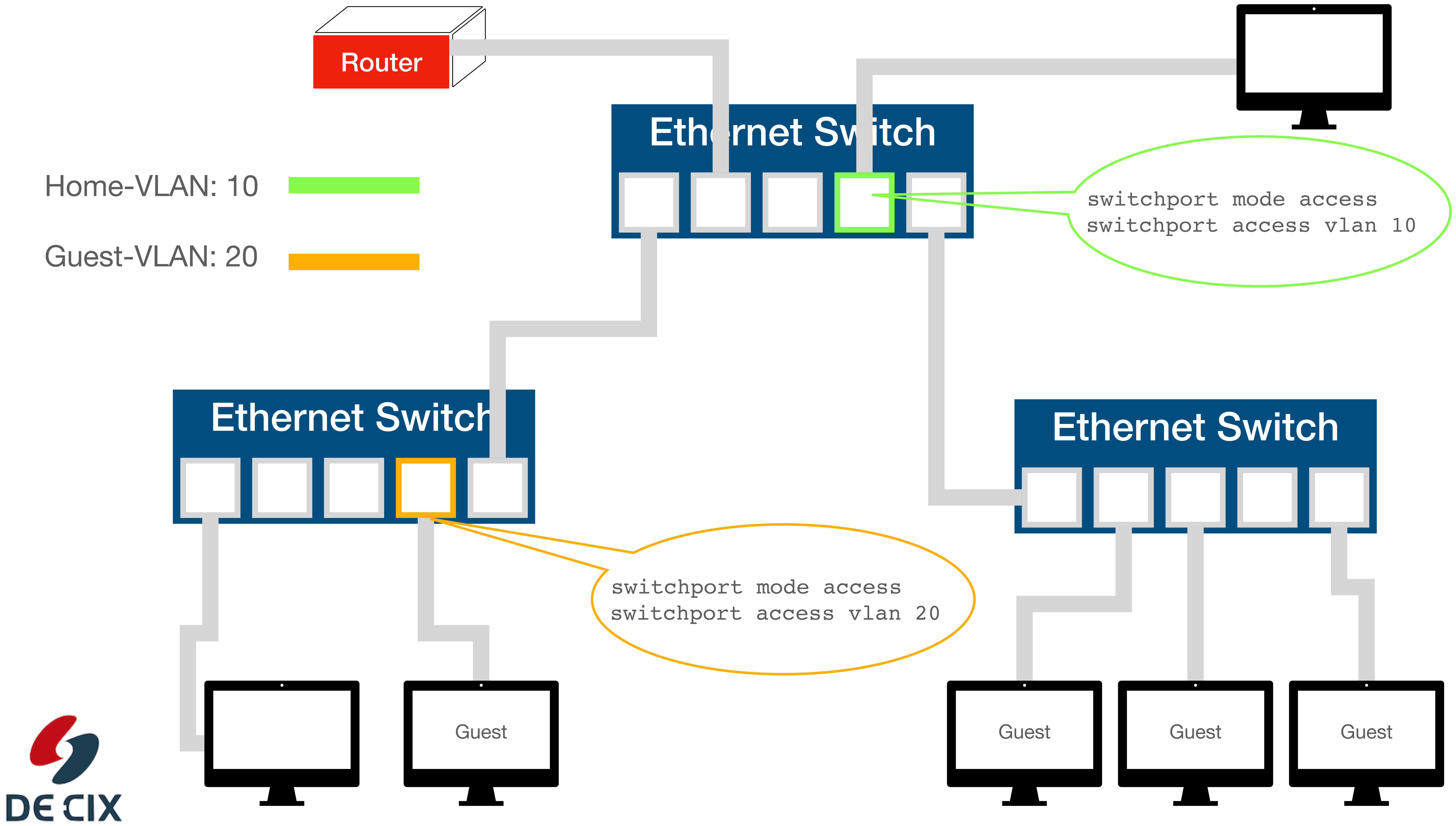

Router
Ethernet Switch
Ethernet Switch
Ethernet Switch
Guest
Guest
Guest
Guest

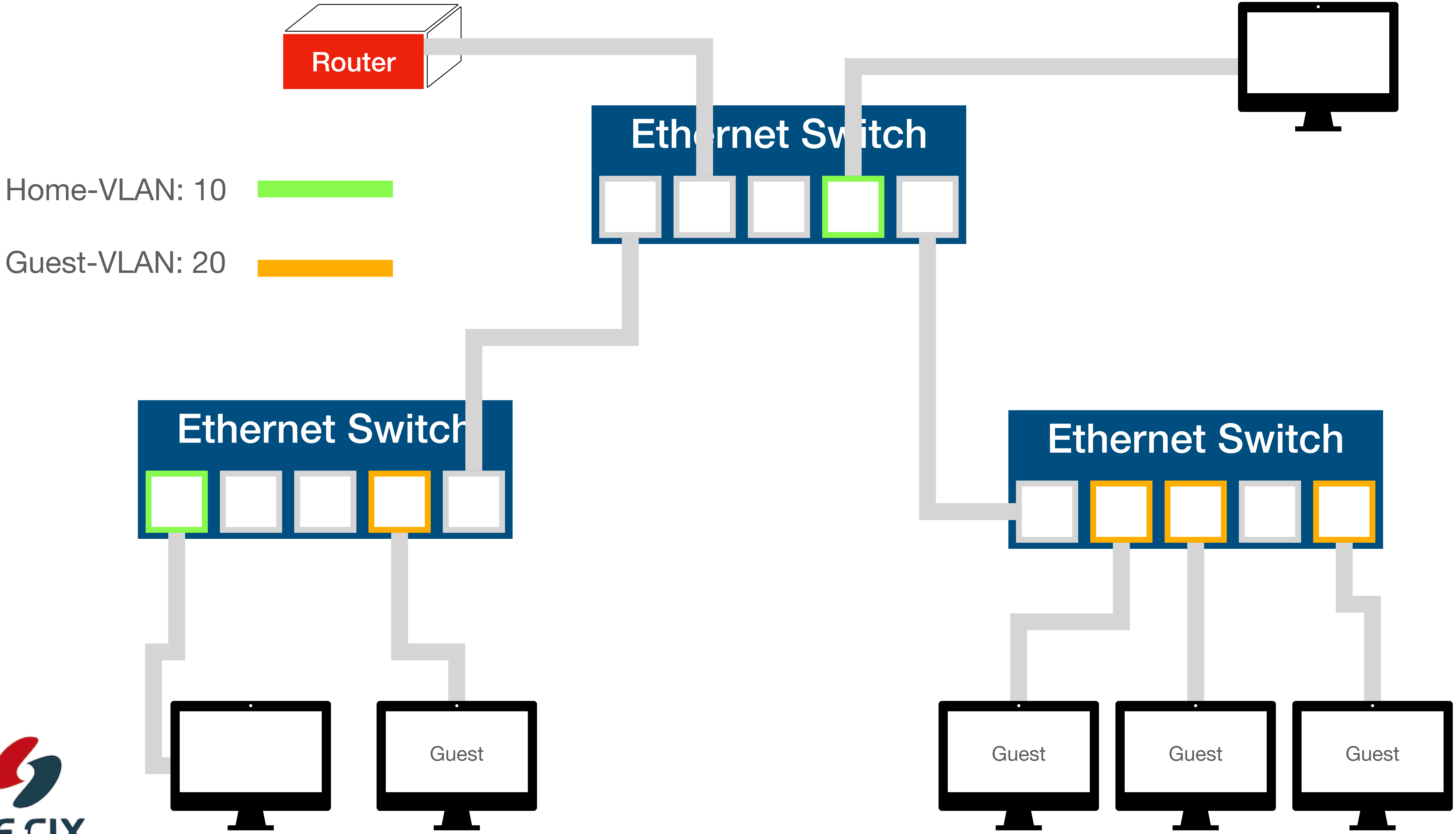


Router
Ethernet Switch
Ethernet Switch
Ethernet Switch
Guest
Guest
Guest
Guest

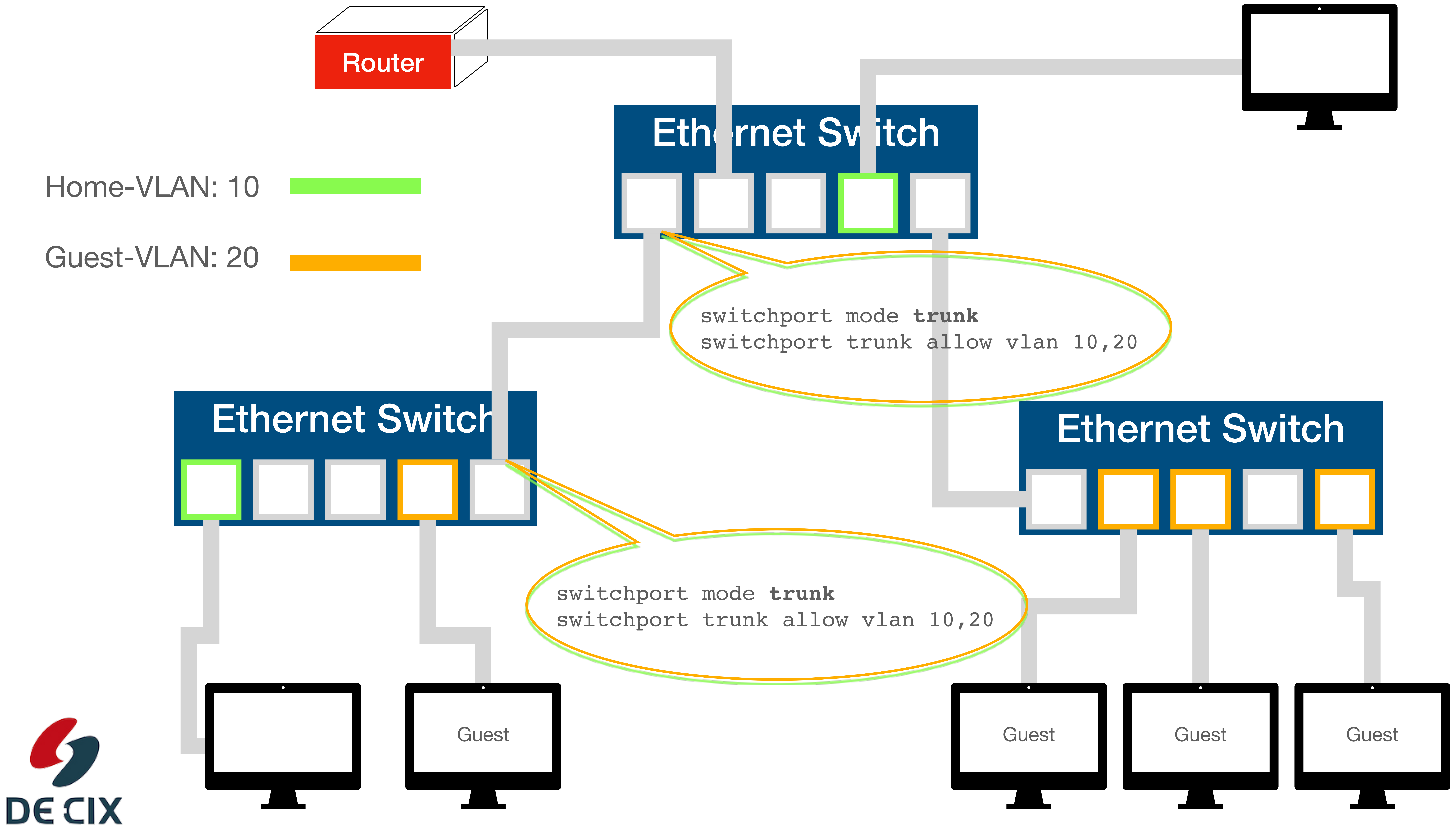

Router
Home-VLAN: 10
Guest-VLAN: 20
Ethernet Switch
Ethernet Switch
Guest
Guest
Guest
Guest


Router
Ethernet Switch
Home-VLAN: 10
Guest-VLAN: 20
switchport mode access
switchport access vlan 10
Ethernet Switch
Ethernet Switch
switchport mode access
switchport access vlan 20
Guest
Guest
Guest
Guest

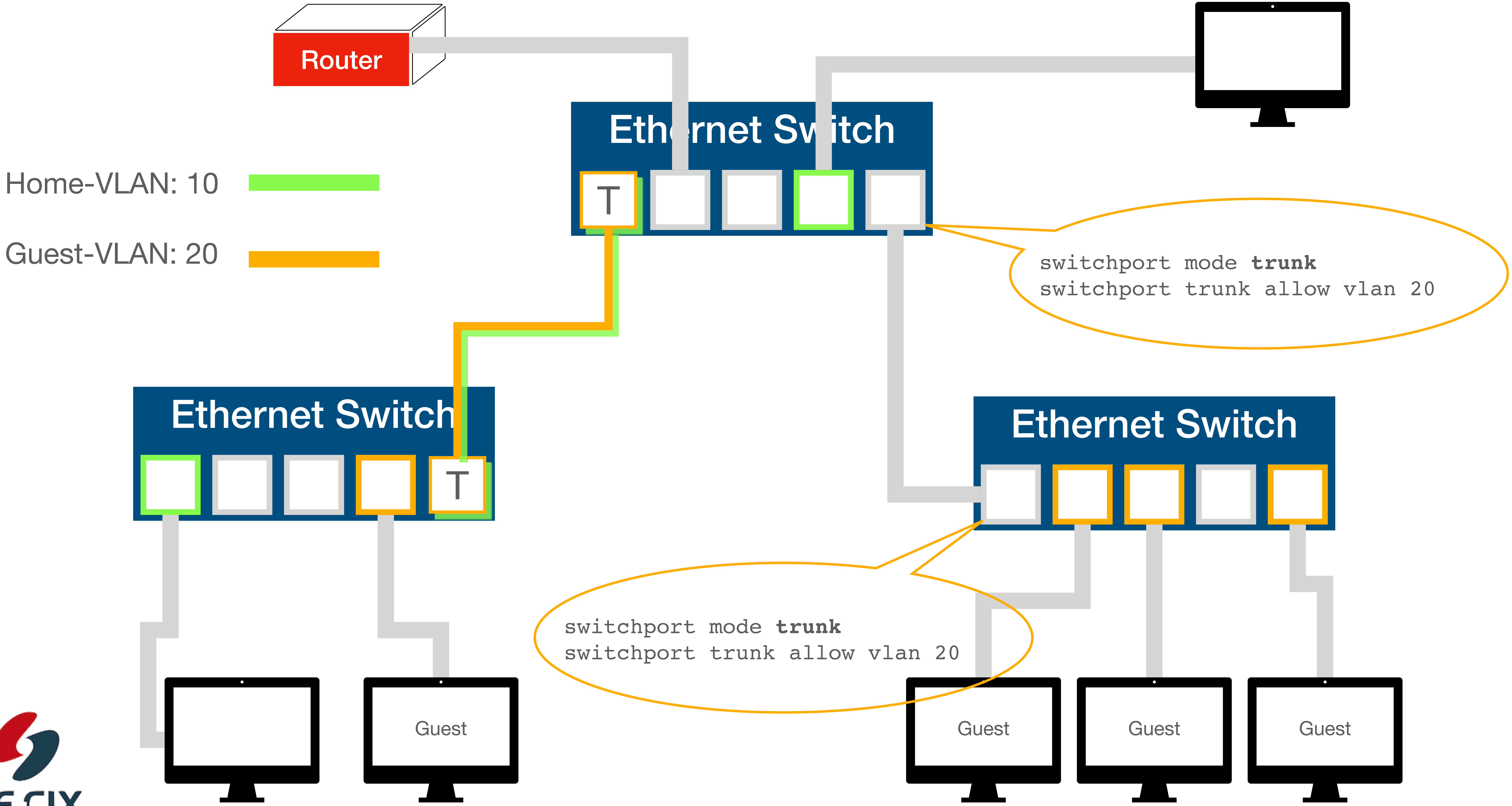

Router
Home-VLAN: 10
Guest-VLAN: 20
Ethernet Switch
switchport mode access
switchport access vlan 10
Ethernet Switch
Ethernet Switch
switchport mode access
switchport access vlan 20
Guest
Guest
Guest
Guest
DE CIX


Router
Ethernet Switch
Home-VLAN: 10
Guest-VLAN: 20
Ethernet Switch
Ethernet Switch
Guest
Guest
Guest
Guest

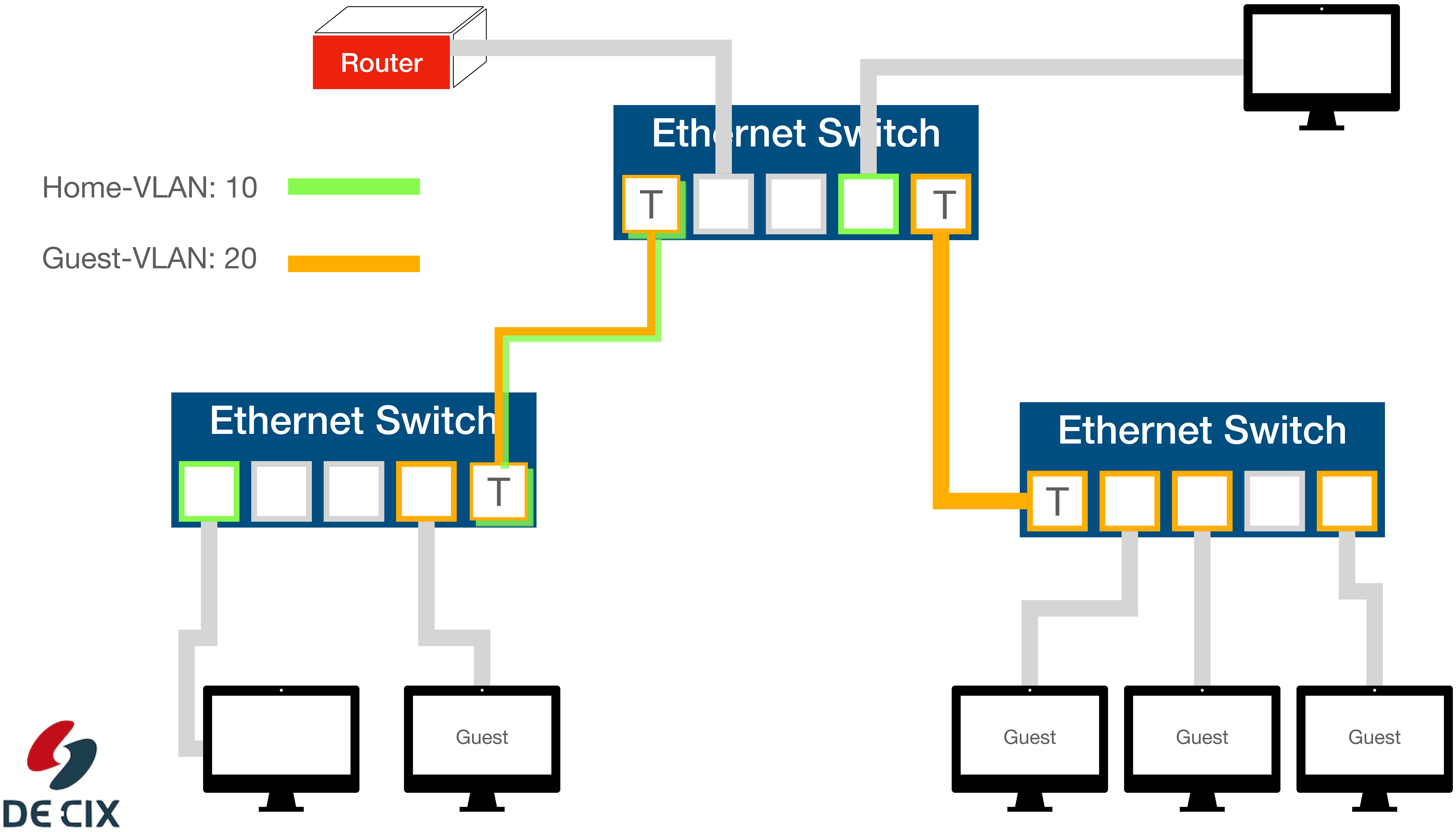
DE CIX


Router
Ethernet Switch
Home-VLAN: 10
Guest-VLAN: 20
switchport mode trunk
switchport trunk allow vlan 10,20
Ethernet Switch
Ethernet Switch
switchport mode trunk
switchport trunk allow vlan 10,20
Guest
Guest
Guest
Guest
DE CIX

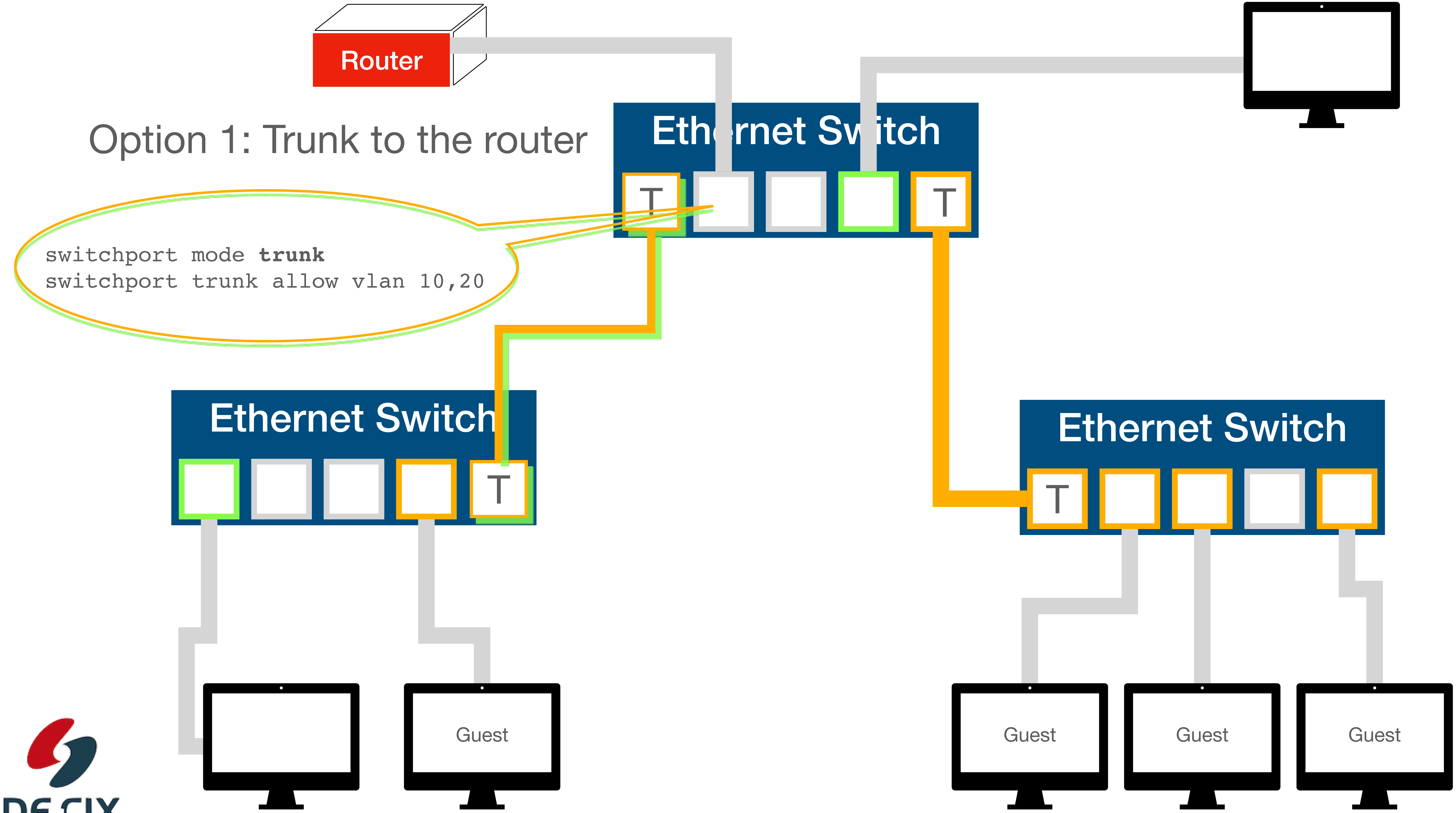

Router
Ethernet Switch
Home-VLAN: 10
Guest-VLAN: 20
T
switchport mode trunk
switchport trunk allow vlan 10,20
Ethernet Switch
T
Ethernet Switch
switchport mode trunk
switchport trunk allow vlan 10,20
Guest
Guest
Guest
Guest
DE CIX



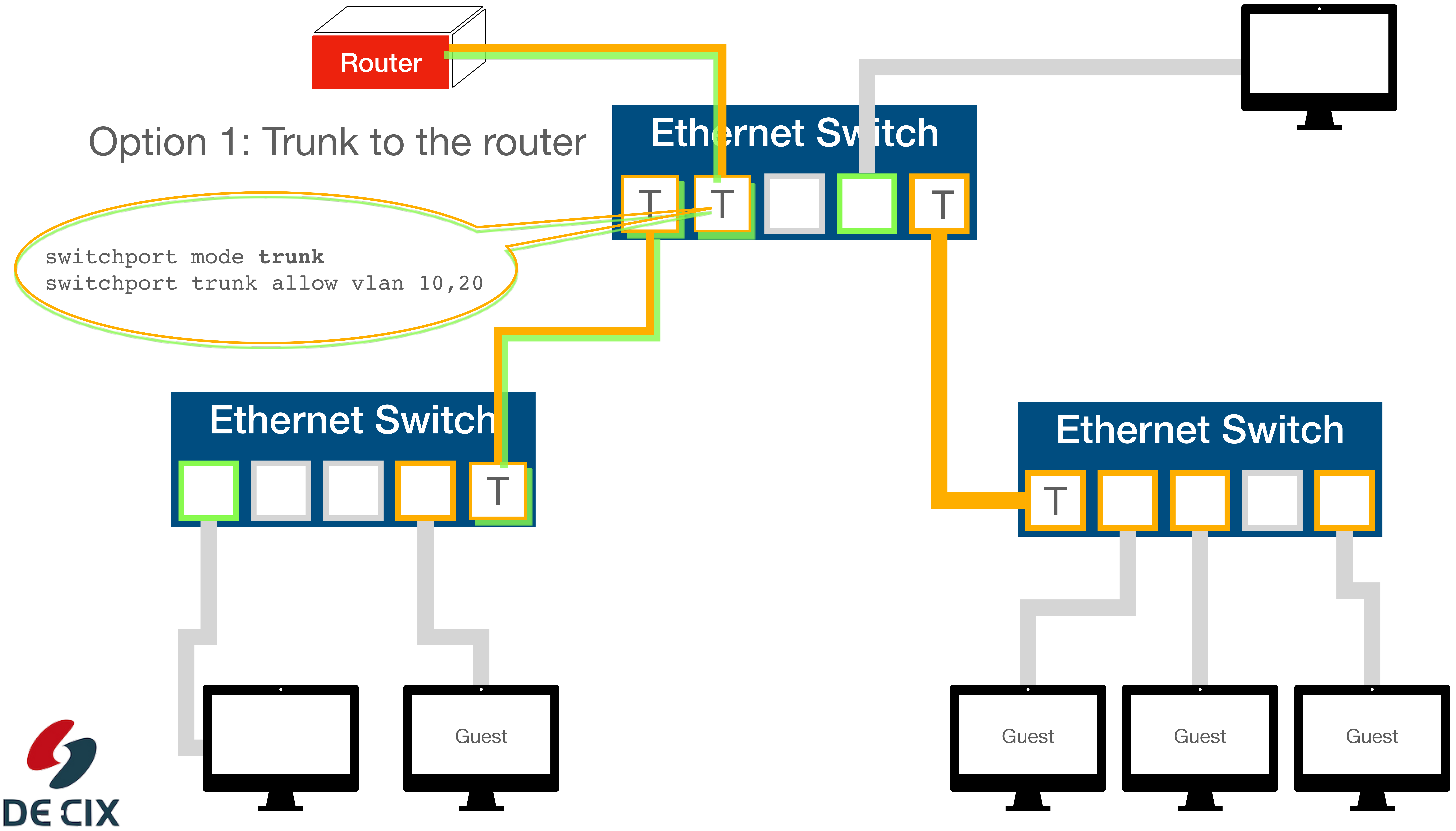
Router
Ethernet Switch
Home-VLAN: 10
Guest-VLAN: 20
T
switchport mode trunk
switchport trunk allow vlan 20
Ethernet Switch
T
Ethernet Switch
switchport mode trunk
switchport trunk allow vlan 20
Guest
Guest
Guest
Guest


Router
Ethernet Switch
T
T
Home-VLAN: 10
Guest-VLAN: 20
Ethernet Switch
T
Ethernet Switch
T
Guest
Guest
Guest
Guest
DE CIX

Option 1: Trunk to the router

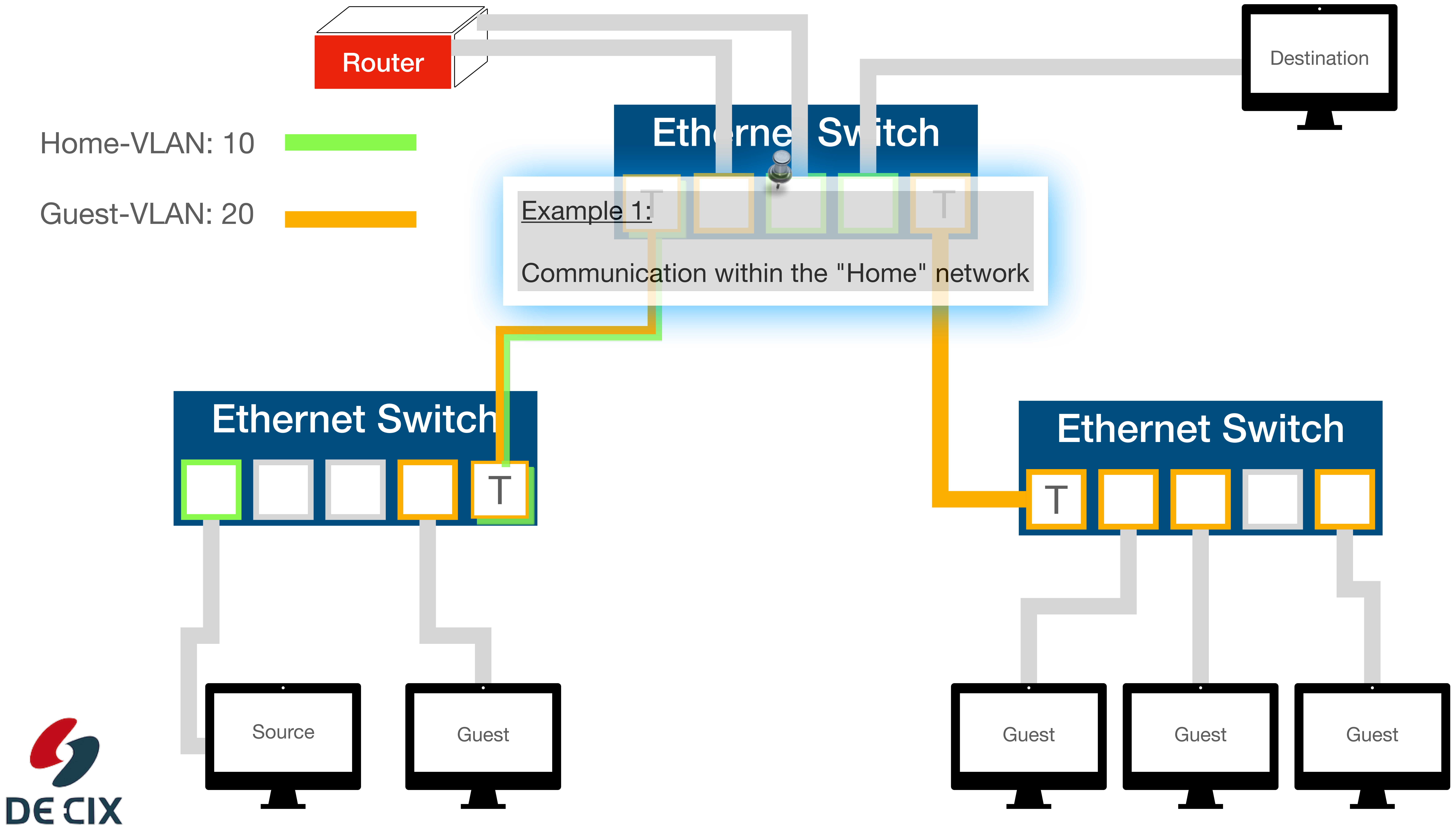


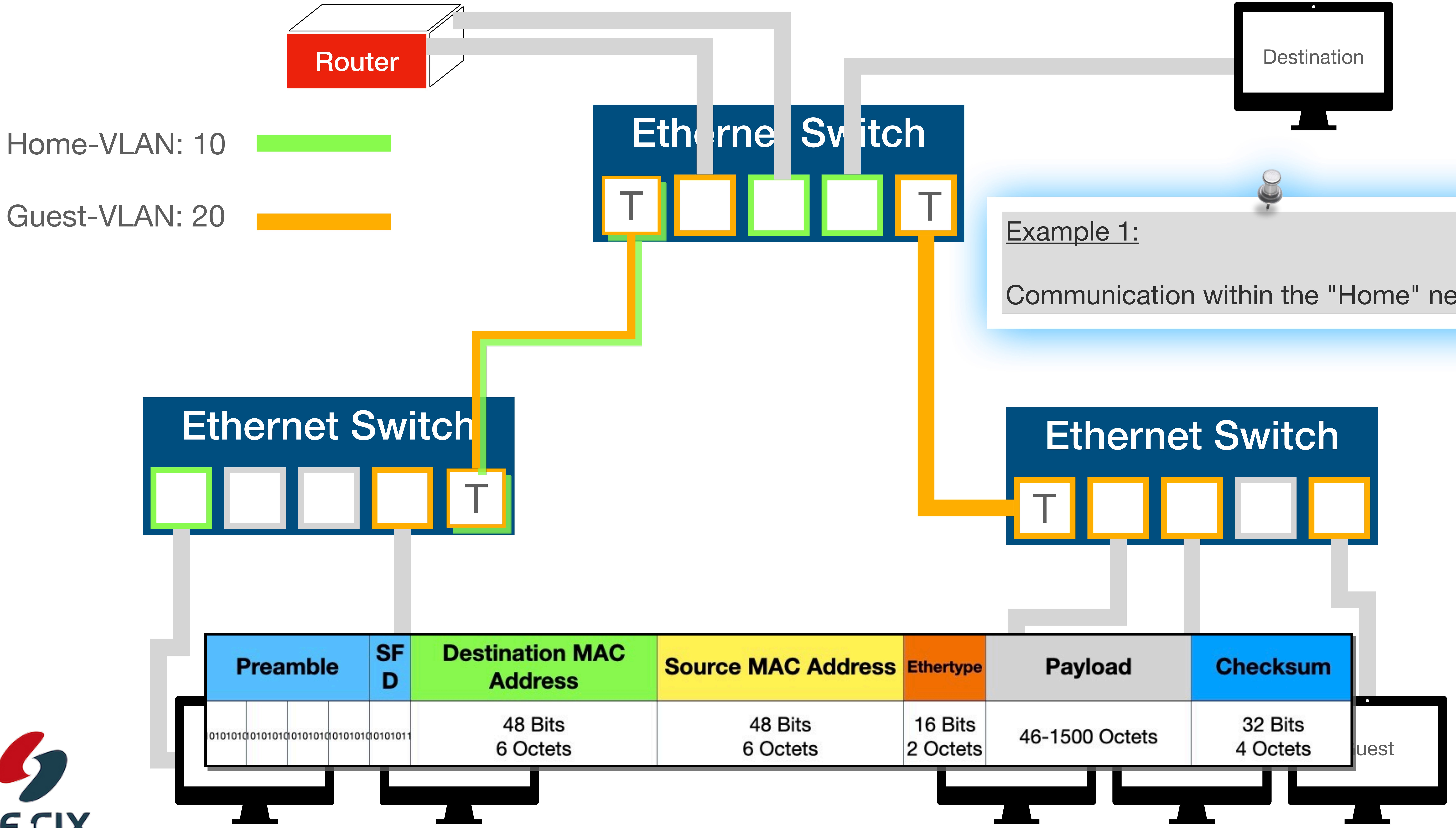
Option 1: Trunk to the router




Home LAN
Router
Option 2: Two access ports
Guest LAN
Ethernet Switch
T
T
Ethernet Switch
T
Ethernet Switch
T
Guest
Guest
Guest
Guest
DE CIX

And how does it work?

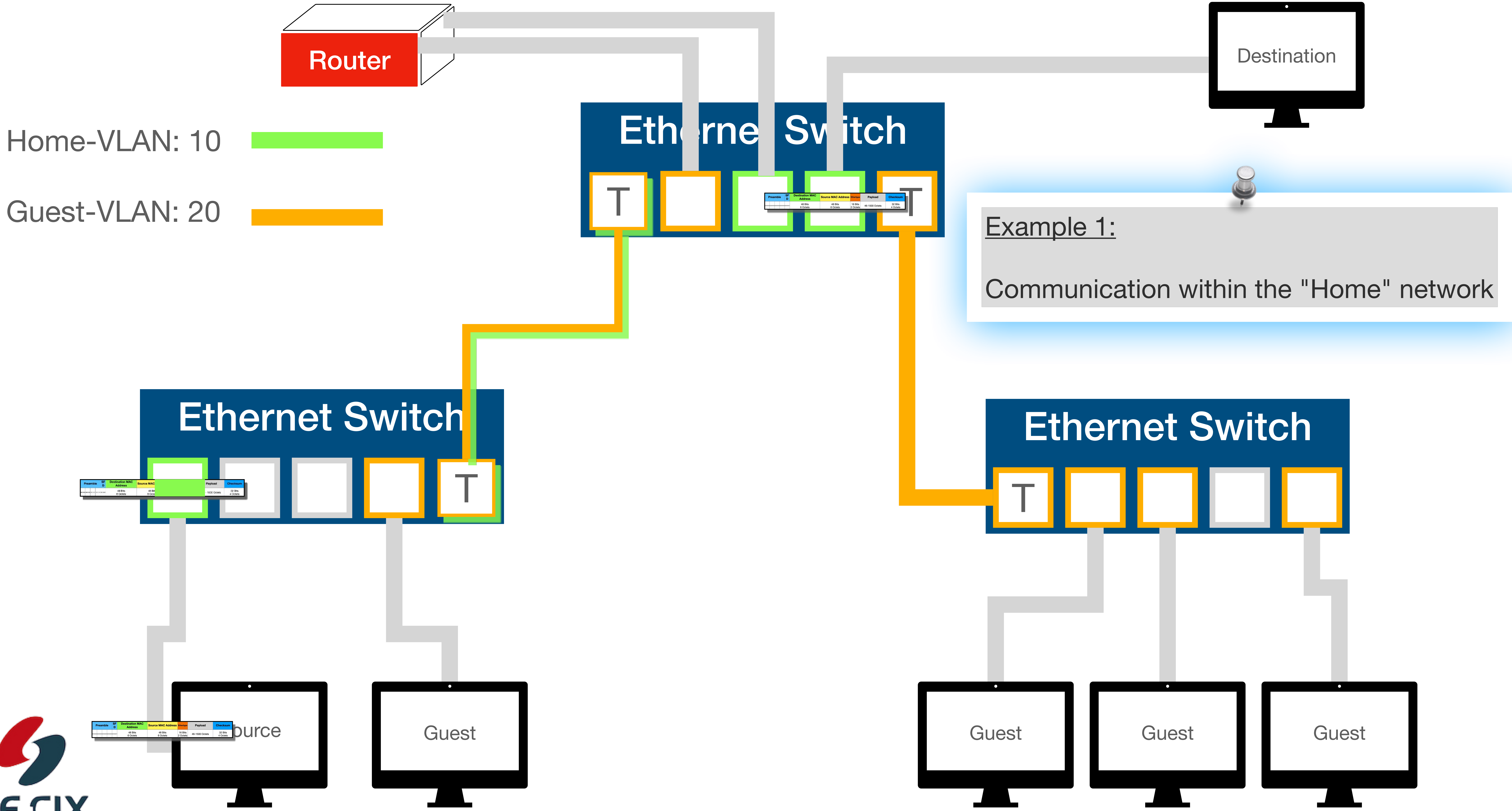

Router
Home-VLAN: 10
Guest-VLAN: 20
Ethernet Switch
T
Example 1:
Communication within the "Home" network
Destination
Ethernet Switch
T
Ethernet Switch
T
Source
Guest
Guest
Guest
Guest

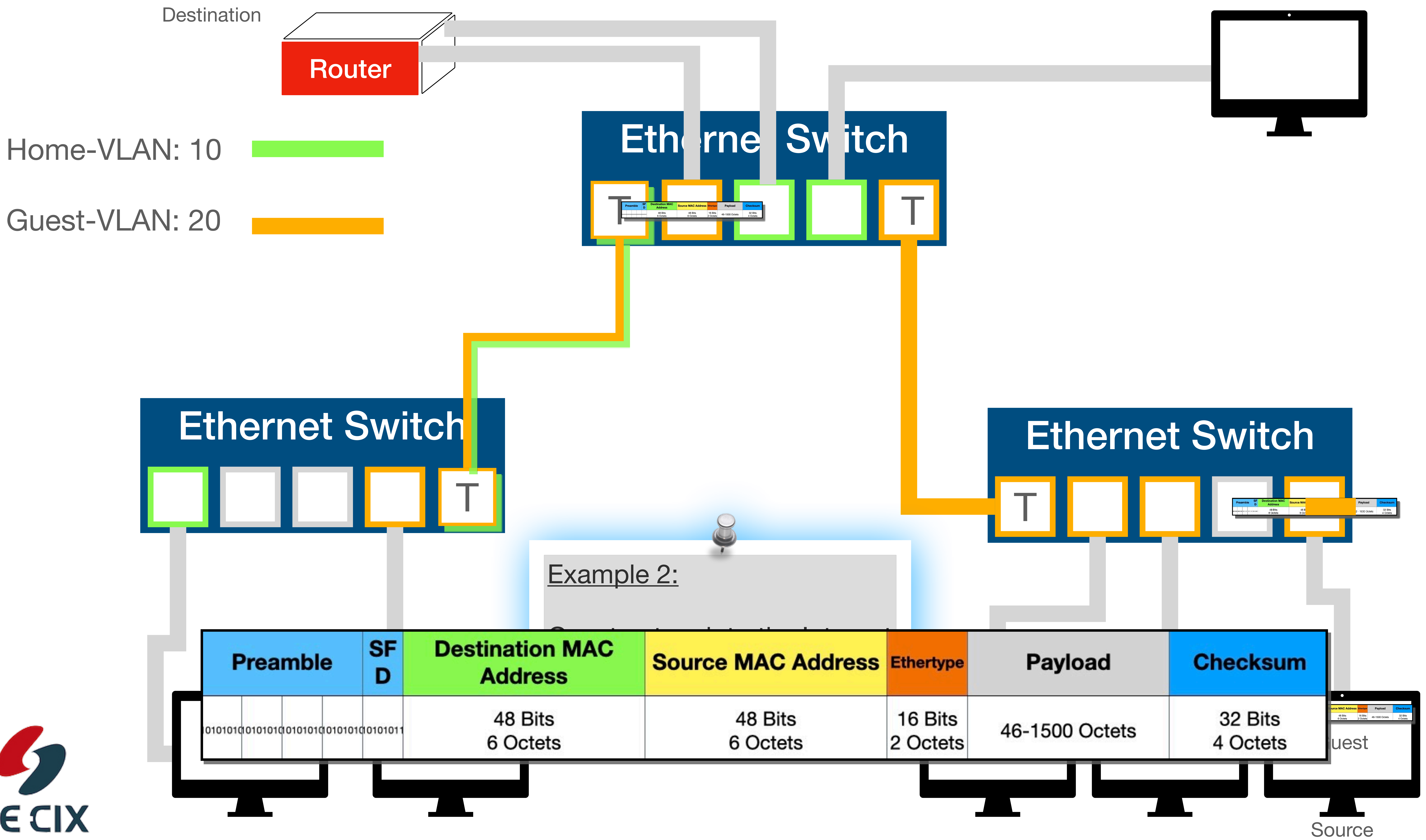


Example 1:

Communication within the "Home" network

Preamble				SFD	Destination MAC Address	Source MAC Address	Ethertype	Payload	Checksum
0101010	0101010	0101010	0101010	0101011	48 Bits 6 Octets	48 Bits 6 Octets	16 Bits 2 Octets	46-1500 Octets	32 Bits 4 Octets


Router
Destination
Home-VLAN: 10
Guest-VLAN: 20
Ethernet Switch
T
T
Example 1:
Communication within the "Home" network
Ethernet Switch
T
Ethernet Switch
T
Source
Guest
Guest
Guest
Guest



Preamble					SFD	Destination MAC Address	Source MAC Address	Ethertype	Payload	Checksum
10101010	10101010	10101010	10101010	10101010	10101011	48 Bits 6 Octets	48 Bits 6 Octets	16 Bits 2 Octets	46-1500 Octets	32 Bits 4 Octets

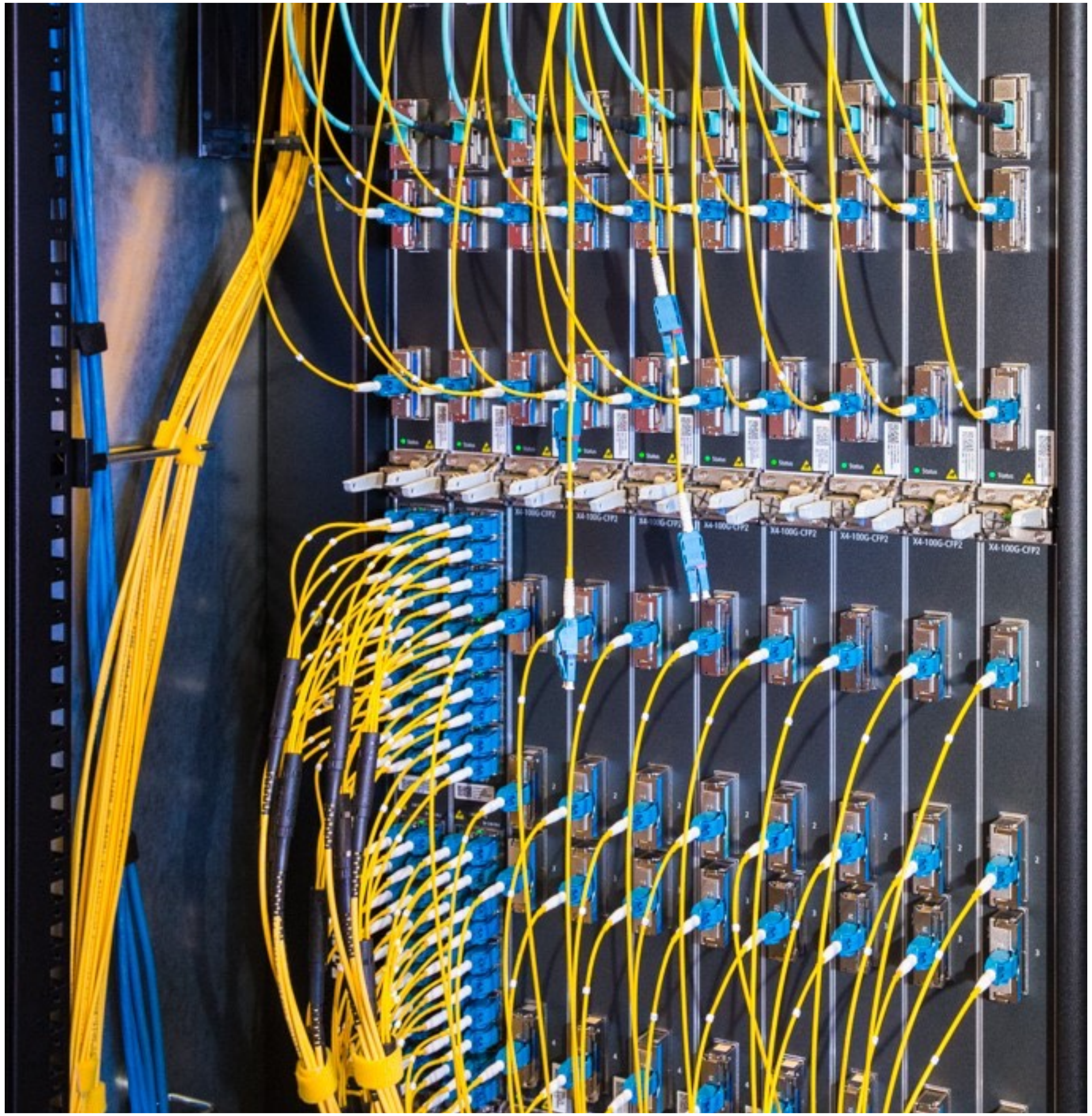
DE CIX

VLANs at DE-CIX

VLANs at DE-CIX

How we use them

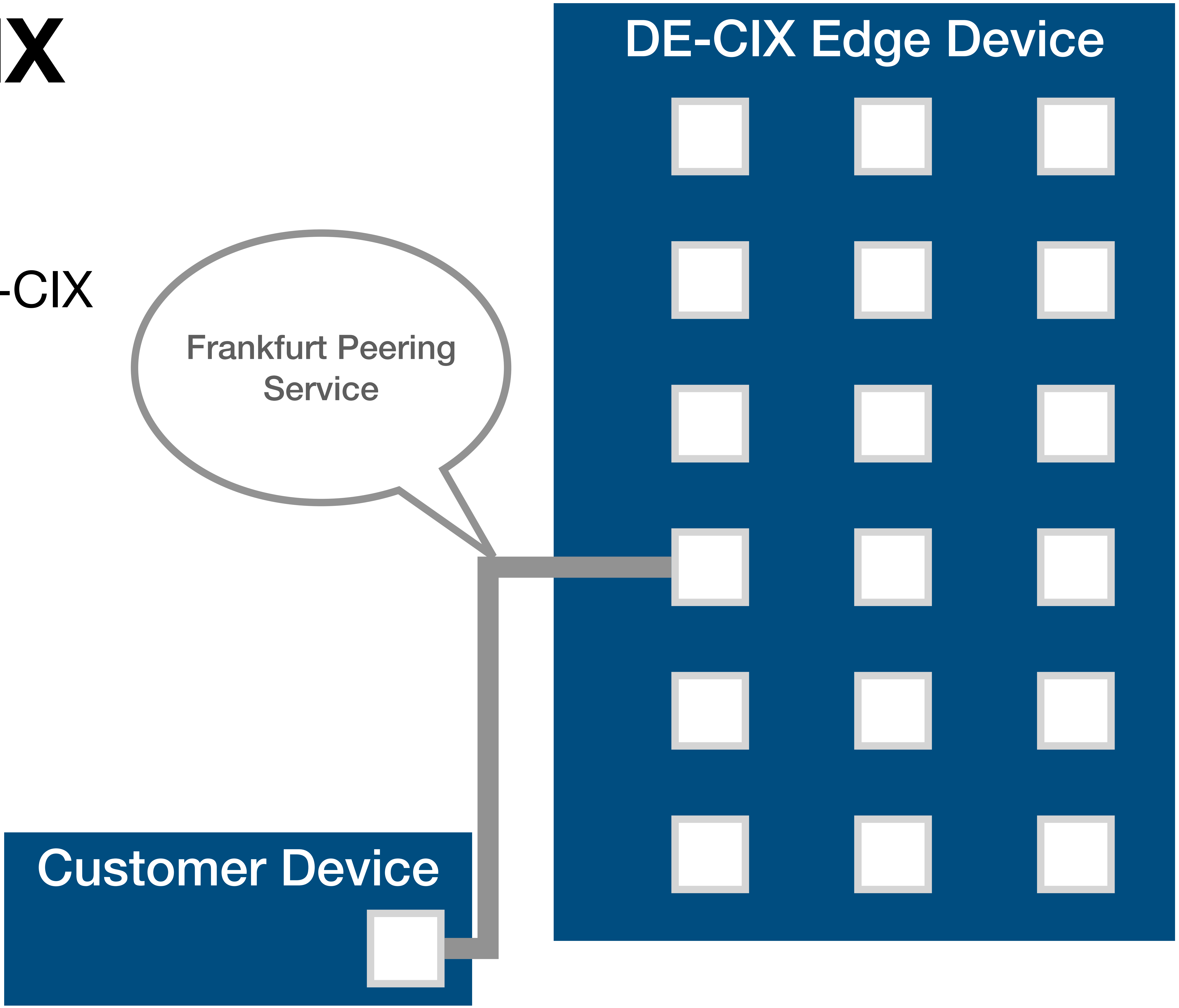
- VLANs can deliver multiple LANs on one trunked port
- Each tagged with a different VLAN ID
- Like we used to separate "Home" and "Guest" network



VLANs at DE-CIX

How we use them

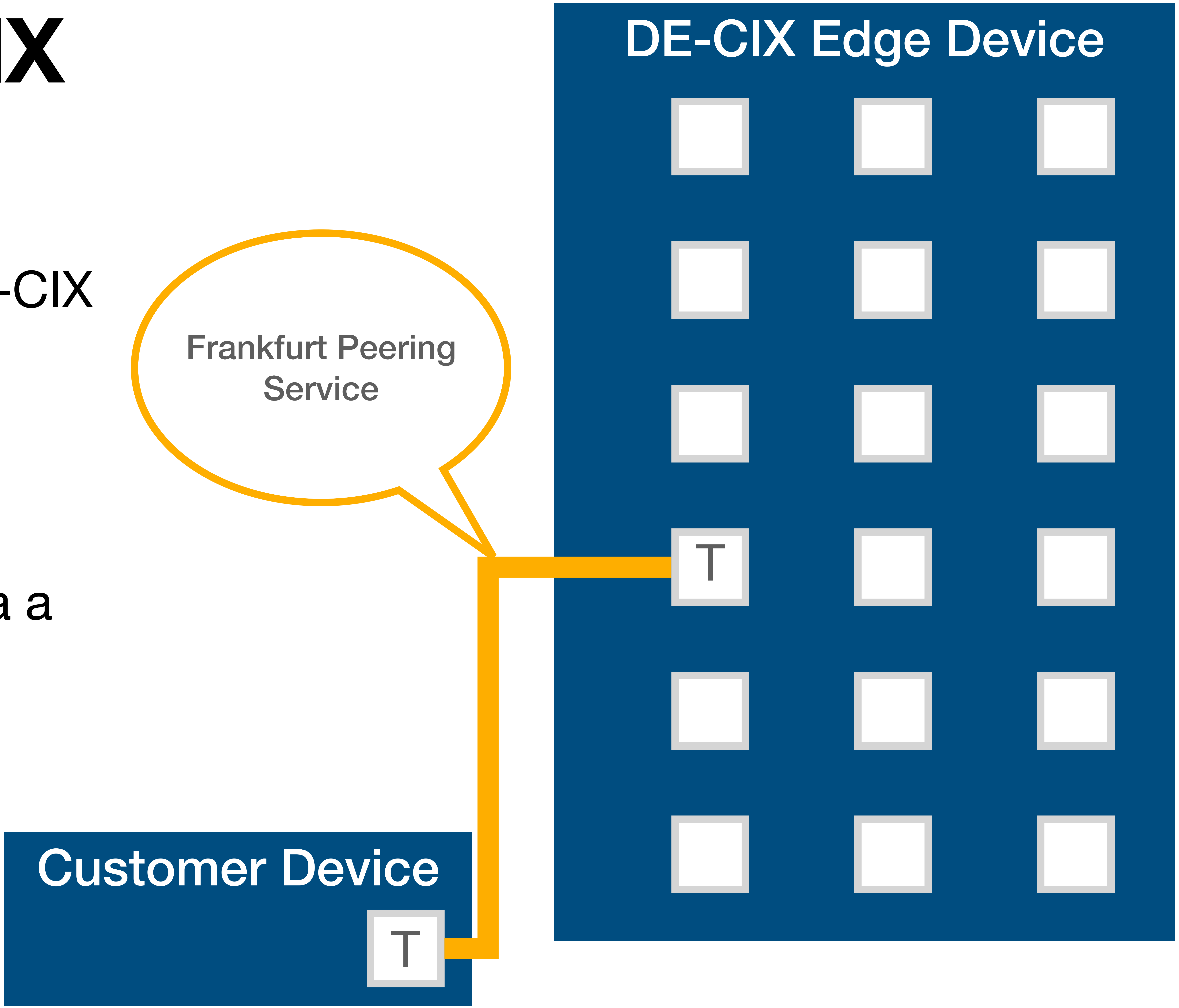
- Customers connect to DE-CIX via Ethernet
- Standard connection is a untagged access port



VLANs at DE-CIX

How we use them

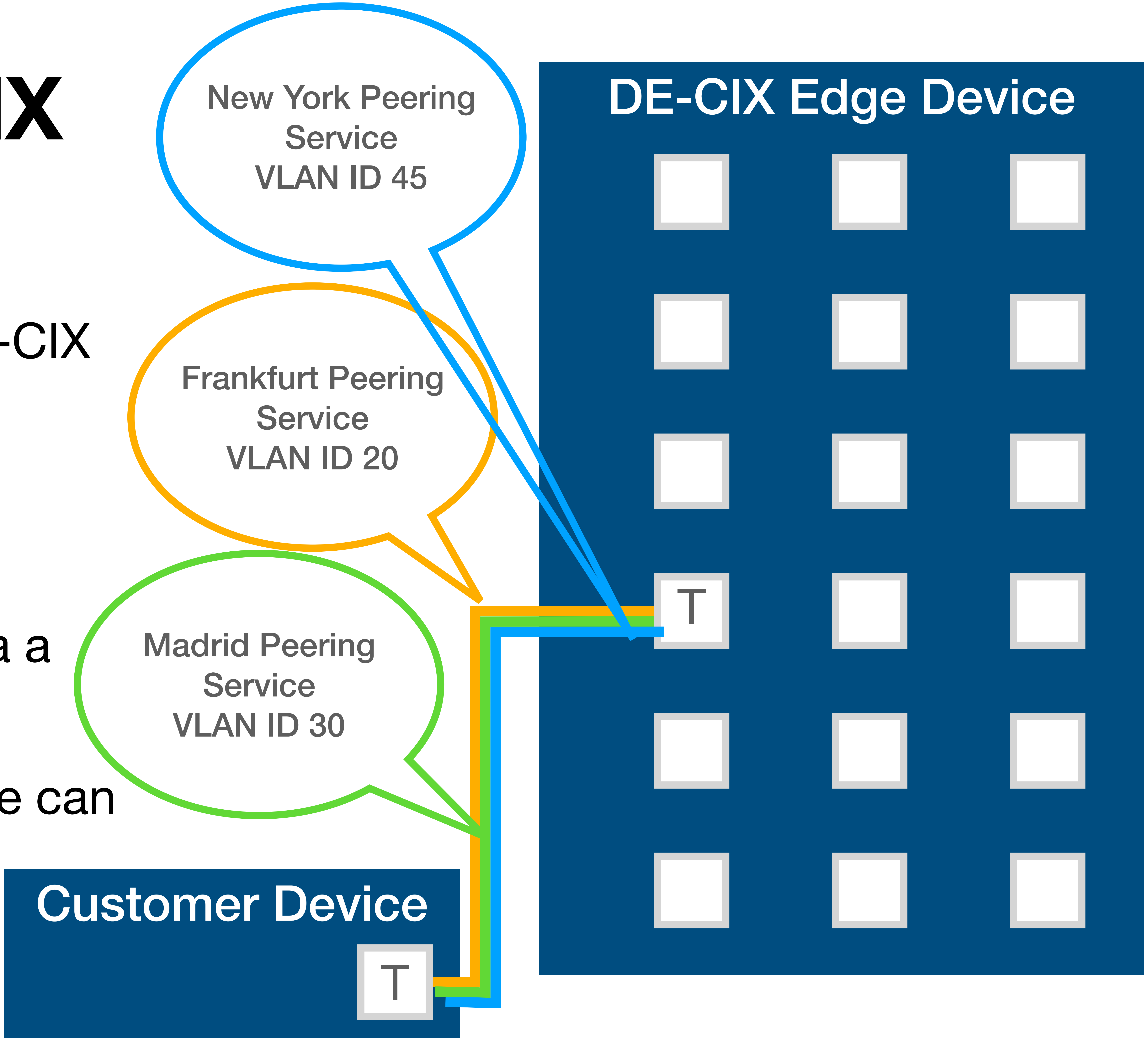
- Customers connect to DE-CIX via Ethernet
- Standard connection is a untagged access port
- But we can also deliver via a tagged trunk-like port



VLANs at DE-CIX

How we use them

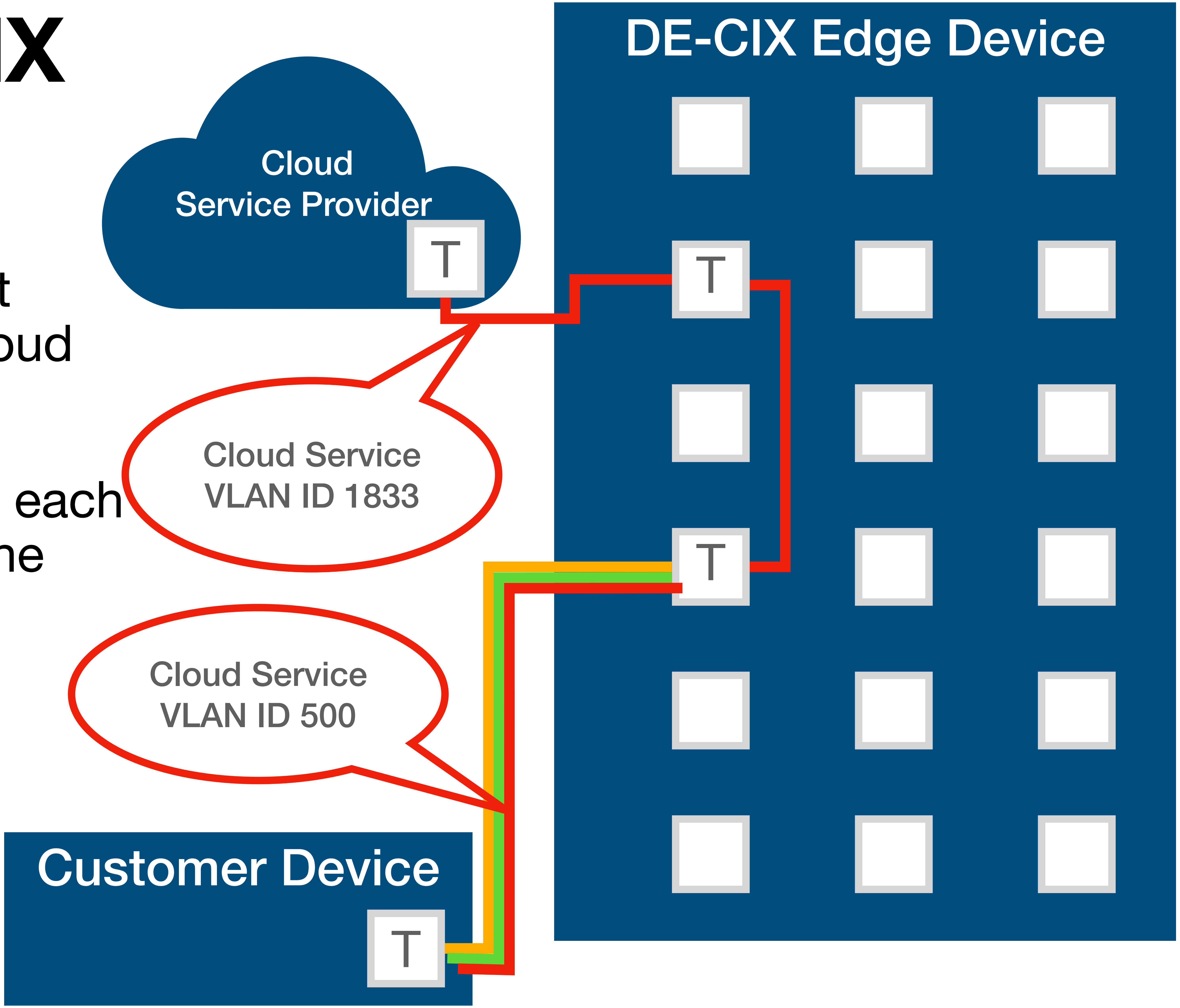
- Customers connect to DE-CIX via Ethernet
- Standard connection is a untagged access port
- But we can also deliver via a tagged trunk-like port
- And on a trunk-like port we can deliver multiple services



VLANs at DE-CIX

Connect to the Cloud

- The same way we connect customers to (multiple) Cloud service providers
- At DE-CIX the VLAN ID on each end does not have to be the same!



Conclusion

Please remember....

Facts about VLANs

- Ethernet is a **broadcast** network
- VLANs set up **virtual LANs** on a **common physical infrastructure**
- VLAN **IDs** run from 1 - 4094
    - It is recommended to **not use VLAN 1** (if possible)
- DE-CIX uses VLANs for multiple service delivery on one physical port

DE-CIX

Networking Basics

03 - The Internet Protocol (IP)

DENOG 13
GERMAN NETWORK OPERATORS GROUP

Wolfgang Tremmel
academy@de-cix.net

DE CIX
Where networks meet

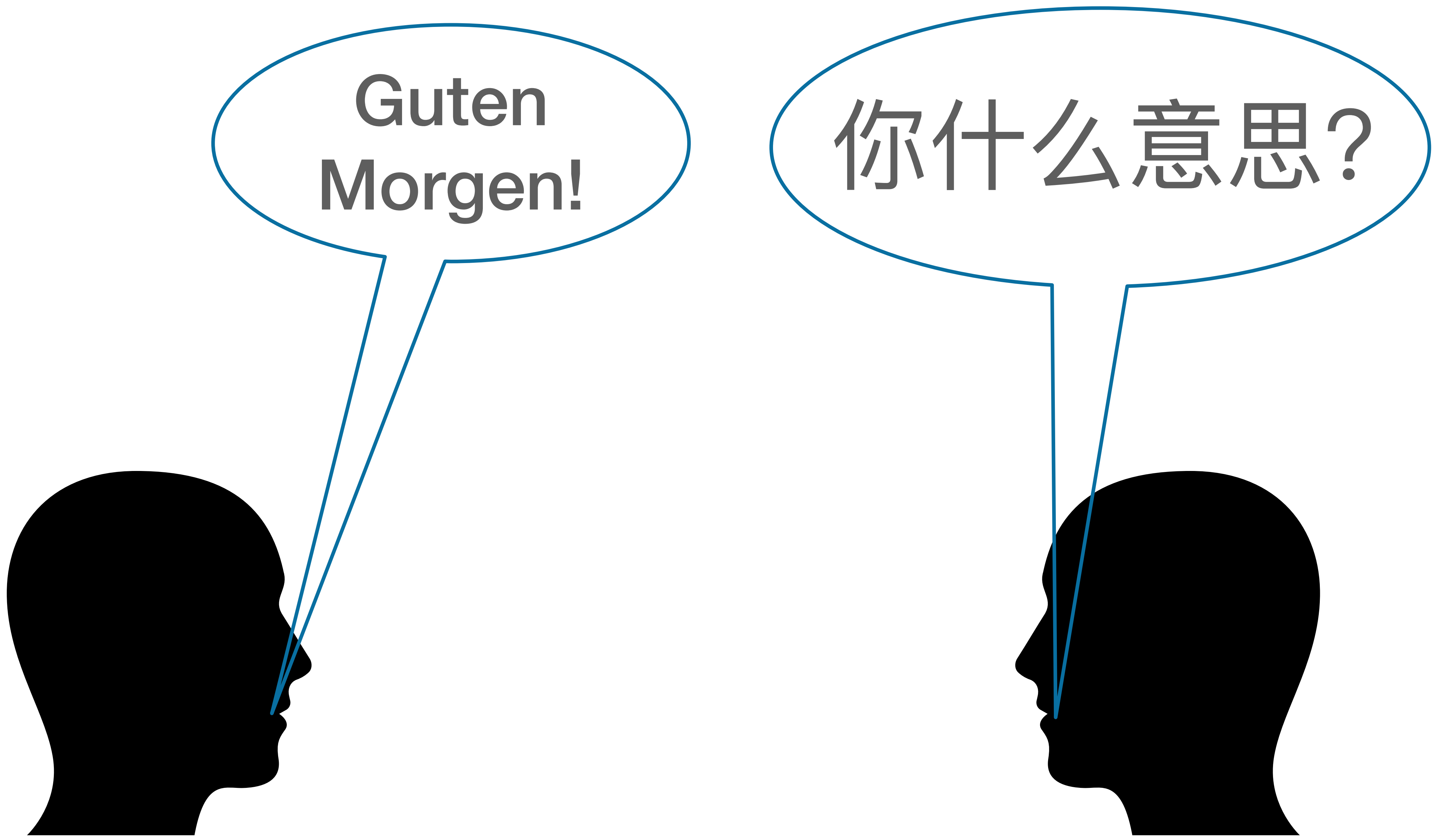
DE-CIX Management GmbH | Lindleystr. 12 | 60314 Frankfurt | Germany
Phone + 49 69 1730 902 0 | sales@de-cix.net | www.de-cix.net

Networking Basics
DE-CIX Academy

Protocol

What is a "Protocol"?

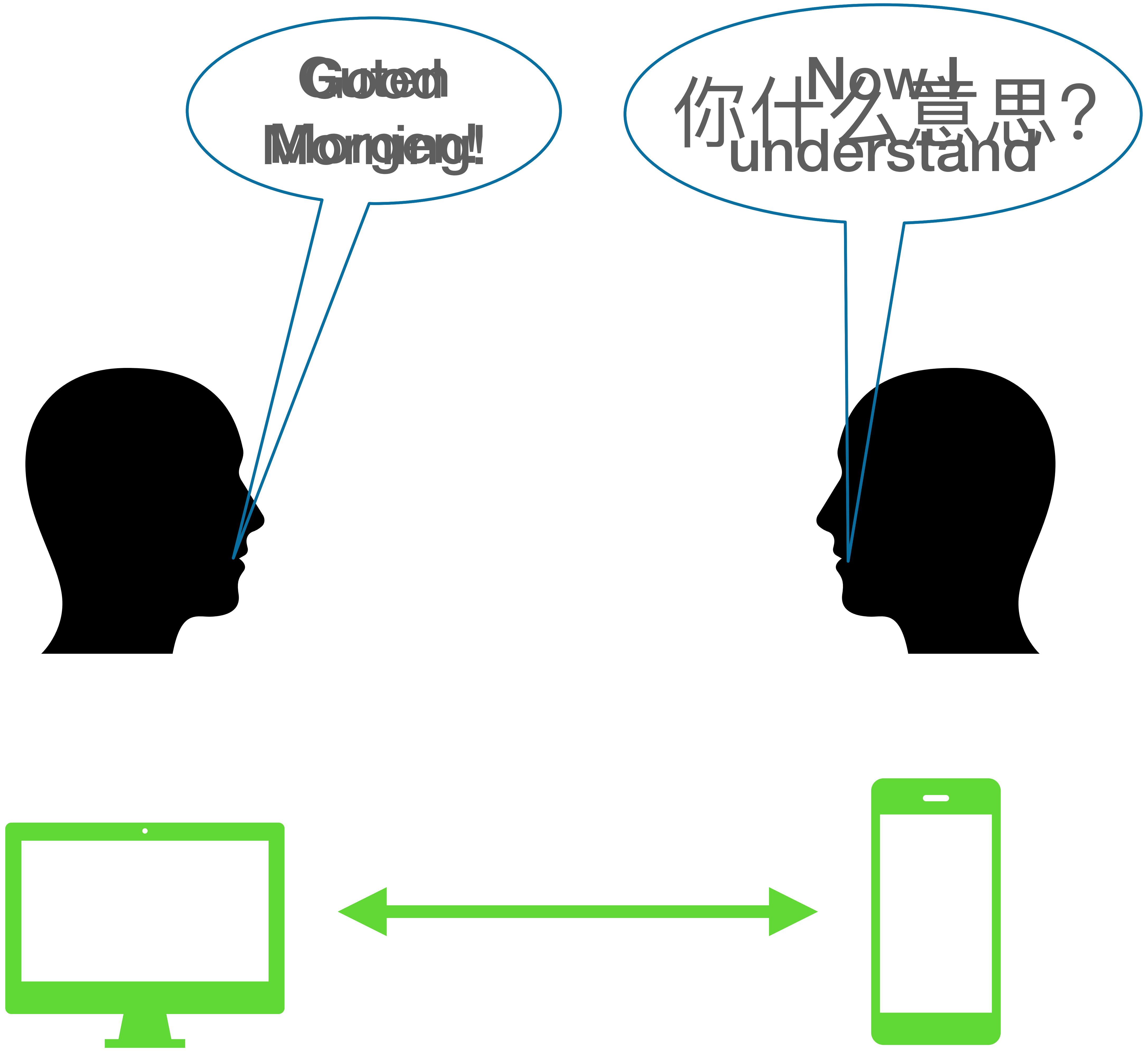
- If you want to communicate, you need to speak a common language
- Otherwise you will not understand each other



PS: I used Google Translate. Hope it says "I do not understand"

What is a "Protocol"?

- If you want to communicate, you need to speak a common language
- Otherwise you will not understand each other
- The same is true for computers or other network devices



Protocol Stack

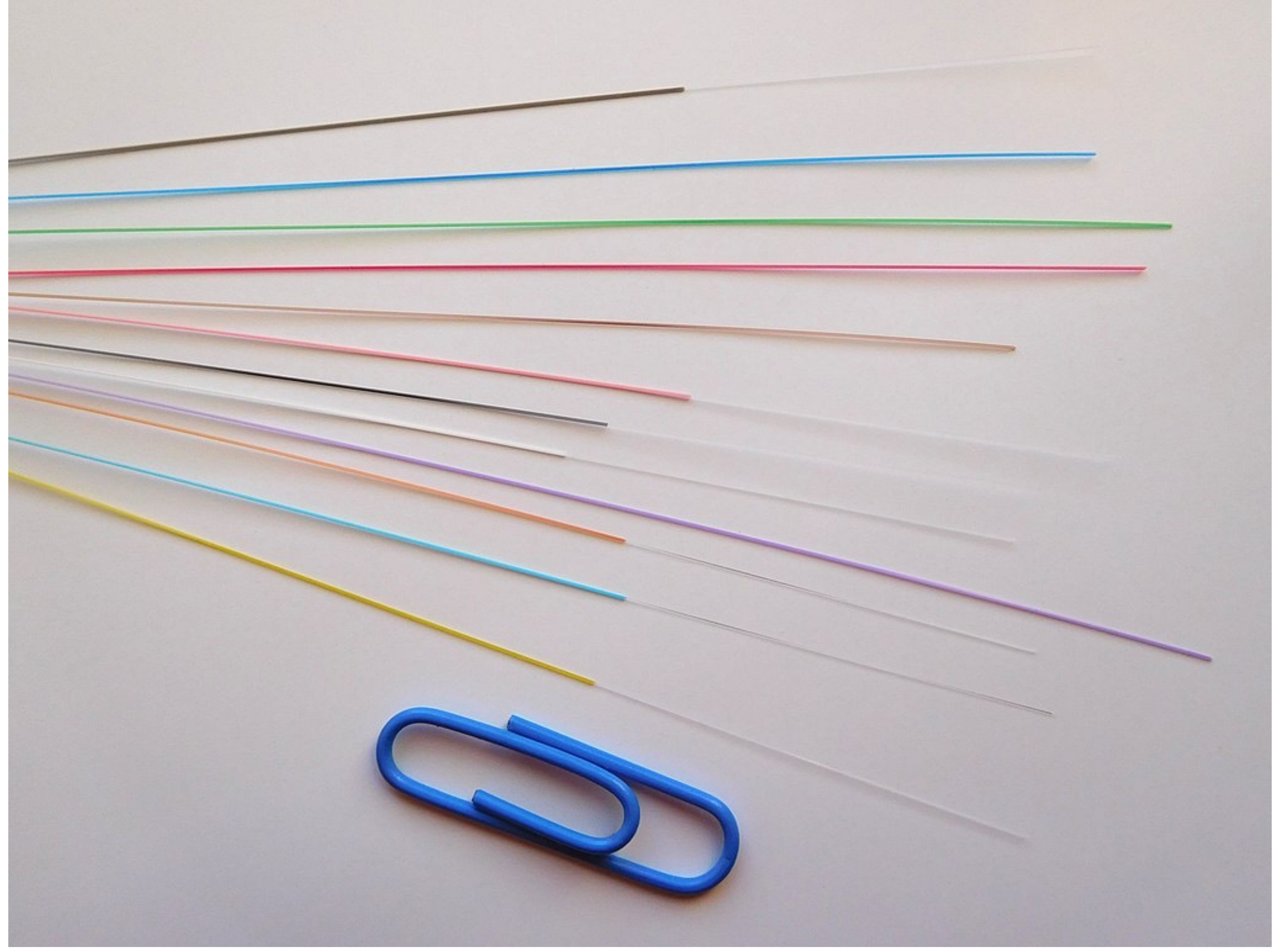
Multiple protcols building on each other

Internet Model

Physical Layer

- Light pulses and electrical signals
- Lasers and fibres
- Electrical cables

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical



Attribution: Cjp24
https://commons.wikimedia.org/wiki/File:12_Optical_fibers_(1).jpg

DE CIX

Internet Model

Link Layer

- Data units are called "Frames"
- Provides hop-to-hop (node-to-node) data transfer
- Examples:
    - Ethernet

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

Attribution: Wolfgang Tremmel

Ethernet

Frame Structure

- EtherType
- Payload

Preamble				SFD	Destination MAC Address	Source MAC Address	Ethertype	Payload	Checksum
10101010	10101010	10101010	10101010	10101011	48 Bits 6 Octets	48 Bits 6 Octets	16 Bits 2 Octets	46 - 1500 Octets	32 Bits 4 Octets

Ethernet

Frame Structure

	Ethertype		Payload		Checksum
	16 Bits 2 Octets		46 - 1500 Octets		32 Bits 4 Octets

Encapsulation

Packets inside packets

- The payload of Ethernet is IP
- Encapsulation is like Russian dolls
- So we have an IP packet inside an Ethernet frame

Attribution: Fanghong. derivative work: Greyhood
https://commons.wikimedia.org/wiki/File:Matryoshka_transparent.png

Internet Model

IP / Internet Layer

- Data units are called "Packets"
- Provides source to destination (end-to-end) transport
- Needs addresses for entities
- Examples:
  - IPv4
  - IPv6

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

DE CIX

IP - Version 4 (IPv4)

Header + Payload

Ethernet Payload	
IPv4 Header	**IP Payload**
20-60 Bytes	1440-1480 Bytes

IPv4 Header

Some parts to point out

- Starts with version and length
- Total length of packet
- Important: Time to live (TTL)
- Protocol: Type of payload
- Source / Destination address 32 bits
- Options (optional)

<table>
<tr><th>Byte</th><th>0</th><th>1</th><th>2</th><th>3</th></tr>
<tr><td>0</td><td>Version | Header Length
always 4 | 5..15</td><td>DSCP / ECN</td><td colspan="2">Total Length
20..65535</td></tr>
<tr><td>4</td><td colspan="2">Identification</td><td colspan="2">Flags / Fragment Offset</td></tr>
<tr><td>8</td><td>Time To Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td>12</td><td colspan="4">Source IPv4 Address</td></tr>
<tr><td>16</td><td colspan="4">Destination IPv4 Address</td></tr>
<tr><td>20
24
28
32</td><td colspan="4">Optional (if HeaderLength > 5)</td></tr>
</table>

IP - Version 6 (IPv6)

Header + Payload

Ethernet Payload	
IPv6 Fixed*) Header	**IP Payload**
40 Bytes	1460 Bytes

*) IPv6 packets can contain "extension headers" after the fixed header

IPv6 Header

Looks less complicated!

- Starts with version and some labels
- Payload length in bytes (0-65535)
- Next Header - you can chain more headers
    - replaces protocol field
- Hop Limit replaces TTL
- Addresses are now 128bits

Byte	0	1	2	3
0	Version = 6 / Traffic Class / Flow Label			
4	Payload Length in bytes		Next Header	Hop Limit
8	Source IPv6 Address			
12				
16				
20				
24	Destination IPv6 Address			
28				
32				
36				

IP Addresses - IPv4

IP Addresses

IPv4

192.0.2.123

- 32 bit in length
- you might have heard of Class-~~A~~, -~~B~~, -~~C~~ addresses
- there is no such thing anymore!
    - since 1993!
- all usable IP addresses are equal
- more about this in another webinar

1100	0000	0000	0000	0000	0010	0111	1011
1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24	25 25 27 28	29 30 31 32

DE CIX

IP Addresses
IPv4

192.0.2.123

- 32 bit in length
  - 4.294.967.296 possible addresses
- written as 4 decimal numbers separated by dots "."
- some addresses are reserved / not usable
- all usable IPv4 addresses have been assigned to users

1100	0000	0000	0000	0000	0010	0111	1011
1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20	21 22 23 24	25 25 27 28	29 30 31 32

IPv6!

Development started: 1994
First published: 1995

DE CIX

IP Addresses - IPv6

IP Addresses

IPv6

2001:db8:274f:400:226:b0ff:fed8:3d8a

0 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f

- 128 bit in length - possible addresses:
  340282366920938463463374607431768211456
- there are lots of IPv6 addresses available
- written as hexadecimal numbers separated by colons ":"
  - double-colon "::" means fill up with zeros here
- some addresses are reserved / not usable

2001:db8::1

2001:db8:0:0:0:0:0:1

2001:0db8:0000:0000:0000:0000:0000:1

DE CIX

Internet Protocol

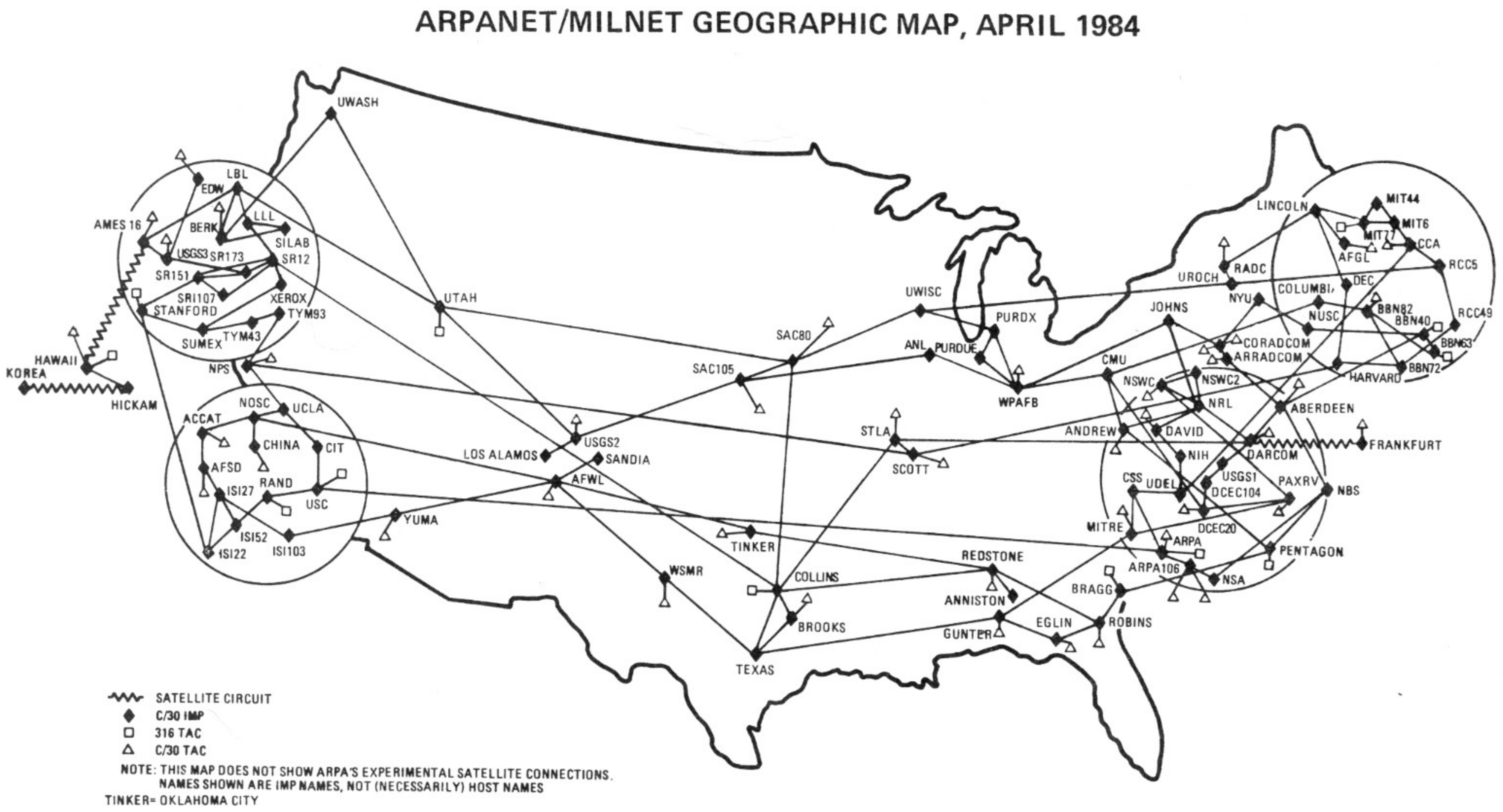
How did it all start?

DE CIX

History of IP

It started in the 60s

- To debunk a myth:
    - It was not invented to survive a nuclear war!
- But it was funded by DARPA - a military research agency
- To connect research facilities to share (computing) resources

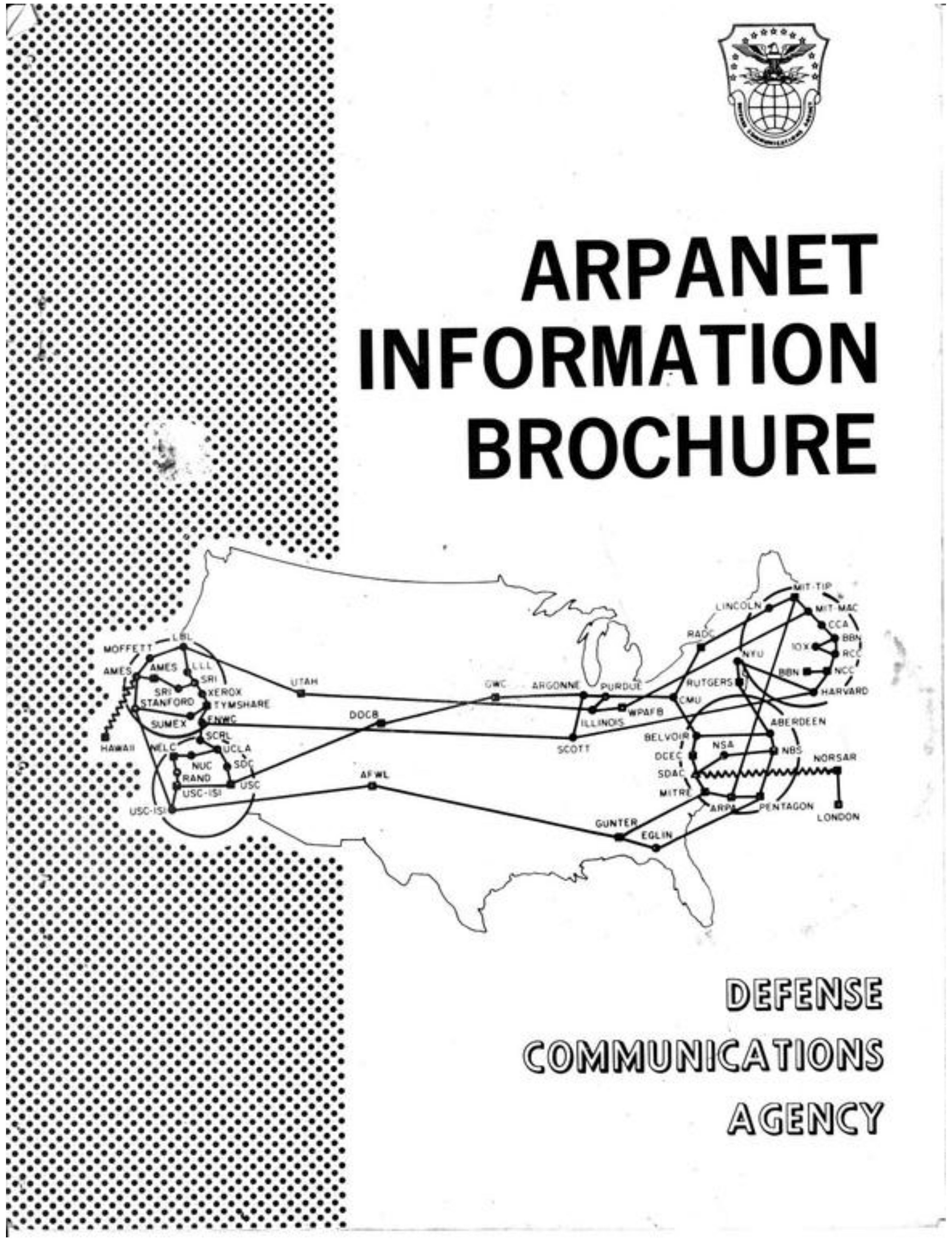


Attribution: Public Domain
https://commons.wikimedia.org/wiki/File:ARPANET_-_MILNT_Diagram_1984.jpg

Timeline

Some days in the early history of IP

- 1961 - concept of packet switching network
- 1967 - Plan for "ARPAnet"
- 1969 - first ARPAnet node, first **RFC** published
- 1972 - first public demonstration of ARPAnet
- 1974 - TCP/IP protocol described, "Internet" first used
- 1983 - ARPAnet switches from NCP to TCP/IP

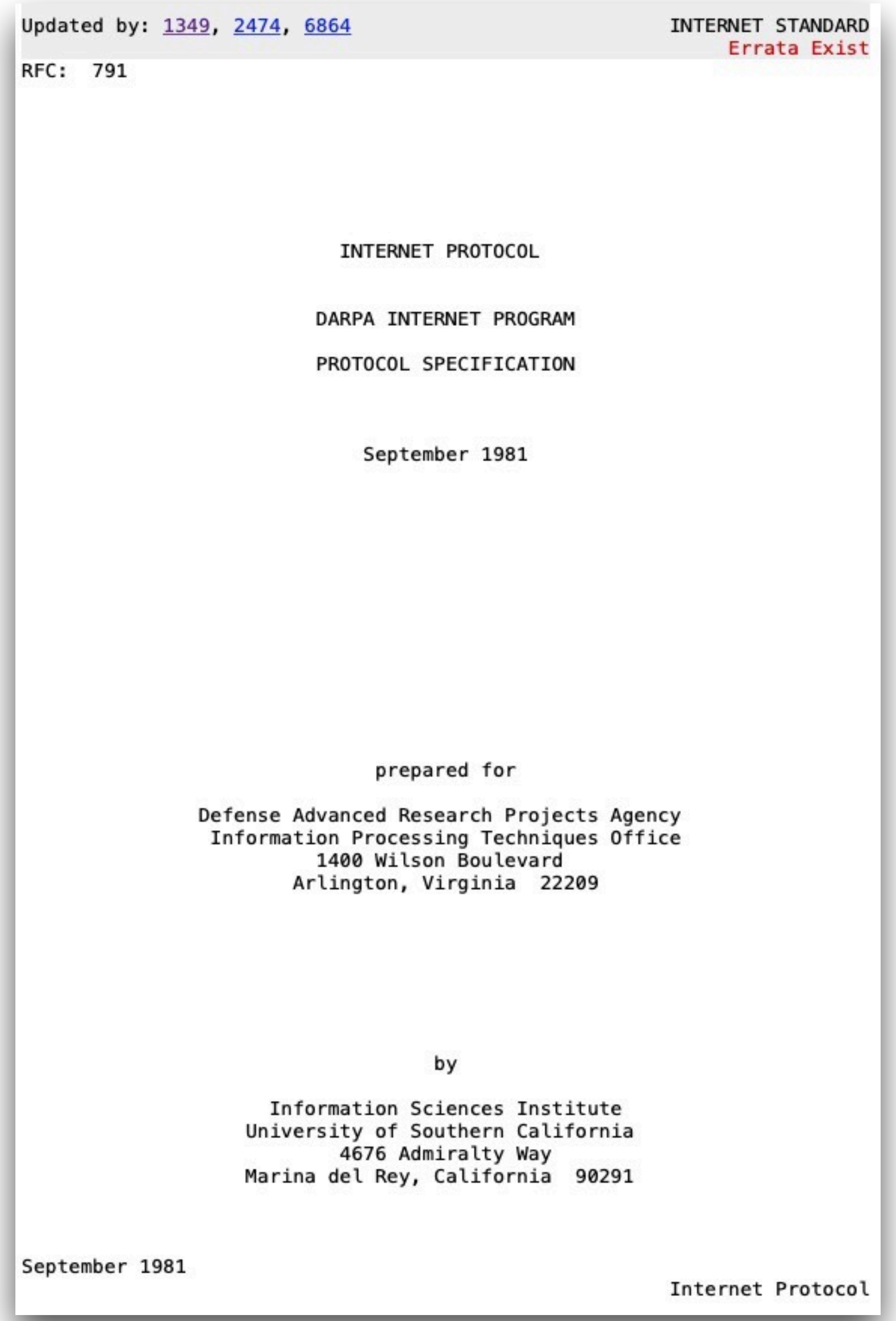


Attribution: Public Domain
https://commons.wikimedia.org/wiki/File:ARPANET_Info_Brochure.pdf

Why was IP so successful?

The role of documentation

- There were other, competing protocols
  - Do you remember BITnet, DECnet? OSI?
  - Either vendor-proprietary or just theory
- IP Protocols were evolving more quickly
- Everything was open - and still is
  - 1969 - first Request for comments (**RFC**) published
  - Memos, best practices, standards - published as RFC
  - Today: Well established and open standard for publishing



Updated by: 1349, 2474, 6864 INTERNET STANDARD
Errata Exist
RFC: 791

INTERNET PROTOCOL

DARPA INTERNET PROGRAM

PROTOCOL SPECIFICATION

September 1981

prepared for

Defense Advanced Research Projects Agency
Information Processing Techniques Office
1400 Wilson Boulevard
Arlington, Virginia 22209

by

Information Sciences Institute
University of Southern California
4676 Admiralty Way
Marina del Rey, California 90291

September 1981 Internet Protocol

Attribution: Public Domain
https://commons.wikimedia.org/wiki/File:ARPANET_-_MILNT_Diagram_1984.jpg

DE CIX

Conclusion

Things you should remember

The IP Protocol(s)

- Internet Protocol (IP) takes care of **end-to-end** communication
- **IPv4** and **IPv6** coexist
- IP packets consist of **header** and **payload**
- **IPv4** and **IPv6** headers are different
  - But both contain source- and destination **addresses**
  - IPv4 addresses are 32 bit long, IPv6 addresses are 128 bit long
- **Payload** can yet be **another protocol**

Networking Basics

03a - IP: Addresses, Prefixes and Routing

Wolfgang Tremmel
academy@de-cix.net

13

DENOG

GERMAN NETWORK OPERATORS GROUP

Networking Basics
DE-CIX Academy

IP - the Internet Protocol

Internet Model

IP / Internet Layer

- Data units are called "Packets"
- Provides source to destination (**end-to-end**) transport
- Needs **addresses** for entities

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

DE CIX

IPv4 Addresses

32 bit long

- 32 bit in length
  - 4.294.967.296 possible addresses
- written as 4 decimal numbers separated by dots "."
- some addresses are reserved / not usable
- all usable IPv4 addresses have been assigned to users

192.0.2.123

1100 0000 0000 0000 0000 0010 0111 1011

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 25 27 28 29 30 31 32

IPv6

Development started: 1994
First published: 1995

IPv6 Addresses

128 bit long

- 128 bit in length - possible addresses: 340282366920938463463374607431768211456
- there are lots of IPv6 addresses available
- written as hexadecimal numbers separated by colons ":"
  - double-colon "::" means fill up with zeros here
- some addresses are reserved / not usable

2001:db8:0:0:0:0:0:1

2001:db8::1

2001:0db8:0000:0000:0000:0000:0000:1

Internet Model

IP / Internet Layer

- Data units are called "Packets"
- Needs **addresses** for entities
- Provides source to destination transport
    - End-to-End Transport

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

End-to-End Transport

DE CIX

DE CIX

DE CIX

DE CIX

DE CIX

Routing

Intermission: Language

Routing

"A method of finding paths from origins to destinations in a network such as the Internet, along which information can be passed."

https://en.wiktionary.org/wiki/routing

UK	/ˈɹuːtɪŋ/
US	/ˈɹutɪŋ/
	/ˈɹaʊtɪŋ/

DE CIX

Routing

"A method of finding paths from origins to destinations in a network such as the Internet, along which information can be passed."

https://en.wiktionary.org/wiki/routing

routing /ˈɹaʊtɪŋ/

root

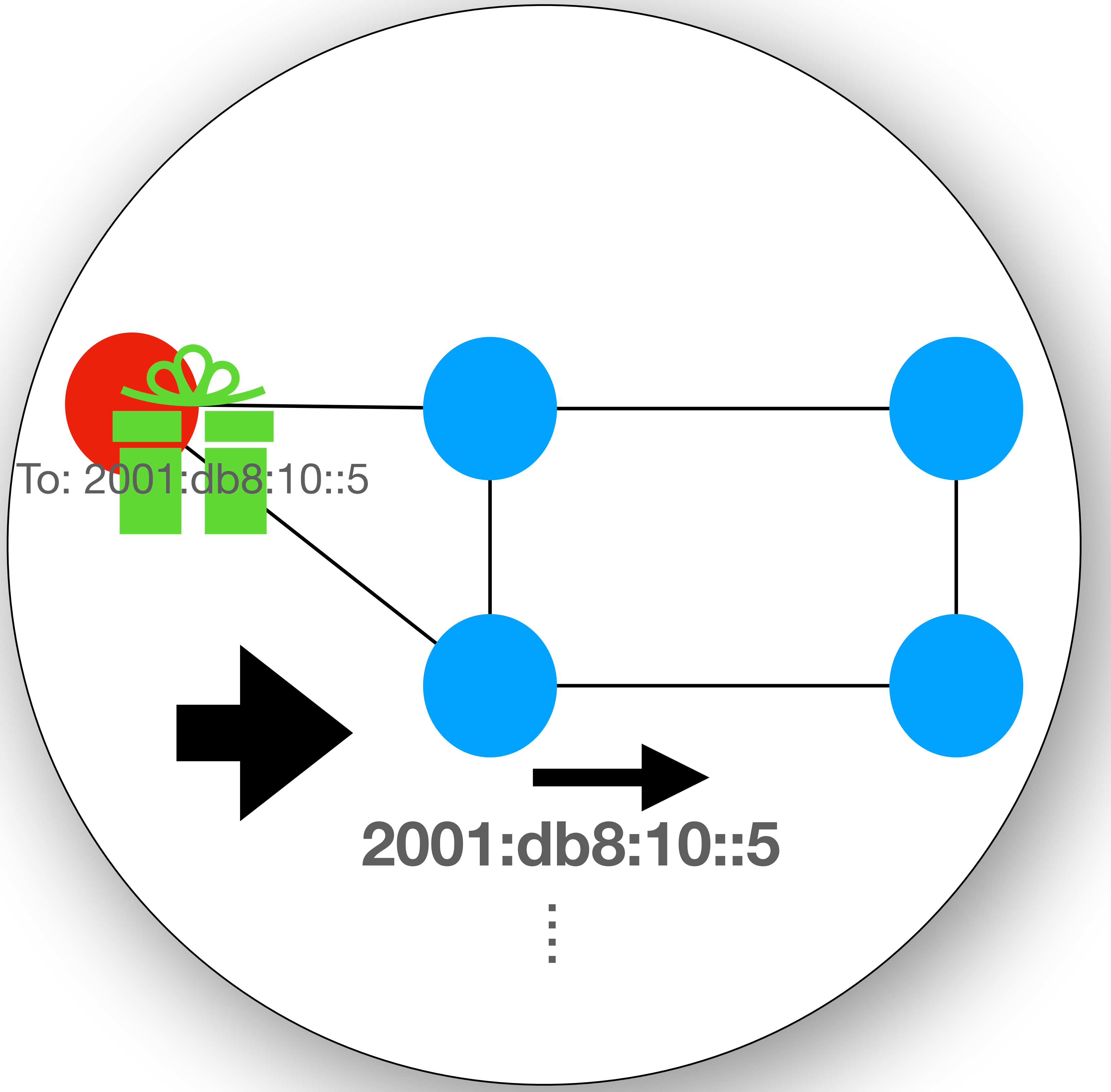
rooting "A hole formed by a pig when it roots in the ground"

https://en.wiktionary.org/wiki/rooting

Routing

How a *router* works

- All IP packets have a *destination IP address*
- Depending on the destination IP address a *next hop* is chosen
- For this, each router has a large lookup-table
    - This is called the *routing table*
- It contains not single IP addresses, but *Prefixes*



IP Prefixes

IPv6 - Addresses

2003:de:274f:400:226:b0ff:fed8:3d8a

DE CIX

IPv6 - Addresses

IPv6 - Prefixes

2003:de:274f:400:226:b0ff:fed8:3d8a

/64

00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f

Notation:

- 4 digit hex numbers (0-9,a-f)
- Separated by ":"
- "::" = fill up with zeros

128 Bits long

IPv6 - Prefixes

Prefix-Length: 0-128

2003:de:274f:400::/64

0 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 4 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f

__Notation__:

- 4 digit hex numbers (0-9,a-f)
- Separated by ":"
- "::" = fill up with zeros

Host-part all zero

128 Bits long

IPv4 - Addresses

10.3.8.17

DE CIX

IPv4 - Addresses

10.3.8.0/22

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 25 27 28 29 30 31 32

Notation:

- 4 numbers (0-255)
- Separated by "."

32 Bits long

IPv4 - Prefixes

Prefix-Length: 0-32

10.3.8.0/22

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 25 27 28 29 30 31 32

Host-part all zero

32 Bits long

<u>Notation</u>:

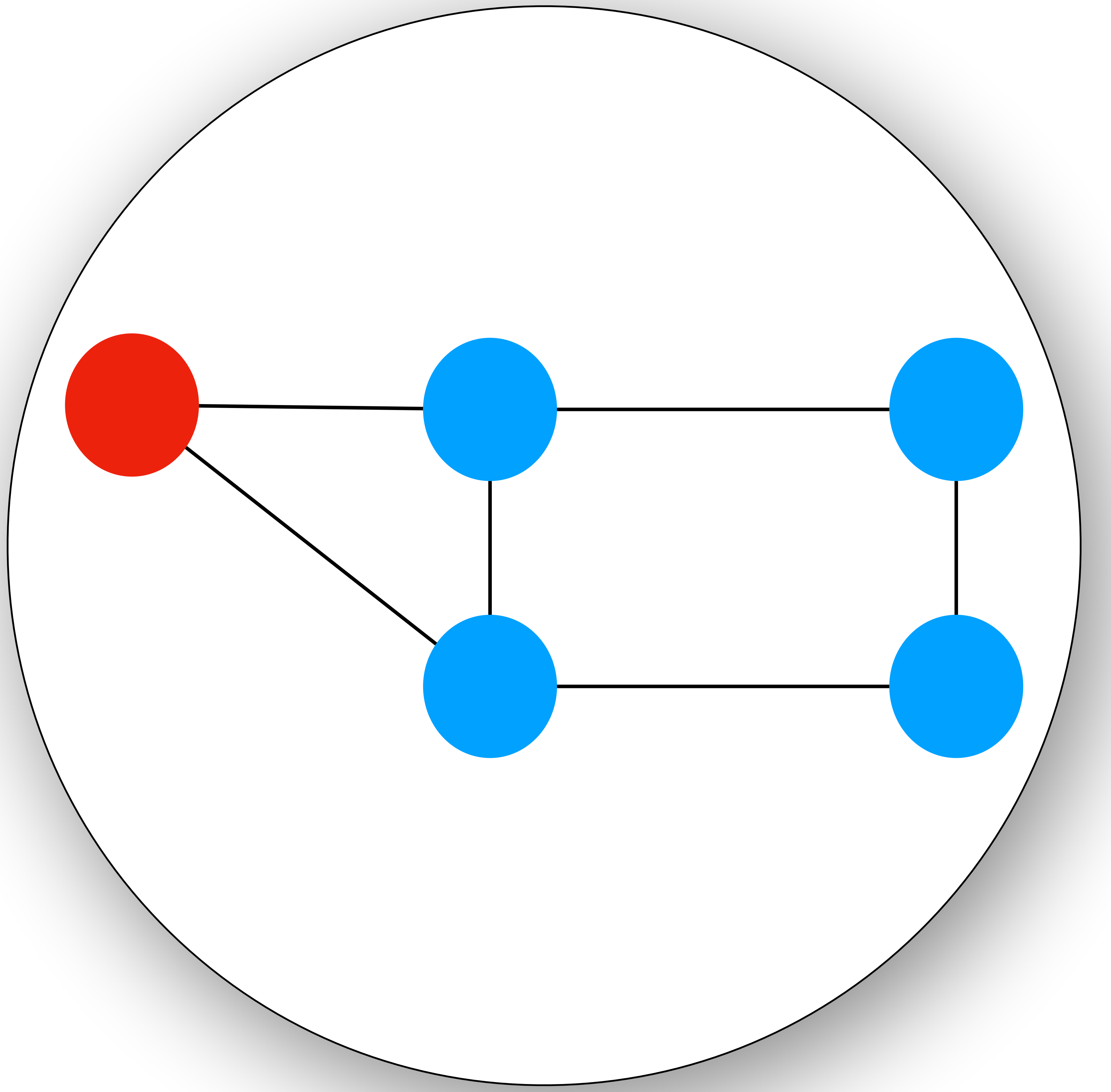
- 4 numbers (0-255)
- Separated by "."

IP Addresses and Prefixes

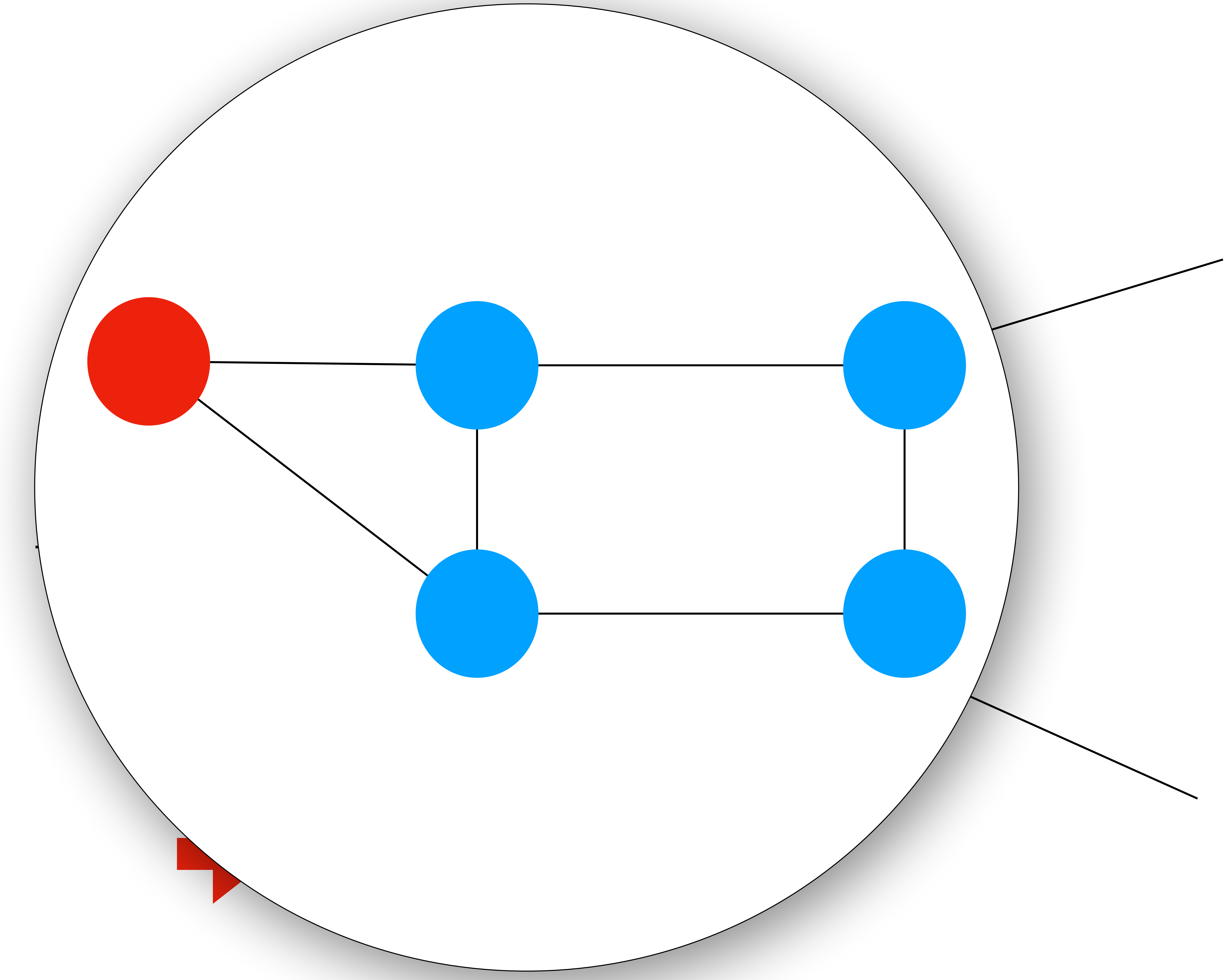
Prefix or not?

	IPv4	IPv6
Length	32 Bit	128 Bit
	0-32 Prefix Length	0-128 Prefix Length
Notation	4 Numbers, 0-255	8 Numbers, 0-fffff
Separator	.	:
Prefix: Host part	all zero	
Address: Host part	**not** all zero / **not** all one	
Example (Prefix)	198.51.100.0/24	2001:db8:4f30::/48

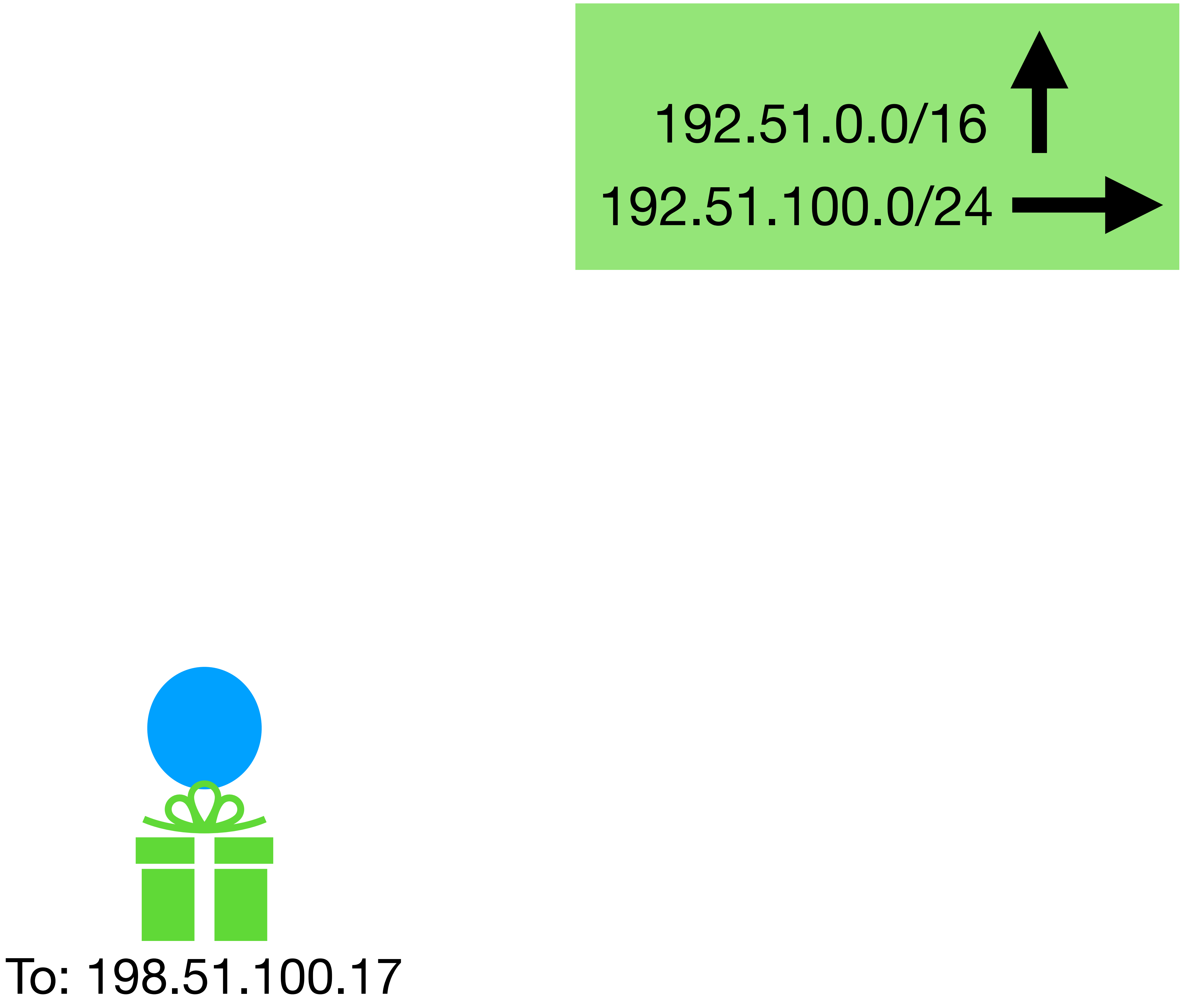
IP Routing



IP Routing



IP Routing



IP Routing

To: 198.51.100.17

Prefix	Destination
198.51.0.0/16	↘
44.0.0.0/8	↙
198.51.100.0/24	←
203.0.113.0/24	→
192.0.2.0/24	↑

IP Routing

To: 198.51.100.17

Prefix	Destination
192.0.2.0/24	↑
198.51.100.0/24	←
203.0.113.0/24	→
198.51.0.0/16	↘
44.0.0.0/8	↙

IP Routing

To: 198.51.100.17

Apply the netmask: /24

/24 = 24 bits in network part
11111111 11111111 11111111 00000000

255.255.255.0
"bitwise logical and" with IP address

198.051.100.017
255.255.255.000
=
198.051.100.000 ≠

Prefix	Destination
192.0.2.0/24 192.000.002.000	↑
198.51.100.0/24	←
203.0.113.0/24	→
198.51.0.0/16	↘
44.0.0.0/8	↙

DE CIX

IP Routing

To: 198.51.100.17

Apply the netmask: /24

/24 = 24 bits in network part
11111111 11111111 11111111 00000000

255.255.255.0
"bitwise logical and" with IP address

198.051.100.017
255.255.255.000
=
198.051.100.000 =

Prefix	Destination
192.0.2.0/24	↑
198.51.100.0/24	←
203.0.113.0/24	→
198.51.0.0/16	↘
44.0.0.0/8	↙

IP Routing

- You now know how routing works
  - The router has a routing table with IP prefixes
  - The destination address is used to select a best matching prefix
  - The routing table tells the router the "next hop"

But how does the information get into the routing table?

DE CIX

IP Routing

But how does the information get into the routing table?

- Someone types it in
  - This is called "*static routing*"
  - Simple, often used, but does not scale
- Routers "talk" to each other
  - This is called "*dynamic routing*"
  - And the *protocols* used are called "*routing protocols*"
  - Examples of such protocols are **BGP**, OSPF, IS-IS, RIP, EIGRP

Conclusion

Conclusion

We introduced a lot of new terms in this webinar

- "Routing"
  - "A method of finding paths from origins to destinations in a network such as the Internet, along which information can be passed." https://en.wiktionary.org/wiki/routing
- "Router"
  - A device which routes
- "IP Prefix"
  - A network address and a prefix length
- "Routing Table"
  - A table of IP prefixes and a next hop addresses

DENOG

GERMAN NETWORK OPERATORS GROUP

Networking Basics

03b - Global IP routing

Wolfgang Tremmel
academy@de-cix.net

DE CIX

Where networks meet

Networking Basics
DE-CIX Academy

01 - Networks, Packets, and Protocols
02 - Ethernet
  02a - Ethernet + VLANs
03 - The Internet Protocol (IP)
  03a - IP addresses, prefixes, and routing
  03b - Global IP routing
04a - UDP
04b - TCP
04c - ICMP
05 - Unicast, Broadcast, Multicast, Anycast

IP - the Internet Protocol

Internet Model

IP / Internet Layer

- Data units are called "Packets"
- Provides source to destination (**end-to-end**) transport
- Needs **addresses** for entities

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

DE CIX

IPv6 - Prefixes

Prefix-Length: 0-128

2003:de:274f:400::/64

0 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 4 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f

Host-part all zero

128 Bits long

<u>Notation</u>:

- 4 digit hex numbers (0-9,a-f)
- Separated by ":"
- "::" = fill up with zeros

D

IPv4 - Prefixes

Prefix-Length: 0-32

10.3.8.0/22

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 25 27 28 29 30 31 32

Host-part all zero

32 Bits long

Notation:

- 4 numbers (0-255)
- Separated by "."

DE CIX

DE CIX

DE CIX

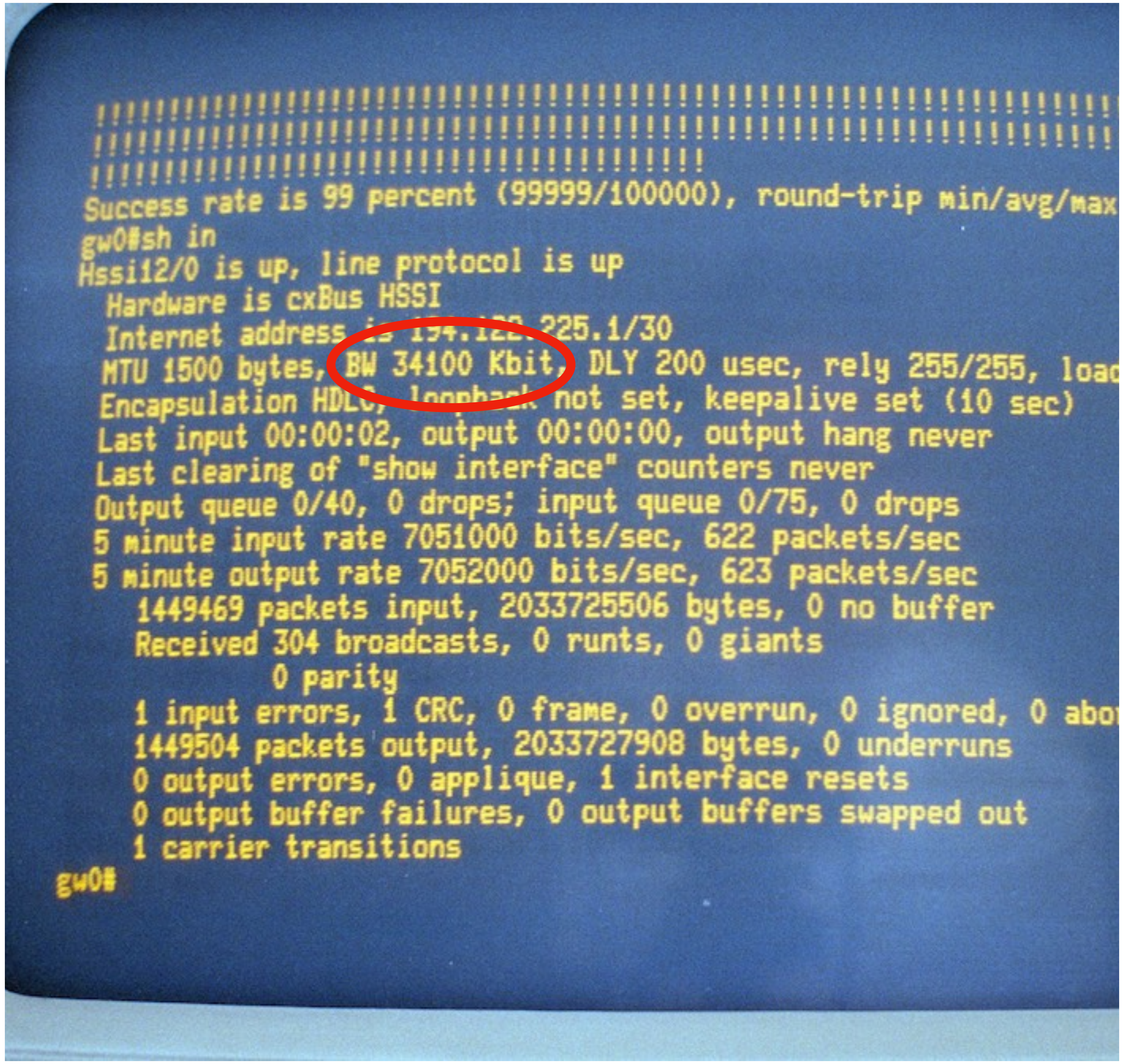

Autonomous
System
AS64500
192.0.2.0/24
198.51.100.0/24
2001:db8::/32

How did it start?

Internet in the 1990s

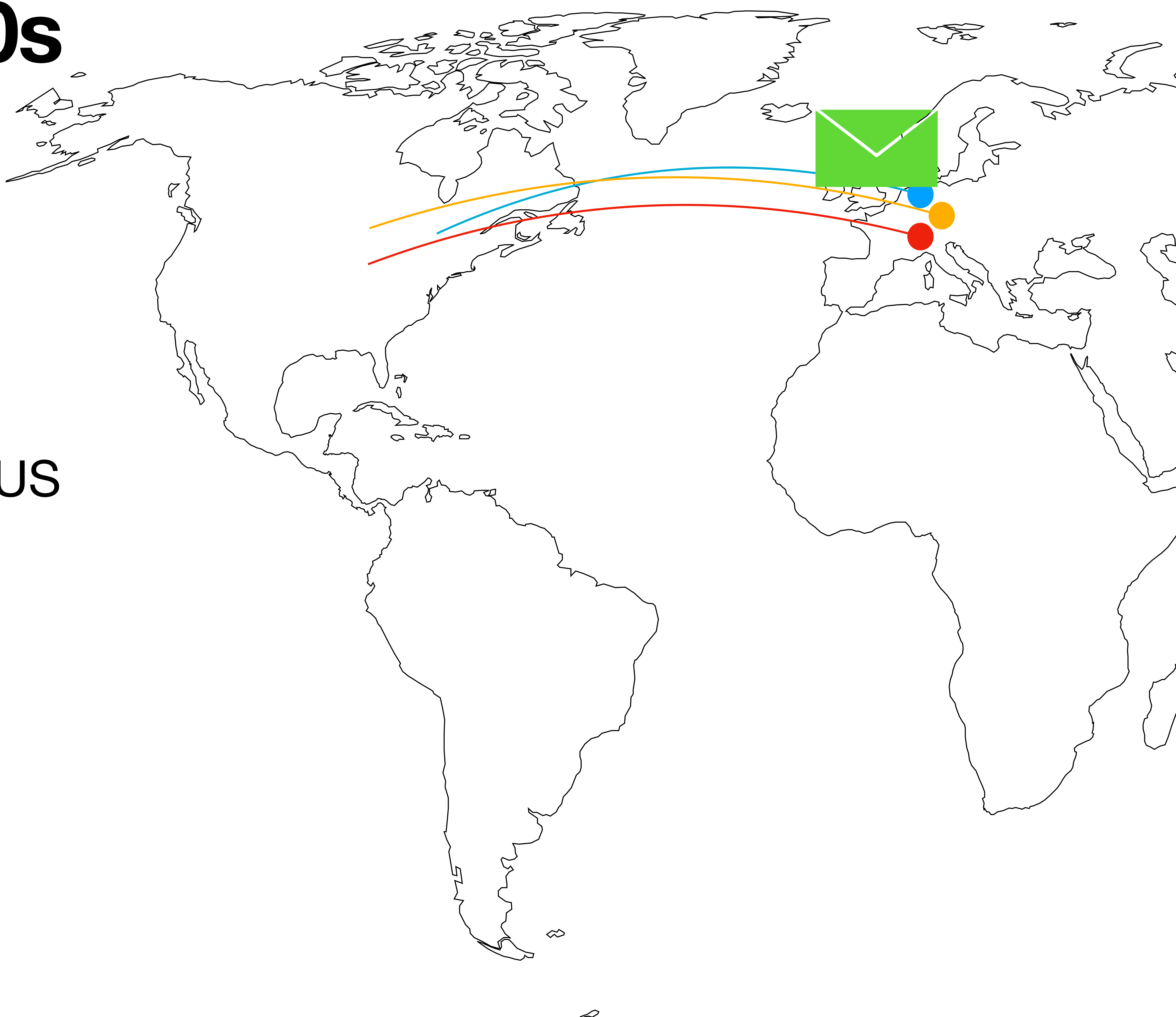
Also some personal history

- 2Mbit/s was a "fast connection"
- Backbone networks were 34Mbit/s
- End customers connected via ISDN (modern) or telephone modems
- Standard end customer speed was 64kBit/s



Internet in the 1990s
Situation in Germany

- In the early 1990s there were three commercial ISPs in Germany
- Each had a connection to the US
- So traffic had to go via the Atlantic twice in worst case
- And was expensive

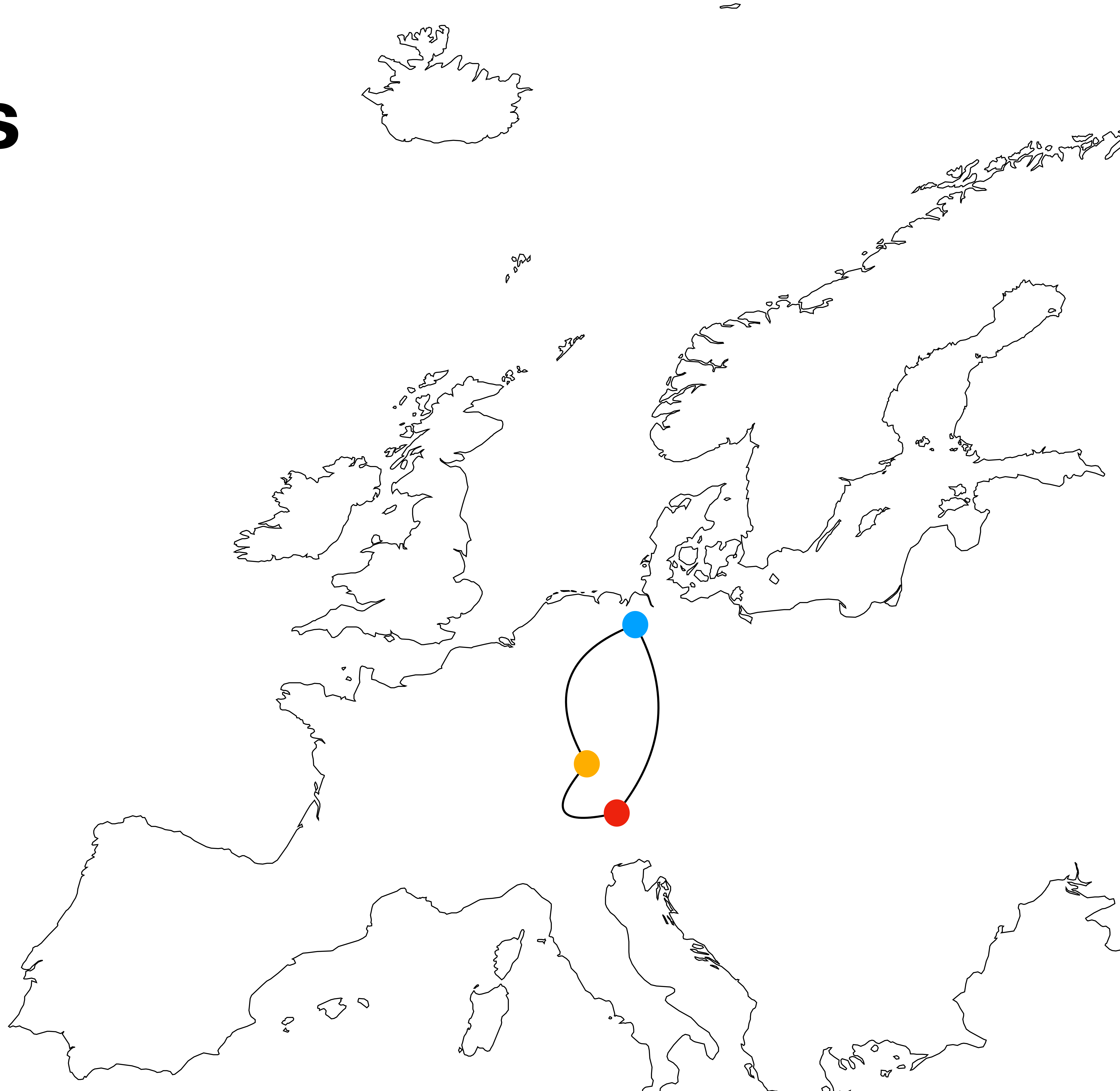


DE CIX

Internet in the 1990s

The idea

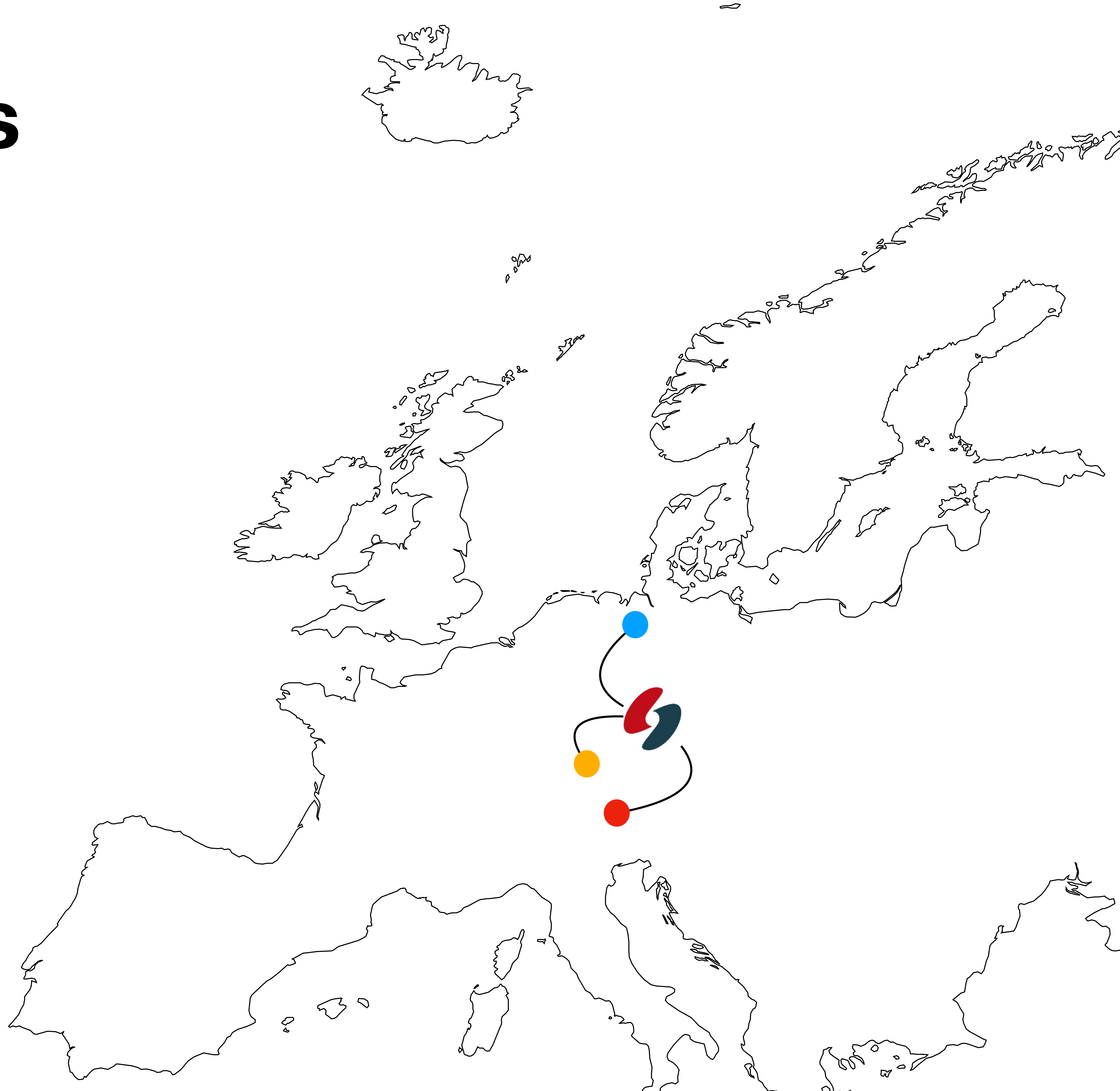
- Idea: Exchange traffic directly
- Via cables?
  - Each of this early ISPs was in a different city
  - Cables / leased lines were expensive
  - Meet in the middle!



Internet in the 1990s

The solution

- Meet in the middle!
    - DE-CIX was born
- Direct connection between commercial providers
- To exchange traffic
    - Only their own and their own customers
    - This is **Peering!**



Peering

Noun

peering (*plural* peerings)

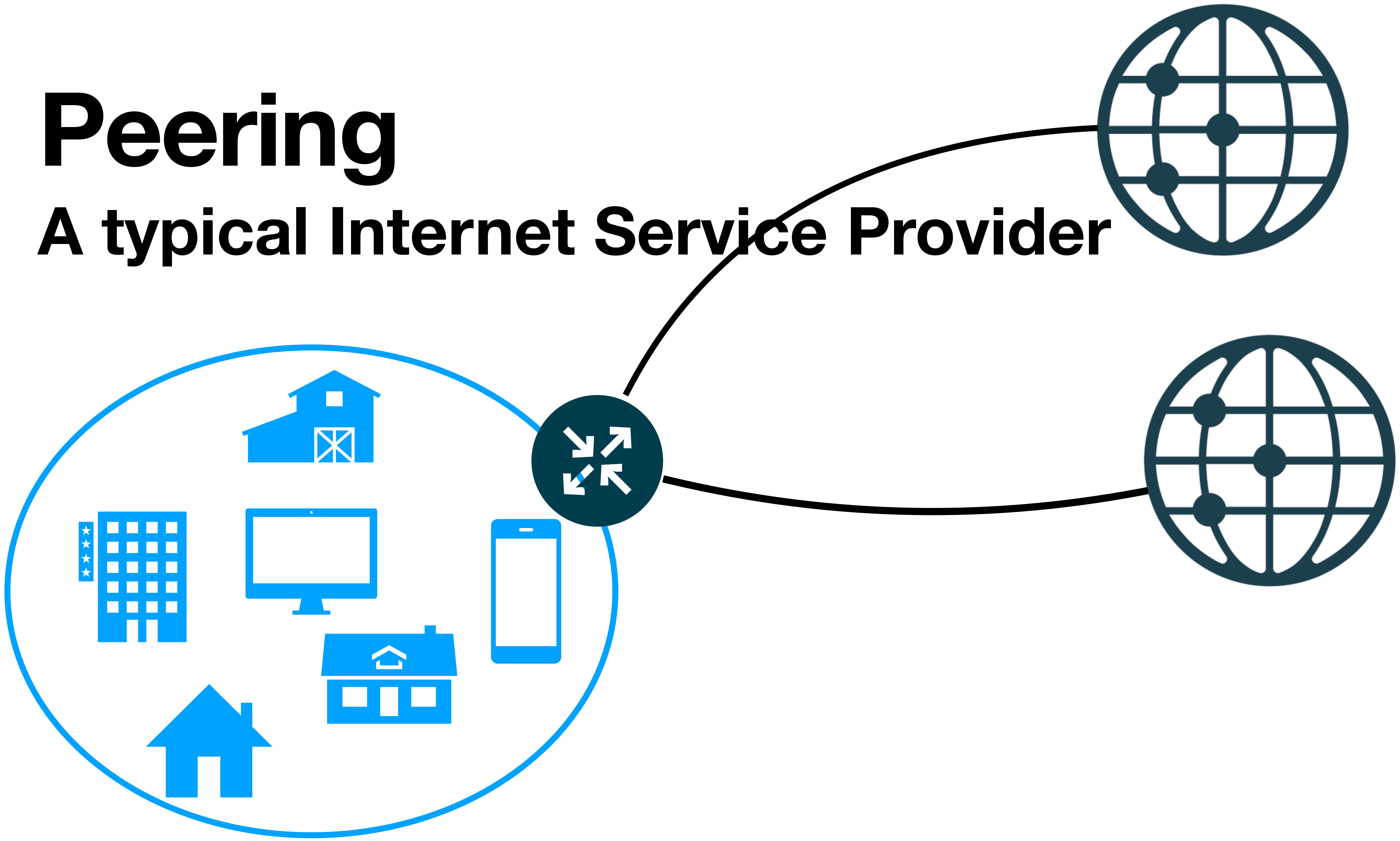
1. The act of one who peers; a looking around.
2. (*Internet*) The act of carrying communications traffic terminating on one's own network on an equivalency basis to and from another network, usually without charge or payment.

https://en.wiktionary.org/wiki/peering

DE CIX

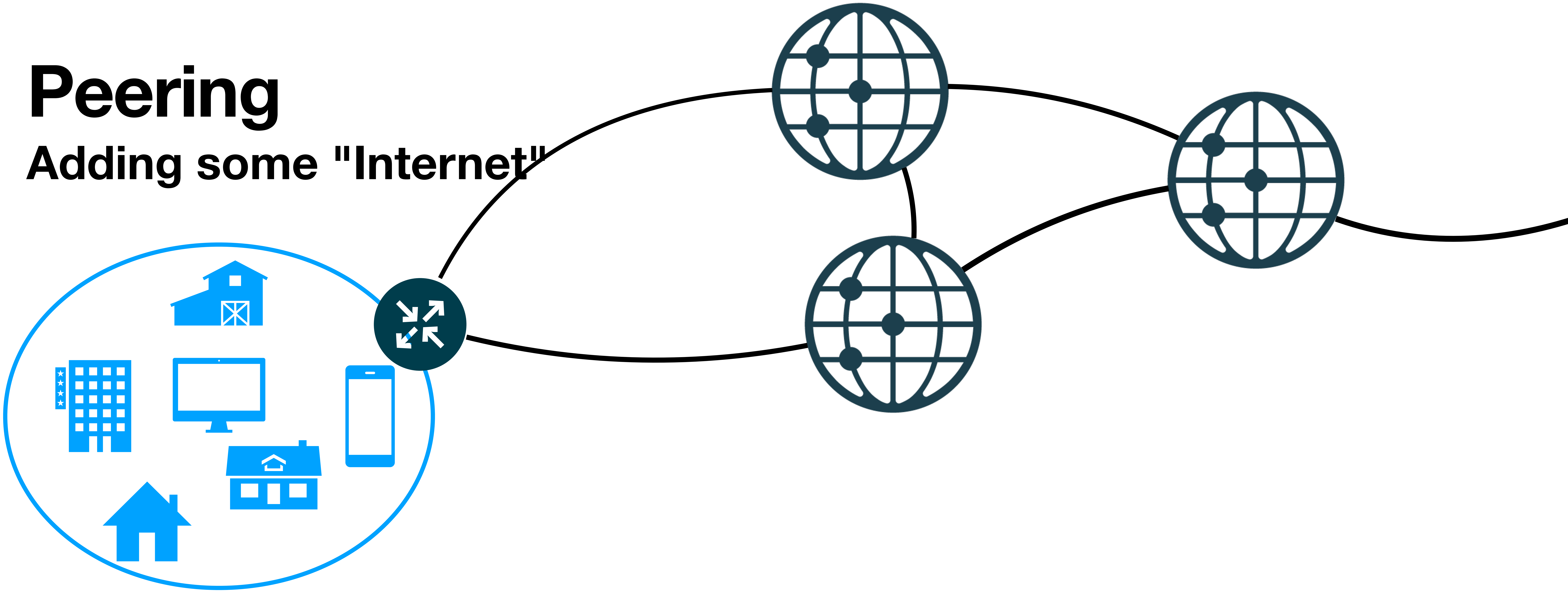
Peering

A typical Internet Service Provider



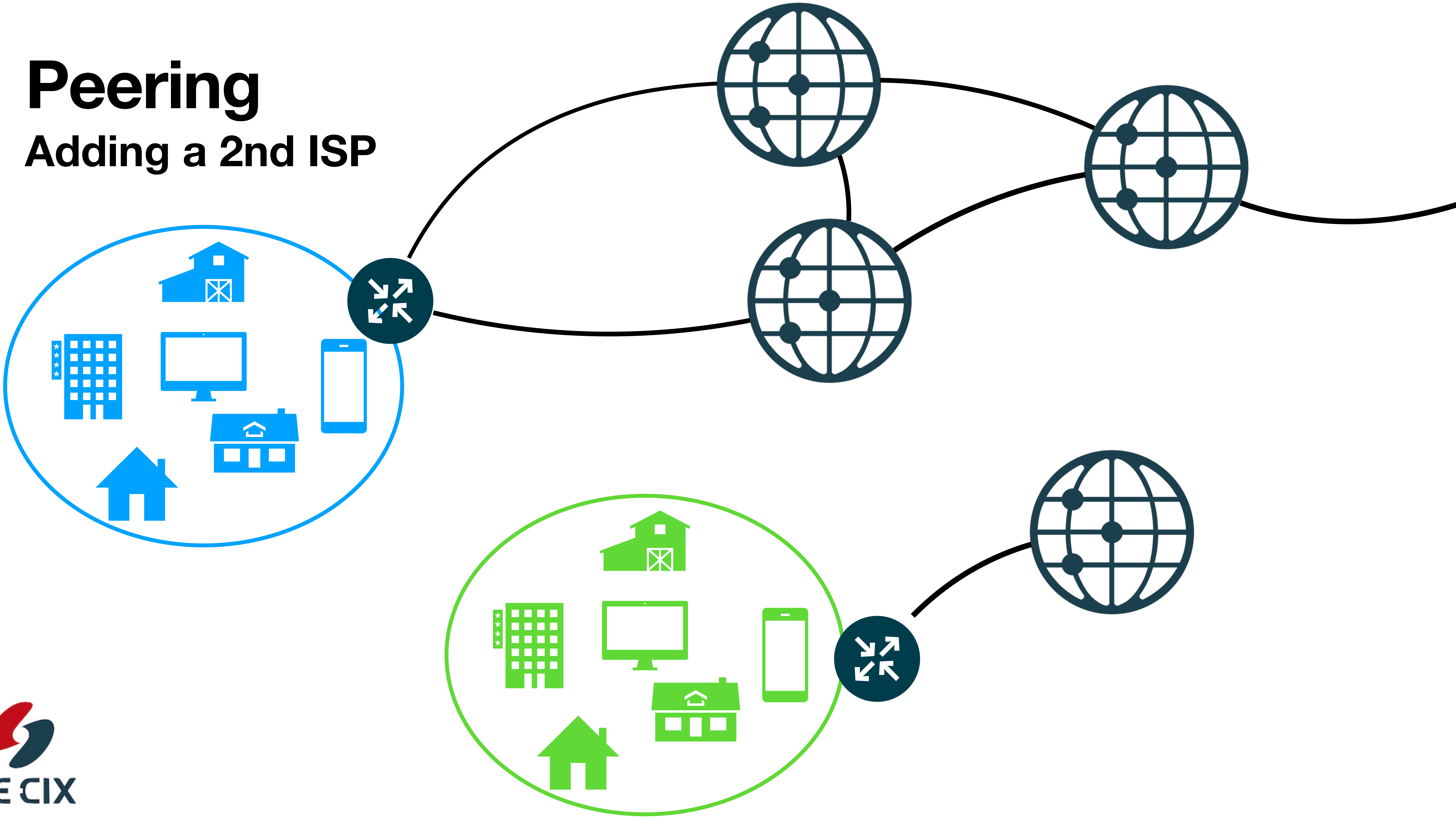
Peering

Adding some "Internet"



Peering

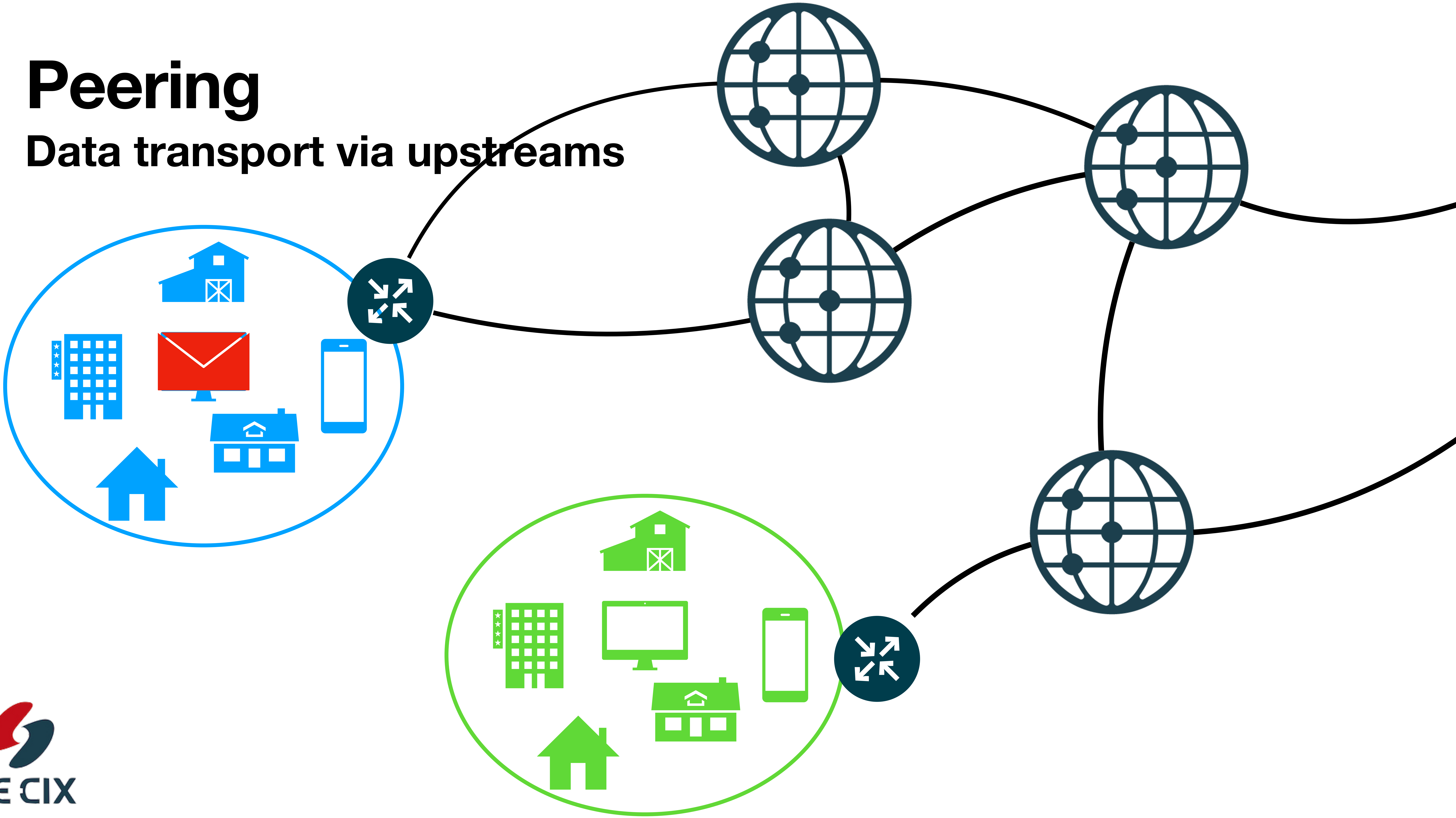
Adding a 2nd ISP



DE CIX

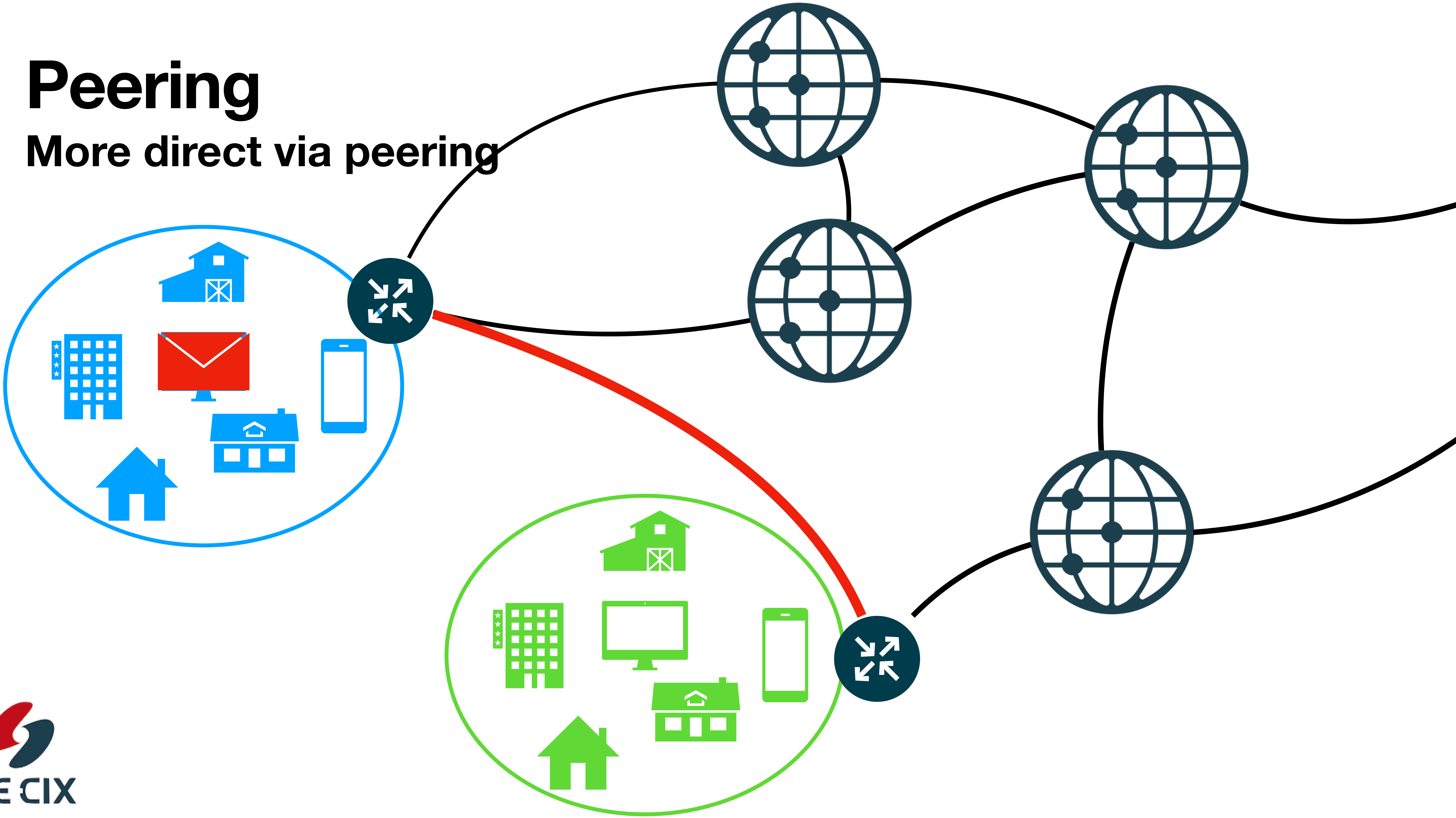
Peering

Data transport via upstreams



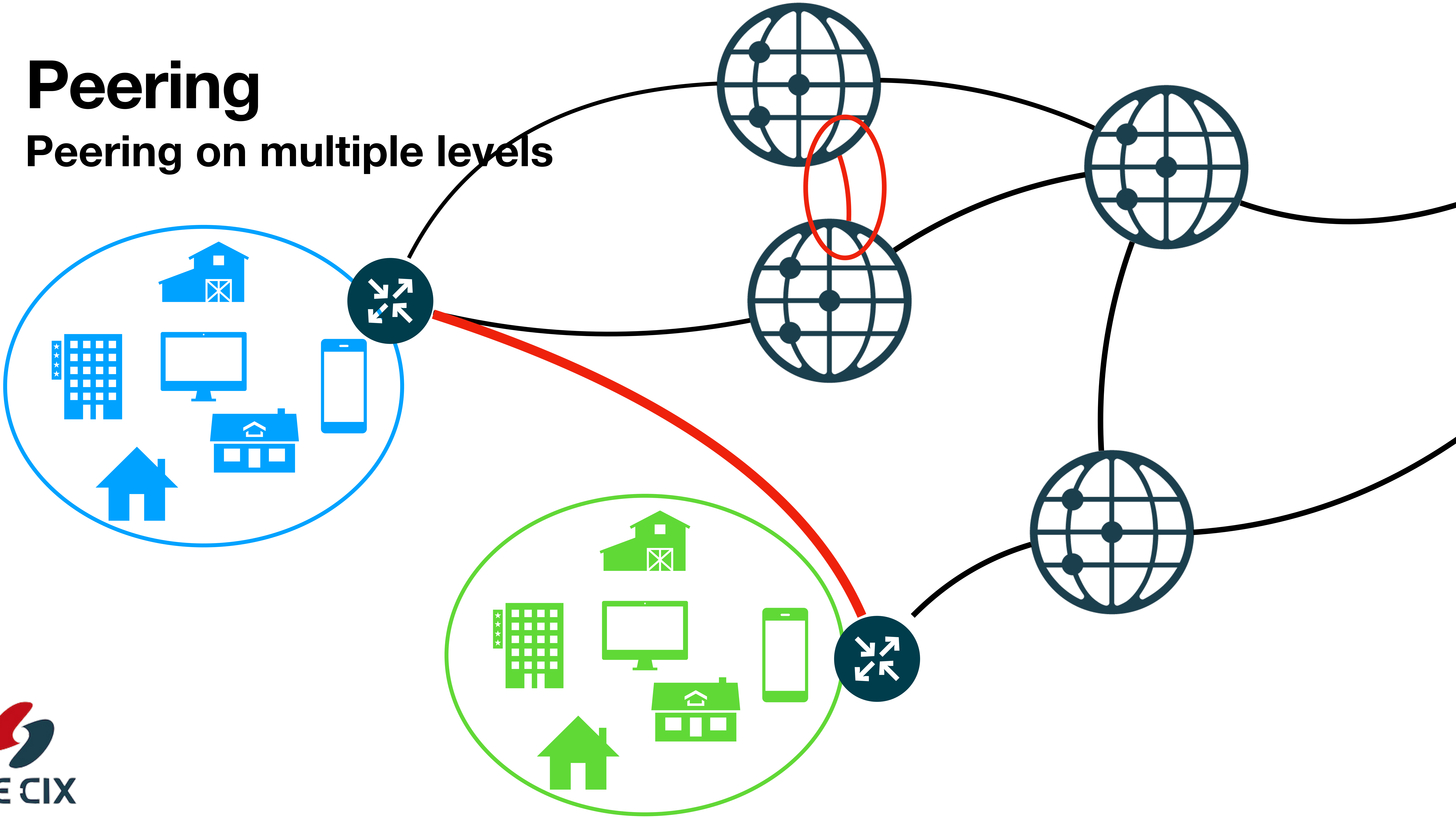
Peering

More direct via peering



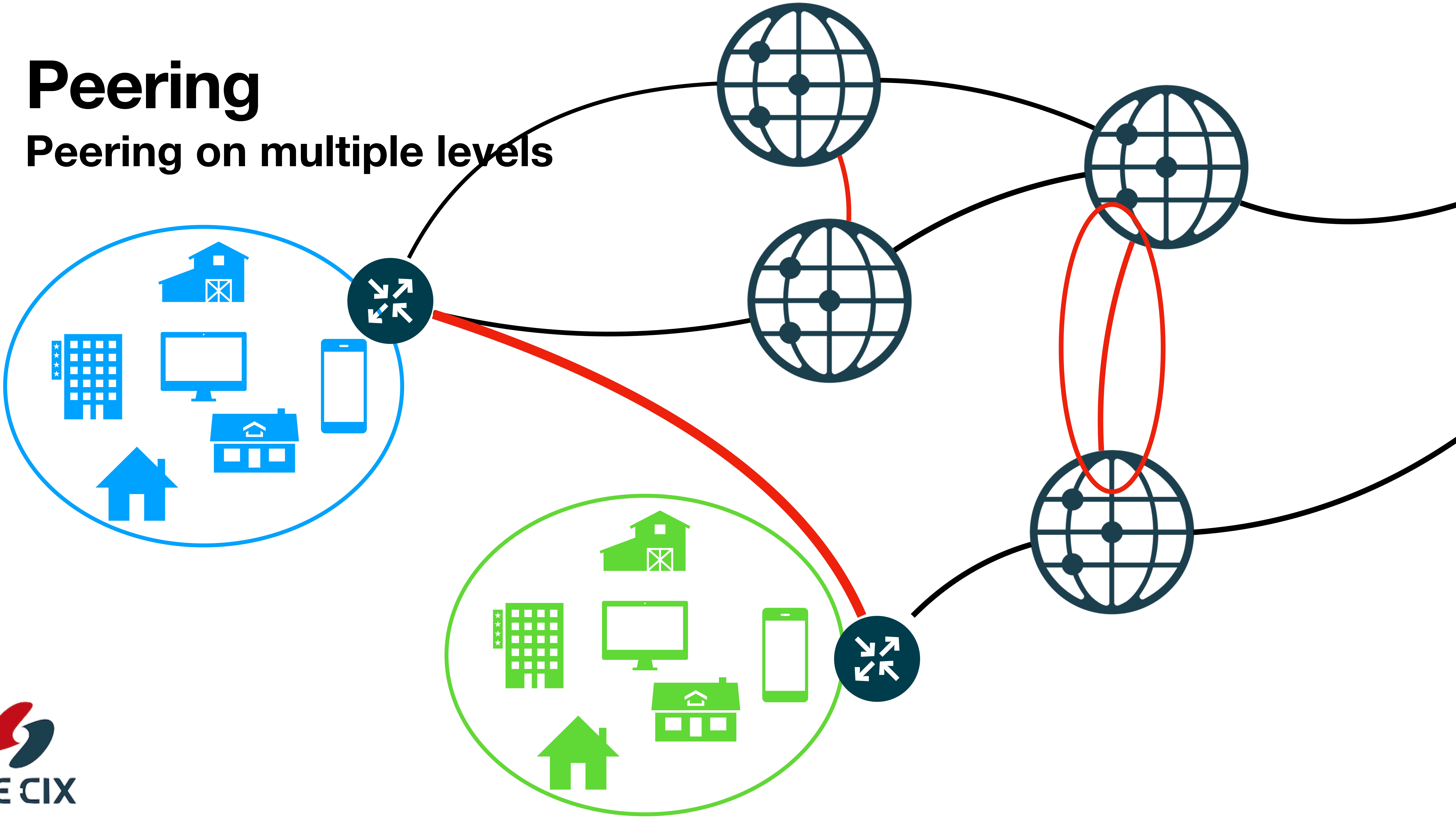
Peering

Peering on multiple levels



Peering

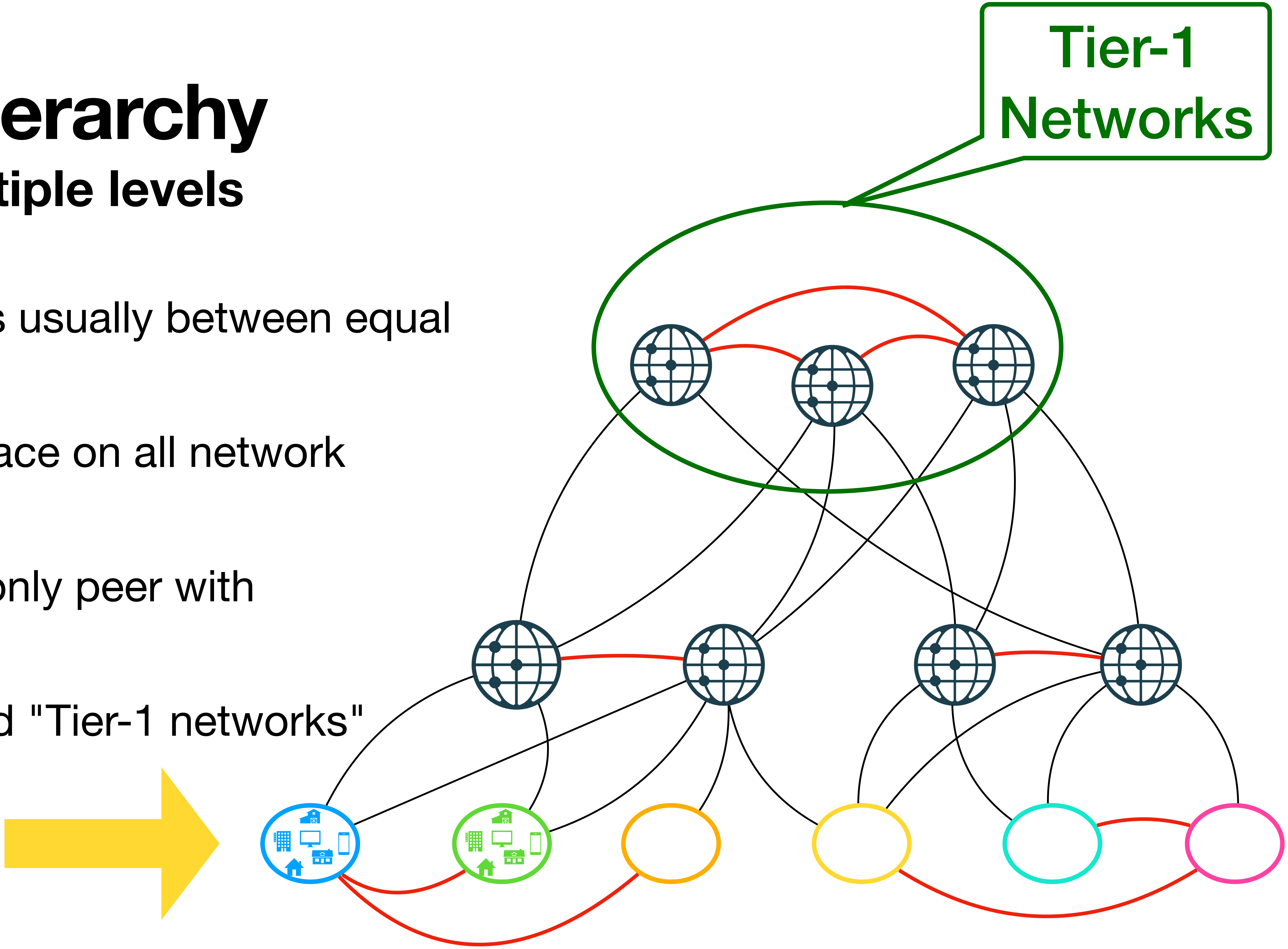
Peering on multiple levels



Peering Hierarchy

Peering on multiple levels

- Peering happens usually between equal size networks
- Peering takes place on all network levels
- The "top ones" only peer with each other
  - They are called "Tier-1 networks"



Why Peering?

Why Peering?

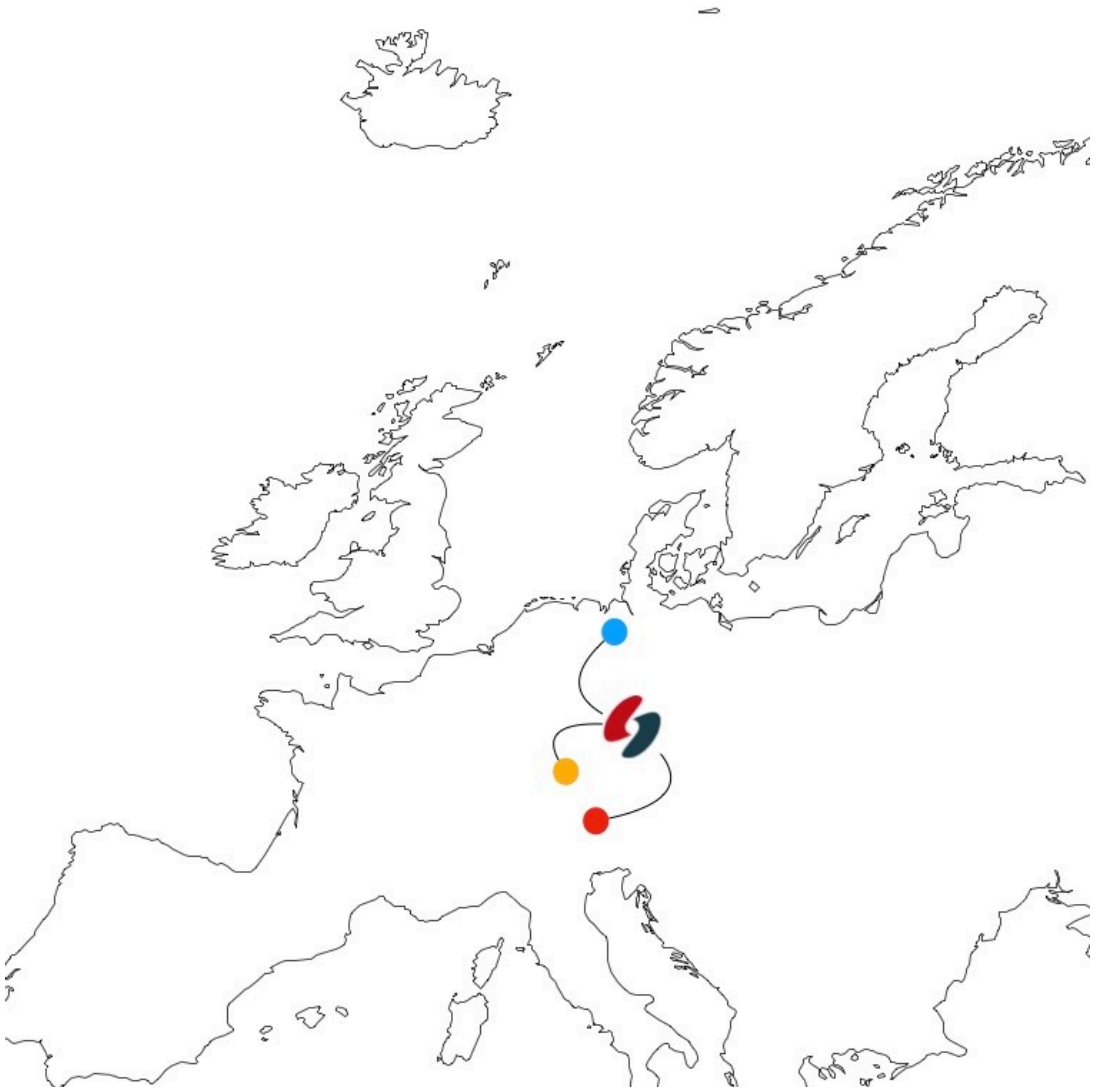
Historical view

- In the early days, peering was cheaper than routing traffic via upstream providers
- Also, it kept traffic from crossing the Atlantic twice

Why Peering?

Peering today

- Upstream prices are down
- But peering is still important
    - Keeping local traffic local
    - Reducing latency
    - Keep your traffic under control
- At an Internet Exchange (IXP) you can peer with multiple networks via one common infrastructure



DE CIX

Conclusion

Conclusion

Global IP routing

- Networks (Internet Service Providers) announce IP Prefixes
- IP Packets are routed to these prefixes by using their IP destination address
- Peering is exchanging traffic between similar sized networks
  - Peering in the past was mainly done to reduce cost
  - Today peering decreases latency and enhances control
  - Internet Exchanges are places where many networks meet and can peer with each other

DE CIX

Networking Basics

04a - User Datagram Protocol (UDP)

Wolfgang Tremmel
academy@de-cix.net

DENOG 13
GERMAN NETWORK OPERATORS GROUP

DE CIX

Networking Basics
DE-CIX Academy

01 - Networks, Packets, and Protocols

02 - Ethernet

  02a - Ethernet + VLANs

03 - The Internet Protocol (IP)

  03a - IP addresses, prefixes, and routing

  03b - Global IP routing

04a - UDP (User Datagram Protocol)

04b - TCP

04c - ICMP

05 - Unicast, Broadcast, Multicast, Anycast

Internet Model

IP / Internet Layer

- Data units are called "Packets"
- Provides source to destination transport
  - For this we need addresses
- Examples:
  - IPv4
  - IPv6

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

DE CIX

Internet Model
Transport Layer

- *May* provide flow control, reliability, congestion avoidance
- Examples:
  - TCP (flow control, reliability, congestion avoidance)
  - UDP (none of the above)
- Also may contain information about the next layer up

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

Encapsulation

Packets inside packets

- Encapsulation is like Russian dolls
- IP Packets have a payload
- This payload is usually UDP or TCP (there are others as well)
- So we have an UDP packet inside an IP packet

Attribution: Fanghong. derivative work: Greyhood
https://commons.wikimedia.org/wiki/File:Matryoshka_transparent.png

DE CIX

IPv4 Header

"Legacy" IP

- Starts with version and length
- Total length of packet
- Important: Time to live (TTL)
- **Protocol: Type of payload**
    - TCP = 6, UDP = 17
- Source / Destination address 32 bits
- Options (optional)

<table>
<tr><th>Byte</th><th>0</th><th>1</th><th>2</th><th>3</th></tr>
<tr><td>0</td><td>Version | Header Length
always 4 | 5..15</td><td>DSCP / ECN</td><td colspan="2">Total Length
20..65535</td></tr>
<tr><td>4</td><td colspan="2">Identification</td><td colspan="2">Flags / Fragment Offset</td></tr>
<tr><td>8</td><td>Time To Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td>12</td><td colspan="4">Source IPv4 Address</td></tr>
<tr><td>16</td><td colspan="4">Destination IPv4 Address</td></tr>
<tr><td>20
24
28
32</td><td colspan="4">Optional (if HeaderLength > 5)</td></tr>
</table>

IPv6 Header

Looks simpler, yes?

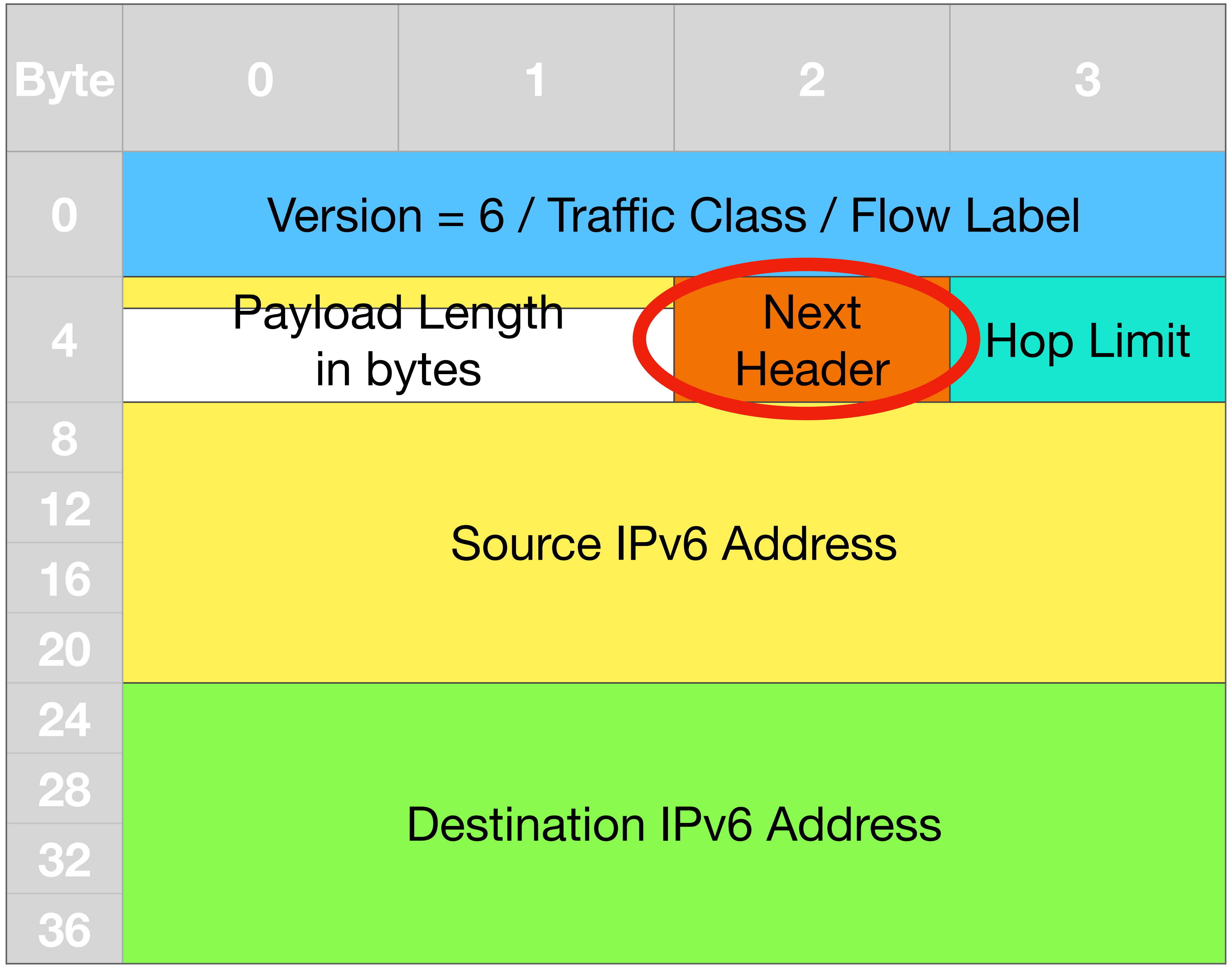
- Starts with version and some labels
- Payload length in bytes (0-65535)
- **Next Header** - you can chain more headers
    - replaces protocol field, same values
- Hop Limit replaces TTL
- Addresses are now 128bits

Byte	0	1	2	3
0	Version = 6 / Traffic Class / Flow Label			
4	Payload Length in bytes		Next Header	Hop Limit
8	Source IPv6 Address			
12				
16				
20				
24	Destination IPv6 Address			
28				
32				
36				

Next header: Transport layer header

TCP, UDP, and more

- We start with the "easiest" protocol
- UDP
  - User Datagram Protocol
  - Protocol ID is **17**
  - Introduced in 1980
- Lets have a look at the header



DE CIX

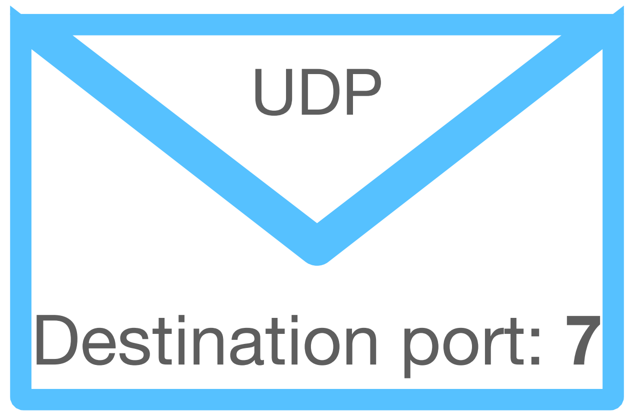
UDP Header

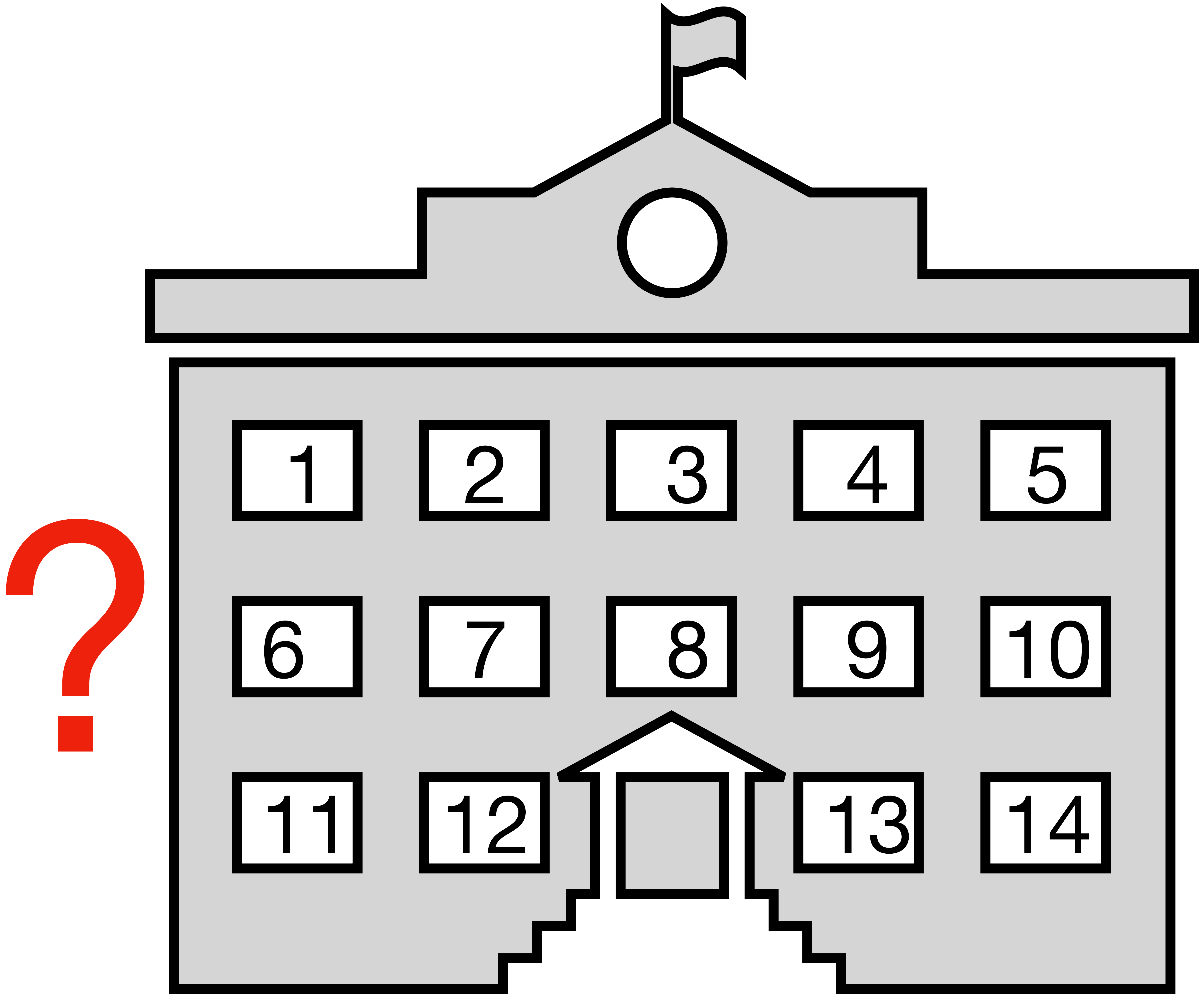
- 4 fields, each of them 16 bits
- Length: UDP header + UDP payload
- Checksum
  - Optional for IPv4, required for IPv6
  - IP header + UDP header are covered
- Source Port
  - Optional, zero if not used
- Destination Port number
  - required

Byte	0	1	2	3
0	Source Port		Destination Port	
4	Length		Checksum	

Port number

Port number

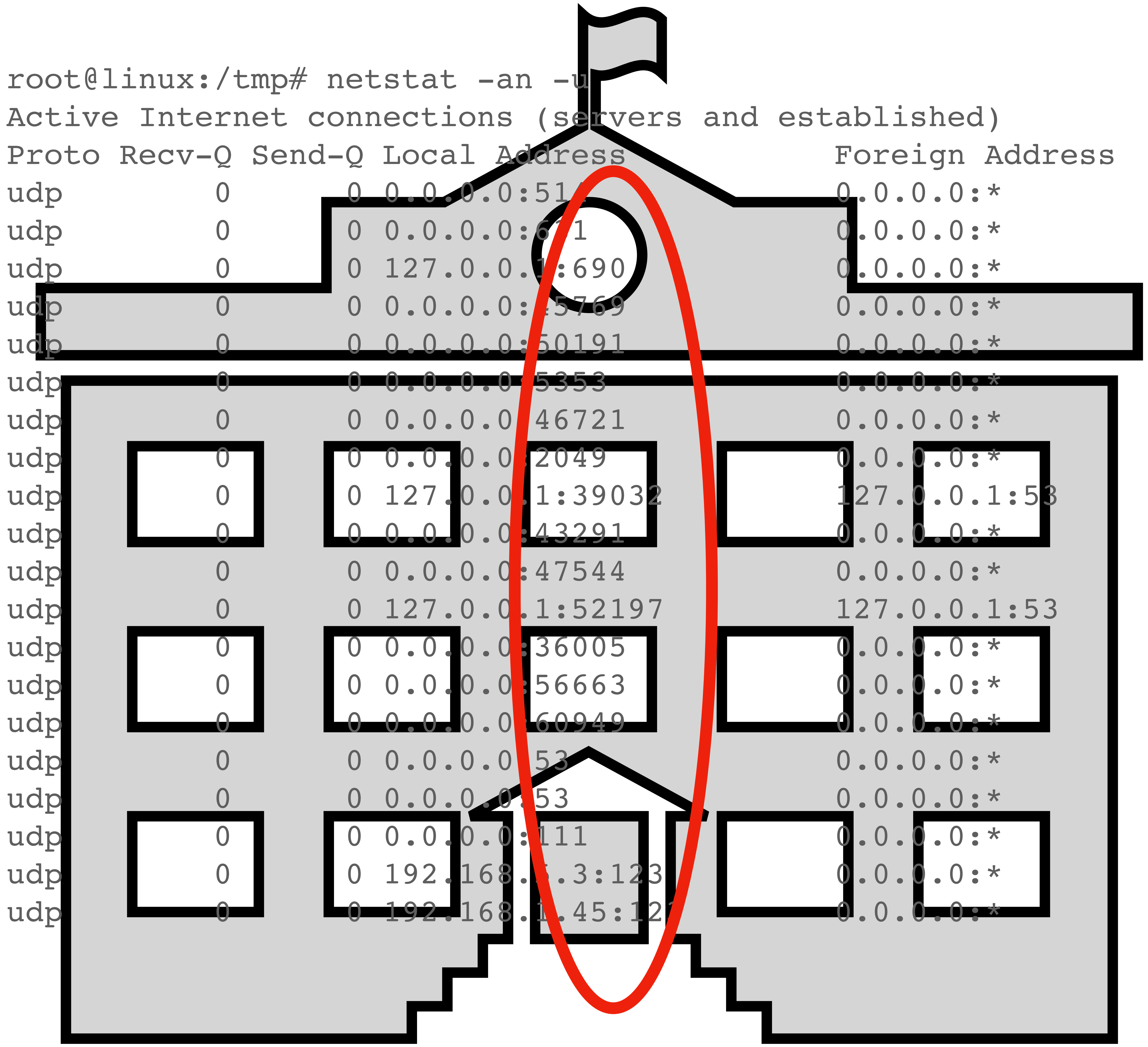




Port numbers

In reality...

- Of course we have not a building
- We have a computer system
- But we have port numbers
- Behind each port sits a piece of software
    - On some systems this software is called a "daemon"



UDP - Connectionless communication

Why is it called connectionless?

- The sender does not know if and when the packet has been received
- There may be an answer, but there also may be not
- If there is an answer, the sender knows the packet got through
- If there is no answer
  - Either the packet did not get through
  - Or the answer did not get through

UDP packet processing

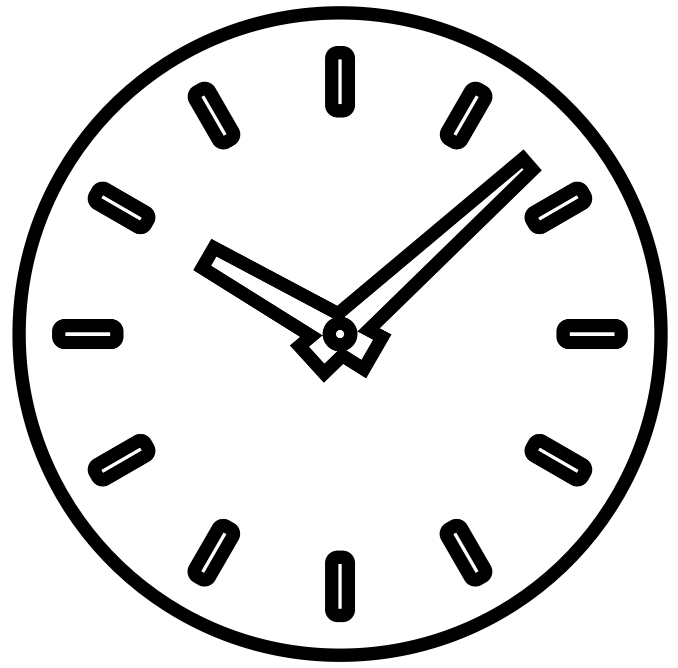
Security issues ahead!

- A UDP packet is received by a system
- It is delivered to the software matching the destination port number
- If a response has to be sent, it is sent to back to sender
    - Using the source IP as destination of the response
    - The source-port becomes the destination port of the response
- Can you see a security problem in that?

UDP - what it is used for

NTP - Network Time Protocol

Synchronizing clocks over the Internet



- NTP is a protocol to synchronize computer clocks using the Internet
- Systems send and receive UDP packets on port 123
  - Packets contain a 32-Bit number for seconds and a 32-bit number for fractional seconds
  - Epoch (start) is 1st of January, 1900
  - Rollover will be on 7th of February, 2036
- Newest version of NTP now uses 64 bits for seconds

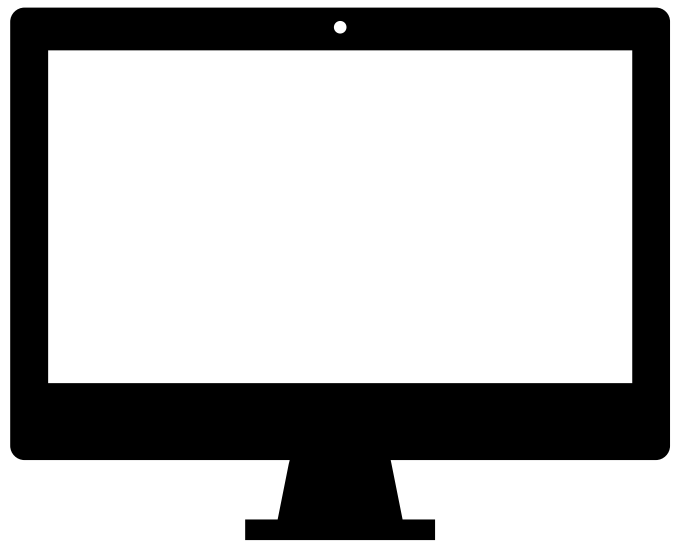
DNS - Domain Name Service

The phonebook of the Internet

- DNS translates names (like "www.de-cix.net") to IP addresses
- DNS is so complex and widely used, it deserves a webinar on its own
- Roughly explained
  - A system sends a name to a name server via UDP
  - The name server sends an UDP packet back containing the IP address where the name is hosted

DHCP - Dynamic Host Configuration Protocol

This is how your PC gets an IP address at home



- If you connect a computer to a network it needs an IP address
- DHCP takes care it gets one, and more
  - Your computer sends out a *DHCP request* via UDP **broadcast** to port 67
  - A DHCP server *replies* via UDP and assigns
    - an IP address
    - the default gateway
    - a nameserver (where to send DNS requests to)

DE CIX

UDP and network security

UDP normal communication

Request and answer

UDP as attack tool

Faked request and misdirected answer


Attack Target

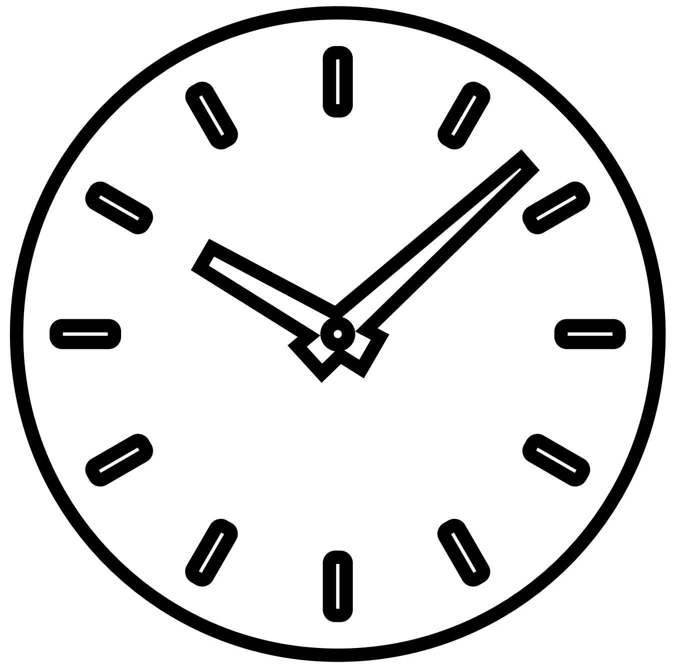
A real world example

Memcached

- memcached is a software to cache objects in RAM for fast retrieval
- Attack method:
  - tell an unsecured installation of *memcached* to store an object
  - send an UDP packet to that installation with a **faked source IP** to retrieve that object
  - this gives you an amplification factor of up to 51000
- Solution: Remove UDP from memcached

A real world example

NTP - Network Time Protocol (2010)



- NTP is a protocol to synchronize computer clocks using the Internet
- The "*monlist*" command, sent via UDP to an NTP server returns the list of the last 600 hosts who have connected to that server
  - If sent from a faked IP source address, this list is sent via UDP to the faked source
- Solution: "*monlist*" command was removed from the software

Conclusion

Conclusion

UDP - User Datagram Protocol

Layer	Name
5	Application
4	Transport
3	Internet
2	Link
1	Physical

- UDP is a connectionless protocol on the transport layer
- UDP packets are also called "datagrams"
  - the UDP header contains a source and a destination port number
- If misconfigured, UDP services can be used for network attacks
- More and more services which relied on UDP are moved to TCP
  - But TCP is the topic of the next episode