Computer Networks II.

Gábor Gyurák

Computer Networks II.

Pécs

2019

The Computer Networks II. course material was developed under the project EFOP 3.4.3-16-2016-00005 "Innovative university in a modern city: open-minded, value-driven and inclusive approach in a 21st century higher education model".

EFOP 3.4.3-16-2016-00005 "Innovative university in a modern city: open-minded, value-driven and inclusive approach in a 21st century higher education model".

Gábor Gyurák

Computer Networks II.

Pécs

2019

A Computer Networks II. tananyag az EFOP-3.4.3-16-2016-00005 azonosító számú, „Korszerű egyetem a modern városban: Értékközpontúság, nyitottság és befogadó szemlélet egy 21. századi felsőoktatási modellben” című projekt keretében valósul meg.

EFOP-3.4.3-16-2016-00005 Korszerű egyetem a modern városban: Értékközpontúság, nyitottság és befogadó szemlélet egy 21. századi felsőoktatási modellben

COMPUTER NETWORKS II.

Gyurák Gábor

Chapter 01

Networking fundamentals

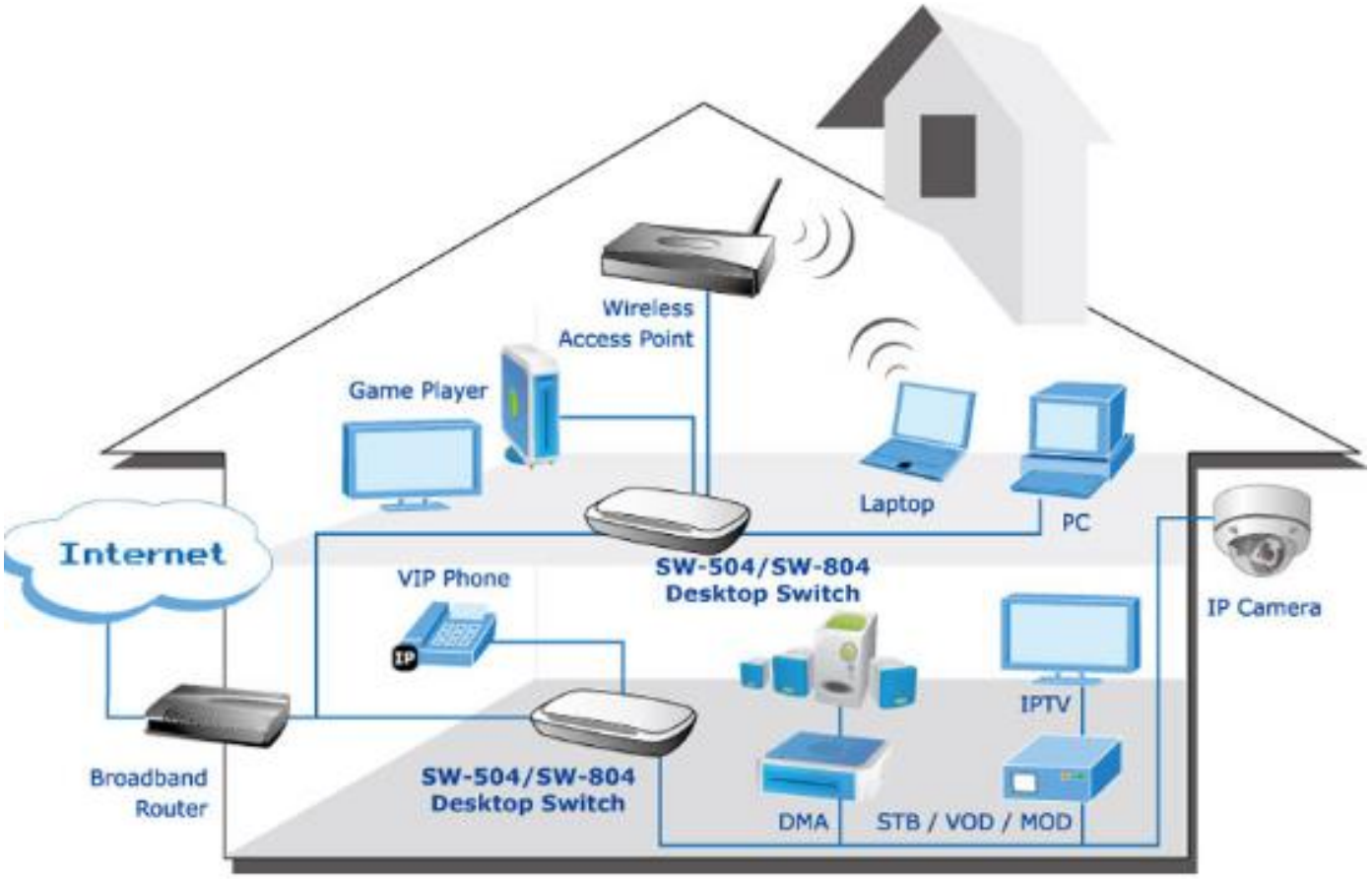
Let’s build a simple network

- What do we need?
  - Active network elements
    - Hosts (client, server), HUB, switch, router
  - Passive network elements
    - Cables, connectors
      - UTP, RJ45…

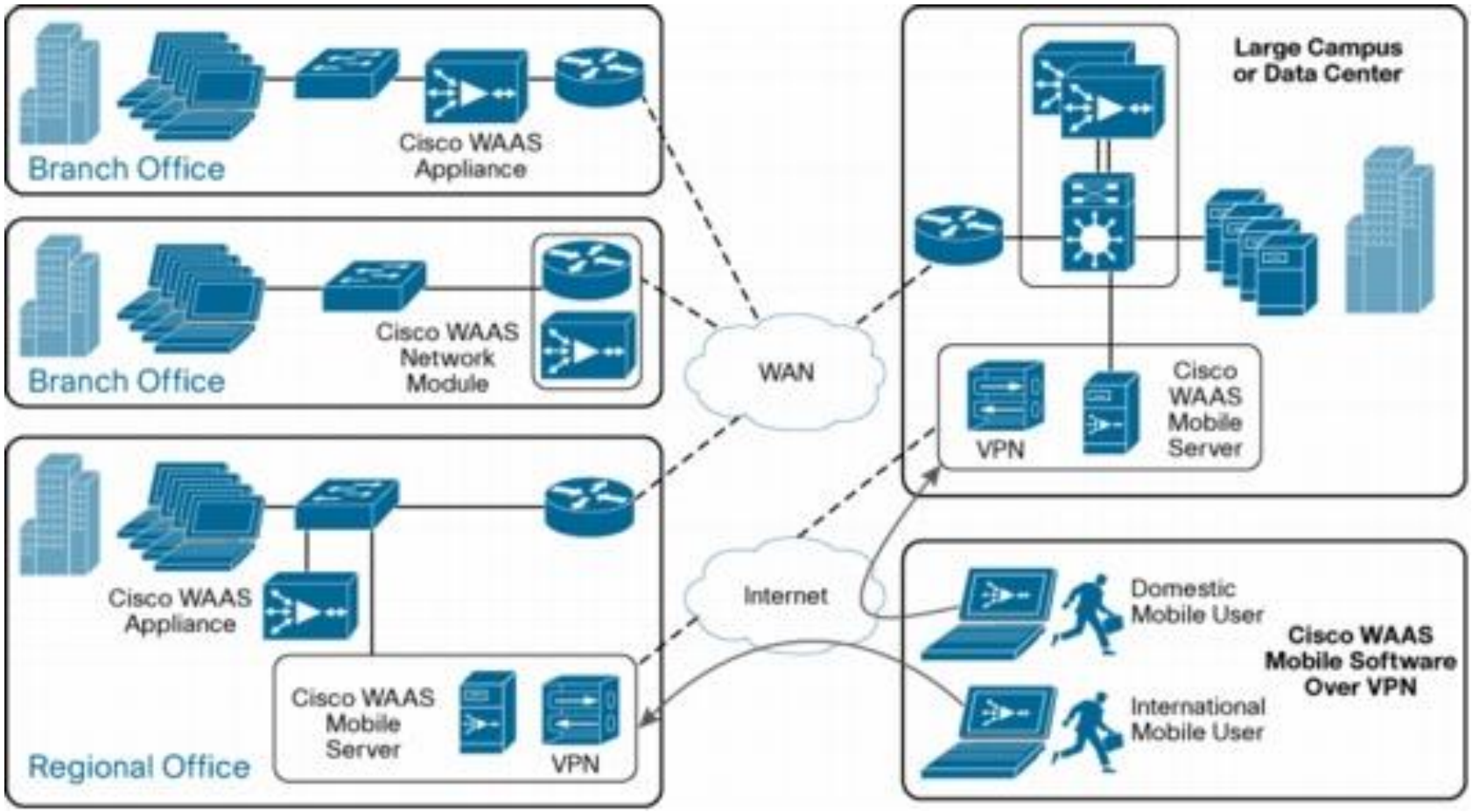
Is it enough?

SOHO networks

- SOHO (Small Office Home Office)



Enterprise networks



Enterprise network needs

- Planning
  - Building cabling plans
  - IP addressing plans
  - …
- Knowledge
  - Protocols
  - Configuring devices

Different dimensions

SOHO router

Enterprise router

Different dimensions

SOHO switch

Enterprise switch

Curiosity

Cisco
CRS (Carrier Routing System)
Internet core router
~90%

CRS-3

322 Tbit/sec switching capacity

13,2kW

TCP/IP and OSI Network Model

- A network model refers to a comprehensive set of documents that define how a network should work
- Protocols are a set of logical rules that devices must follow to communicate
- Physical requirements for networking define the voltage and current levels used on a cable when transmitting.

Main networking models

- There are two main networking models that people refer to when talking about networking models
  - OSI – Ended up “loosing” the race but we almost always use it’s layers when describing networking functions. It was made by the “International Organization for Standardization”.
  - TCP/IP – Ended up “becoming” the standard that every single computer, tablet and phone now uses. It was made at Universities for a DoD contract.

Overview of the TCP/IP Networking Model

- TCP/IP (like OSI) both DEFINES and REFERENCES a large collection of protocols. The protocols allow devices like computers to communicate.
- To define a protocol, TCP/IP uses documents called Requests for Comments (RFC)
- To avoid repeating work, it will sometimes refer to standards or protocols created by other groups
  - IEEE Defined Ethernet LANS
  - TCP/IP does not define Ethernet in a RFC, rather it refers to IEEE Ethernet as an option
- Each Layer includes protocols & standards that relate to that category of functions

	TCP/IP Original	TCP/IP Updated	Protocols
Focuses on applications	Application	Application	SMTP,FTP,HTTP, POP3...
	Transport	Transport	TCP, UDP
Focuses on delivery	Internet	Network	IP
Transmitting bits over a link	Link	Data Link	Ethernet
		Physical	

TCP/IP Application Layer

- Provides services to the application software running on a computer
- Application layer does NOT define the application itself. Rather it defines the services that the application needs. There are many Web browser application on the market. Internet Explorer, Firefox, Safari and Chrome. The Application layer does NOT define these applications. It defines how web servers and web browsers talk to each other.

TCP/IP Transport Layer

- Transport Layer includes a smaller number of protocols than the application layer
- Two most common protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
- Transport layer provides services to the application layer that resides one layer higher in the TCP/IP model.

TCP/IP needs a mechanism to guarantee delivery of data across the network. To recover from errors , TCP uses the concept of ACKNOWLEDGEMENTS.

TCP/IP Network Layer

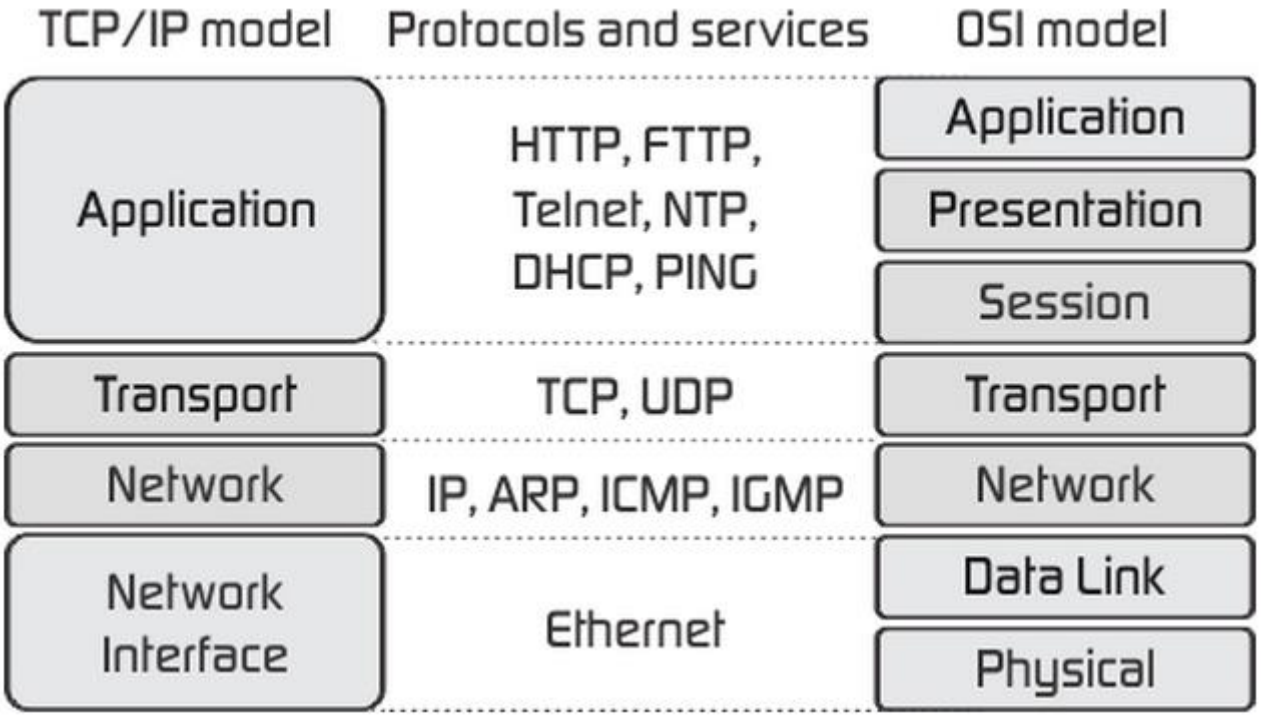
- The transport layer contains fewer protocols than the application layer. The following are TCP and UDP.
- TCP/IP is simply the names of the two most common protocols (TCP and IP).
- The main IP functions are addressing and routing.

TCP/IP Link Layer

- The TCP/IP model's original link layer defines the protocols and hardware required to
- deliver data across some physical network.
- The link layer contains many protocols and standards. For example, the link layer includes all versions of Ethernet protocols, the LAN standard, wide-area network (WAN) standards.

OSI Networking Model

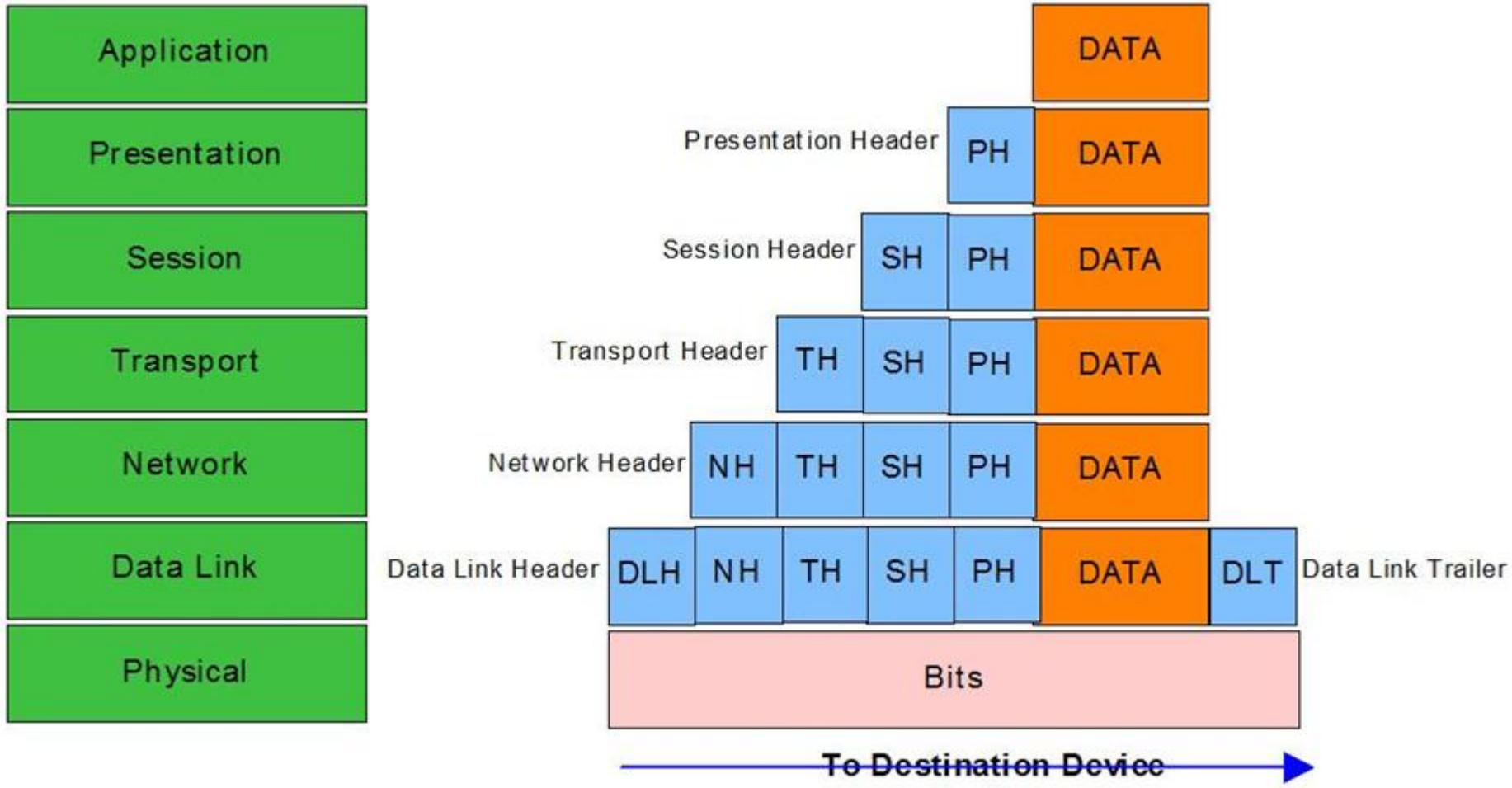
- The OSI model has 7 layers.
- Each layer defines a typical network function.



OSI Encapsulation Terminology

- Like TCP/IP, each OSI layer asks for services from the next lower layer. To provide the services, each layer makes use of a header and possibly a trailer. The lower layer encapsulates the higher layer's data behind a header.

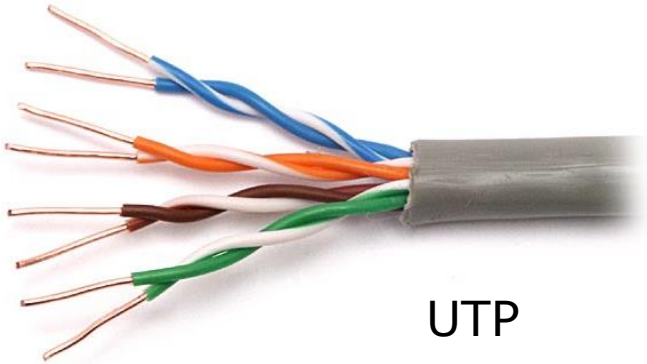
OSI Encapsulation Terminology



Physical layer technical overview

- Twisted pair
  - UTP (Unshielded Twisted Pair)
  - Cable categories (CAT5, CAT6, CAT7…etc)
  - How many pairs are in operation?
- RJ45 plug connectors

RJ11

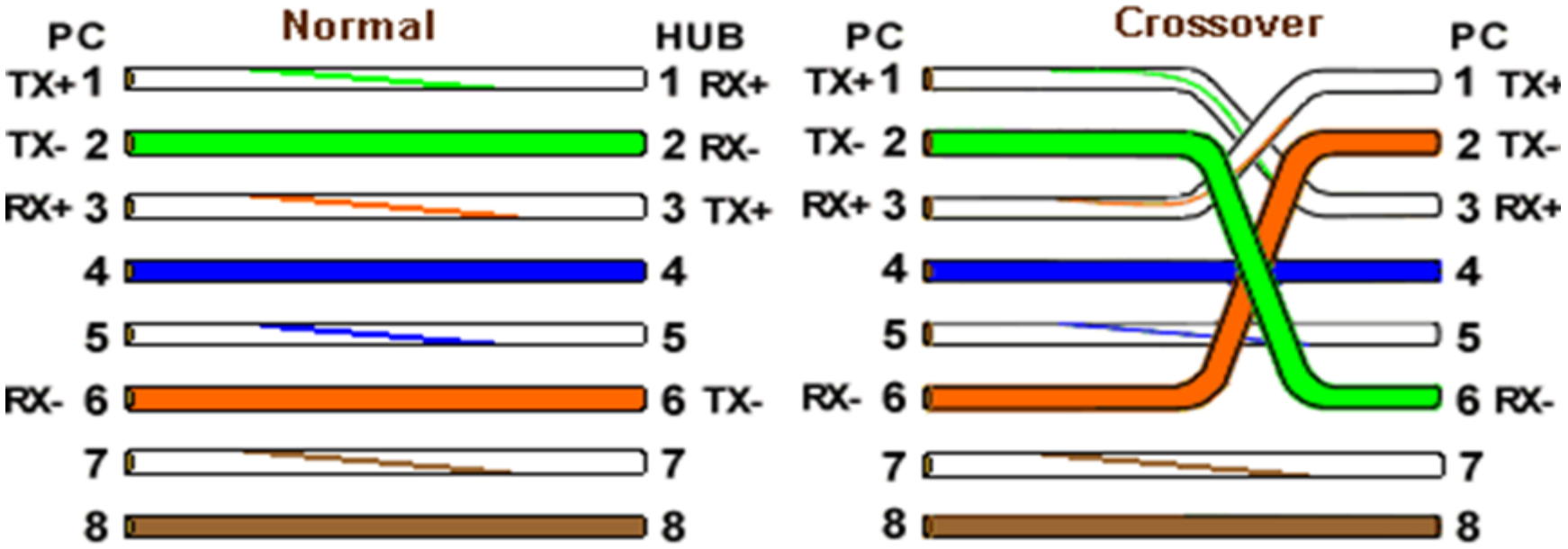


UTP

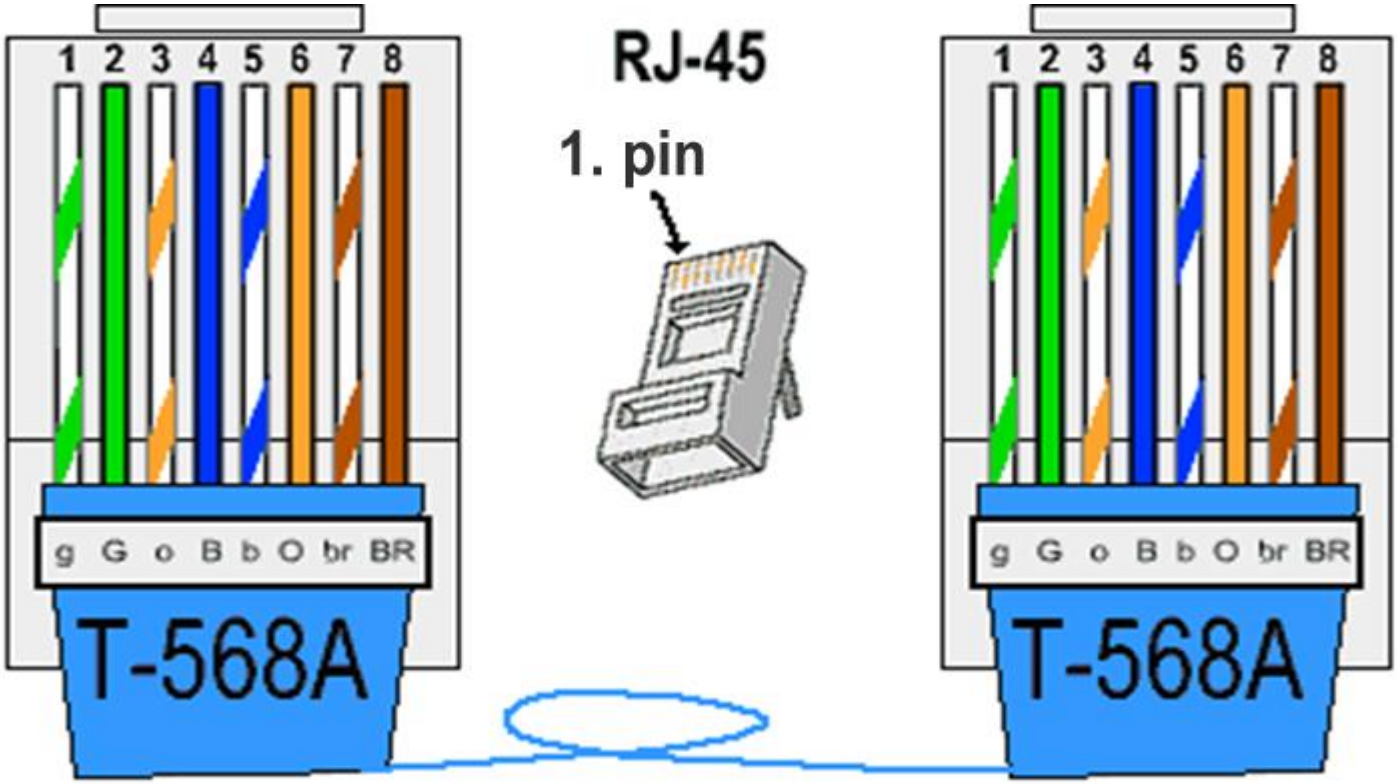
RJ45

RJ: Registered Jack

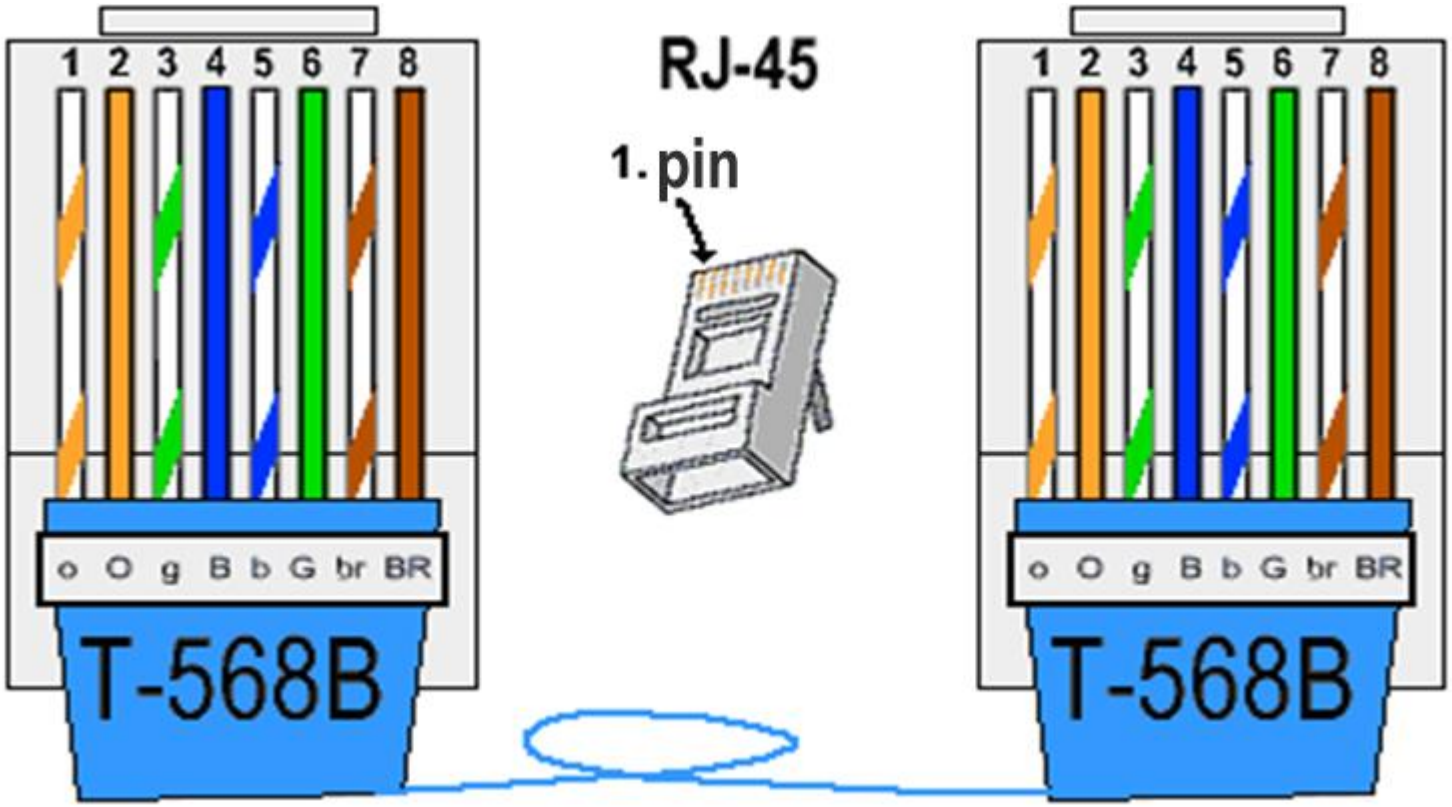
UTP formations



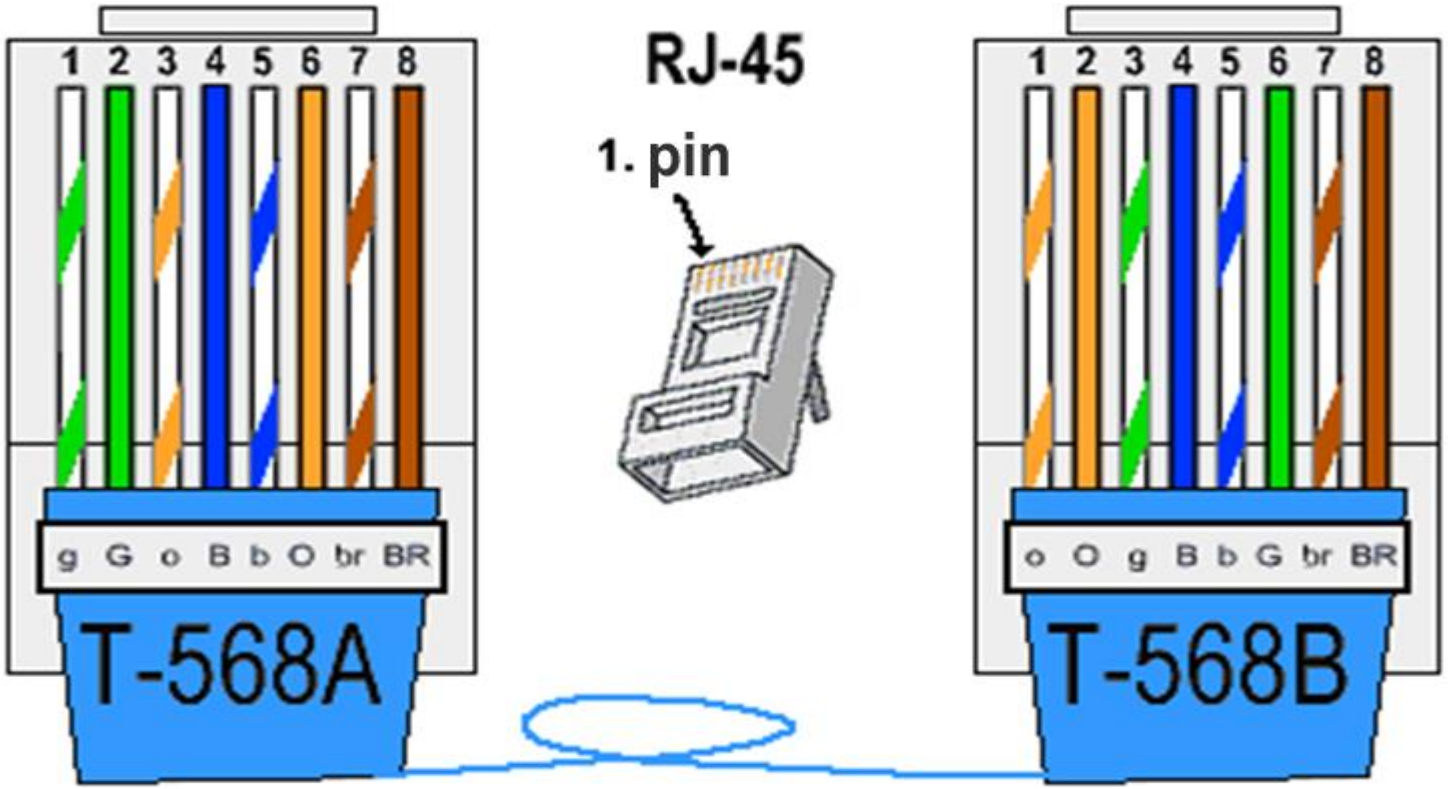
UTP color coding (straight through)



UTP color coding (straight through)



UTP color coding (crossover)



Straight or cross?

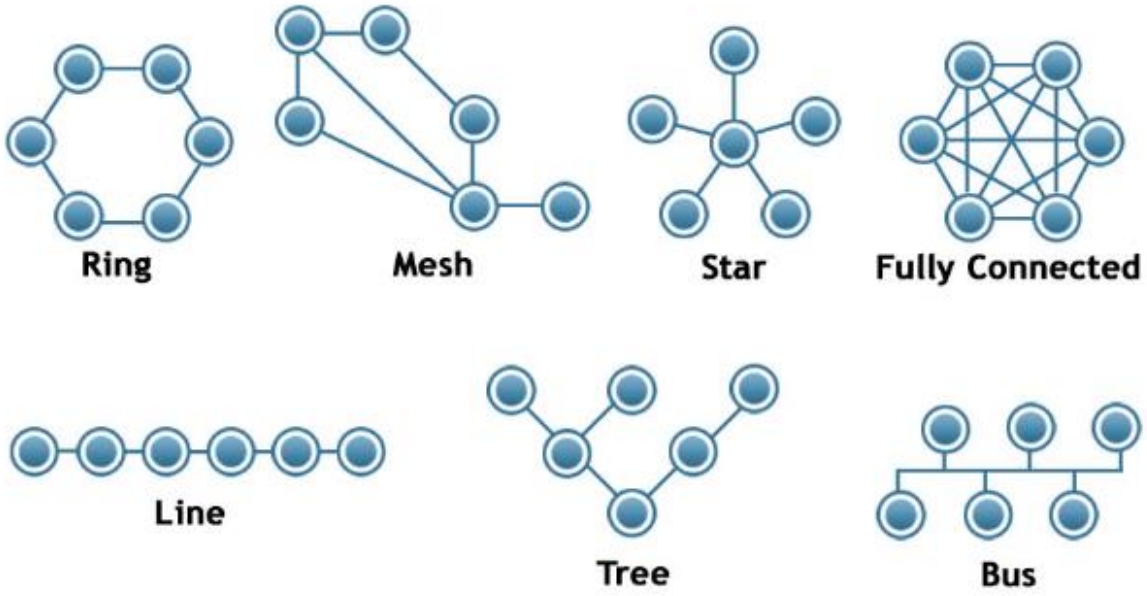
- Straight
  - PC-SWITCH
  - SWITCH-ROUTER
- Cross
  - PC-PC
  - SWITCH-SWITCH
  - ROUTER-ROUTER
  - PC-ROUTER
- Autosense!!!

UTP cable types

- Place of application
  - wall cable vs patch cable
  - outdoor vs indoor
  - …stb…already mentioned in Computer networks I.

- What are the differences?

Medium access



- Medium access
  - Accessing the commonly used media

Analyzing Campus LAN Topologies

- *Campus LAN*
  - A LAN, created to support the devices in a building or more buildings close to each other
  - When designing a campus LAN, engineers have to consider many things
    - Types of Ethernet
    - Cabling lengths
    - Speeds
    - Connections
    - Already installed equipments

Analyzing Campus LAN Topologies

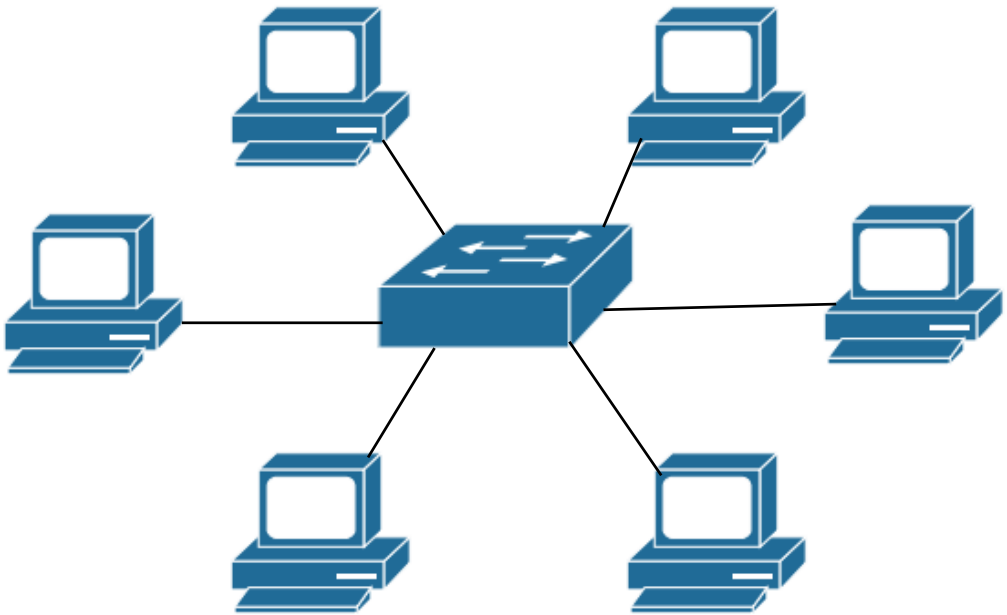
- Two-Tier Campus Design (Collapsed Core)
  - Describing the role of switches in a campus design
    - Access switches
      - Provides user devices access to LAN
    - Distribution switches
      - Provides access switches access to each other
      - Every access switch connect to at leat one distribution switch
    - Core
      - Connects the distribution switches
  - Two-tier design
    - Provides connection to end-user devices
    - Connects the switches with reasonable number of cables and ports

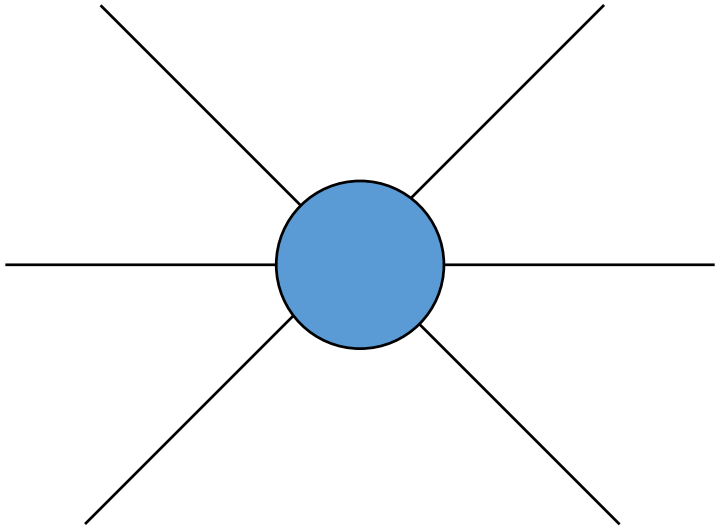
Analyzing Campus LAN Topologies

- Topology Terminology Seen Within a Two-Tier Design
  - Star: one central device connect to several others
  - Full mesh: connects a link between each pair of nodes
  - Partial mesh: connects a link between some pairs of nodes, not a full mesh
    - Distribution layer
  - Hybrid: combines topology concepts into larger, more complex design
    - Two-tier design

Analyzing Campus LAN Topologies

- Topology Terminology Seen Within a Two-Tier Design

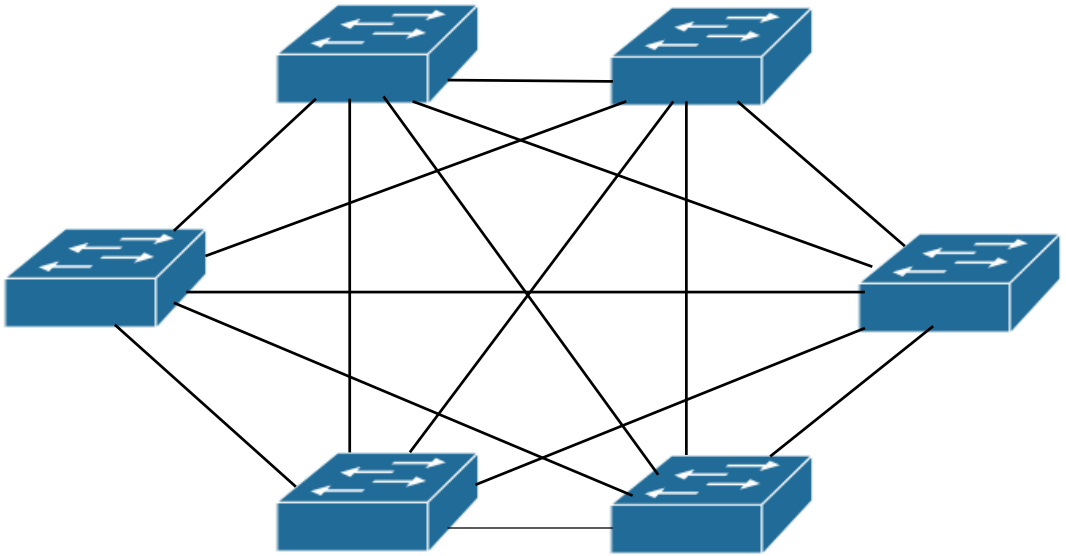




Star Topology Design

Analyzing Campus LAN Topologies

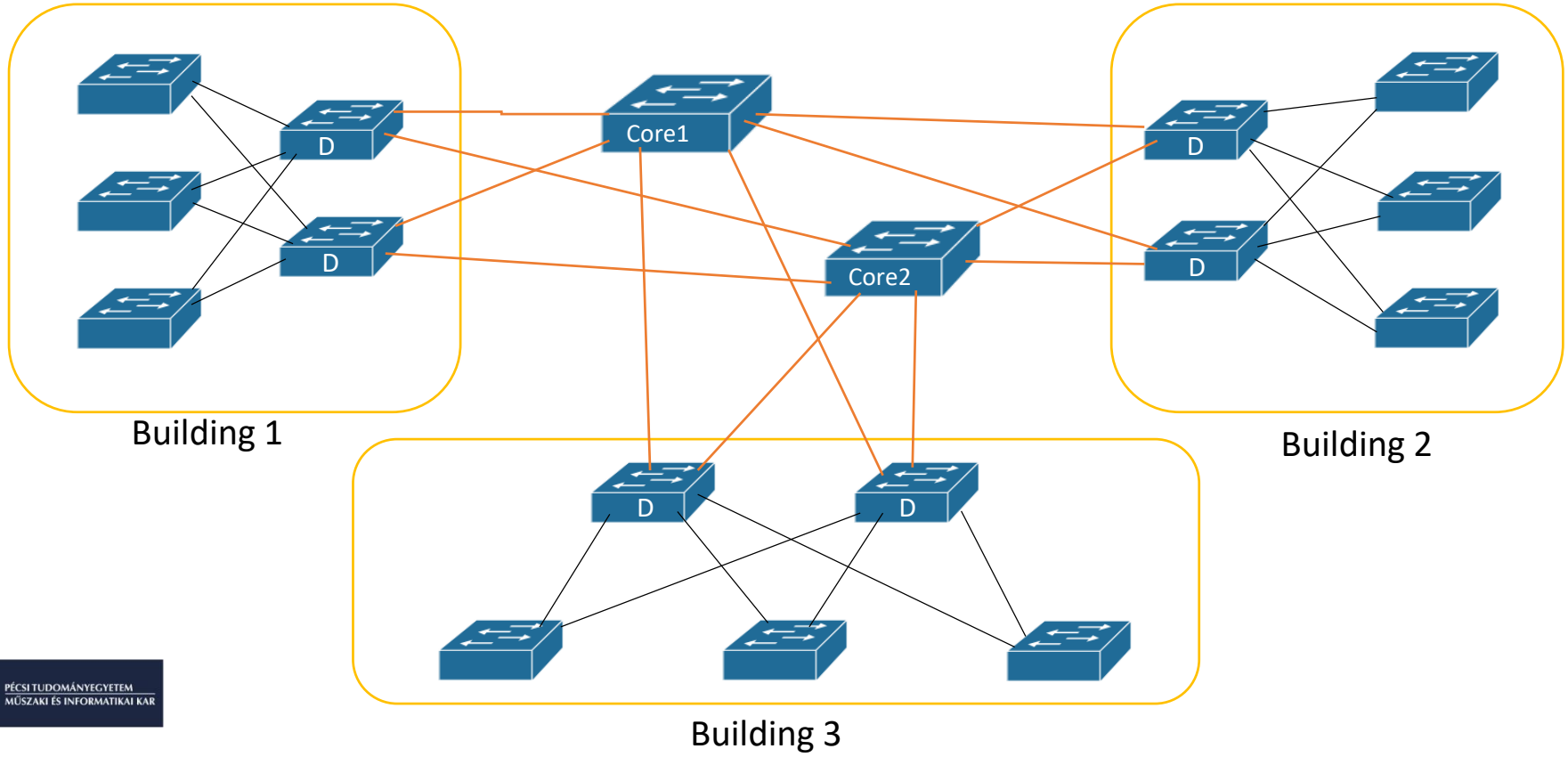
- Topology Terminology Seen Within a Two-Tier Design



Using a Full Mesh at the Distribution Layer

Analyzing Campus LAN Topologies

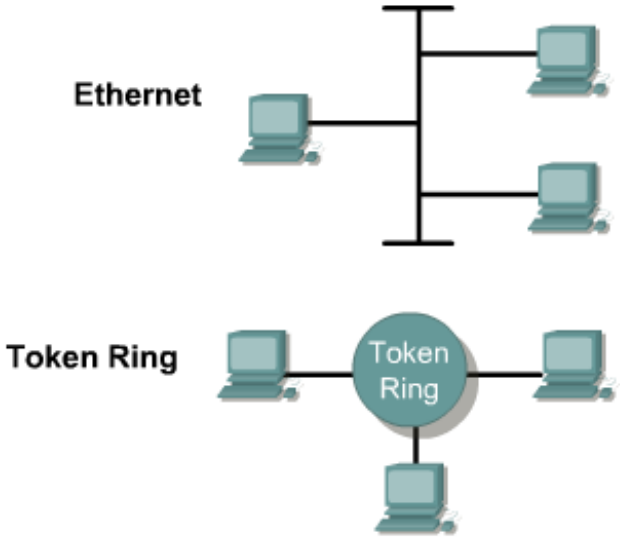
- Three-Tier Campus Design (Core)
  - Distribution + Access layer + Core



Analyzing Campus LAN Topologies

- Three-Tier Campus Design (Core)
  - Core design with full mess or partial mesh provides connection to all parts of the LAN
  - In smaller campus LANs we can use two-tier design, but in bigger ones, (with higher amount of buildings) three-tier with core switch(es) is better

Medium Access Control (MAC)



- MAC protocols
  - Deterministic
    - Collision-free
    - i.e., Token Ring
    - token rounding
  - Non deterministic
    - **Collision possible**
    - Ethernet
    - CSMA/CD

Problems (I)

- **COLLISION**
  - simultaneous transmission
  - frames go bad
  - decreased network bandwidth
  - decreased network performance

Problems (II)

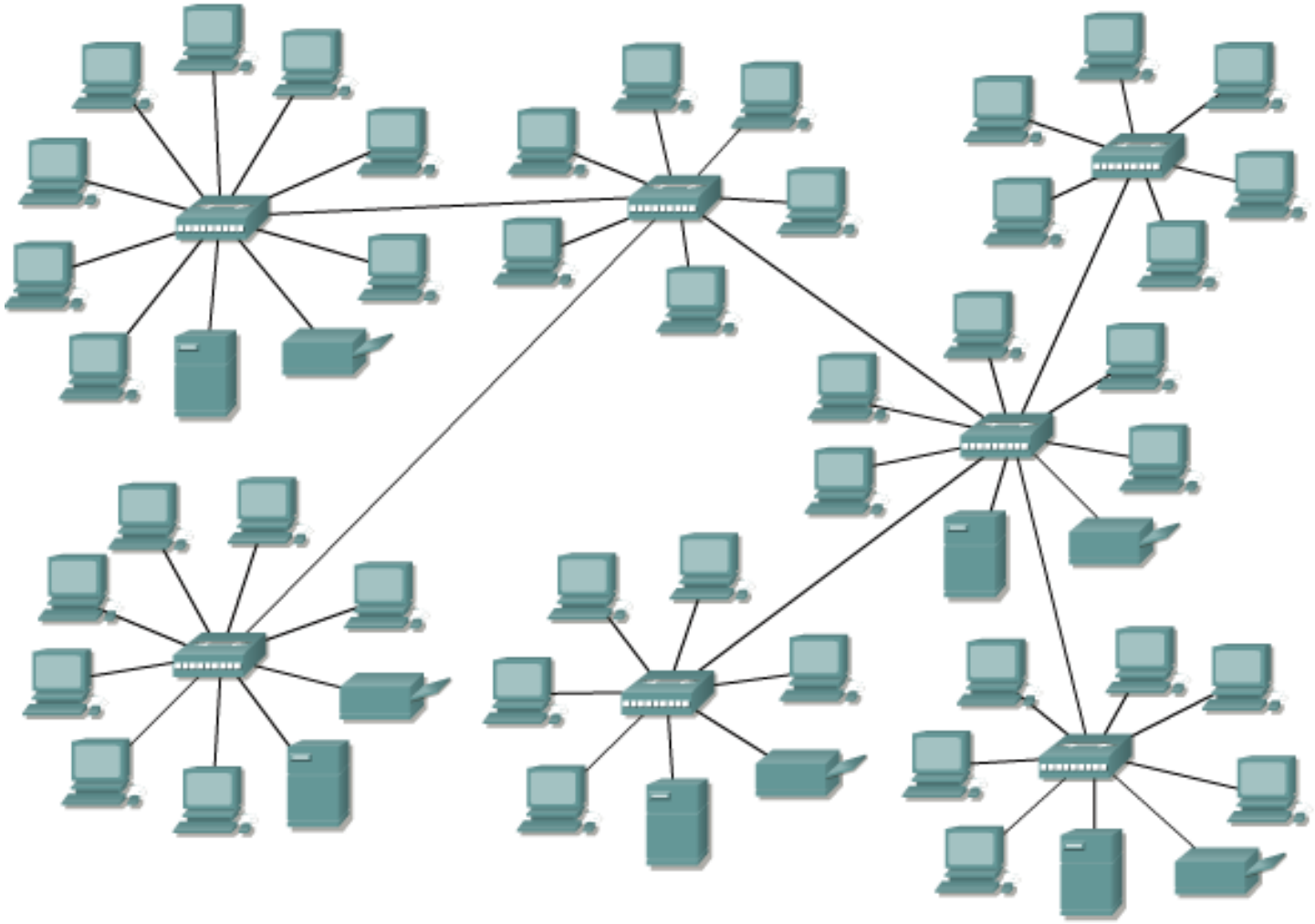
- Ethernet collisions
  - Many hosts → many collisions → slow network
  - More and more hosts→network outage

- Solution
  - making smaller collision domains
  - applying bridges and switches

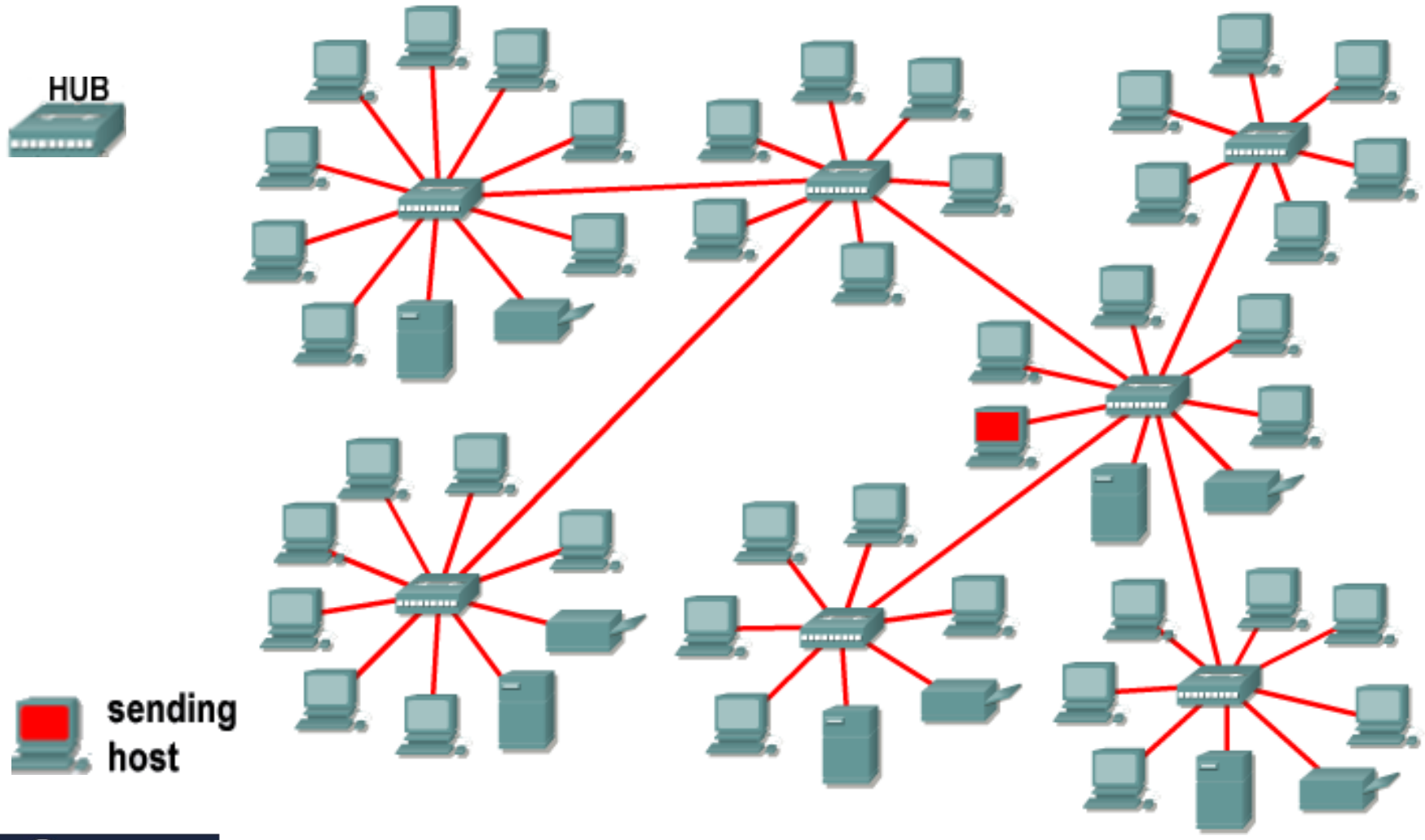
Collision domain

- **Definition.:** a connected physical network section in which collision can occur.

Collision domain



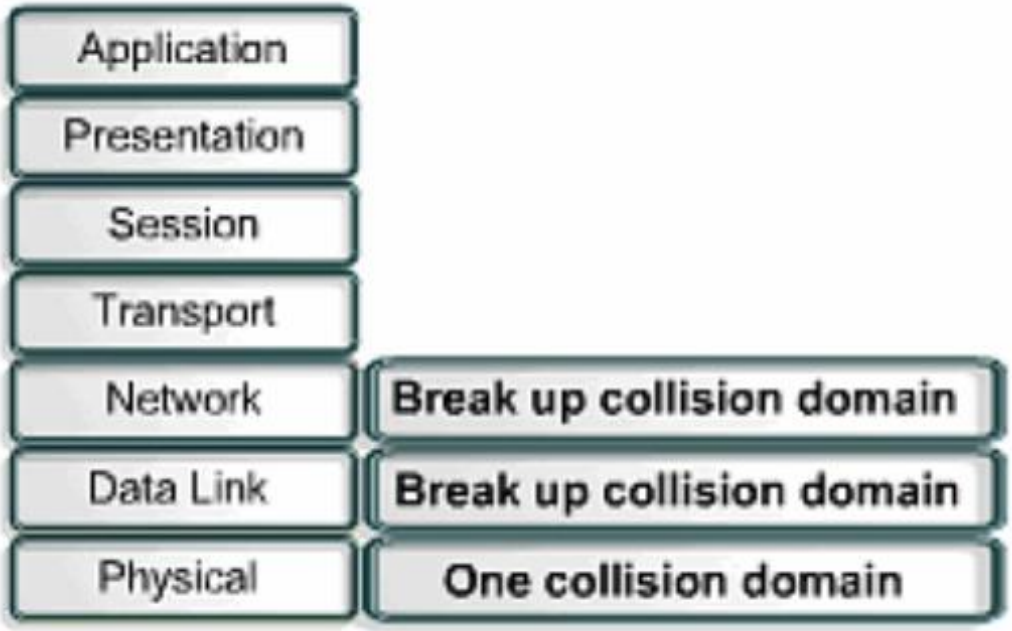
Collision domain



Collision domain

Break up by

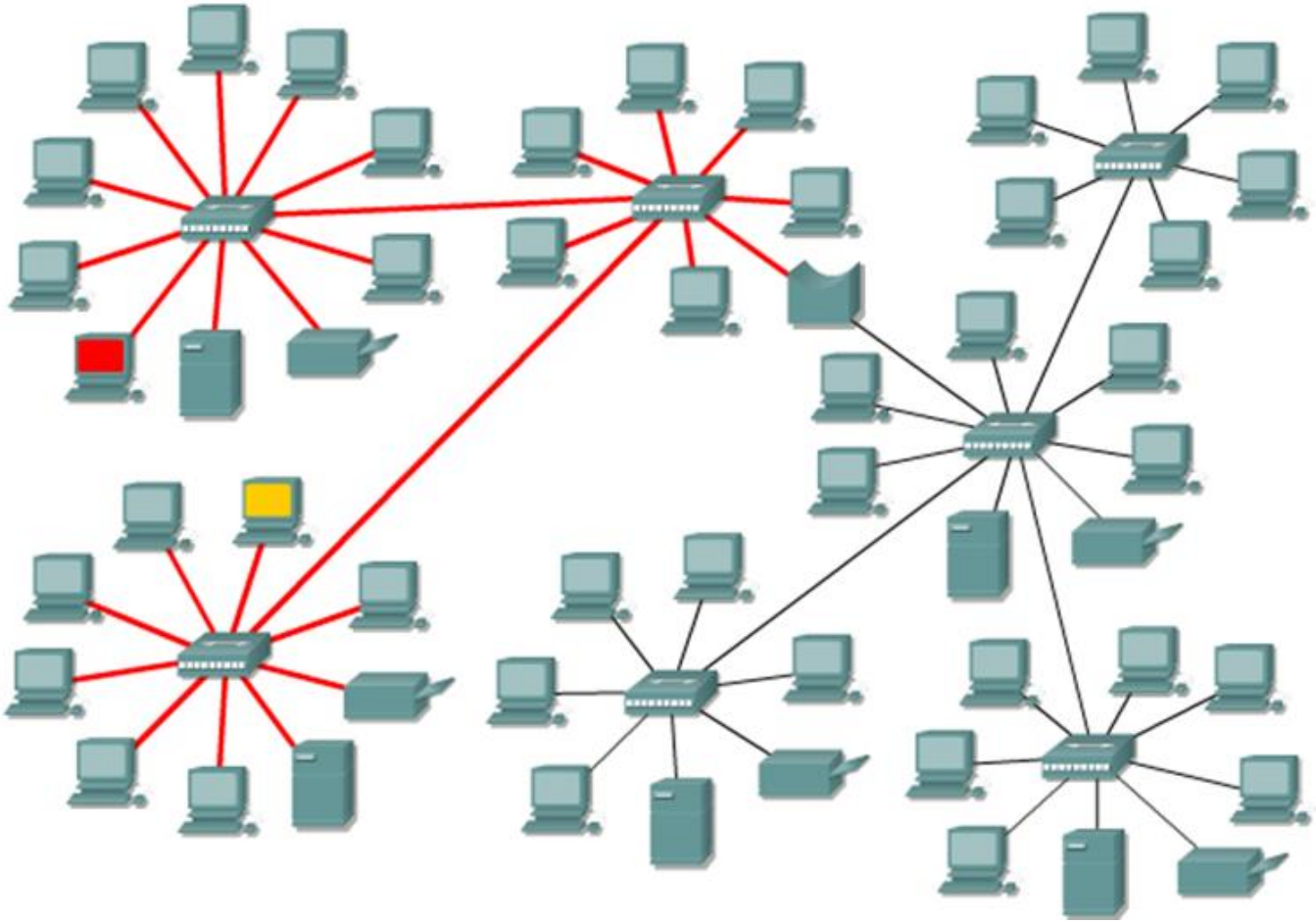
- Layer 2 devices (switch)
- Layer 3 devices (router)



Limiting the collision domain

- Segmenting the network by
  - decreasing the size of collision domains
  - increasing the number of collision domains

Segmentation



Broadcast domain

- Definition: A broadcast domain is a grouping of collision domains that are connected by layer 2 devices.
- Broadcast have to be controlled at layer3

- Addresses:
  - Unicast
  - Multicast
  - Broadcast

- A frame addressed to FF:FF:FF:FF:FF:FF (broadcast) MAC are received by all NIC's of a broadcast domain.

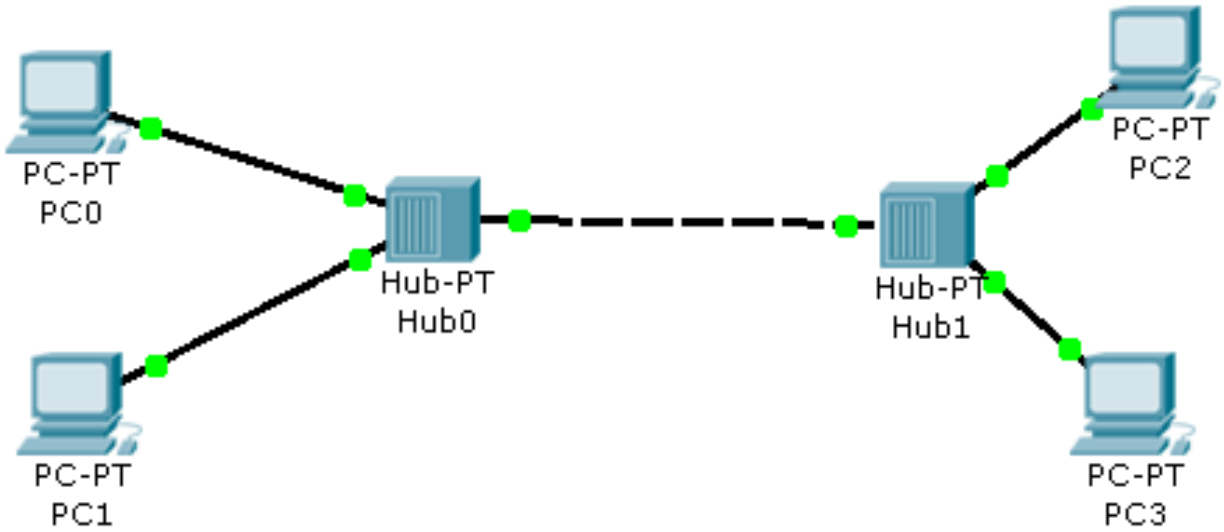
Network devices

- Repeater Layer 1
- HUB Layer 1
- Bridge Layer 2
- Switch Layer 2
- Router Layer 3

Switch = multiport bridge

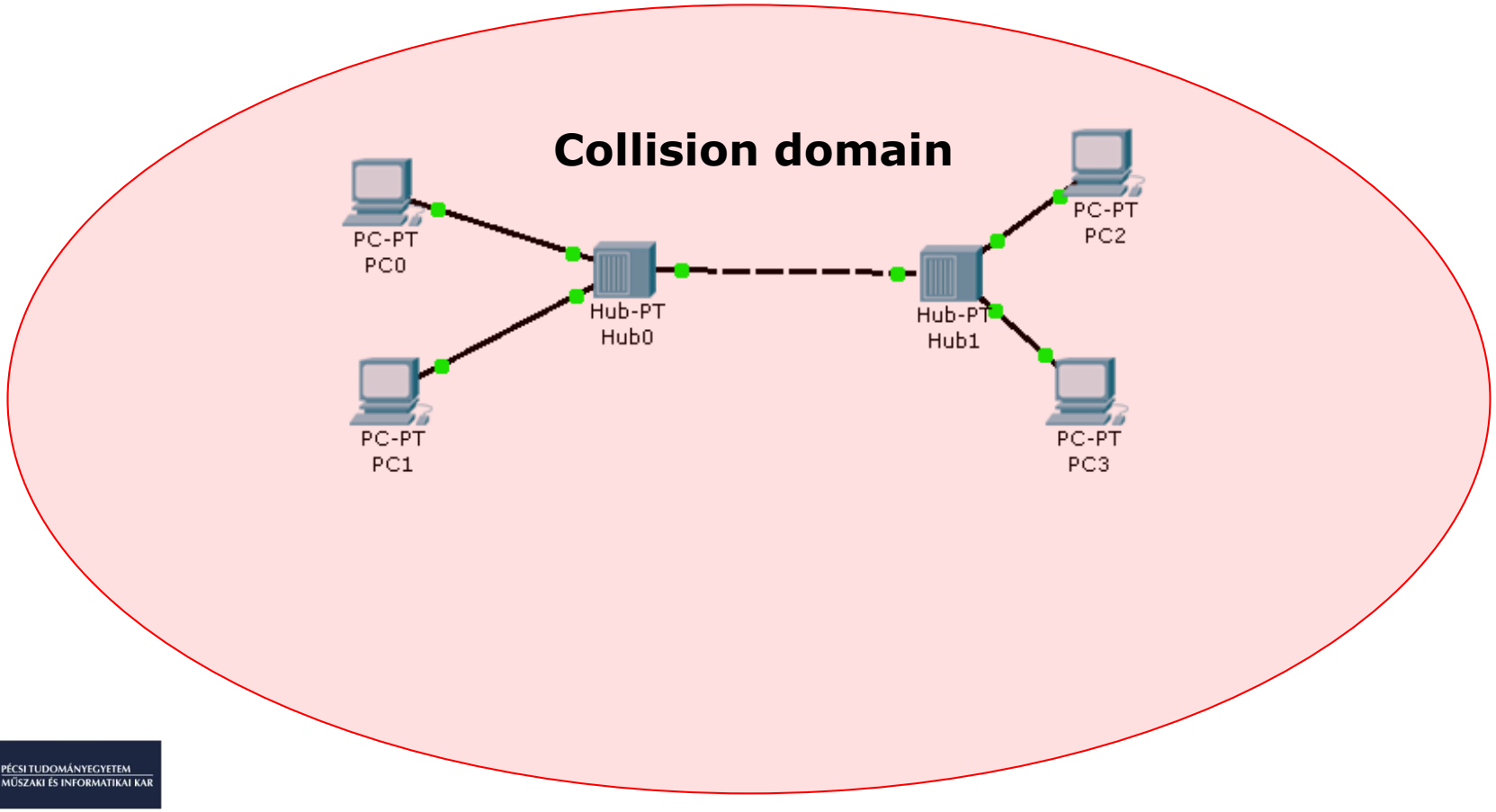
Hub

- Repeat sign on every ports (except of the incoming port)



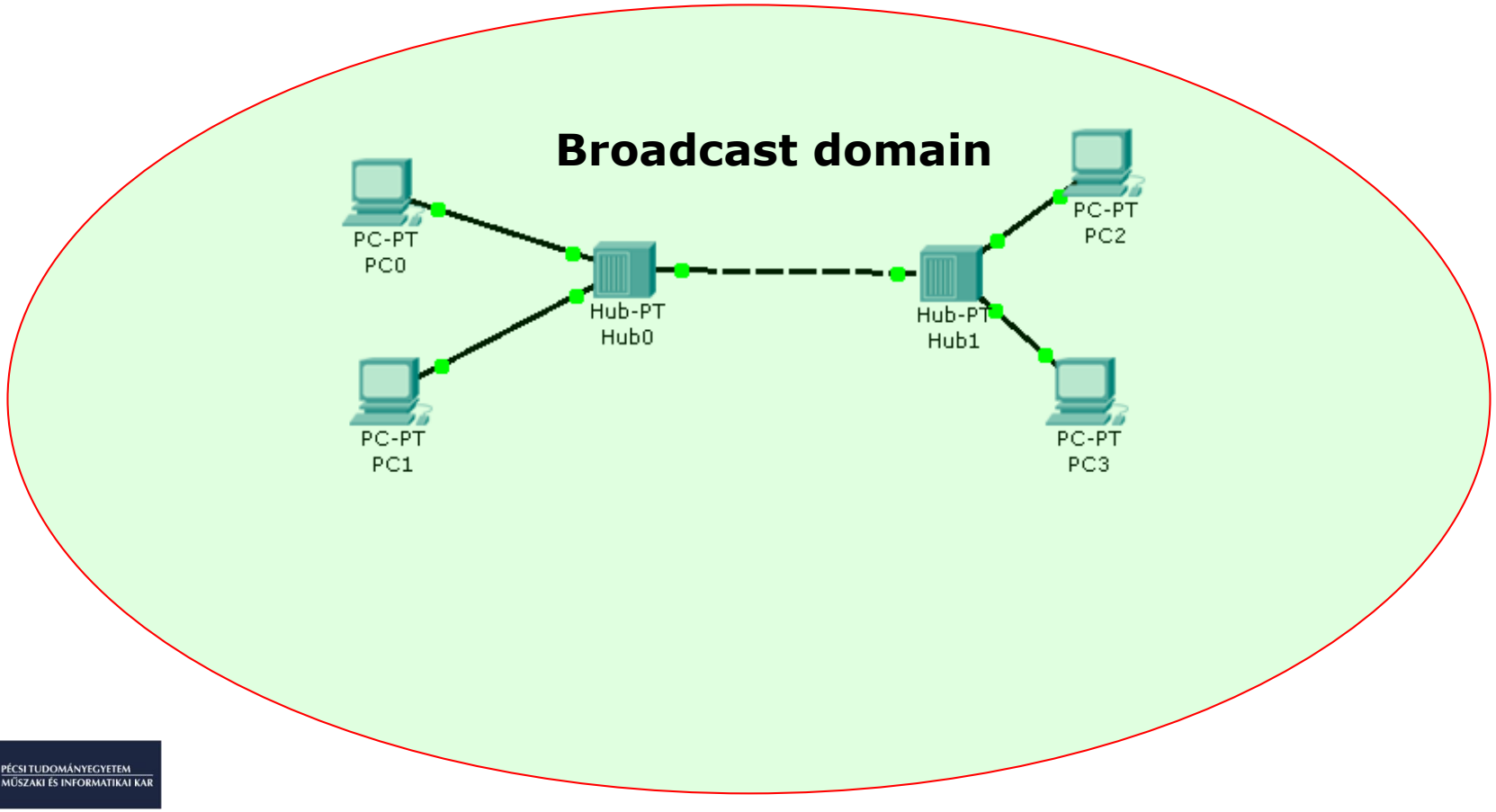
Hub

- Repeat sign on every ports (except of the incoming port)



Hub

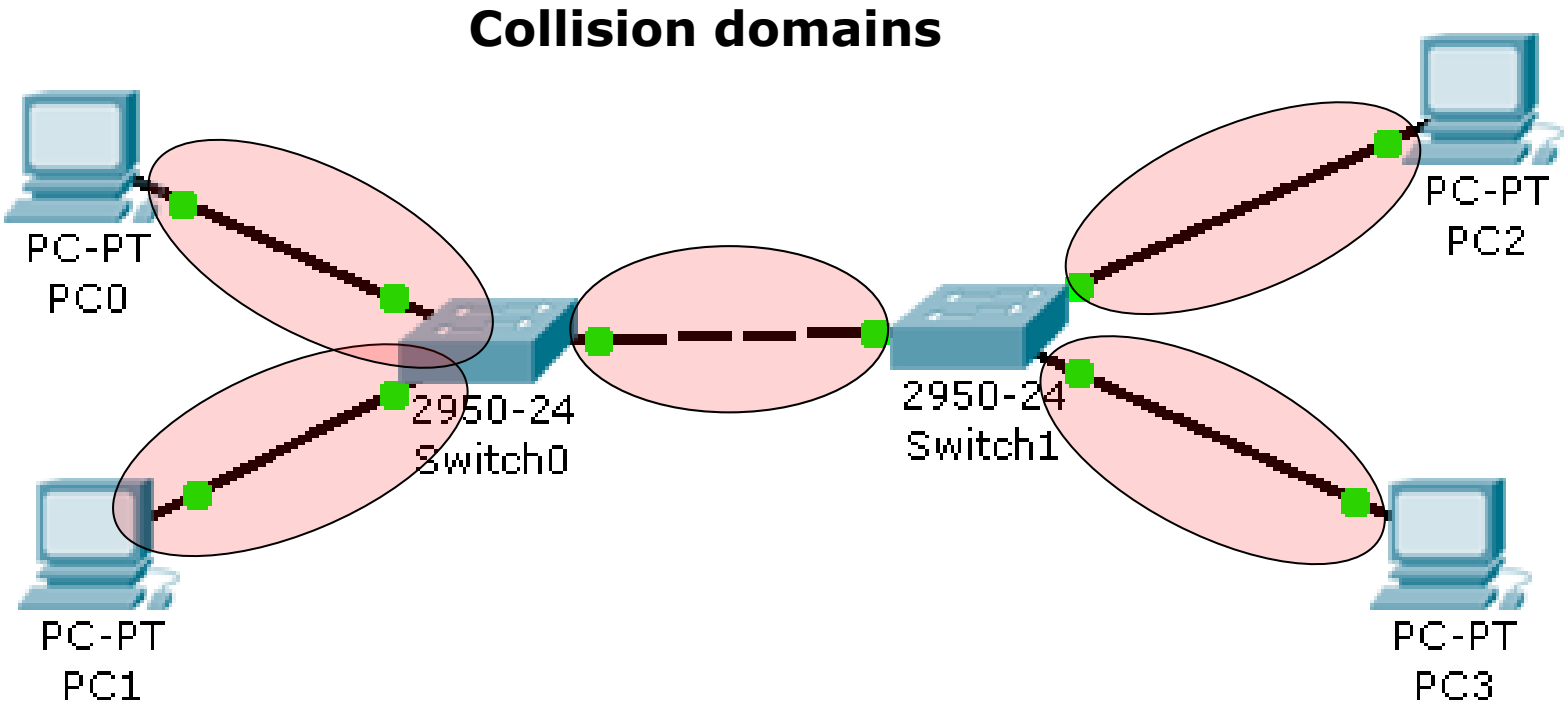
- Repeat sign on every ports (except of the incoming port)



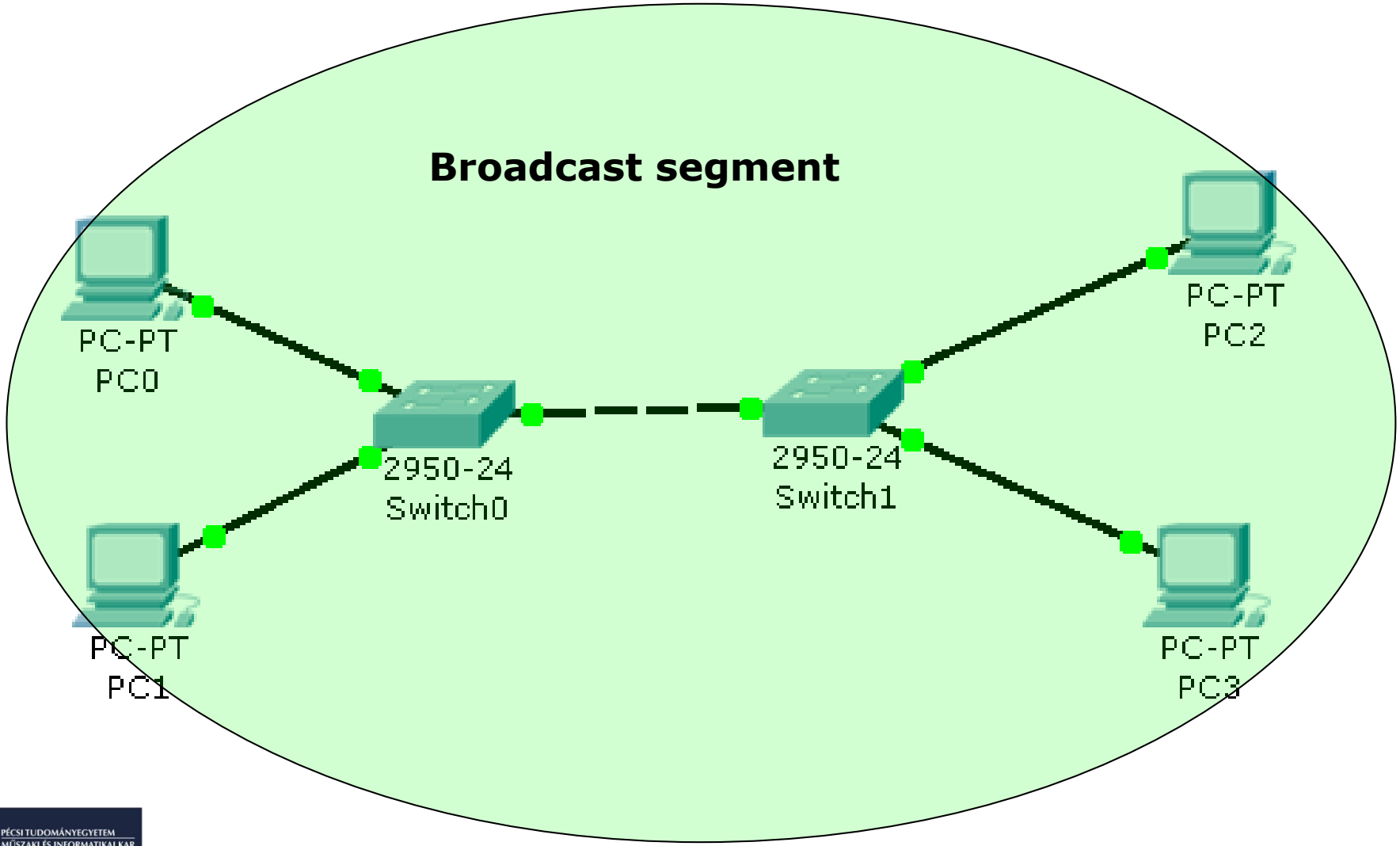
Switch

- Operating with a switching table
  - learning capability
- Reduces collision domain size, increases collision domain number
- Each port is a different collision segment

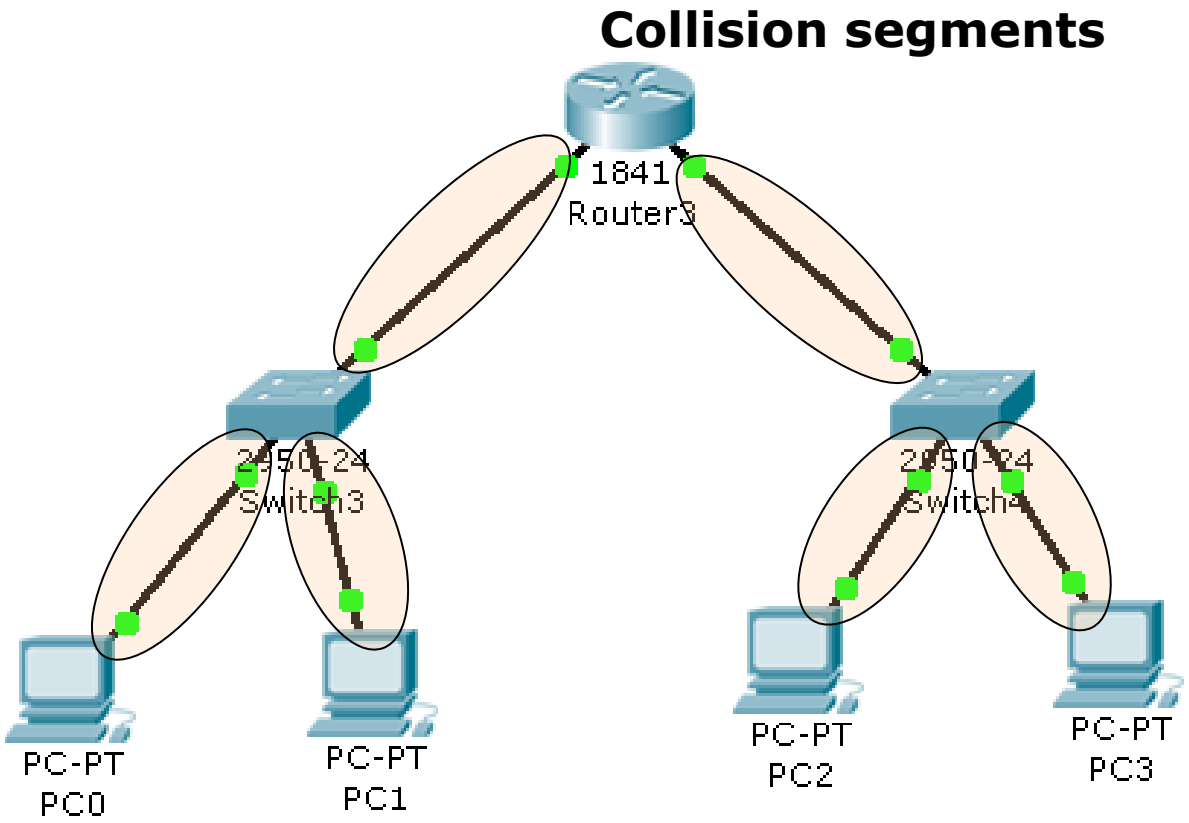
Switch


Collision domains
PC-PT
PC0
PC-PT
PC1
2950-24
Switch0
2950-24
Switch1
PC-PT
PC2
PC-PT
PC3

Switch

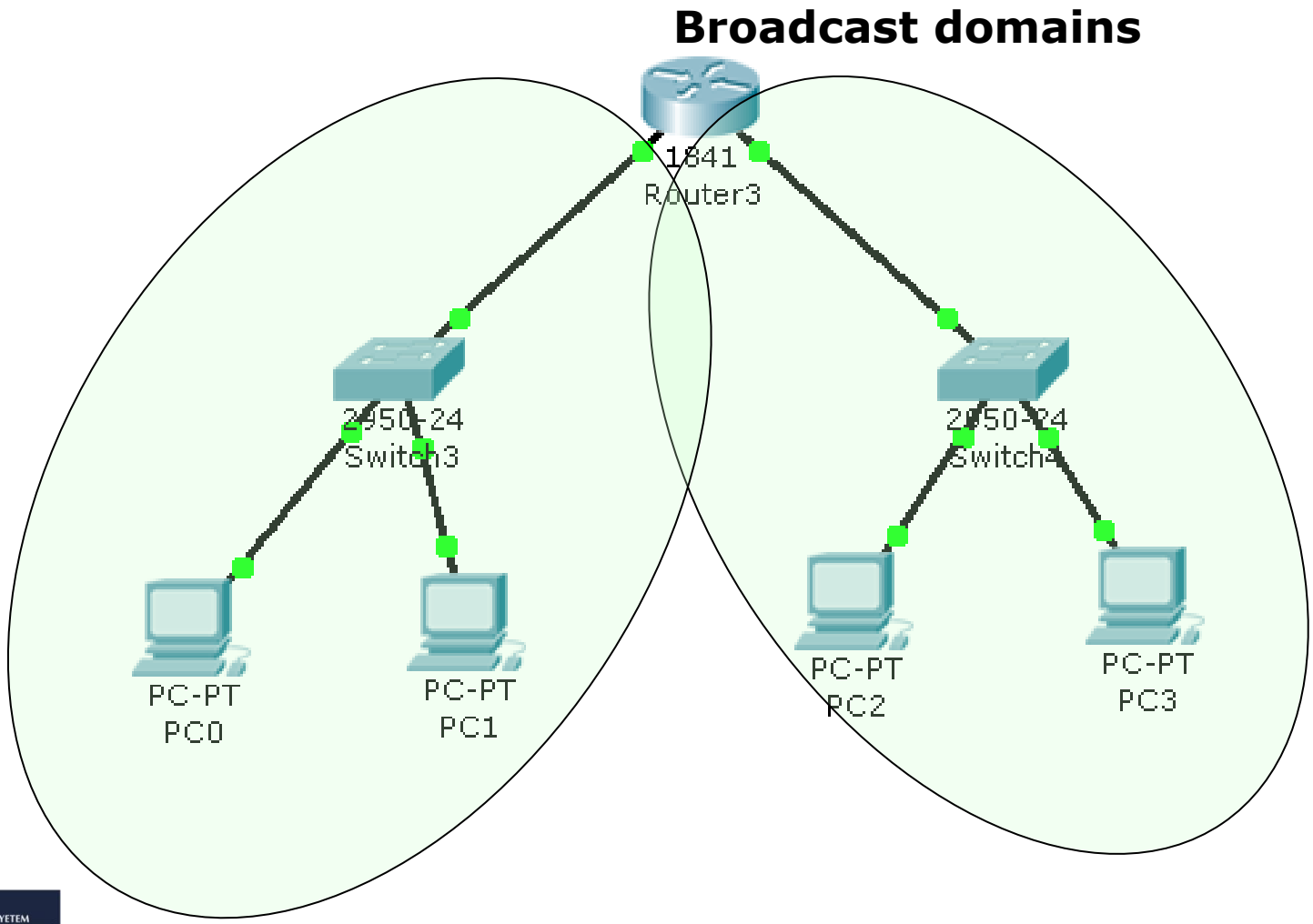


Router



Details about routers during the following labs…

Router


Broadcast domains
1841
Router3
2950-24
Switch3
2950-24
Switch4
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3

Chapter 02

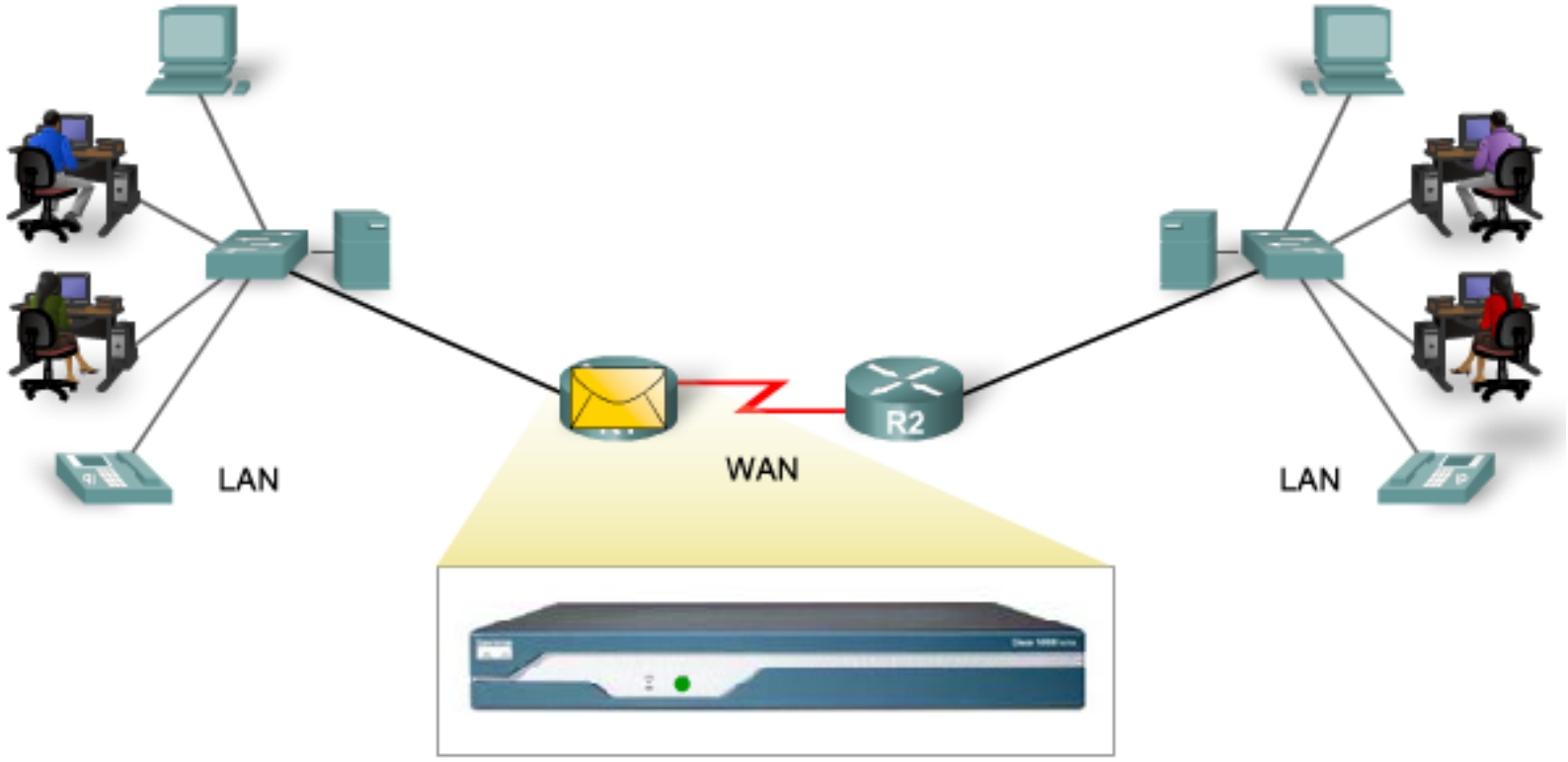
Routers

Router

- Special computer
  - designed for routing
  - similar components to PC
  - PC-Router : this is why we use crossover cable

Functions

- Connecting different networks
- Control (to route) packets between networks



Functions

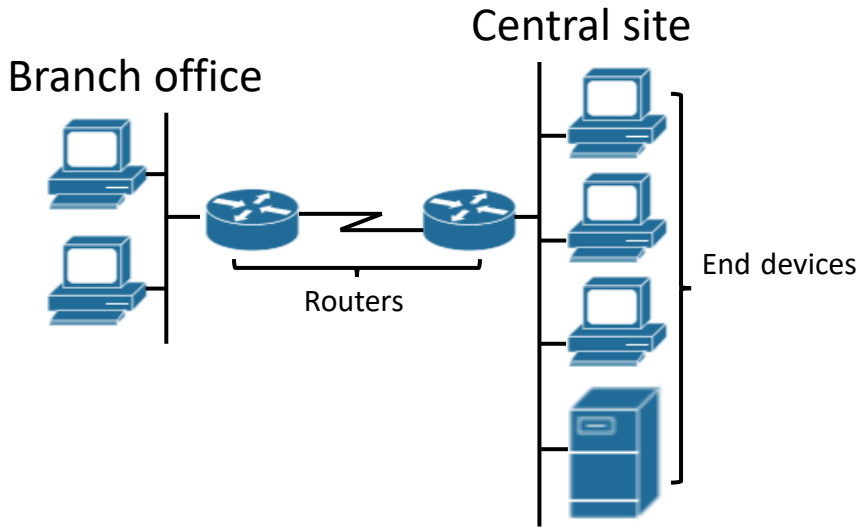
- Determine the best route between networks and forward packets
  - according to the routing table


```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 is directly connected, Serial0/0/0
```

Routing table is
similar to a map which shows
the best way to the destination

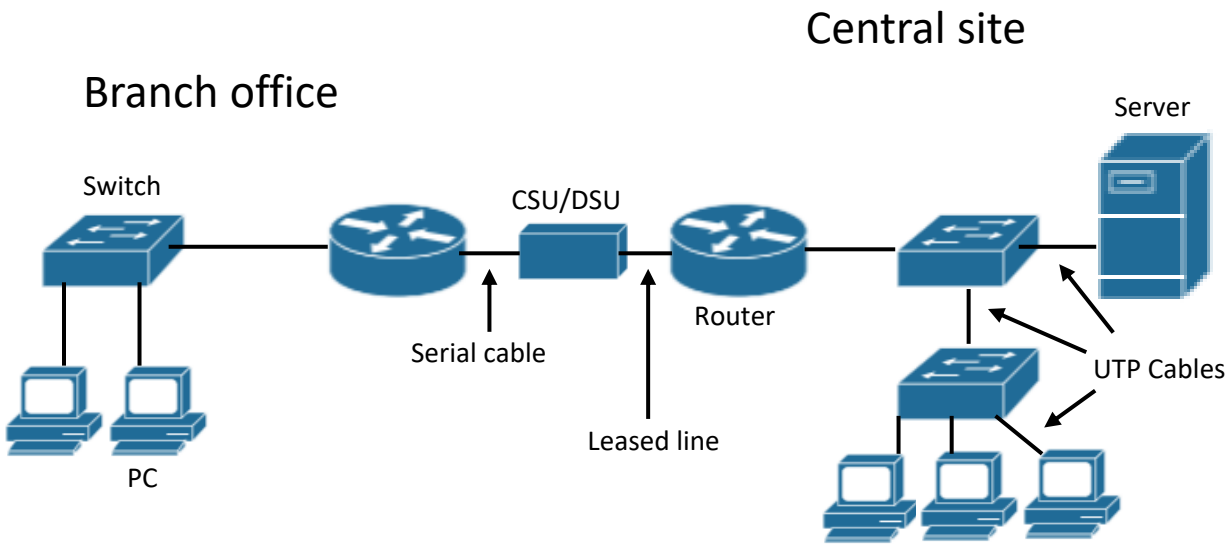
Topology

- Installing Routers
  - Routers are the most important devices of the network layer
  - Enterprise network
    - A few number of centralized sites
    - Plenty of smaller remote sites



Topology

- Installing Routers
  - Enterprise network (more detailed)



Cisco 2911 router family

Front panel

ON/OFF button

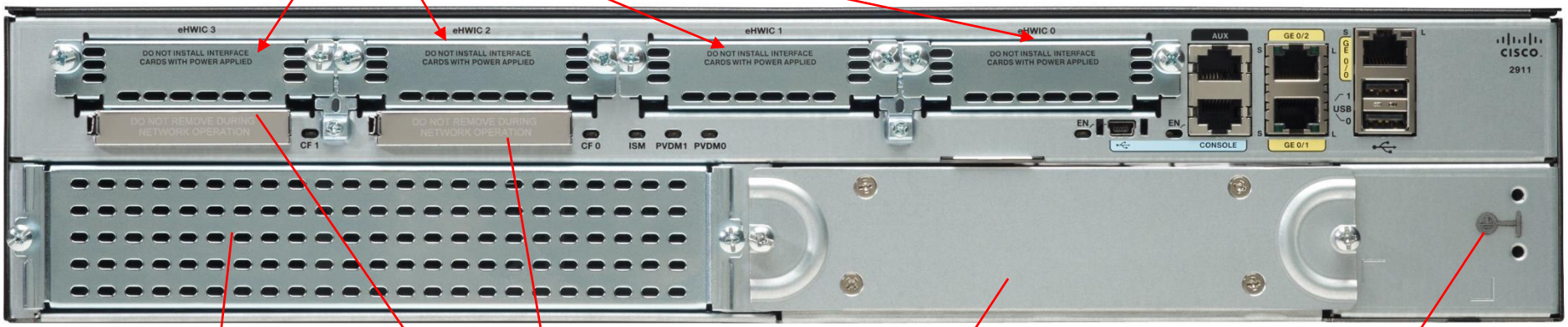
Power LED

System Activity LED

Power connector

Back panel

eHWIC (Enhanced High Speed WAN Interface Slot)



Service Module
(ISM or PVDM)

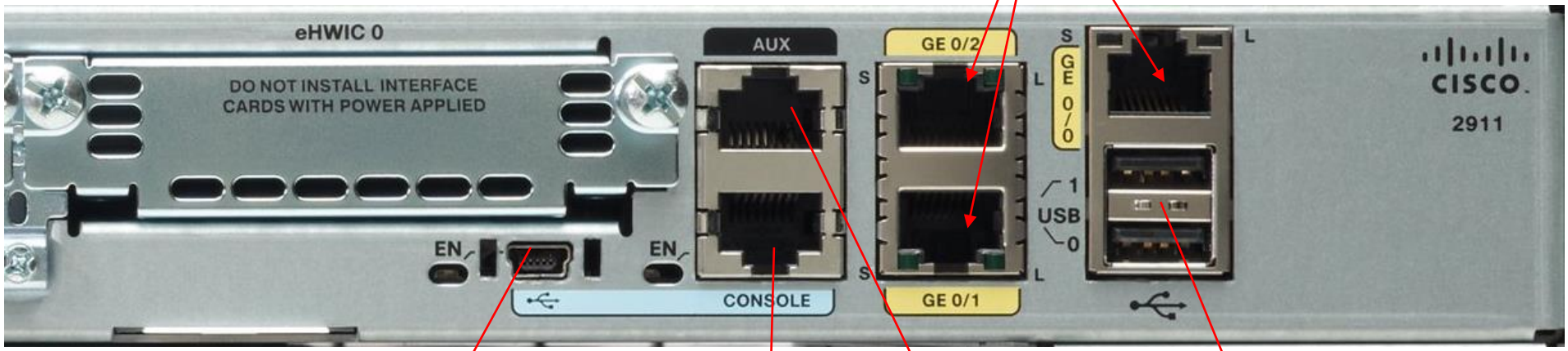
CompactFlash

Power Module

Grounding

(ISM: Integrated Services Module, PVDM: Packet Voice and Video Digital Signal Processor Module)

Back panel



GigabitEthernet ports

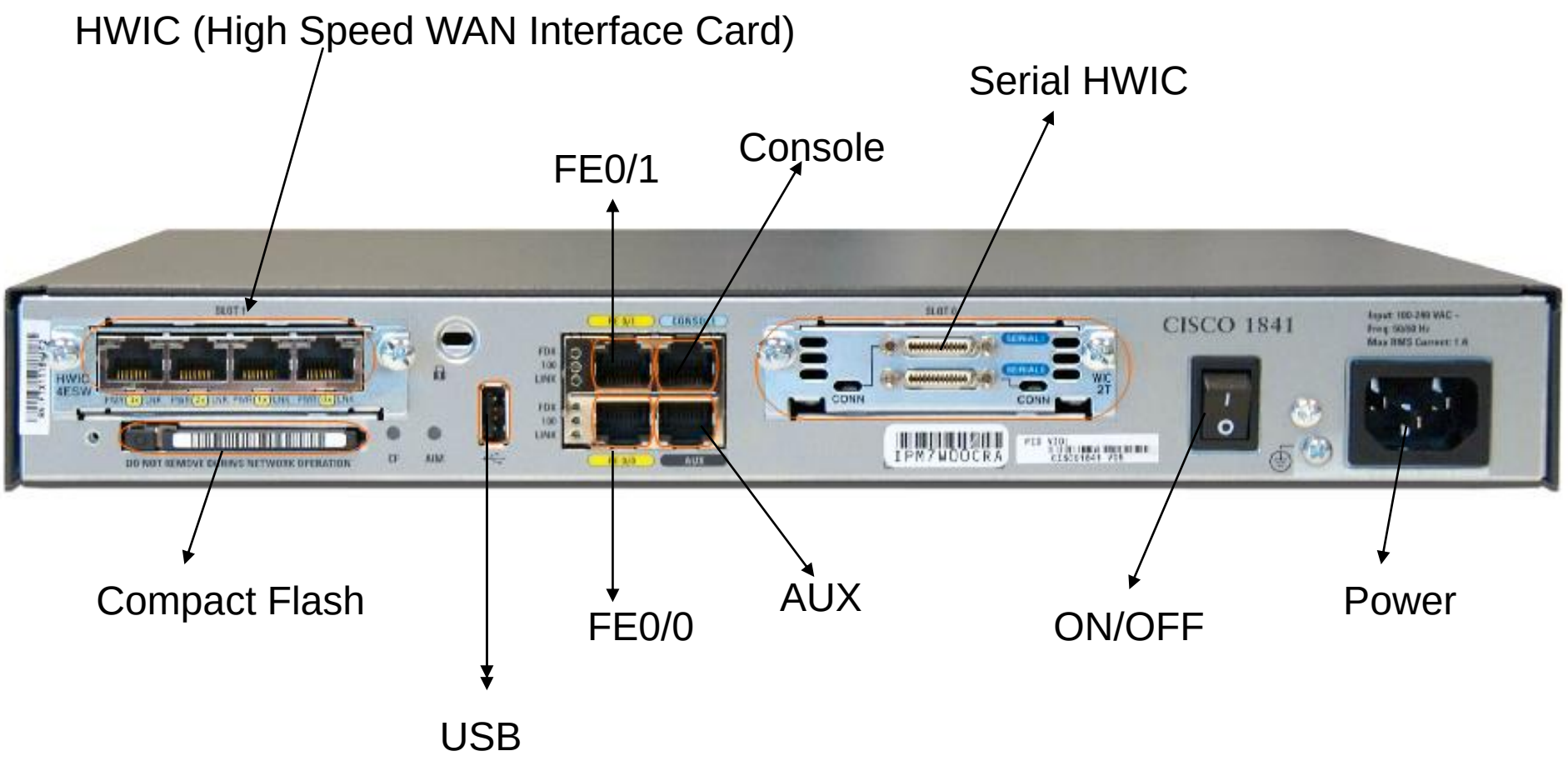
USB console

RJ45 console

AUX

USB

Cisco 1841 back panel



Modular architecture

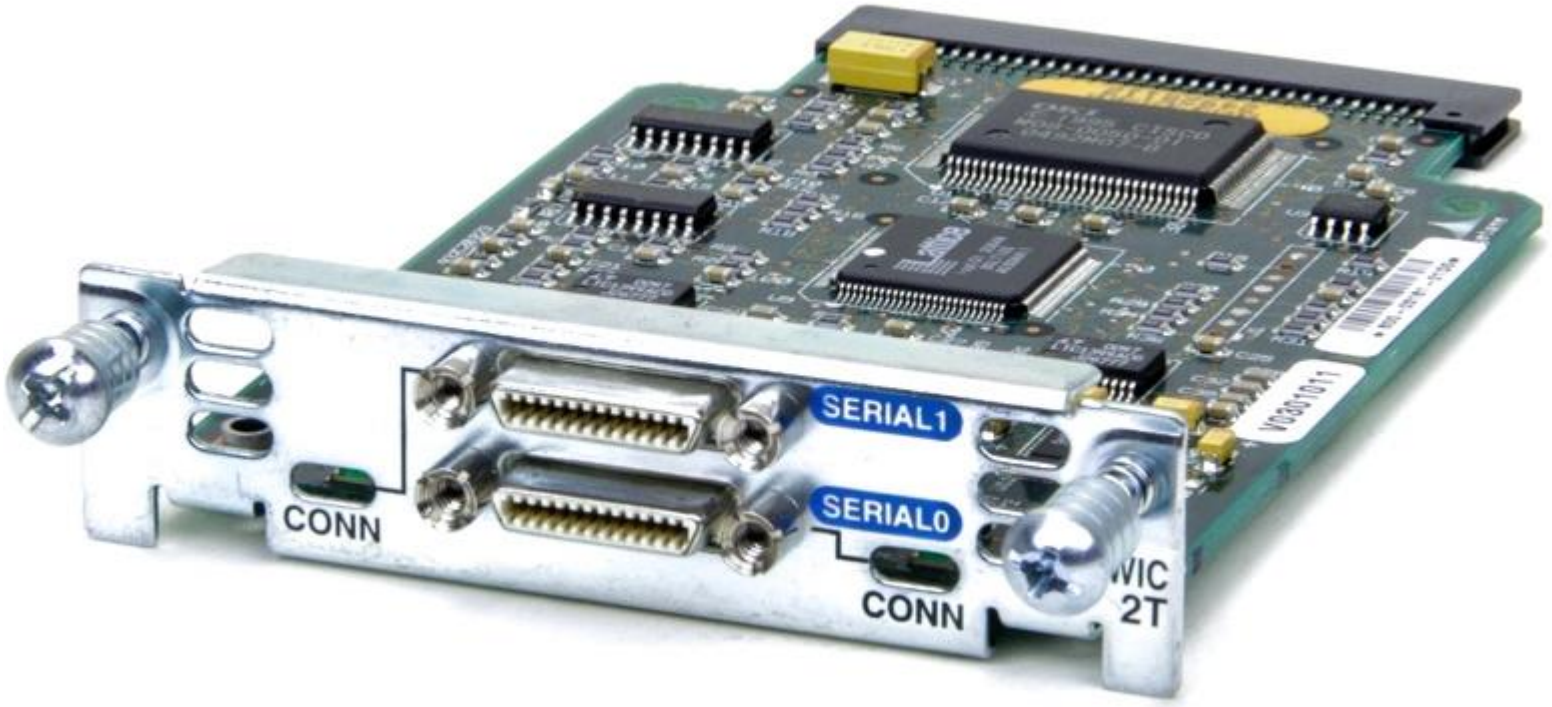
- NM-1FE-TX (Fast Ethernet interface card)

Modular architecture

- WIC1T (Serial interface card)

Modular architecture

- WIC2T (Serial interface card)



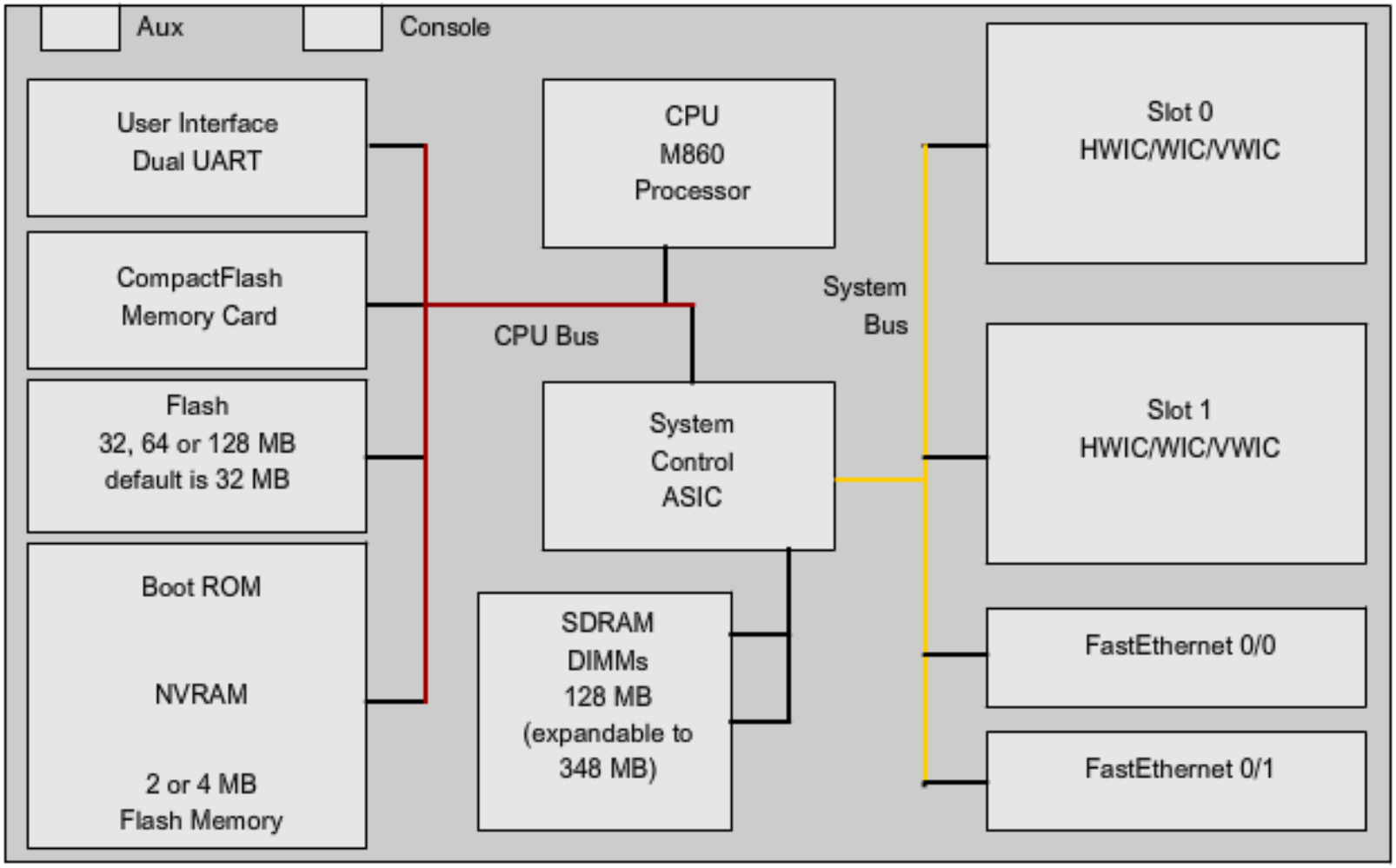
Modular architecture

- EHWIC-1GE-SFP-CU (Optical interface)

SFP (Small Form-factor Pluggable)

Router inside

Logical architecture



Hardware elements

- CPU
  - processing unit
- RAM
  - volatile memory
  - running OS
  - actual configuration (running-config)
  - routing table
  - buffers

Hardware elements

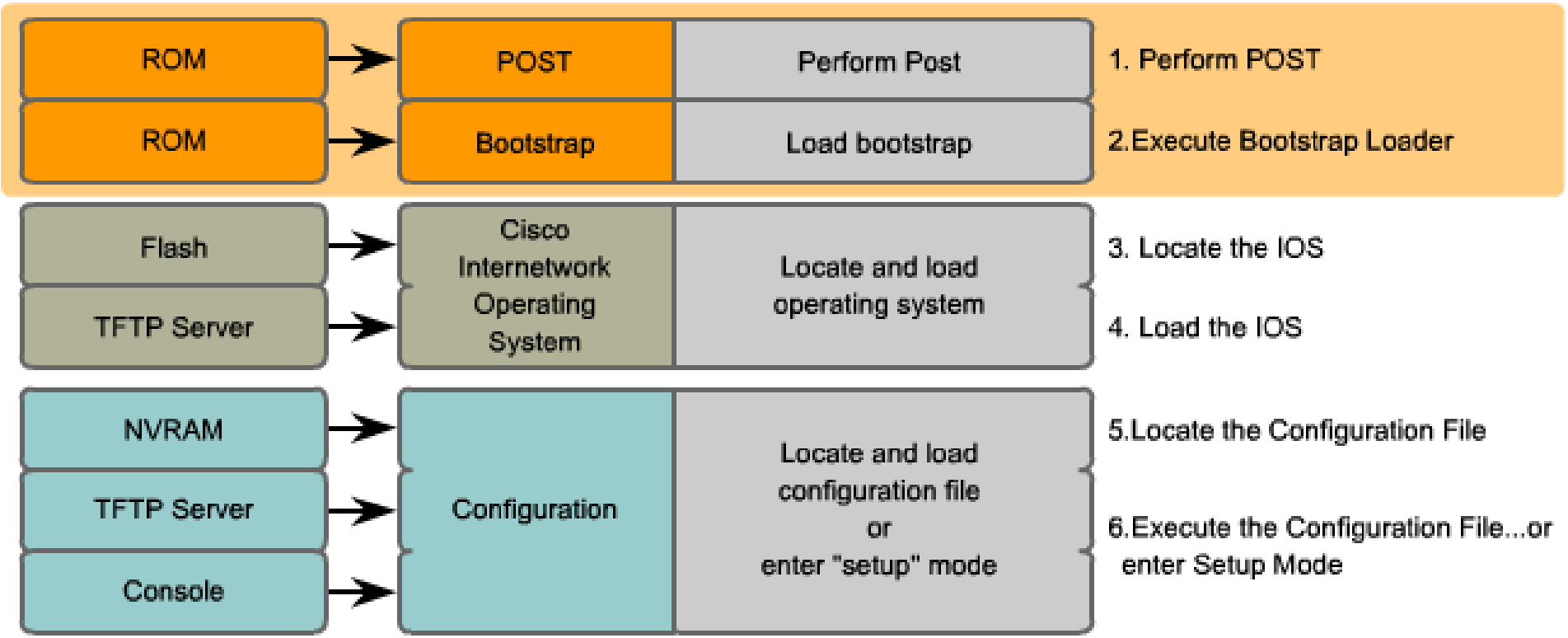
- ROM
  - Non-volatile memory
  - bootstrap program
  - diagnostic programs
  - minimal OS
- FLASH memory
  - OS
- NVRAM
  - saved configuration files (startup-config)

Operating System

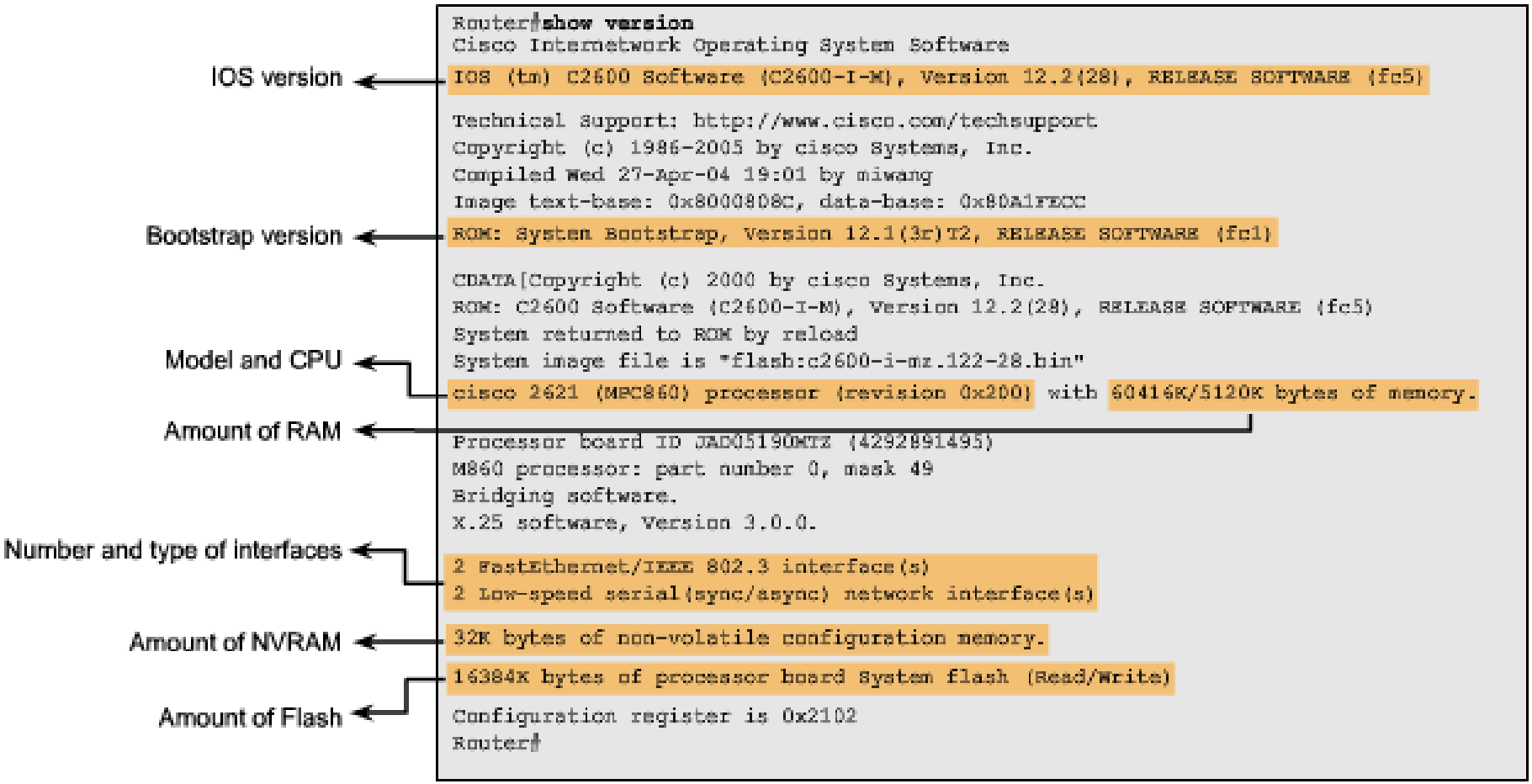
IOS

- **I**nternetwork **O**perating **S**ystem
  - Developer: Cisco Systems
  - Proprietary code
  - Versions
    - v15
    - v12
    - older
  - Interface
    - CLI, Command Line Interface
    - sometimes GUI is available

Boot process



Power on self test information



Router programming

- Using CLI interface
- Configuration modes
  - User execution mode
    - `Router>`
    - only limited operations possible
  - Privileged execution mode
    - `Router#`
    - you can config the router here
  - User exec mode → Privileged execution mode
    - `enable`

Router programming

- IOS assistance
  - ?
  - TAB
  - command recall (up arrow)

  - Command interrupt
    - Ctrl+break → in reality
    - Ctrl+shift+6 → in Packet Tracer

Basic configuration

Router# configure terminal → GLOBAL Configuration mode

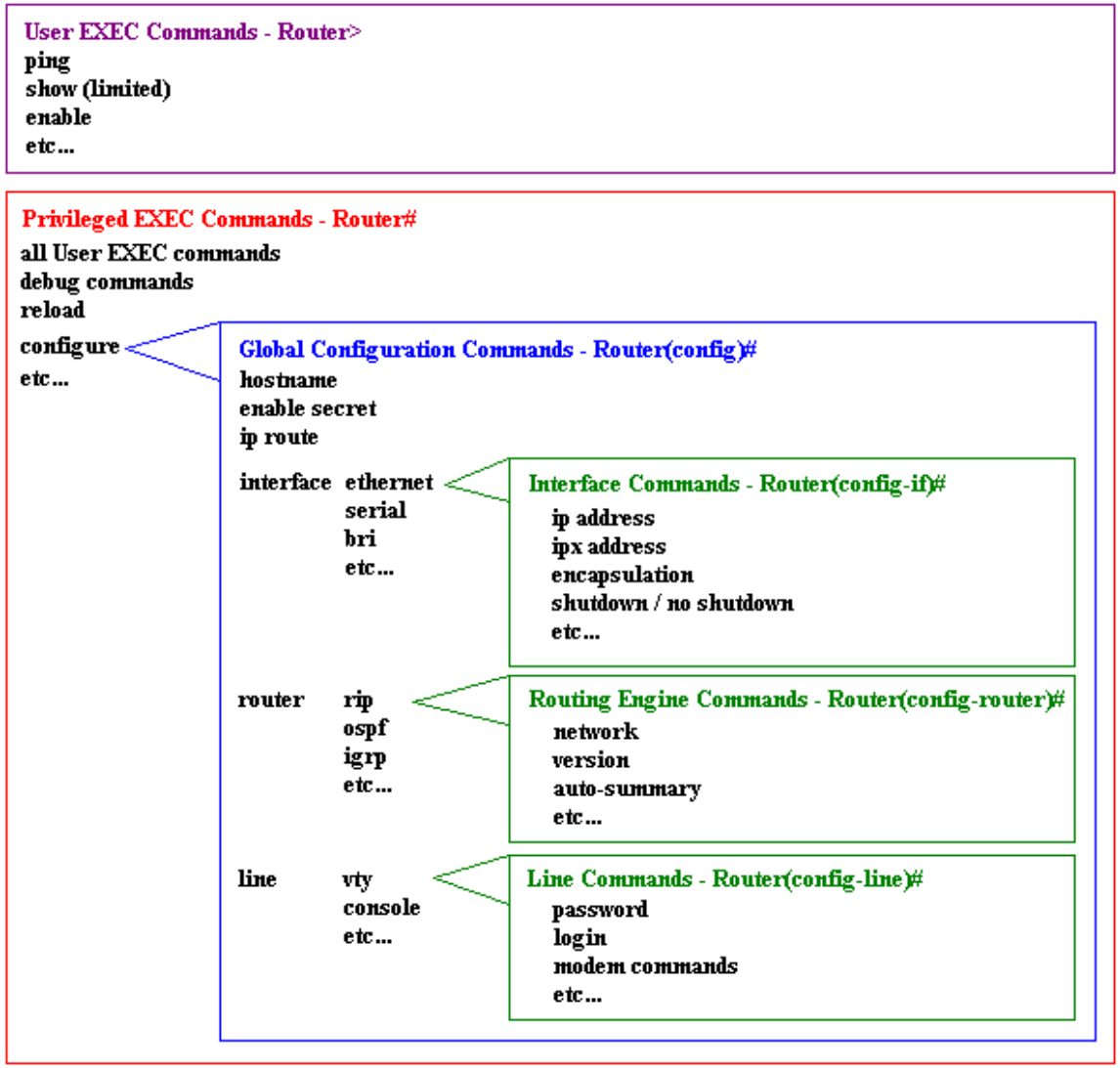
Basic Router Configuration Command Syntax	
Naming the router	`Router(config)#hostname name`
Setting Passwords	`Router(config)#enable secret password`
	`Router(config)#line console 0`
	`Router(config-line)#password password`
	`Router(config-line)#login`
	`Router(config)#line vty 0 4`
	`Router(config-line)#password password`
	`Router(config-line)#login`
Configuring a message-of-the-day banner	`Router(config)#banner motd # message #`

Interface configuration

Basic Router Configuration Command Syntax	
Configuring an interface	`Router(config)#interface type number`
	`Router(config-if)#ip address address mask`
	`Router(config-if)#description description`
	`Router(config-if)#no shutdown`
Saving changes on a router	`Router#copy running-config startup-config`
Examining the output of **show** commands	`Router#show running-config`
	`Router#show ip route`
	`Router#show ip interface brief`
	`Router#show interfaces`

Type e.g., FastEthernet0/0 … GigabitEthernet0/1 … Serial0/0/2

Configuration modes



Configuration summary

Basic router config steps

1. Naming the router
2. Set passwords (console, vty, enable)
3. Ensure access (console, vty)
4. Config interfaces
5. Save configuration
6. Check configuration

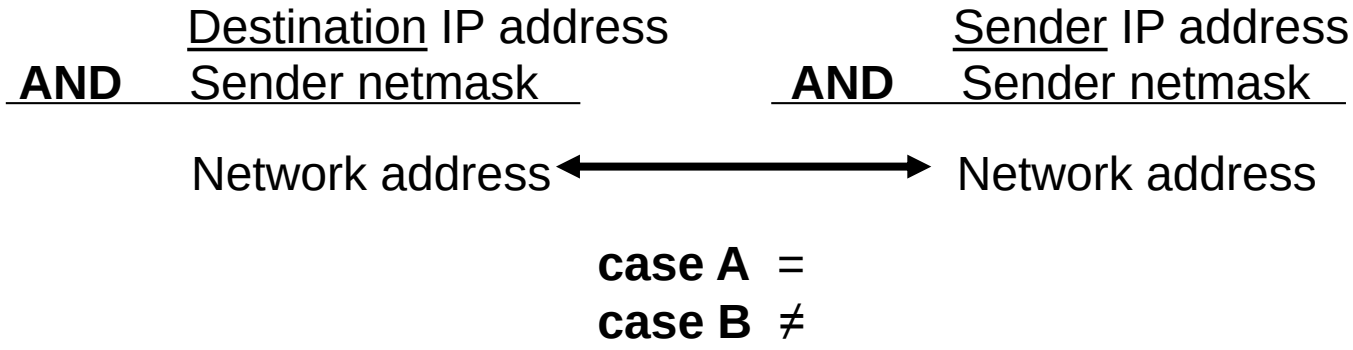
Chapter 03

Routing

Host communication

- Two possibilities
  - Partners are in same (sub)net (A)
  - Partners are in different (sub)net (B)

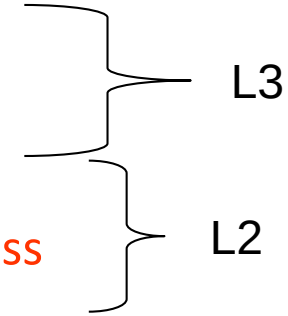
- How to determine A or B?



(A) Same subnet partners

- (1)Sending host finds the MAC of the destination
  - read it from his own ARP table or
  - use the ARP mechanism to resolve the IP to MAC

- (2)Build and send a packet into the network
  - Addressing
    - Source IP address
    - Destination IP address
    - Source MAC address
    - Destination MAC address

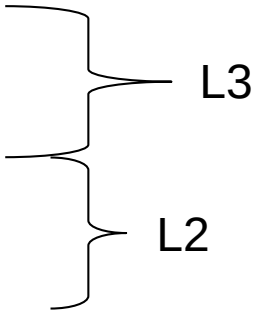


(B) Different subnet partners

- Sender address the frame to the default gateway, who'll forward it to the appropriate destination

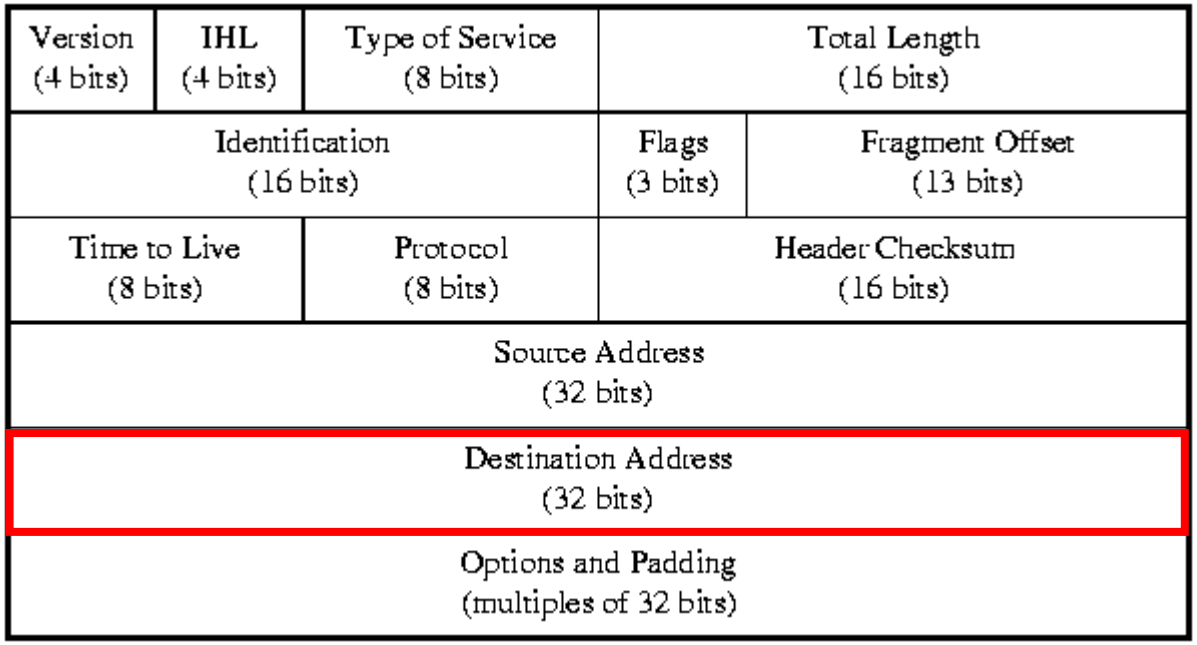
- (1)Sending host finds the MAC of the gw
  - same process as we saw before

- (2)Sends frame into the network
  - Addressing
    - Source IP
    - Destination IP
    - Source MAC
    - Default gateway MAC

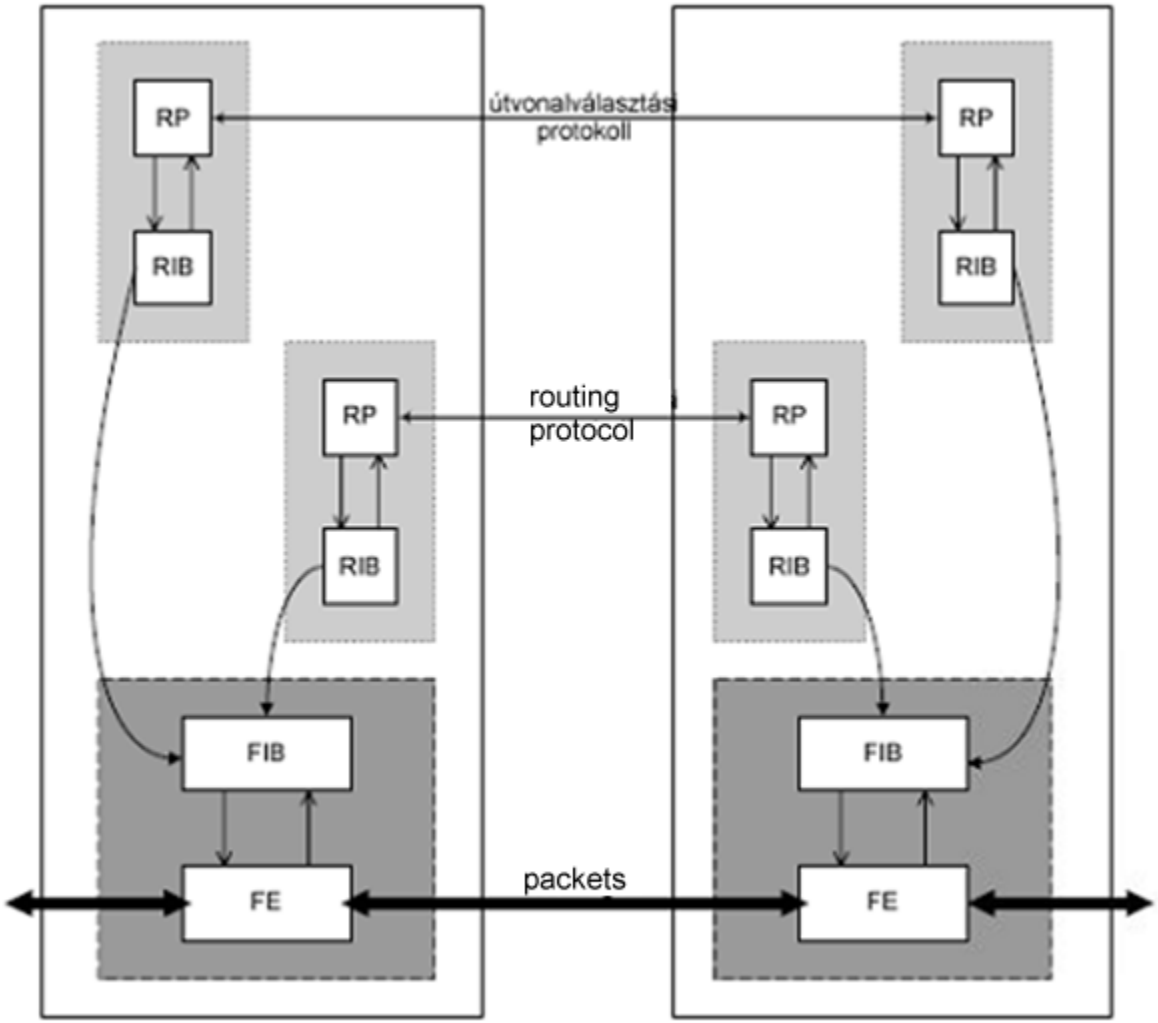


Communication between networks

- Router is needed
  - Forwarding packets towards to the destination
    - IP packet (destination IP address) → it is routed
    - Routing table → routing information

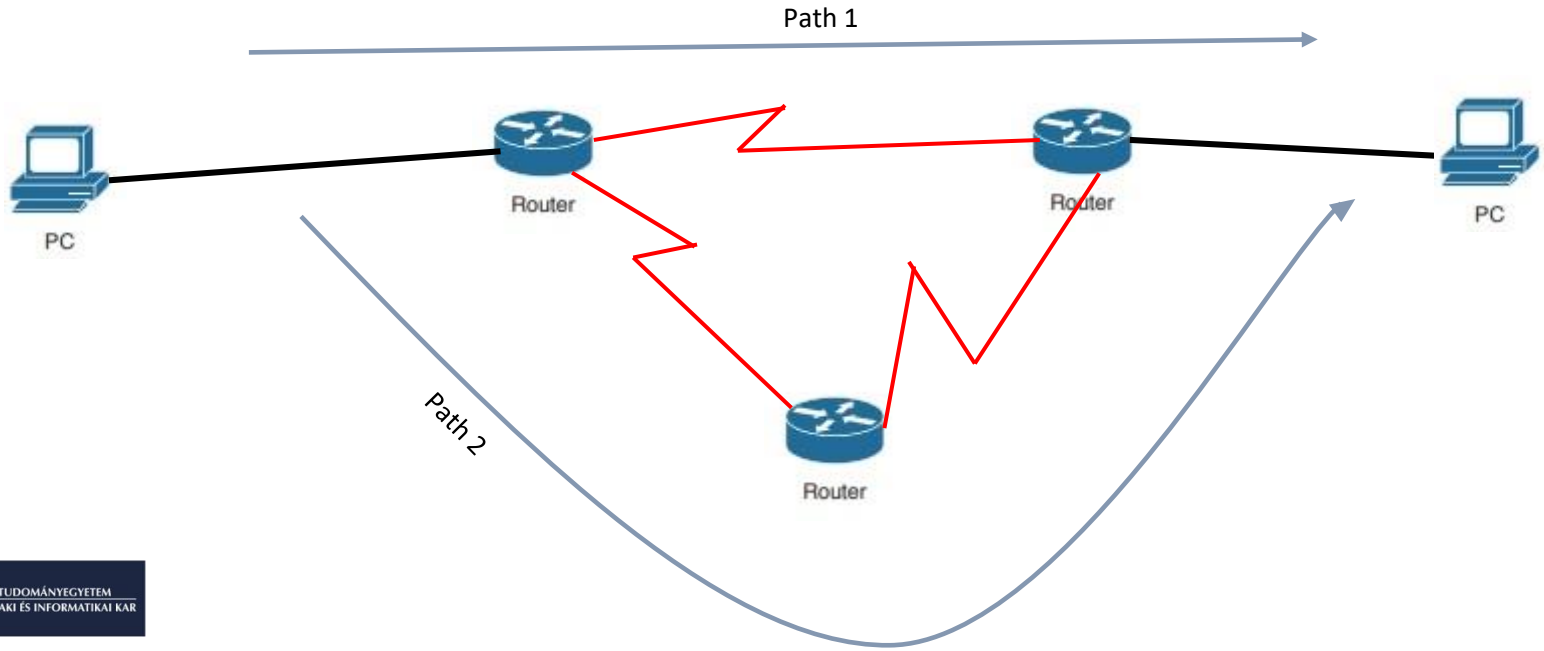


Routing process



What is routing?

- Routing is the process of selecting a path for traffic in a network, or between or across multiple networks.

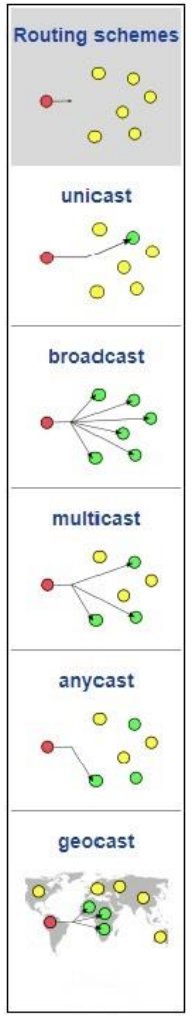


What is routing?

- Routing is performed for many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), computer networks, such as the Internet.
- Routing technologies manage the flow of data (IP packets) between network segments, which are also known as *subnets*.

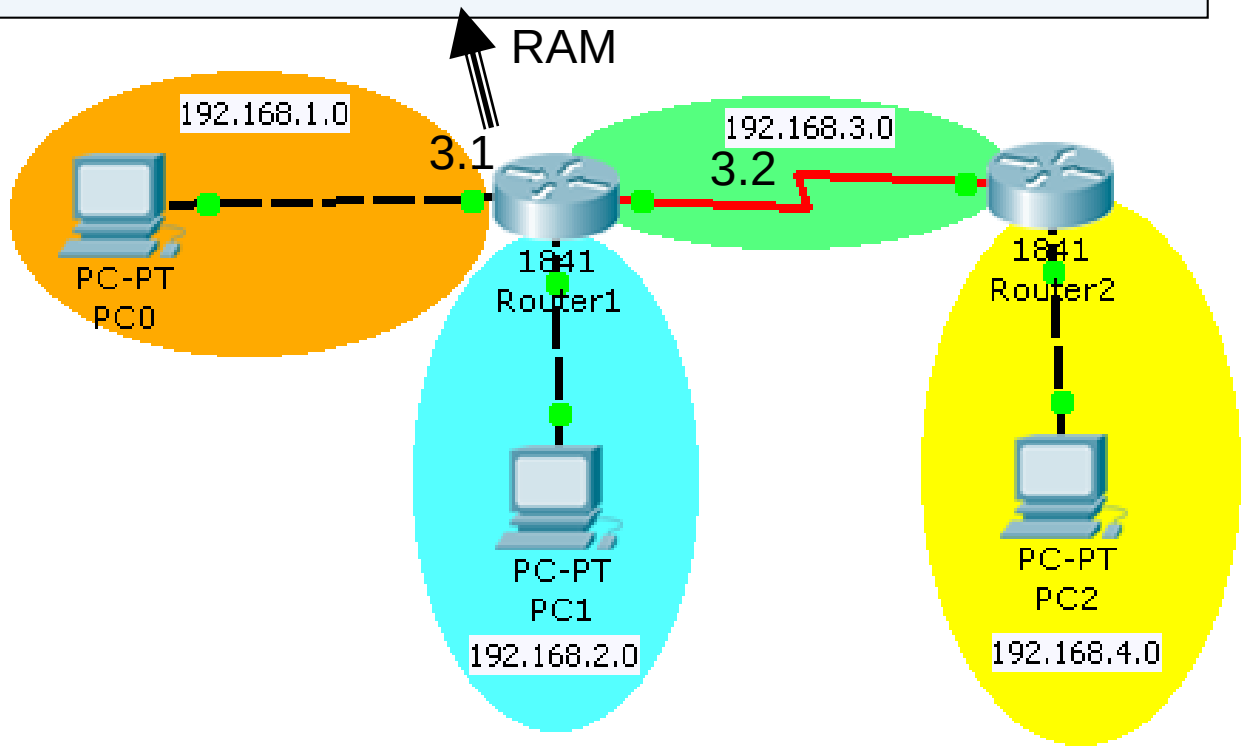
Types of routing

- Routing schemes differ in how they deliver messages
  - unicast delivers a message to a single specific node
  - broadcast delivers a message to all nodes in the network
  - multicast delivers a message to a group of nodes that have expressed interest in receiving the message
  - anycast delivers a message to any one out of a group of nodes, typically the one nearest to the source
  - geocast delivers a message to a geographic area



Routing table

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/24	FastEthernet0/0	---	0/0
C	192.168.2.0/24	FastEthernet0/1	---	0/0
C	192.168.3.0/24	Serial0/0/0	---	0/0
S	192.168.4.0/24	---	192.168.3.2	1/0



Routing table

Type	Network	Port	Next Hop IP	Metric

- *Type*
  - network type
- *Network*
  - destination networks address (with mask)
- *Port*
  - router interface id facing to the destination network
- *Next Hop IP*
  - IP address of the next router on the path to the destination
- *Metric*
  - goodness of the route

Type

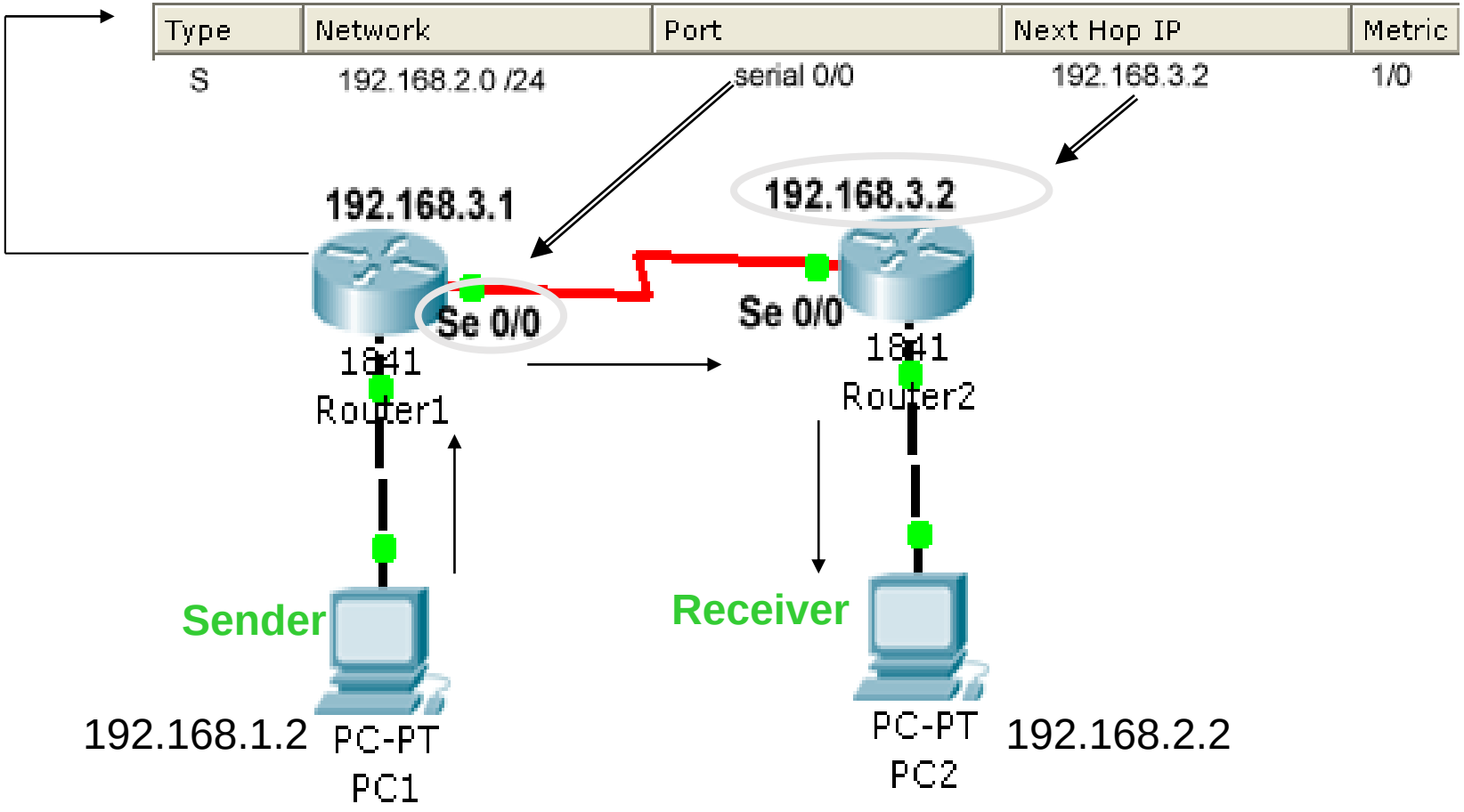
- **Local** (Directly Connected Network)
  - router have direct interface in this network
  - Sign: C
- **Remote** (Remote Network)
  - router doesn’t have direct connection with the network
  - Network is reachable only indirectly (through other routers)

Type (remote network)

- **Static**
  - Set by the administrator
  - sign: S
- **Dynamic**
  - reported by other routers
  - with a dynamic routing protocol
    - RIP (sign: R)
    - OSPF (sign: O)
    - EIGRP (sign: D)

(Exit)port, Next Hop IP

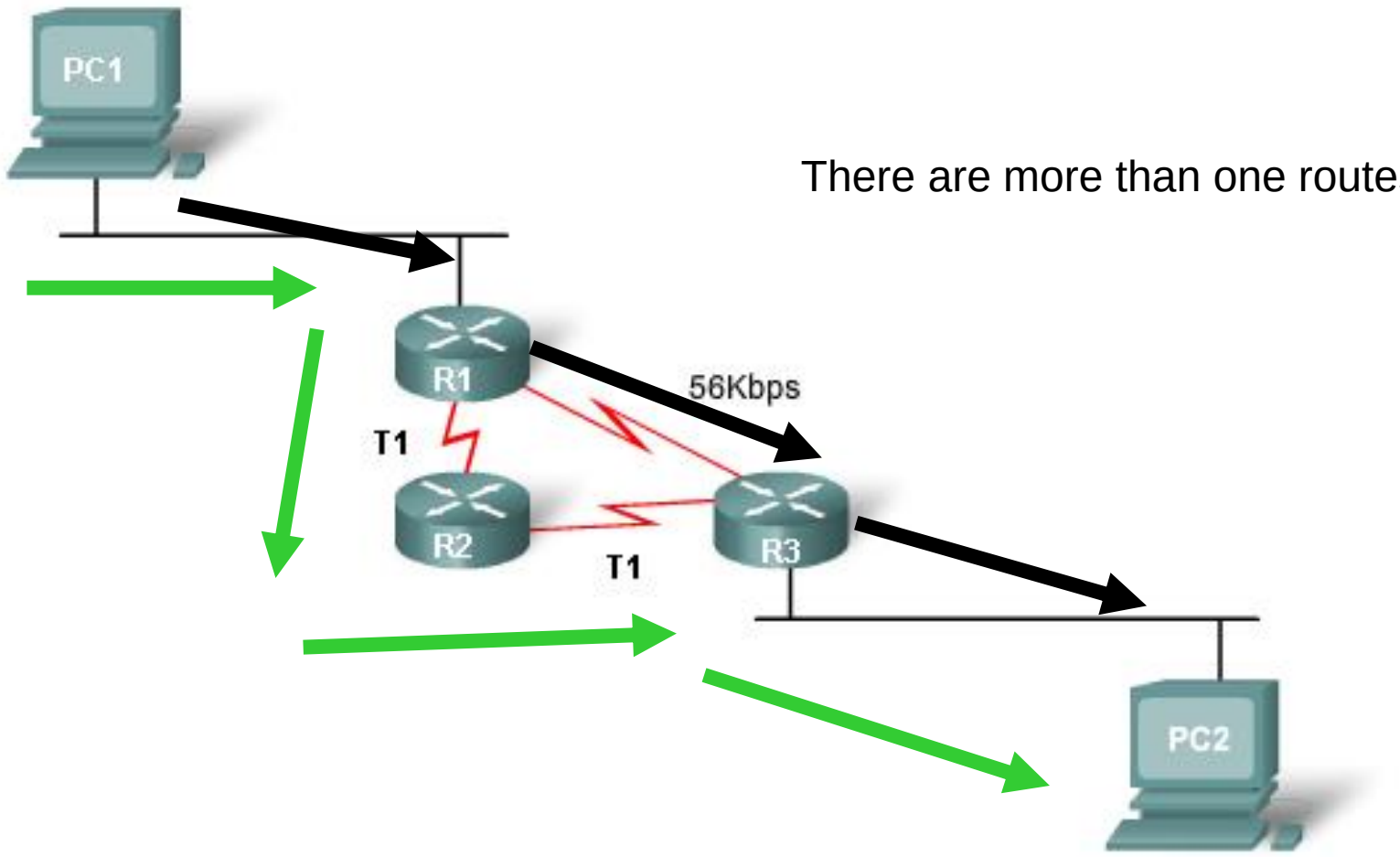
- Both shows the direction to the packet



Metric

- „Cost”
  - refers to the goodness of the route
  - the smaller the better
- Default value
  - Directly connected network (C) : 0/0
  - Static route (S) : 1/0

Best route

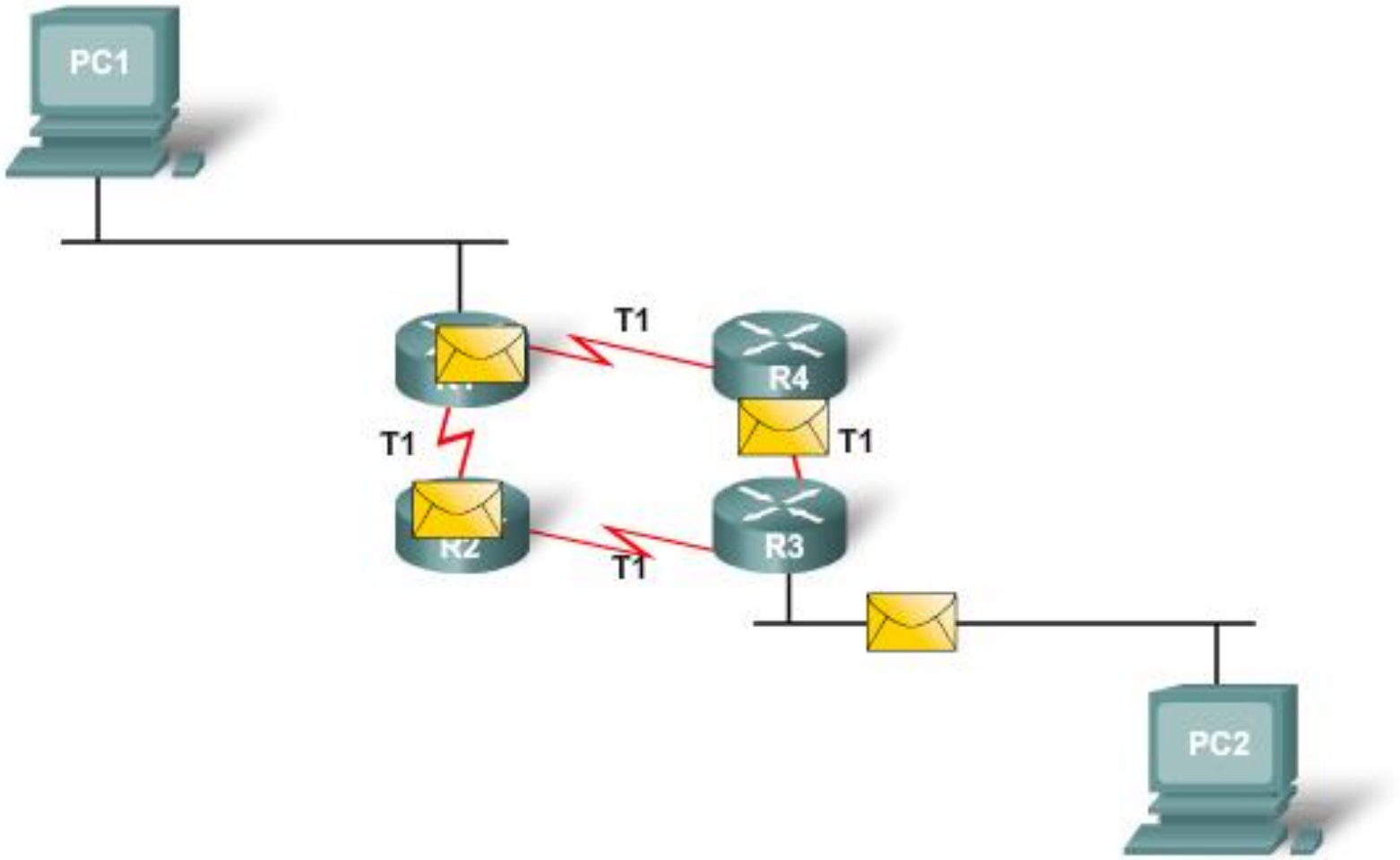


There are more than one routes.

Best route- metric

- Different costs
  - Distance (hop count)
  - Speed (Bandwidth)
  - Mixed
- Numerical value
  - The smaller the better
  - If we have more than one **live route** to the destination, the routing table will containt the route with the **smallest metric**.

Equal cost load balancing



Equal cost routes

- Routes have
  - same source (static, RIP, OSPF…)!!!
  - same destination
  - same metric
  - BUT!!! Different direction

- What happens?
  - Load balancing
  - Between equal cost routes
  - **Equal cost load balancing**

- (note that unequal cost load balancing is also possible…)

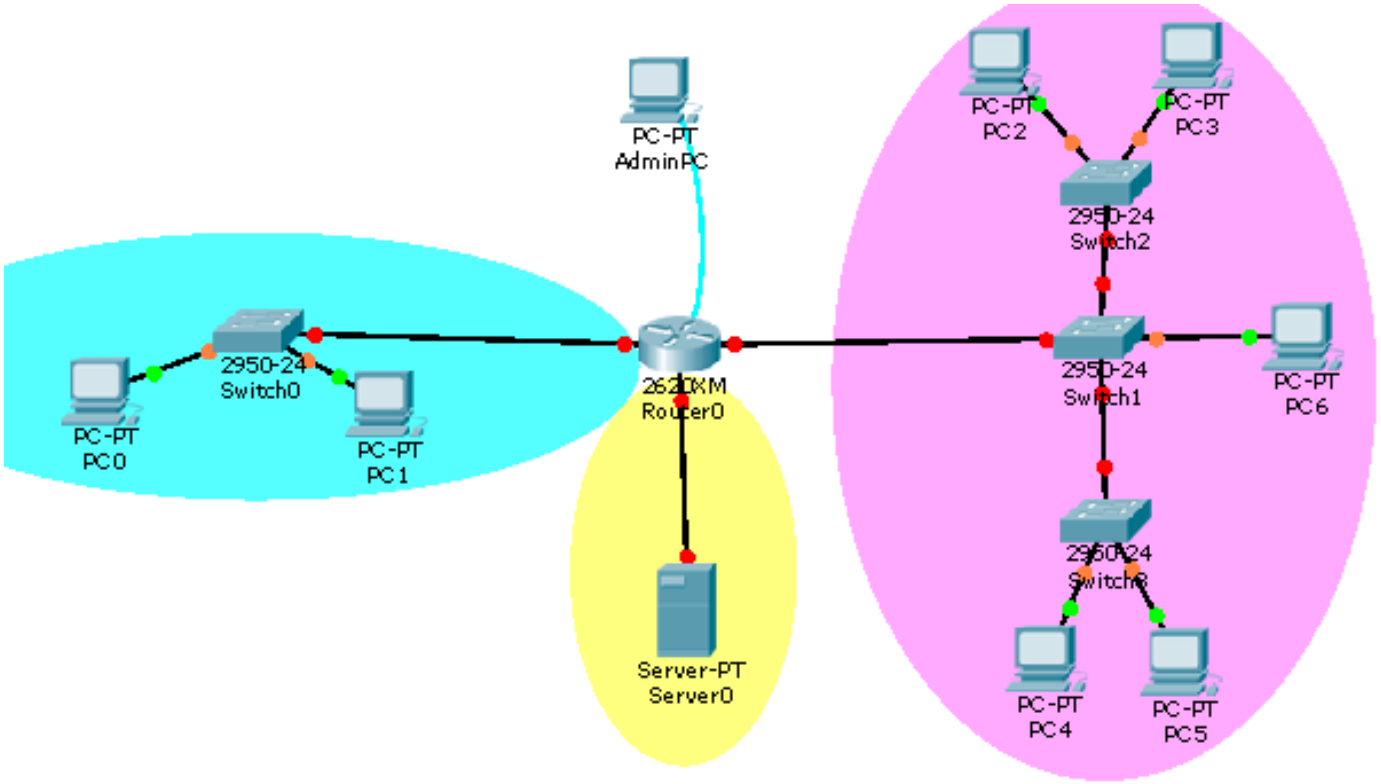
Show routing table

- Cisco IOS
  - Router# show ip route
- PC (Windows)
  - c:/>route print

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
```

Directly Connected Network

- Router have a direct interface in this network
- route automatically placed into the table when it is alive (no shutdown)



Directly Connected Network

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
```

Static routing

- Must be configured manually
  - which network, which direction
- Effective only in small networks
- Reconfiguration if something changes
- Problems in case of error (e.g., link disruption)

Static route

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
```

Static routing configuration

R(config)# **ip route** [*network-address*] [*subnet-mask*] [*next-hop-ip*] *{metric}*

optional

R(config)# **ip route** [*network-address*] [*subnet-mask*] [*exit-interface*] *{metric}*

optional

Deleting: **no** before the command

Default route

R(config)# ip route 0.0.0.0 0.0.0.0 [*exit-if*]

- any route fits
- we can say: every packet not fitting to the given routes must transmitted on the default route

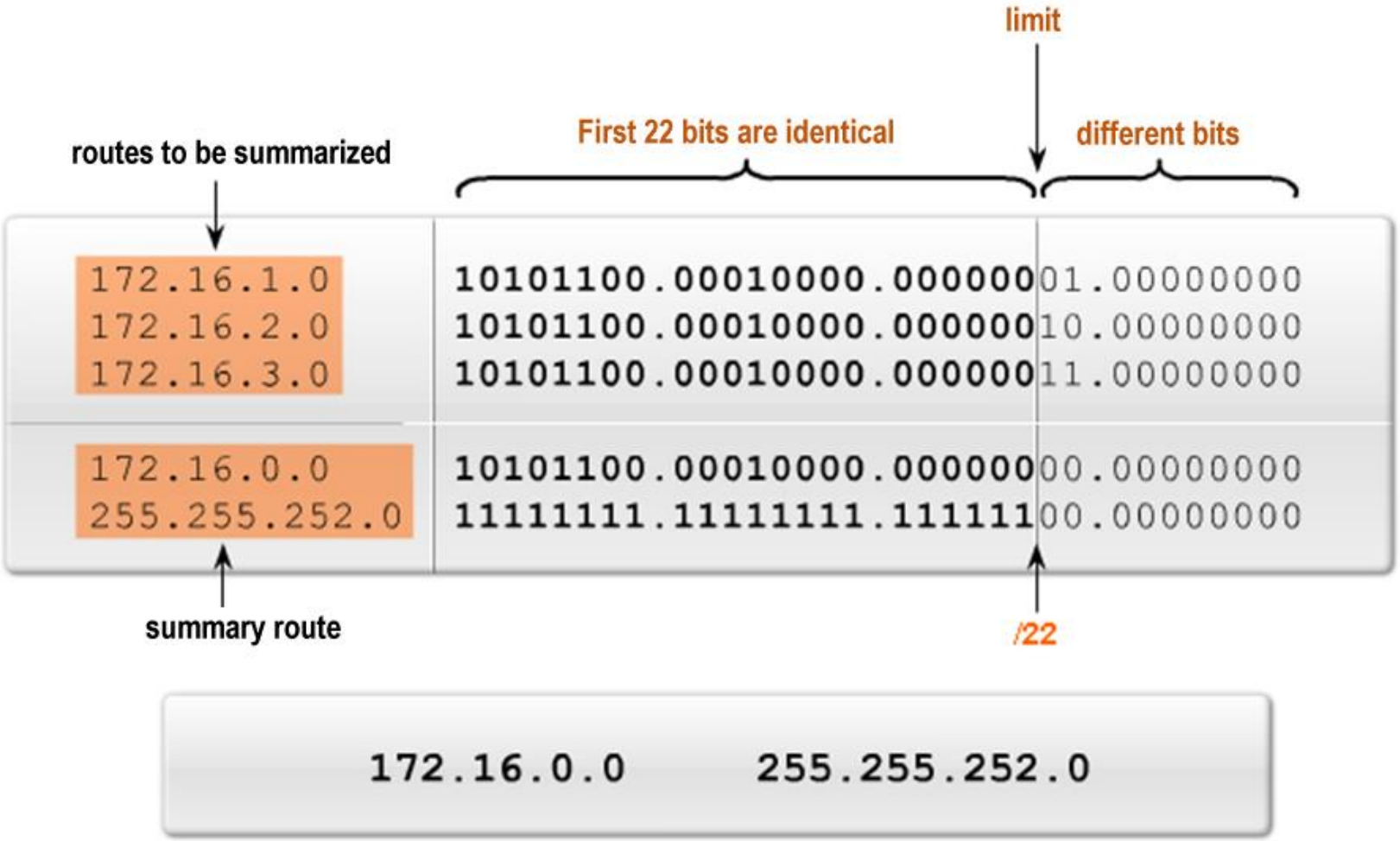
- Sign: **S***

Route summarization

- Routes in the same direction can be replaced by a single summary route
- reducing the size of the routing table
- more effective routing

- Usage
  - take the common part of the routes you want to summarize (common bits)
  - routes only in the same direction

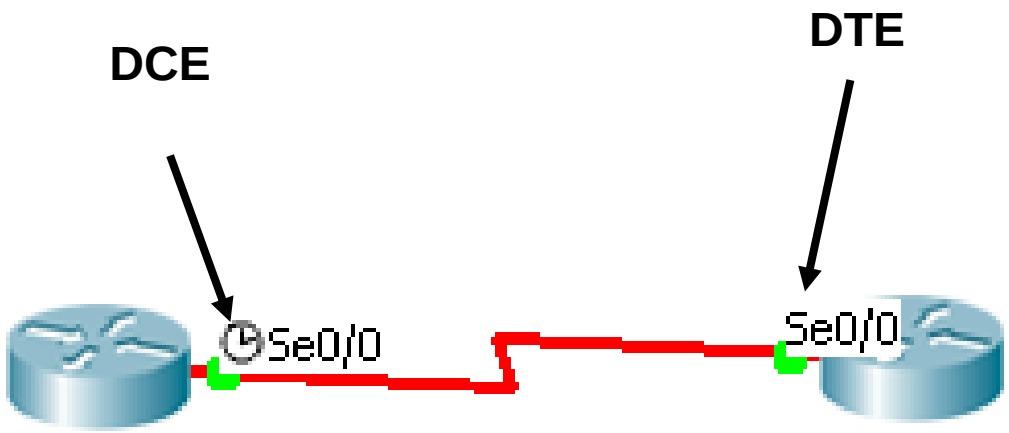
Route summarization



Route summarization

- **Example**
  - You have two networks in the same direction
    - 18.43.0.0/16
    - 18.48.192.0/18
  - Complete the summarization of the routes!
  - Summary route?

Serial interface



DCE: Data Control Equipment DTE: Data Terminal Equipment

Serial interface config

- R(config)# interface serial 0/0(/0)
- R(config-if)# ip address 192.168.1.1 255.255.255.0

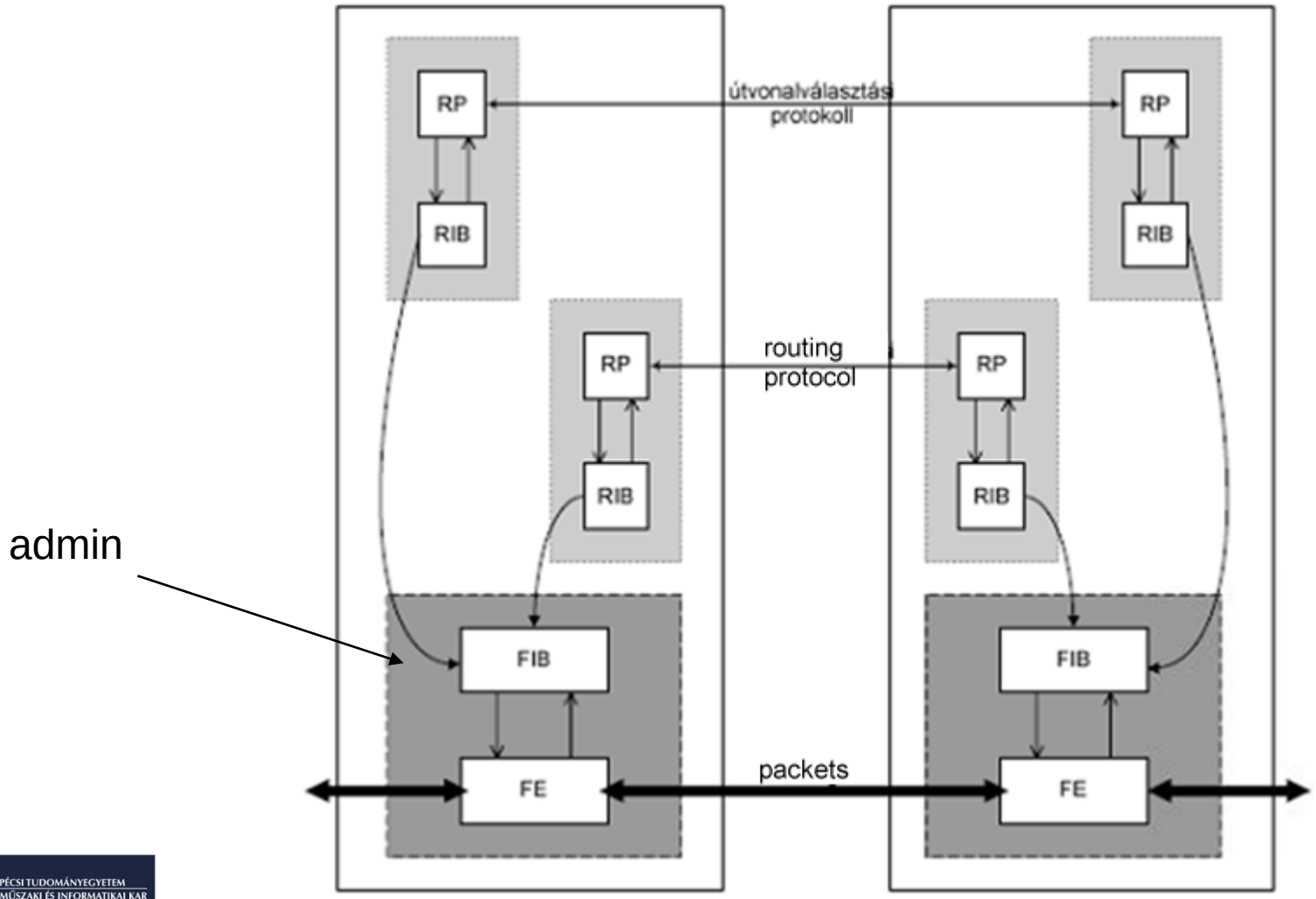
- ***Setting the clock rate!***
  - Should be configured only at DCE side
  - R(config-if)# clock rate 64000 (bps)

- R(config-if)# no shutdown

Check settings

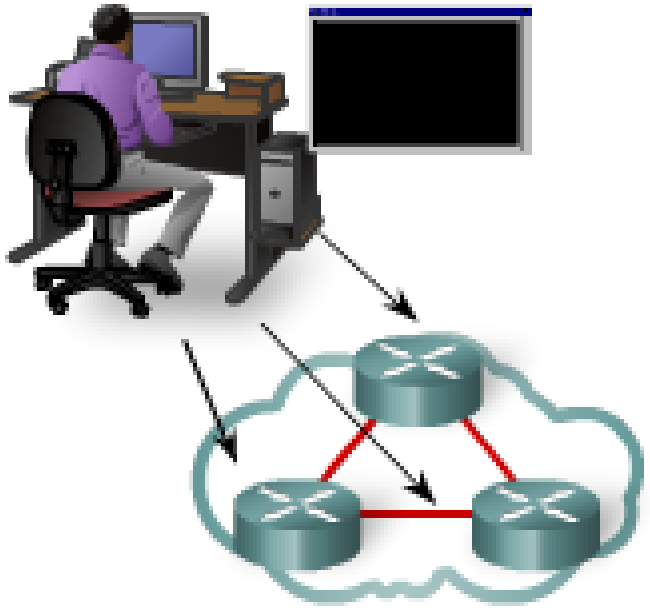
- R#show ip route
- R#show interfaces
- R#show ip interface brief

Routing process



Static vs Dynamic routing

Static Routing



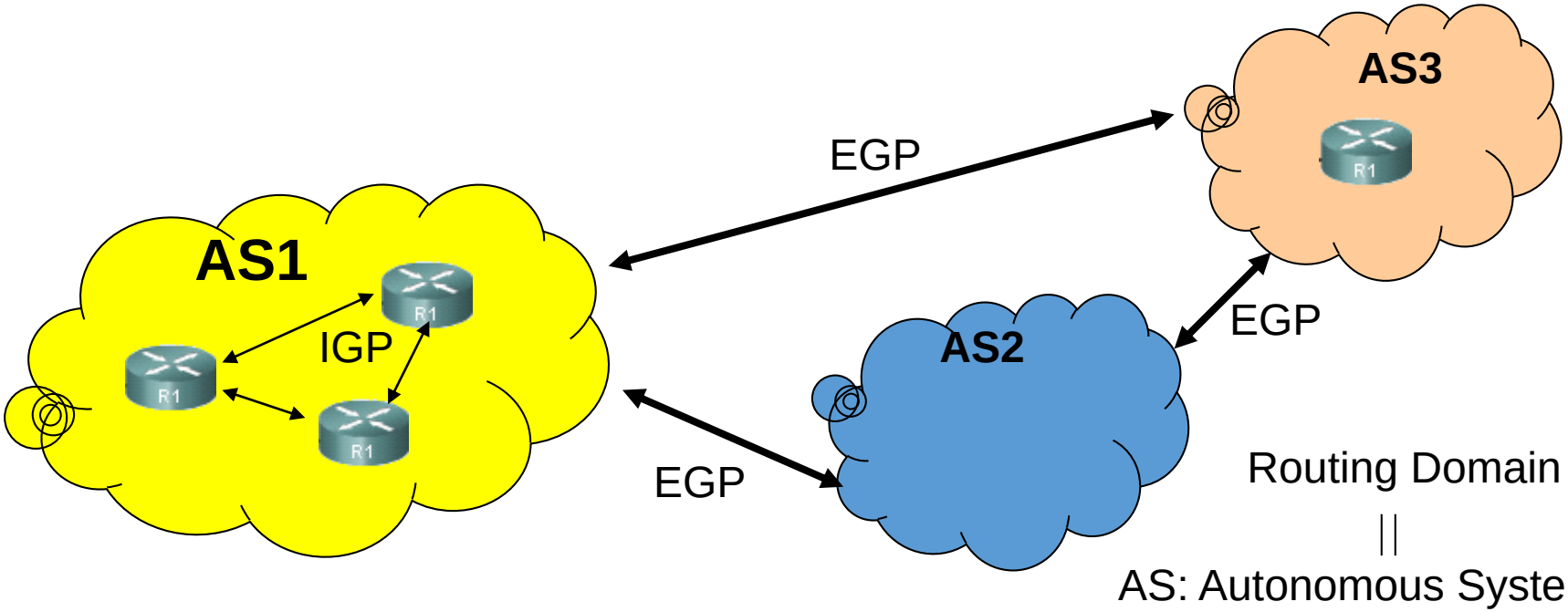
Dynamic Routing

Static vs Dynamic

	Dynamic	Static
Config complexity	Independent from network size	proportional to network size
Competence	Advanced	Intermediate
Topology changes	Automatic	Administrator
Network size	Any size	Small size
Security	Less secure	Secure
Resource need	More CPU, memory, bandwidth	No extra resources

Classification

- Interior Gateway Protocol (IGP)
- Exterior Gateway Protocol (EGP)



Classification

- IGP protocols
  - Distance vector routing protocol
    - Traffic light analogy: we know only the distance and the direction
  - Link state routing protocol
    - Traffic light analogy: we have a detailed map about the entire network

Routing technologies

- There are many IP routing protocols, some similiar, some not, but...
- They all have some common core features.
- These protocols make the routers and Layer3 switches do the following things:
  - Learn routing information from other routers concerning IP subnets.
  - Advertise these informations to other routers.
  - Choosing the best way based on metric if more than one is available.
  - React to changes in the network.

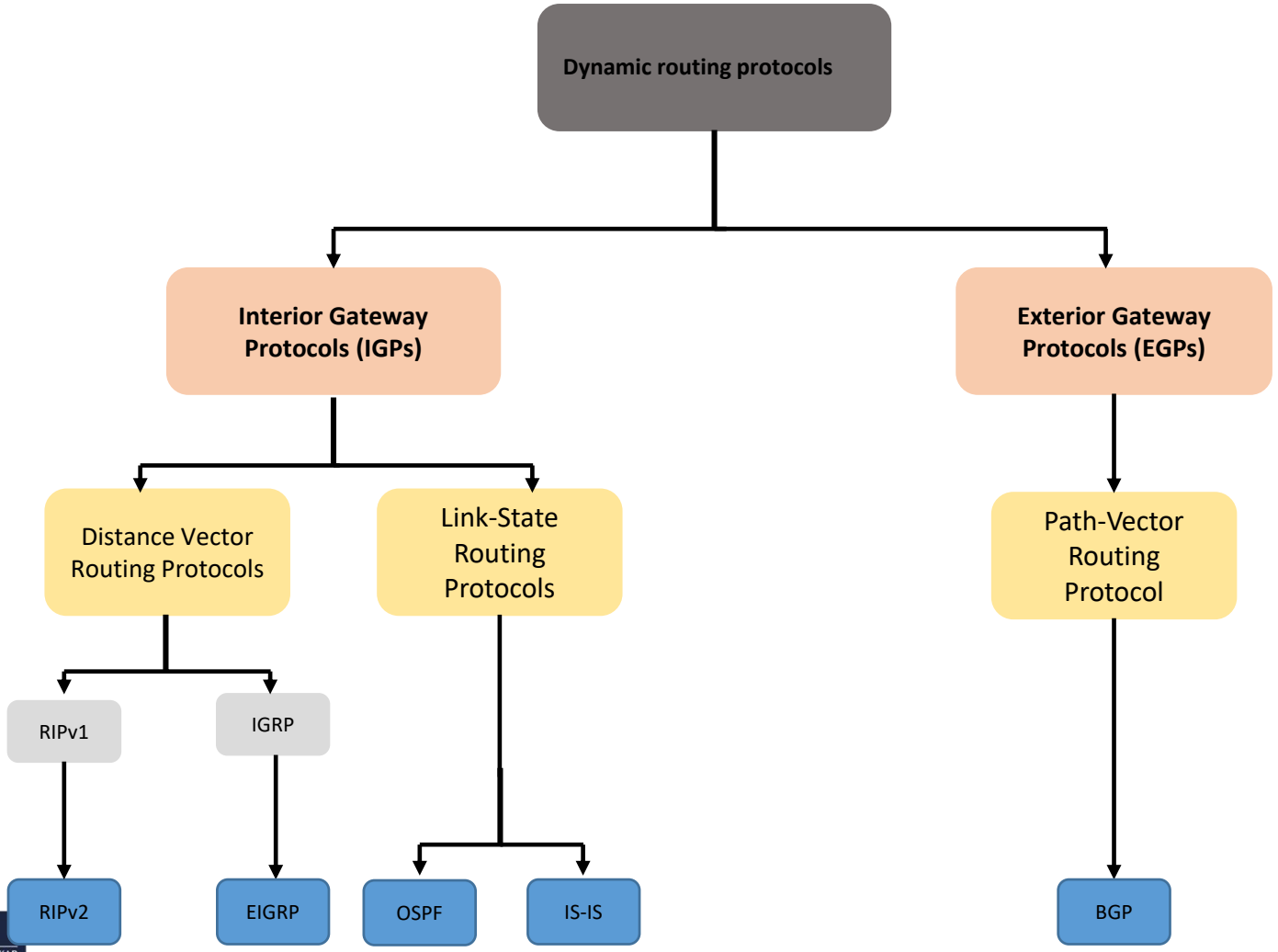
Routing technologies

- All of the routing protocols can do these things, the difference is how they do it.
- Historically, it started with RIP Version 1.
- Then came a second wave of routing protocols and RIPv2, OSPF, EIGRP came to be.
- First these worked only with IPv4.
- IPv6 support came in the mid 1990s.
- Routing protocols are often called interior gateway protocols or IGP for short.

Comparing IGPs

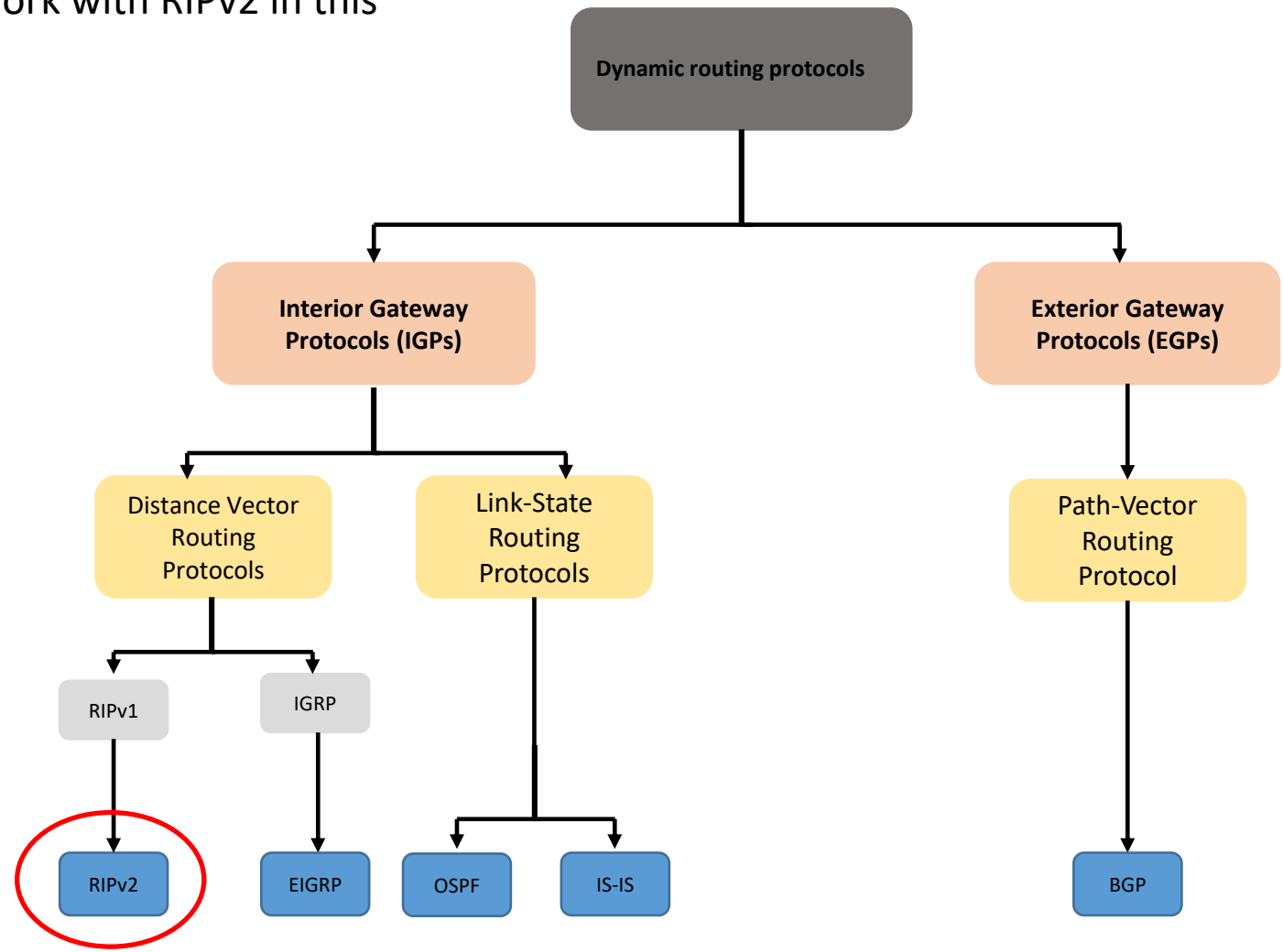
- We have 4 major points to consider when choosing what IGP to use.
  - **The routing protocol algorithm.**
  - **The metric:** it's important when choosing the best route.
  - **Speed of convergence time:** the time it takes to learn about changes in the network.
  - **Whether it's a standard IGP, or it's a private, defined by a big company.**

Routing protocols



Routing protocols

- We are going to work with RIPv2 in this presentation.



Well known routing protocols

- **RIP** (Router Information Protocol)
- **OSPF** (Open Shortest Path First)
- IGRP (Interior Gateway Routing Protocol)
- **EIGRP (Enhanced IGRP)**
- IS-IS (Intermediate System to Intermediate System)
- BGP (Border Gateway Routing Protocol)

Classful or classless

- It is important to know if the routing protocol is classful or classless
  - Classfull routing protocols
    - Does not advertise mask
    - Uses classful addressing (A,B,C…)
    - Subnets not supported
    - VLSM not supported
  - Classless routing protocols
  - Support CIDR and VLSM

Principles

- Routers share information
- With routing protocols
  - Tasks
    - Automatic network discovery
    - Maintaining routing tables
    - Choose best route
    - Discover and maintain alternative routes

Routing protocol components

- Data structures
  - Routing table, routing database (knowledge)
- Algorithm
  - specify the operation
- Protocol messages
  - communication with different messages

Convergence

- Sometimes
  - routers have a different knowledge about network
    - network is just booting
    - topology changed
- Definition
  - When all routers in network are operating with the same knowledge, the network is said to have converged.
    - convergence speed is various

Metric

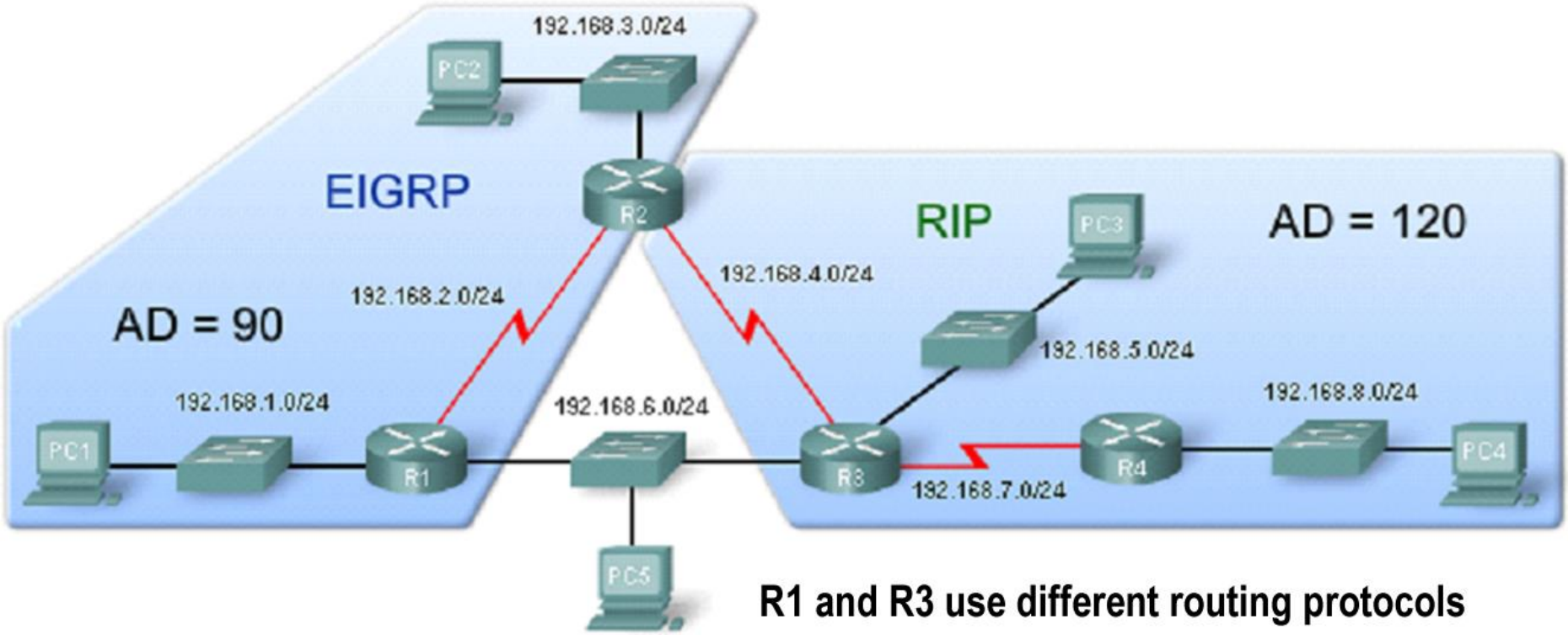
- route goodness, the smaller the better
- Protocols use various metric
  - distance, hop count(e.g., RIP)
  - bandwidth (e.g., OSPF)
  - cost
  - reliability
  - mixed (e.g., EIGRP)

```
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:26, Serial0/1
```

Metric

Problem

- Different protocols use different metric
- Which one is better?
  - Short or fast???



Problem

- Routes with the same metric
- This is not equal cost load balancing
  - Because the source is not the same
    - one source is EIGRP
    - other source is RIP

Administrative Distance

- AD distance
  - Preference of routing sources
    - static
    - RIP
    - OSPF
    - …
  - Numeric value
    - 0-255
    - Every source has a default value (can be changed)
    - the smaller the better

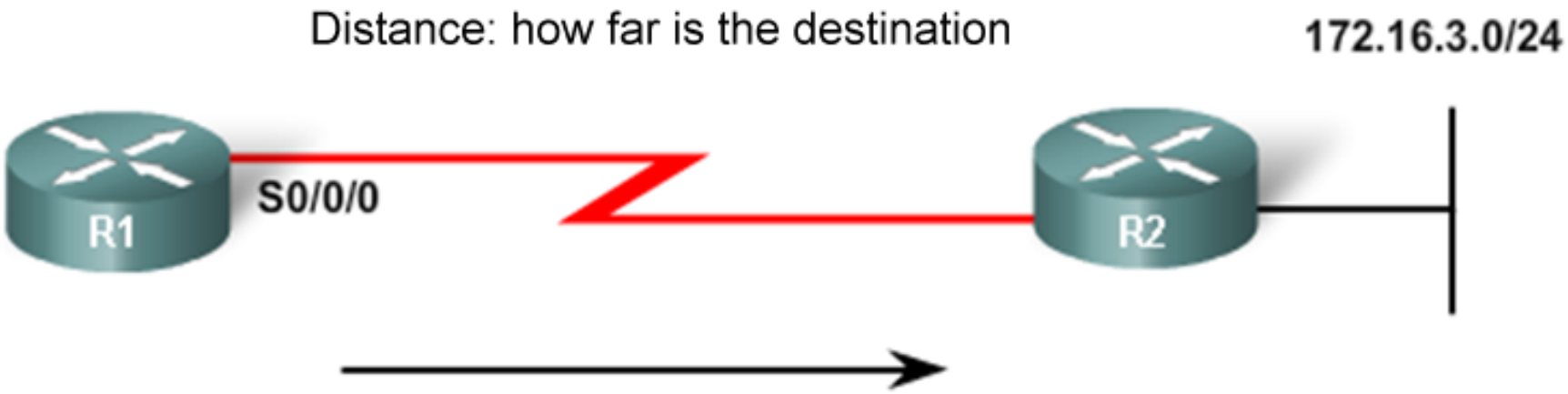
Administrative Distance

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    192.168.1.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
D    192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
R    192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:08, Serial0/0/1
```

Default AD values

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Distance vector routing



172.16.3.0/24 is one hop far (distance)
R2 is the next hop to the destination (vector)

Operation

- Routers send their entire routing table
- use periodic update
- slow convergence
- can be used in small networks
- easy configuration
- use Bellmann Ford algorithm

RIP

- Distance vector routing protocol
  - metric: distance/hop count
- Periodic update
  - interval: 30 sec
- AD distance : 120
- Slow convergence
- Maximum metric is 16 (!!!)
  - It means that the network is unreachable

RIP versions

- RIP v1
  - classful
  - no authentication
  - broadcast advertisment (255.255.255.255)
- RIP v2 new features
  - classless
  - CIDR and VLSM support
    - mask included in the advertisements
  - multicast advertisment (224.0.0.9)
  - available authentication methods
    - cleartext, MD5

RIPv2

- The Routing Information Protocol (RIP) is a distance-vector interior gateway (IGP) routing protocol used by routers to exchange routing information.
- RIP uses the hop count as a routing metric.
- RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination.
- The maximum number of hops allowed for RIP is 15.
- This hop limit, however, also limits the size of networks that RIP can support.
- RIP version 2 (RIPv2) was developed due to the deficiencies of the original RIP.

RIPv2

- Supports VLSMs.
- Supports authentication.
- Implements split horizon with poison reverse.
- Implements triggered updates.
- Administrative distance for RIPv2 is 120.
- Used in small, flat networks or at the edge of larger networks.

RIPv1 vs RIPv2

RIPv2 is actually an enhancement of RIPv1's features and extensions rather than an entirely new protocol.

1. RIPv1 is Classful routing protocol and RIPv2 Classless routing protocol.

2. In RIPv1, subnet masks are NOT included in the routing update and In RIPv2 Subnet masks are included in the routing update.

3. RIPv2 multicasts the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast (255.255.255.255).

Split horizon

- Because RIP functions by periodically flooding the entire routing table out to the network, it generates a lot of traffic.

- The split horizon and poison reverse techniques can help reduce the amount of network traffic originated by RIP hosts and make the transmission of routing information more efficient.

Split horizon

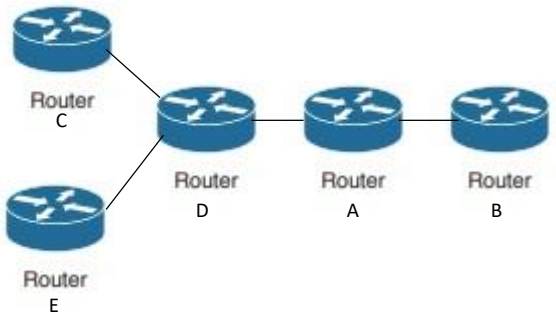
- If a router receives a set of route advertisements on a particular interface, RIP determines that those advertisements do not need to be retransmitted out the same interface.

- This technique, known as split horizon, helps limit the amount of RIP routing traffic by eliminating information that other neighbors on that interface have already learned.

Split horizon

- Router A advertises routes to Routers C, D, and E to Router B.
- In this example, Router A can reach Router C in 2 hops. When Router A advertises the route to Router B, B imports it as a route to Router C through Router A in 3 hops.
- If Router B then readvertised this route to Router A, A would import it as a route to Router C through Router B in 4 hops.
- However, the advertisement from Router B to Router A is unnecessary, because Router A can already reach the route in 2 hops.

The split horizon technique helps reduce extra traffic by eliminating this type of route advertisement.



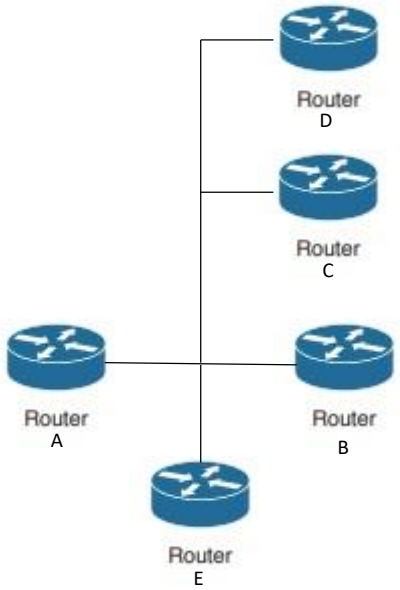
Poison reverse

- Similarly, the poison reverse technique helps to optimize the transmission of routing information and improve the time to reach network convergence.

- If a router learns about unreachable routes through one of its interfaces, it advertises those routes as unreachable (hop count of 16) out the same interface.

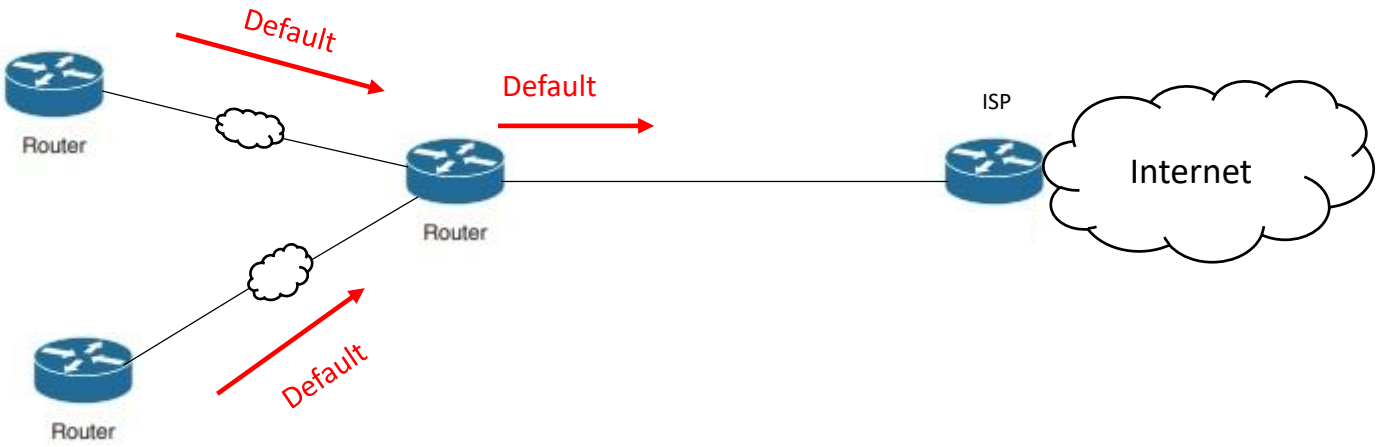
Poison reverse

- Router A learns through one of its interfaces that routes to Routers C, D, and E are unreachable.
- Router A readvertises those routes out the same interface as unreachable.
- The advertisement informs Router B that Hosts C, D, and E are definitely not reachable through Router A.



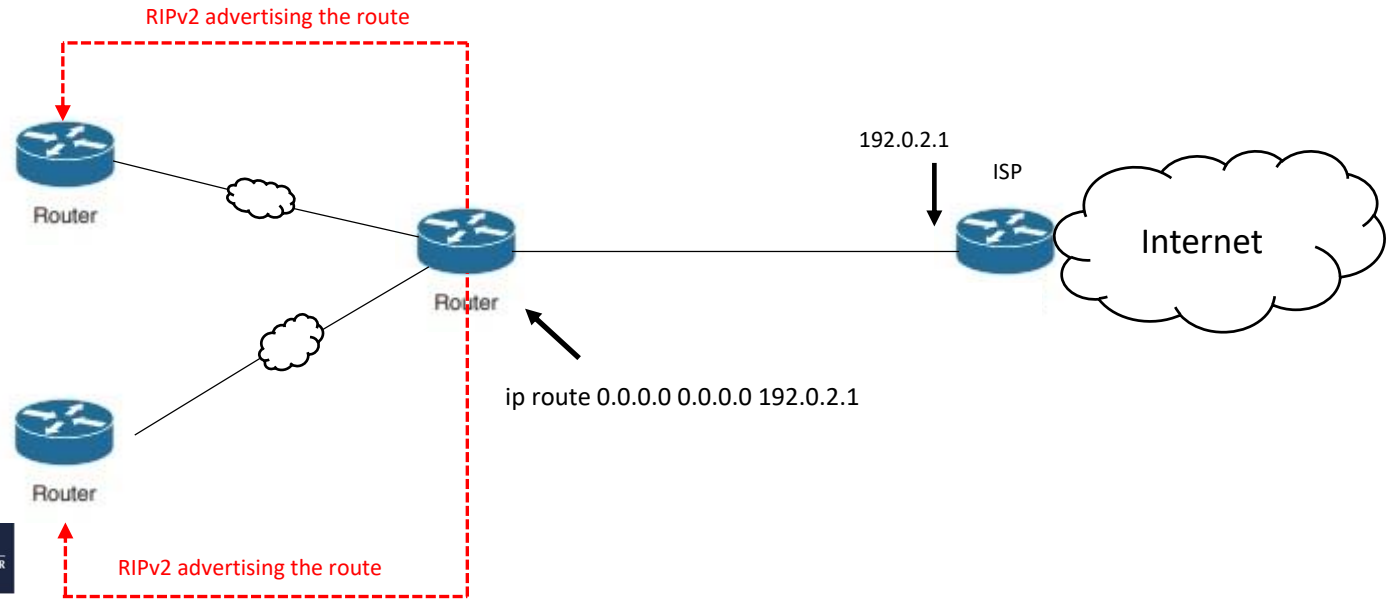
Default route

- Rather than using a routing protocol, routers can use a default route.
- If there are more than one routers in the network, each router could forward their packets to the one router that has a WAN link connected to the Internet or to the core of the enterprise network.



Default route

- Each of these routers could use a static default route, but RIPv2 enables us to only use one static route on only one router.
- The one router that is connected to the true default route configures a static default route(a route to 0.0.0.0).
- RIPv2 then advertises this route to the other routers.
- The key command to this feature is default-information originate on the router where the static default route is configured.



RIP timers

- Update
  - default: 30 sec
- Invalid
  - if the route does not updated during this time, the route set to be unreachable and marked with metric 16
  - default: 180 sec
- Flush
  - after the invalid timer expired the router starts the flush timer. If it expires the route will be deleted from the routing table
  - default: 240 sec

RIP v1 configuration

- Configuration (Cisco routers)
  - Enable RIP

```
Router(config)# router rip
Router(config-router)#
```

  - Diasble RIP

```
Router(config)# no router rip
```

RIP v1 configuration

- Network advertising
  - define networks to be advertised AND
  - define networks where RIP updates are sent and received

```
Router(config)# router rip
Router(config-router)# network <network_address>
```

Classful address

RIP v2 configuration

- Have to specify the version

```
Router(config)# router rip
Router(config-router)# version 2
```

RIP auto summary

- A RIP v2 use auto route summarization by default!
  - Turn off

```
Router(config)# router rip
Router(config-router)# no auto-summary
```

  - Turn on

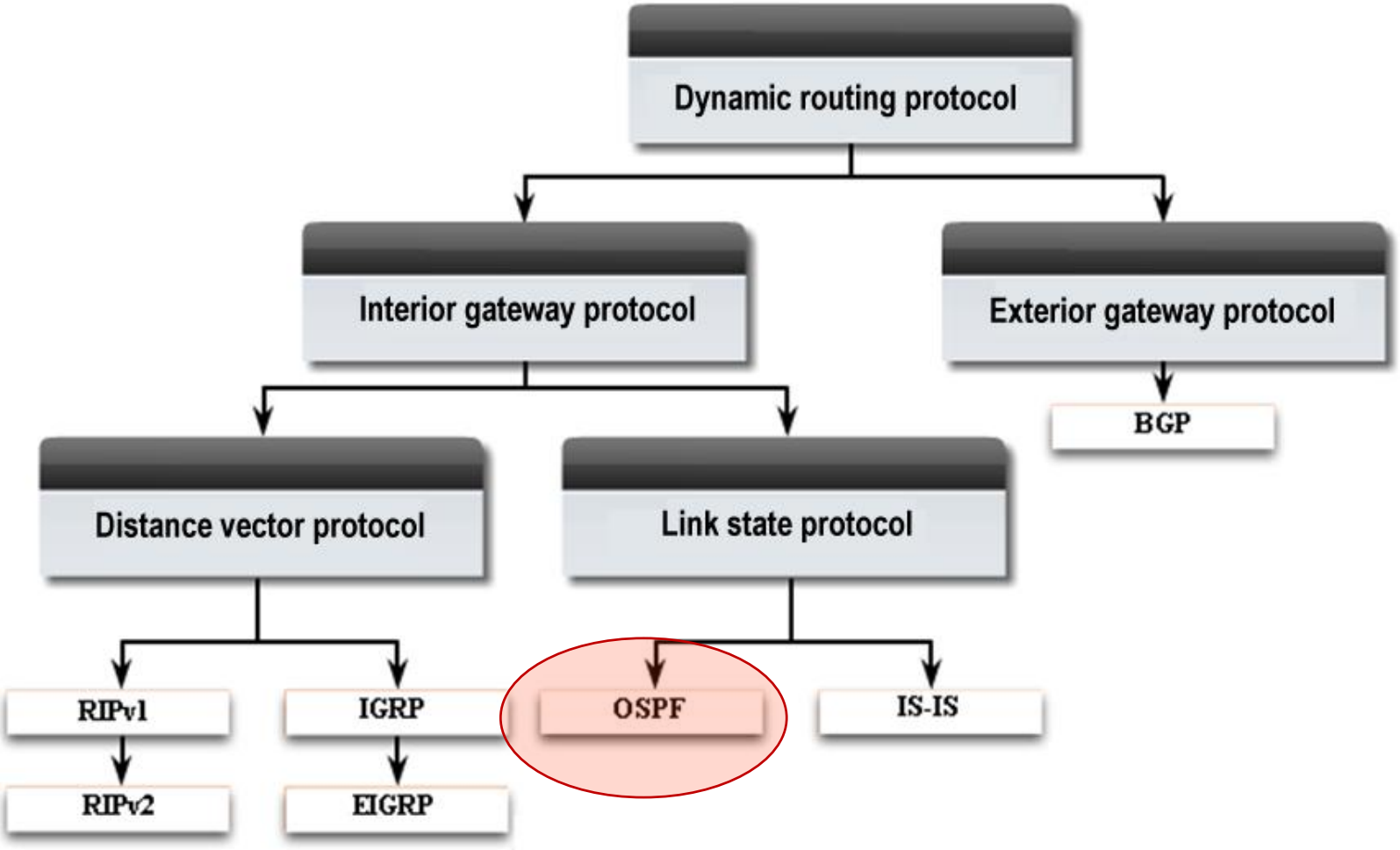
```
Router(config)# router rip
Router(config-router)# auto-summary
```

Check settings

Router# **show ip protocols**

```
R2#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 1 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: static, rip
  Default version control: send version 2, receive version 2
    Interface              Send  Recv  Triggered RIP  Key-chain
    Serial0/0/0            2     2
    Serial0/0/1            2     2
  Automatic network summarization is in effect
  Routing for Networks:
    10.0.0.0
    209.165.200.0
  Passive Interface(s):
```

Classification



Link state routing

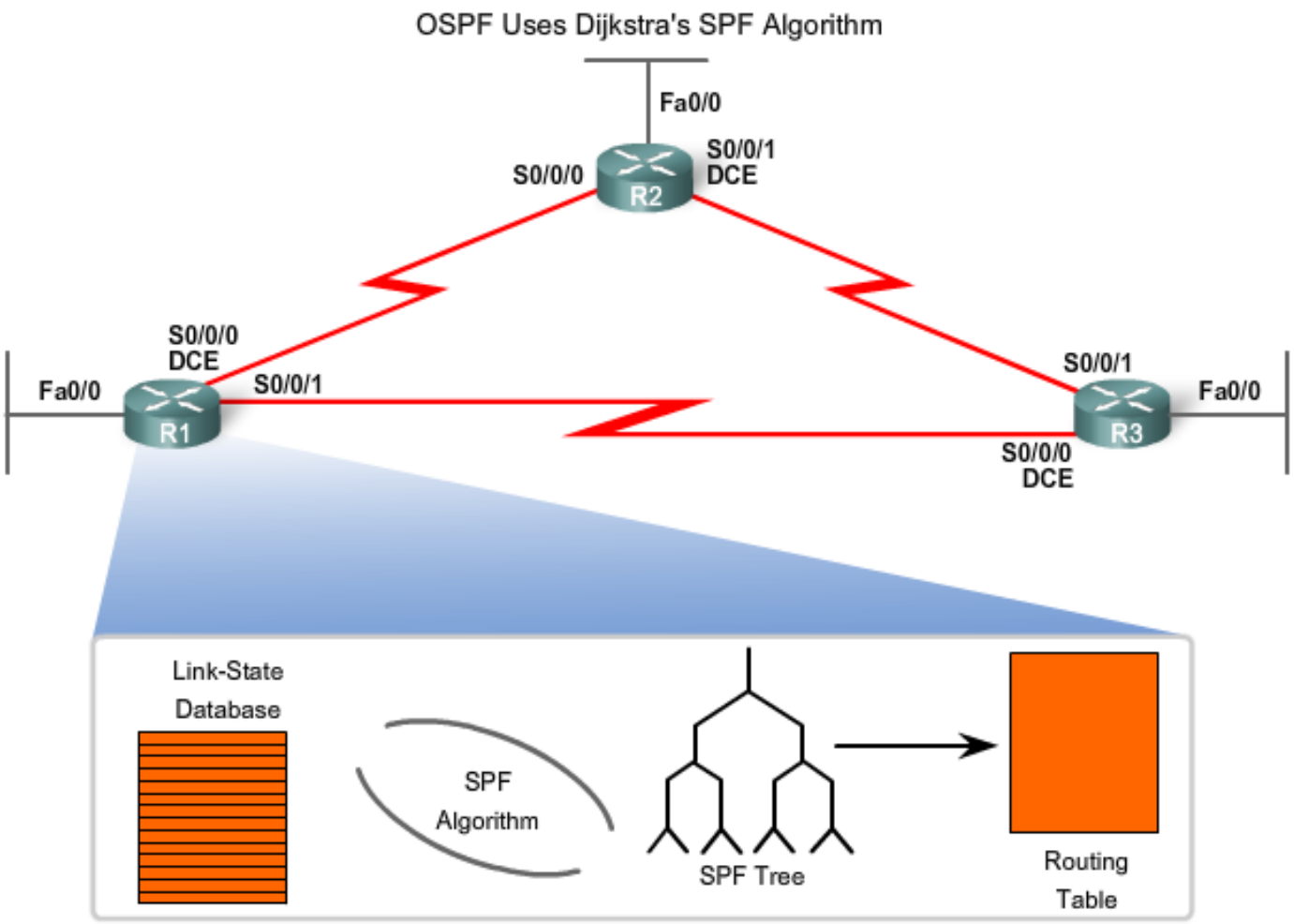
- Based on Dijkstra's SPF algorithm
- Properties
  - Routers have a full picture about network
  - Changes trigger updates
  - No periodic updates

Operation

- Steps
  - make adjacency relationship
    - Hello packets (keepalive)
  - sending LSP (Link State Packet) messages to neighbours (reporting only changes)
  - …etc.

- You can read theoretical details!

OSPF


OSPF Uses Dijkstra's SPF Algorithm
Fa0/0
S0/0/0
S0/0/1
DCE
R2
S0/0/0
DCE
Fa0/0
S0/0/1
R1
S0/0/1
Fa0/0
R3
S0/0/0
DCE
Link-State
Database
SPF
Algorithm
SPF Tree
Routing
Table

OSPF configuration

- Enable OSPF

```
Router(config)# router ospf <process_id>
Router(config-router)#
```

1-65535

- Disable OSPF

```
Router(config)# no router ospf <process_id>
```

OSPF configuration

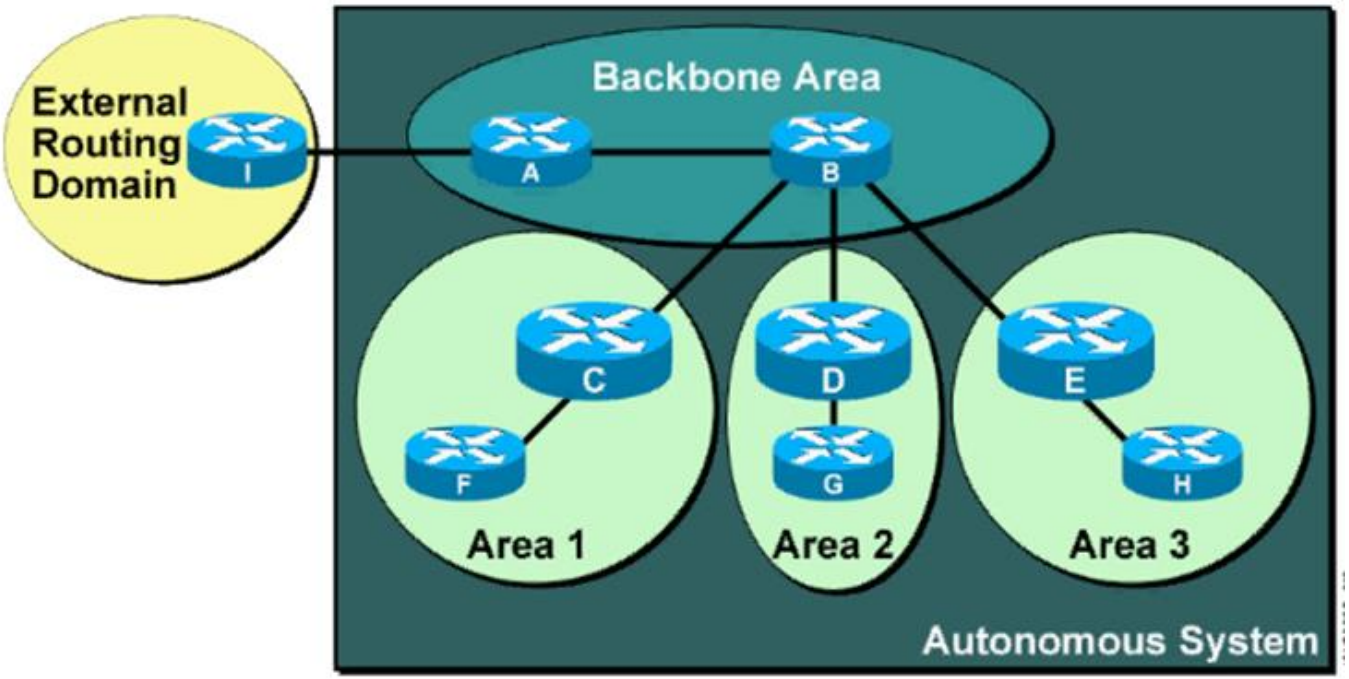
- Network
  - Advertised networks
  - Advertising networks

```
R(config)# router ospf <process_id>
R(config-router)# network <network_address>
                  <wildcard_mask> area <area_id>
```

Wildcard mask: negated netmask
Area_id: OSPF area identifier

Area

- Single area OSPF
- Multi area OSPF



OSPF metric

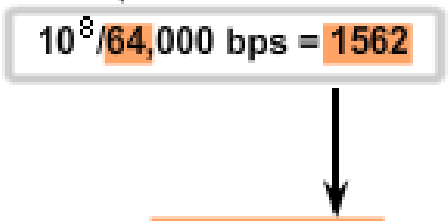
- Bandwidth proportional
  - Value: 10^8/bandwidth in bps
    - (default reference speed: fastEthernet ← can be changed)

Interface Type	10^8/bps = Cost
Fast Ethernet and faster	10^8/100,000,000 bps = 1
Ethernet	10^8/10,000,000 bps = 10
E1	10^8/2,048,000 bps = 48
T1	10^8/1,544,000 bps = 64
128 kbps	10^8/128,000 bps = 781
64 kbps	10^8/64,000 bps = 1562
56 kbps	10^8/56,000 bps = 1785

OSPF metric manipulation

- Iterface bandwidth
  - bandwidth command (interface config mode)
  - value must be set in kbps

```
R1(config)#inter serial 0/0/0
R1(config-if)#bandwidth 64
R1(config-if)#inter serial 0/0/1
R1(config-if)#bandwidth 256
R1(config-if)#end
R1#show ip ospf interface serial 0/0/0
Serial0/0 is up, line protocol is up
  Internet Address 192.168.10.1/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT_TO_POINT, Cost: 1562
  Transmit Delay is 1 sec, State POINT_TO_POINT,
```



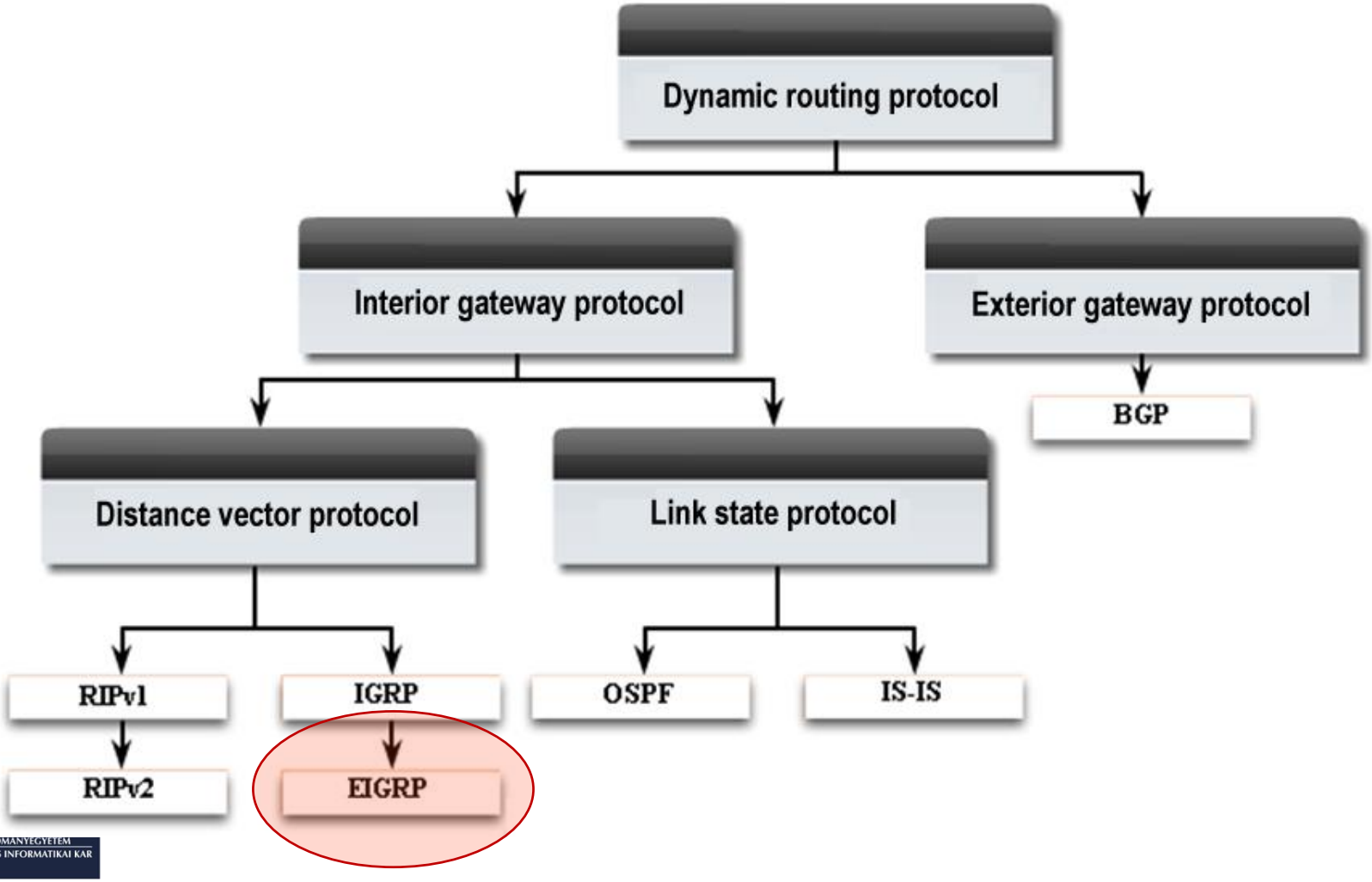
OSPF metric manipulation

- Direct metric settings
  - ip ospf cost command (interface config mode)

```
R1(config)#inter serial 0/0/0
R1(config-if)#ip ospf cost 1562
R1(config-if)#end
R1#show ip ospf interface serial 0/0/0
Serial0/0 is up, line protocol is up
  Internet Address 192.168.10.1/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT_TO_POINT, Cost: 1562
  Transmit Delay is 1 sec, State POINT TO POINT,
```

No Calculation Needed

Classification



EIGRP

- **E**nhanced **I**nterior **G**ateway **R**outing **P**rotocol
  - Hybrid protocol
    - Have distance vector routing protocol features
  - Cisco developed, but made it available for everybody
- Use mixed metric
  - Distance (hop count)
  - Speed (bandwidth)
  - Delay
  - Reliability
  - Load
  - MTU (Maximum Transmission Unit)

EIGRP

- Advantages
  - Fast convergence
  - Bandwidth optimalization (reports only changes)
  - CIDR, VLSM support
  - Less resource needs comparing to OSPF

EIGRP

- Properties
  - Network type: **D**
  - AD: 90
  - Operating 3 tables
    - Neighbor table (register neighbours)
    - Topology table (networks and routes)
    - Routing table (best live routes)

EIGRP

- Configuration

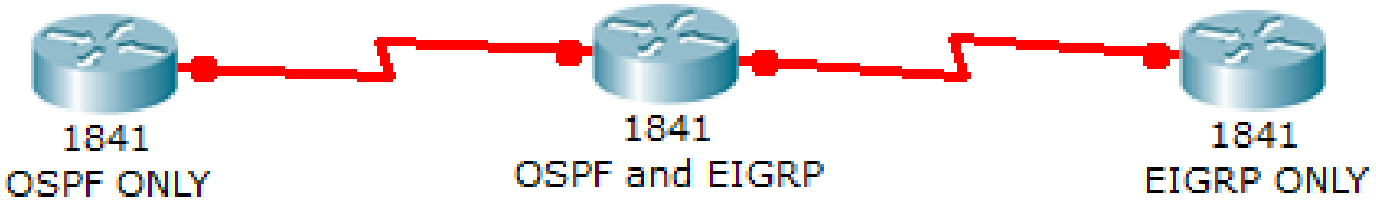
```
Router(config)#router eigrp number
Router(config-router)#network address1 wildcard_mask
```

Redistribution theory

- Routing protocols
  - only the same protocols can change information
  - RIP-RIP, OSPF-OSPF, EIGRP-EIGRP

- Route redistribution
  - information exchange between different routing protocols
    - e.g., RIP transport OSPF information

Example



Example

- OSPF (default metric: 20)

```
Router(config)#router ospf 1
Router(config-router)#redistribute rip subnets
Router(config-router)#redistribute eigrp 1
```

- RIP

```
Router(config)#router rip
Router(config-router)#redistribute ospf 1 …
```

- EIGRP

```
Router(config)#router eigrp 1
Router(config-router)#redistribute ospf 1 …
```

A routing protocols can redistribute static routes as well!
Configuration is very similar as above.

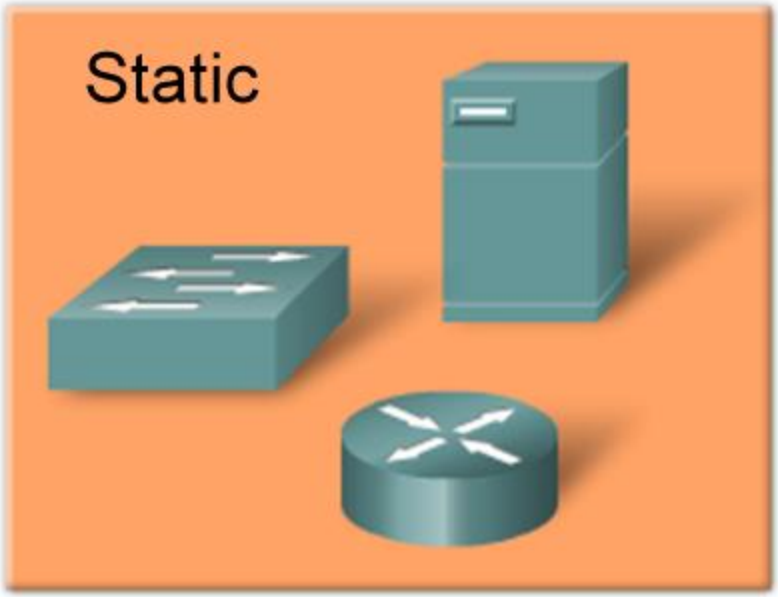
Chapter 04

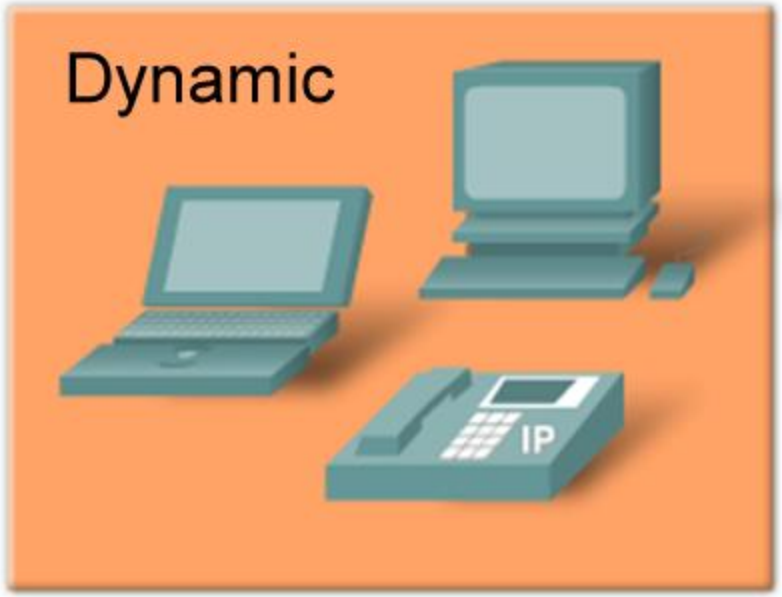
DHCP service

Static IP configuration

- IP settings (parameters)
  - IP address, netmask, gateway, DNS...etc.
- Advantageous
  - if device is not mobile
  - Server, switch, router…etc.
- Disatvantageous
  - mobile devices
  - Laptop, IP telephone…etc.

Static VS Dynamic





IP configuration

- Manual IP configuration
  - Set by the administrator
- Automatic IP configuration
  - BOOTP – static (L5)
  - DHCP – dynamic (L5)

BOOTP

- Previously used (1985-től)
- uses UDP (ports: 67,68)

- Handle only 4 IP parameters
  - IP address, netmask, gateway, DNS server

- Not dynamic
  - BOOTP server has a static list
  - Client MAC – IP address binding
  - Static mapping

DHCP

Dynamic Host Configuration Protocol

- IP parameters set automatically
- More than 30 parameters
- Dynamic address mapping
  - static mapping is also possible
  - IP lease time

What is DHCP?

- DHCP (Dynamic Host Configuration Protocol) is a protocol used to provide quick, automatic, and central management for the distribution of IP addresses within a network.

- It is also used to configure the proper subnet mask, default gateway, and DNS server information on the device.

How does it work?

- In most homes and small businesses, the router acts as the DHCP server. In large networks, a single computer might act as the DHCP server.

- In short, the process goes like this: A device (the client) requests an IP address from a router (the host), after which the host assigns an available IP address to allow the client to communicate on the network.

DHCP

- These IPs can be permanently assigned to that specific host, but it is more common that it’s only a temporarly assigned IP address.

- If the device is no longer in the network, the assigned IP gets reassigned and can be used on another device.

BOOTP VS DHCP

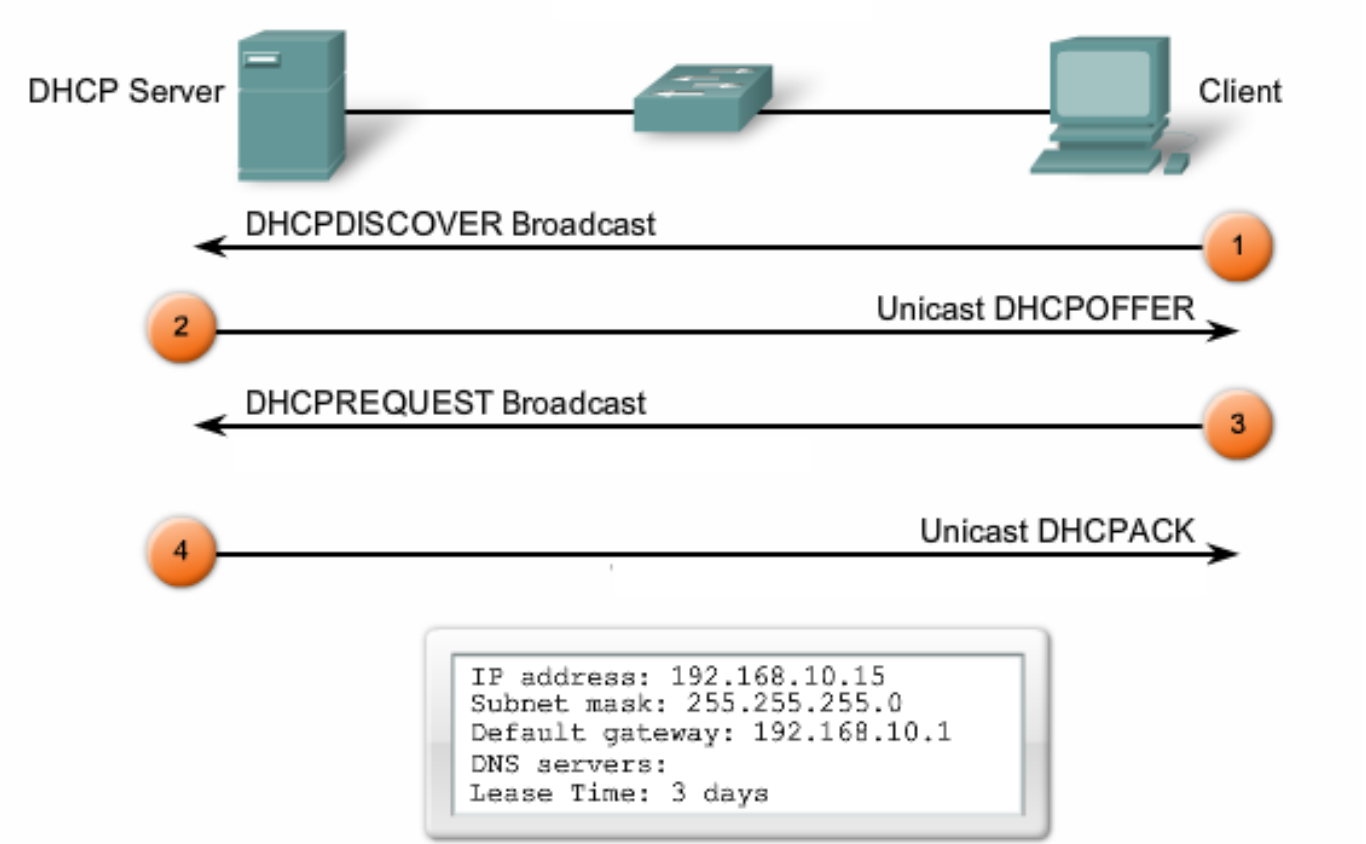
BOOTP	DHCP
Static Mappings	Dynamic Mappings
Permanent assignment	Lease
Only supports four configuration parameters	Supports over 30 configuration parameters

DHCP protocol

- RFC 2131 → IETF standard
- Client server model

DHCP protocol

- using UDP transport protocol
  - Client UDP 67
  - Server UDP 68



DHCP protocol

- Other DHCP messages
  - DHCPNACK, DHCPDECLINE
    - server refuse request
    - address already issued or bad request
  - DHCPRELEASE
    - client don’t need the address anymore
    - IP address became useable again

The process of DHCP

- Once a device is turned on and connected to a network that has a DHCP server, it will send a request to the server, called a DHCPDISCOVER request.

- After the DISCOVER packet reaches the DHCP server, the server attempts to hold on to an IP address that the device can use, and then offers the client the address with a DHCPOFFER packet.

The process of DHCP

- Once the offer has been made for the chosen IP address, the device responds to the DHCP server with a DHCPREQUEST packet to accept it, after which the server sends an ACK(Acknowledgement) that's used to confirm that the device has that specific IP address and to define the amount of time that the device can use the address before getting a new one.

- If the server decides that the device cannot have the IP address, it will send a NACK(Negative Acknowledgement).

DHCP

- There is one problem when it comes to DHCP.
- At first, the clients don’t have an IP address, but they need to send IP packets.
- There are two special IPv4 addresses that helps solve this problem.
  - 0.0.0.0 – it’s reserved for hosts without an IP address
  - 255.255.255.255 – This is the local broadcast IP. Routers don’t forward them, but they are broadcasted on the local network.

DHCP message format

8	16	24	32
OP Code (1)	Hardware type (1)	Hardware address length (1)	Hops (1)
Transaction Identifier			
Seconds – 2 bytes		Flags – 2 bytes	
Client IP Address (CIADDR) – 4 bytes			
Your IP Address (YIADDR) – 4 bytes			
Server IP Address (SIADDR) – 4 bytes			
Gateway IP Address (GIADDR) – 4 bytes			
Client Hardware Address (CHADDR) – 16 bytes			
Server name (SNAME) – 64 bytes			
Filename – 128 bytes			
DHCP Options – variable			

DHCP service

- DHCP server can be
  - DHCP Server computer
  - Active network device (L3)
    - SOHO router
    - Enterprise router

DHCP server

- Core network sevice of server operating systems

SOHO router

- All-in-One
  - Router
  - Gateway
  - Switch
  - NAT
  - …
  - DHCP server

Enterprise router

- DHCP service
  - DHCP pool
  - set by the administrator on router
  - set addresses to be allocated
  - one or more pool per router

```
Router(config)# ip dhcp pool pool_name
```

Enterprise router

- Set up the ip address range
  - router pick an IP from this range

```
Router(config-dhcp)# network
  network_address

  subnet_mask
```

Enterprise router

- Other parameters
  - Default gateway

    ```
    Router(config-dhcp)# default-router IP_address
    ```

  - DNS server

    ```
    Router(config-dhcp)# dns-server IP_address
    ```

  - Lease time

    ```
    Router(config-dhcp)# lease day hour minute | infinite
    ```

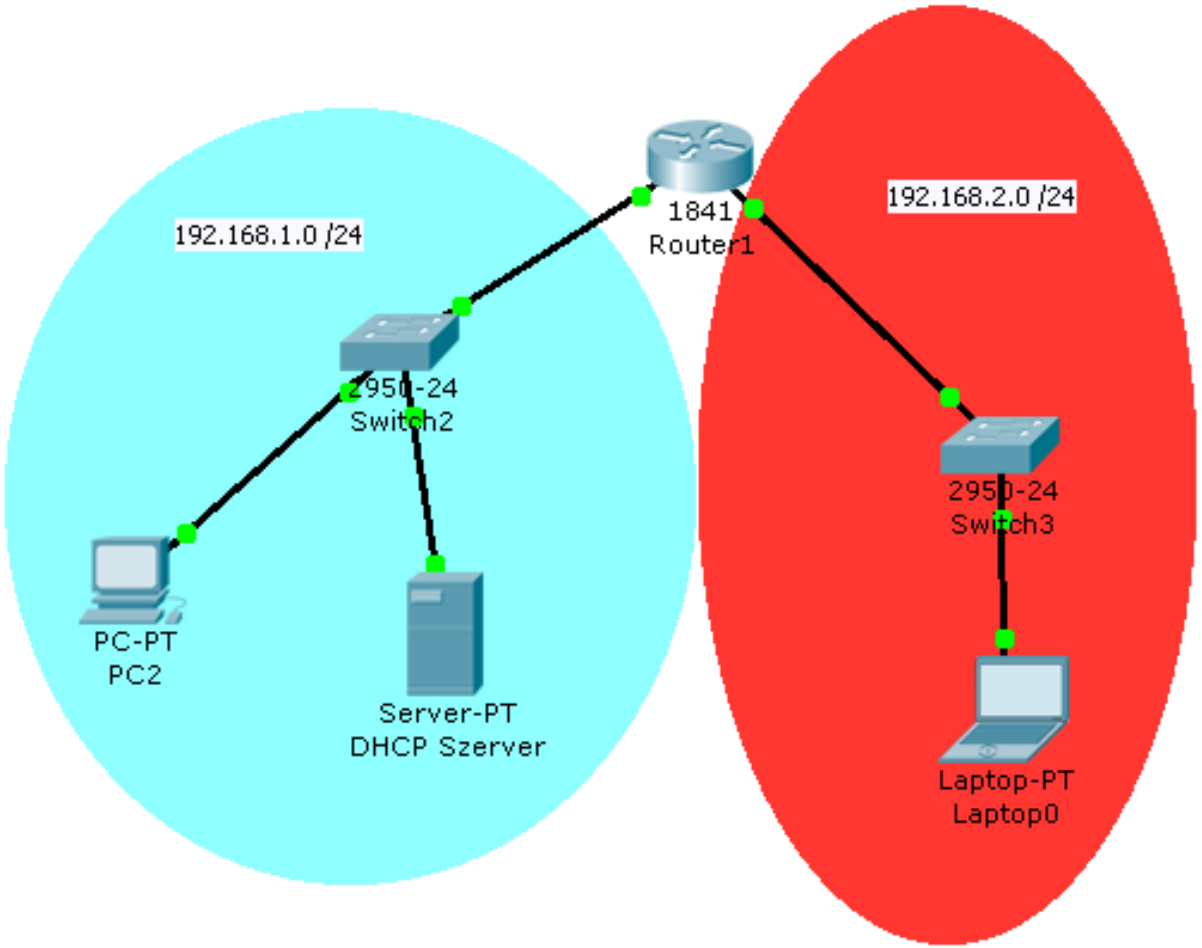
Enterprise router

- Excluding IP addresses
  - not part of the DHCP service

```
Router(config)# ip dhcp excluded-address IP_address
```

```
Router(config)# ip dhcp excluded-address start_IP end_IP
```

What is the problem?



DHCP Relay

- Generally, DHCP messages are broadcasted. So, in order for the messages to be exchanged between a DHCP client (PC) and DHCP server, both the client and server have to reside on the same subnet.

- This restriction requires all individual subnets have its own DHCP server for DHCP operation, which is practically not ideal in bigger or corporate networks.

DHCP Relay

- To address this problem, we use a thing called DHCP relay.
- Enabling the DHCP relay function in the router allows DHCP messages to be exchanged between a DHCP client and DHCP server residing on different subnets.
- The core function of this DHCP relay agent is to convert a broadcast DHCP packet into a unicast one, and forward it to a DHCP server.

DHCP relay

- Summary
  - Broadcast stay inside a broadcast domain
  - Router interfaces are different broadcast domains
    - DHCPDISCOVER message can’t reach server

- DHCP relay configuration

```
Router(config-if)#ip helper-address dhcp_ip
```

More about DHCP

- Check DHCP binding

```
Router# show ip dhcp binding
```

- Router interface IP address
  - Mostly static IP address
  - Sometimes dynamic

```
Router(config-if)# ip address dhcp
```

Chapter 05

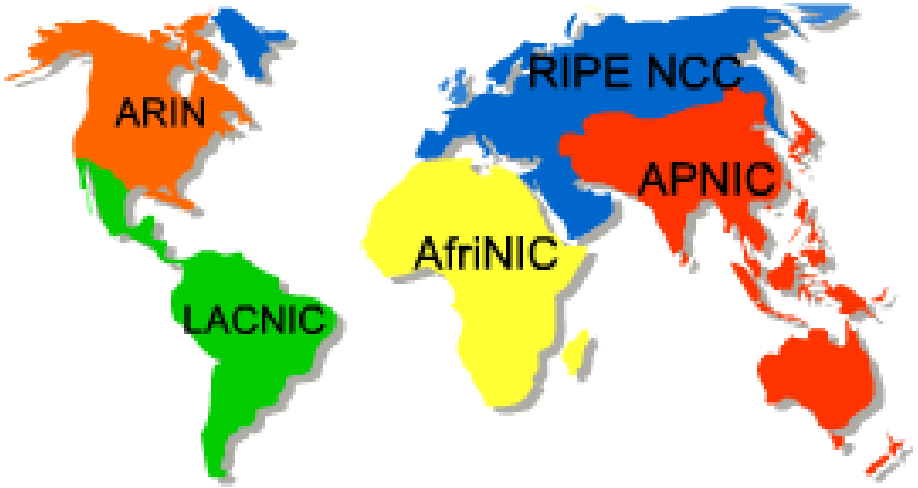
NAT service

IPv4 shortcomings

- IPv4 address space is small
  - exhausted
- Short term solutions
  - Subnets, CIDR, VLSM
  - Private IP addresses, address translation
- Long term solution
  - IPv6

Public IP addresses

- Public IP
  - useable in public
  - registered by authorities
    - ARIN (American Registry for Internet Numbers)
    - RIPE (Réseaux IP Européennes)

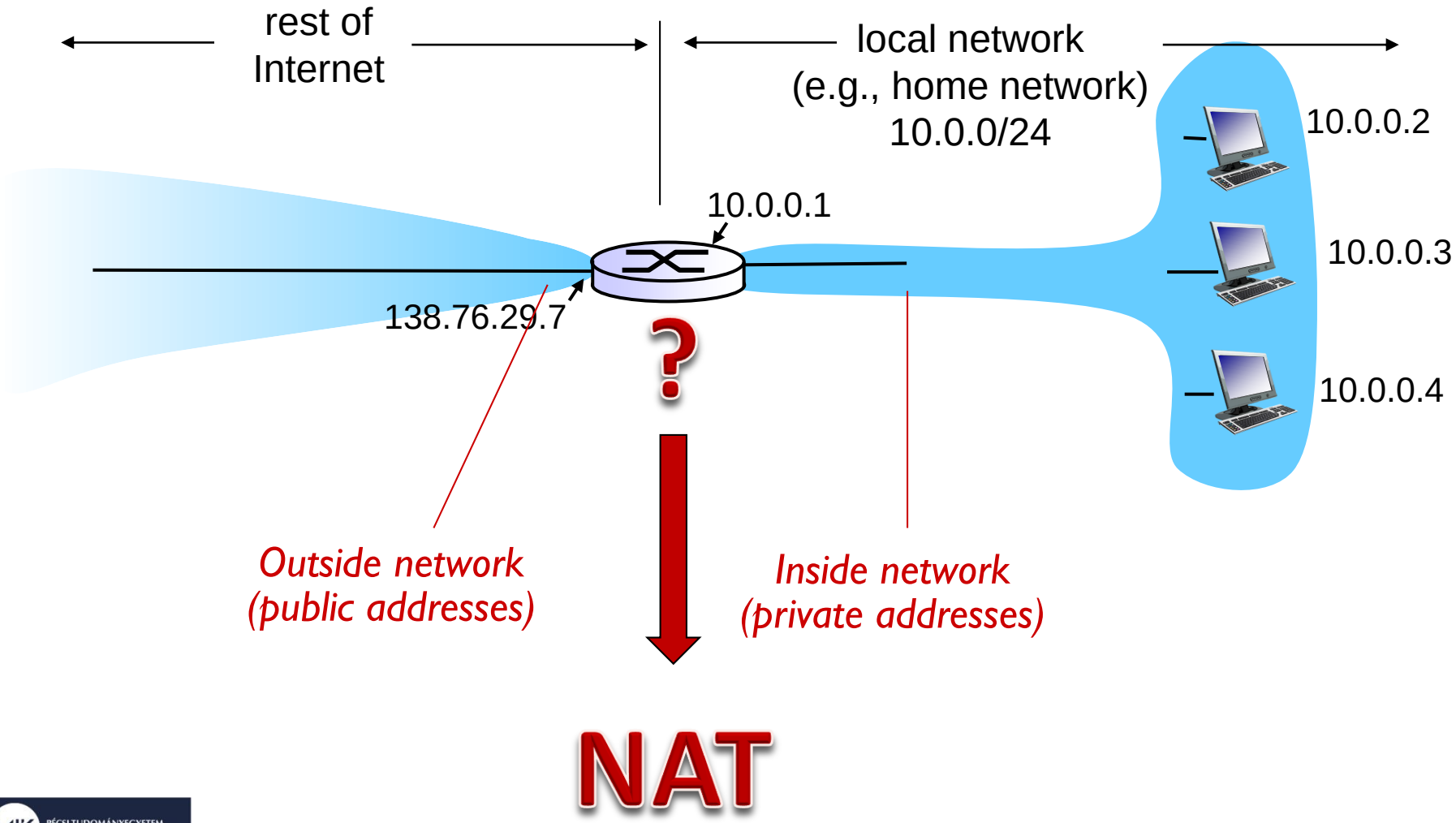


Private IP addresses

- Private IP
  - useable exclusively in local networks

Class	Private IP Addresses (RFC 1918)	Default Subnet Mask	Number of Networks	Hosts per Network	Total Hosts
A	10.0.0.0 to 10.255.255.255	255.0.0.0	1	16,777,214	16,777,214
B	172.16.0.0 to 172.31.255.255	255.255.0.0	16	65,534	1,048,544
C	192.168.0.0 to 192.168.255.255	255.255.255.0	256	254	65,024

Networks

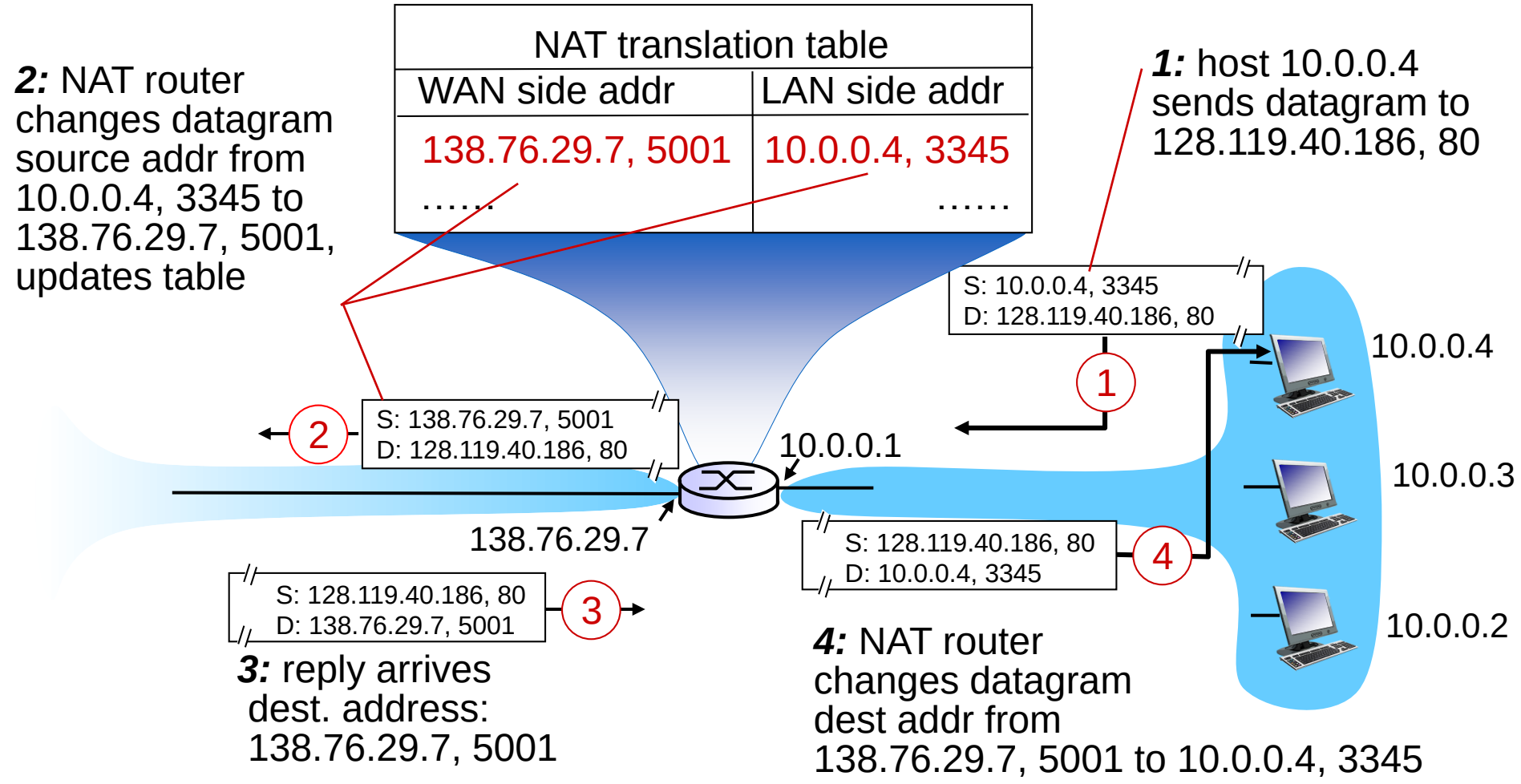

rest of
Internet
local network
(e.g., home network)
10.0.0/24
10.0.0.2
10.0.0.1
10.0.0.3
138.76.29.7
10.0.0.4
?
Outside network
(public addresses)
Inside network
(private addresses)
NAT

NAT

- Network Address Translation

- Purpose:
  - support saving addresses
  - (Security features)
- Operation:
  - Translate inside address to outside address
  - Translate outside address to inside address
  - Operates at the boundary of networks

NAT operation „in nutshell”



NAT: network address translation

Motivation: local network uses just one IP address as far as outside world is concerned:

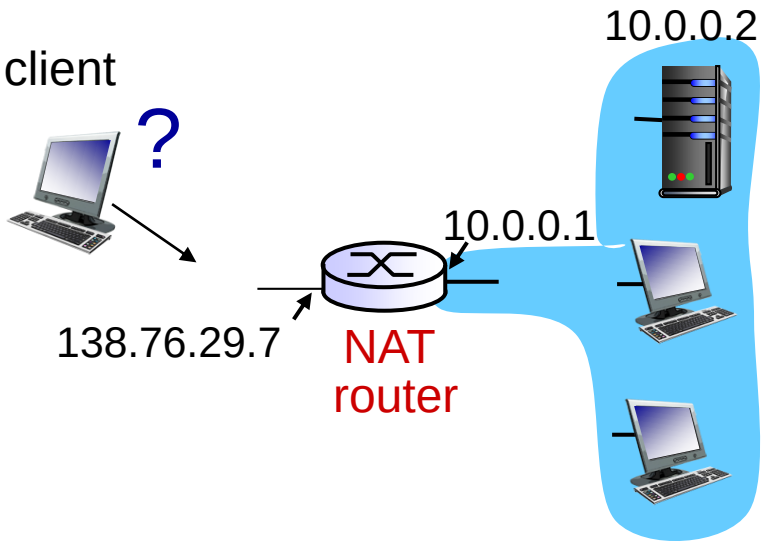
- range of addresses not needed from ISP: just one IP address for all devices
- can change addresses of devices in local network without notifying outside world
- can change ISP without changing addresses of devices in local network
- devices inside local net not explicitly addressable, visible by outside world (a security plus)

NAT: network address translation

- NAT is controversial:
  - routers operate in layer 3
  - violate end-to-end transmission principle
    - application developer must think about NAT
  - lack of IPv4 addresses must be solved with IPv6

NAT traversal problem

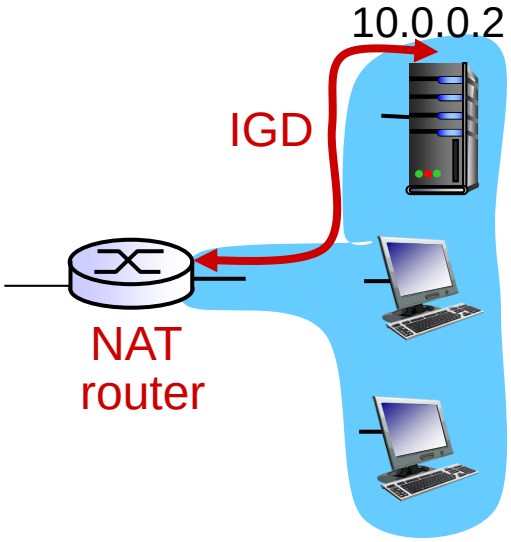
- client wants to connect to server with address 10.0.0.2
  - server address 10.0.0.2 local to lan (client can't use it as destination address)
  - only one externally visible NATed address: 138.76.29.7



- ***Solution 1***
  - statically configure NAT to forward incoming connection requests at given port to server
    - e.g., 138.76.29.7:2500 always forwarded to 10.0.0.2:4444
  - **Static port forward**

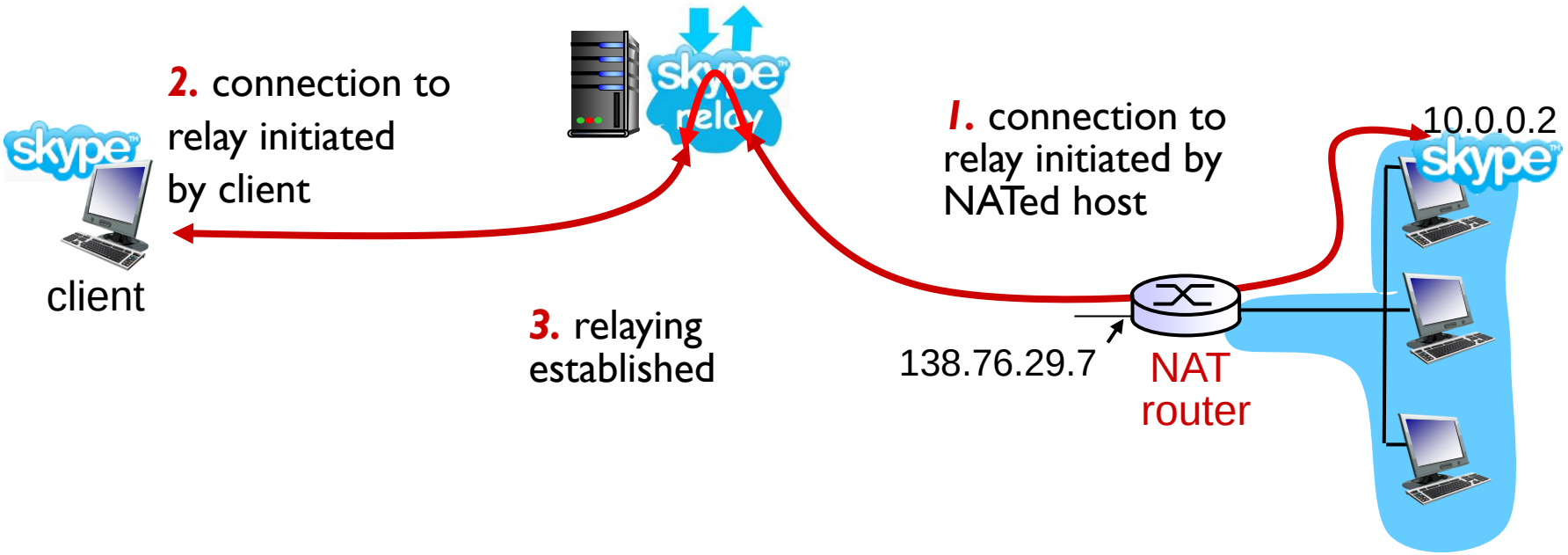
NAT traversal problem

- ***Solution 2***
  - Universal Plug and Play (UPnP) Internet Gateway Device (IGD) protocol.
  - Allow NATed host to:
    - learn public IP address (138.76.29.7)
    - add/remove port mappings (with lease times)
  - **Dynamic port forward**



NAT traversal problem

- ***Solution 3***
  - **Relaying (NAT relay)**
  - NATed client establishes connection to relay
  - external client connects to relay
  - relay bridges packets between to connections



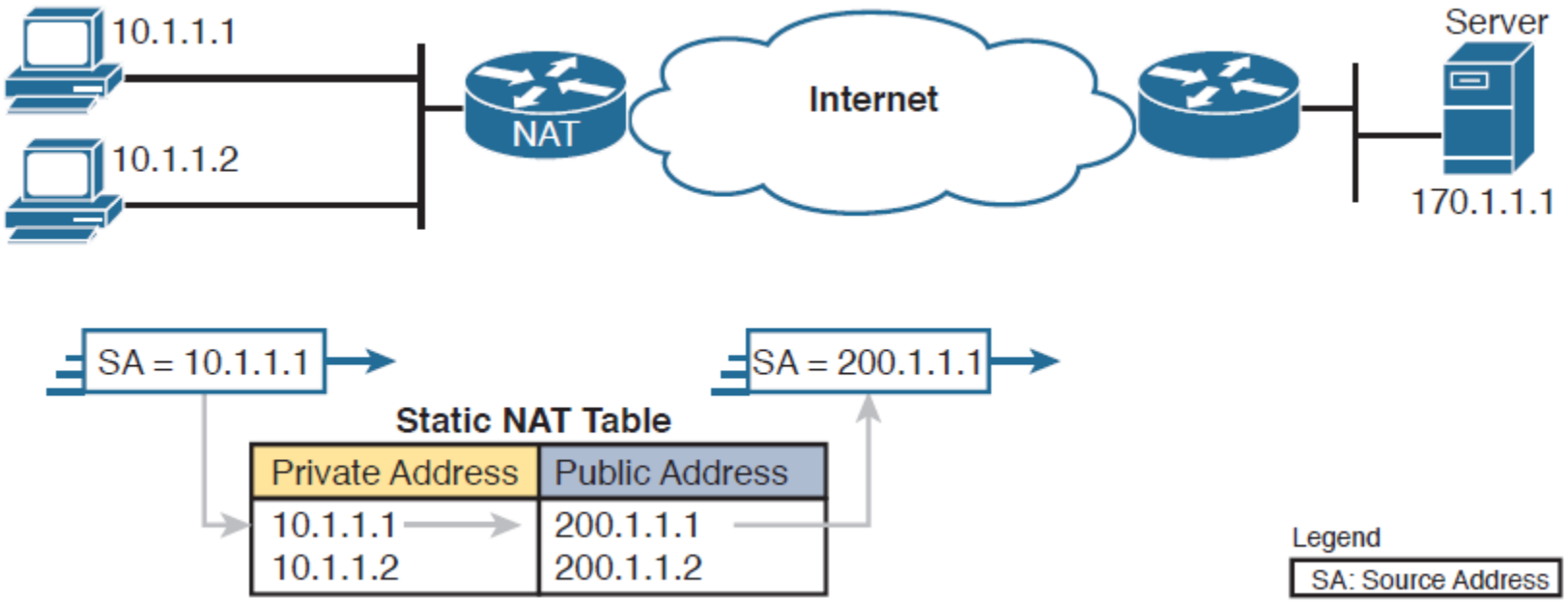
Examine lab network

- Inside local address of your PC?
- Inside global address?
- Conclusion?
  - we are on a NATed network
  - …behind NAT

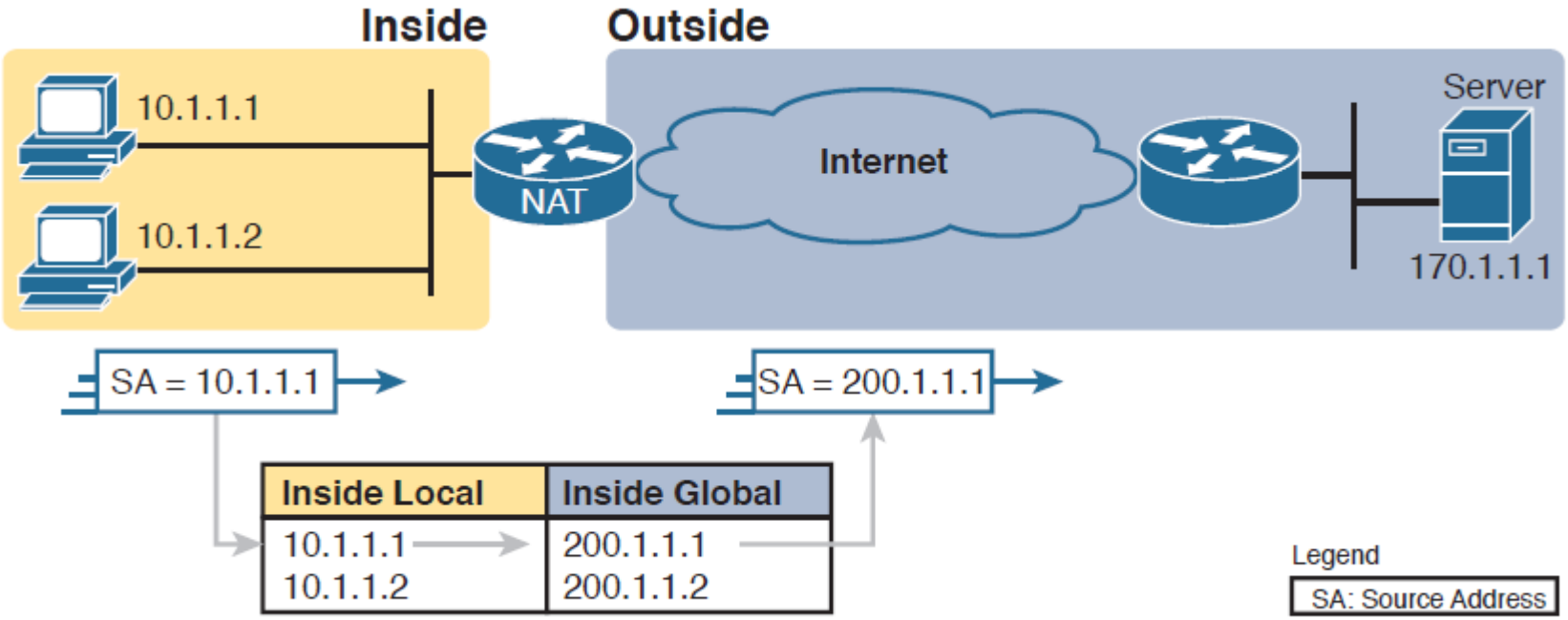
NAT variants

- Static NAT
  - 1 inside IP ←→ 1 outside IP
- Dynamic NAT
  - N inside IP ←→ M outside IP (pool)
- PAT
  - *IP overload*
  - N inside IP ←→ 1 outside IP (IP overload)
  - N inside IP ←→ M outside IP (IP overload)

Static NAT


10.1.1.1
10.1.1.2
NAT
Internet
Server
170.1.1.1
SA = 10.1.1.1
SA = 200.1.1.1
Static NAT Table
Private Address
Public Address
10.1.1.1
10.1.1.2
200.1.1.1
200.1.1.2
Legend
SA: Source Address

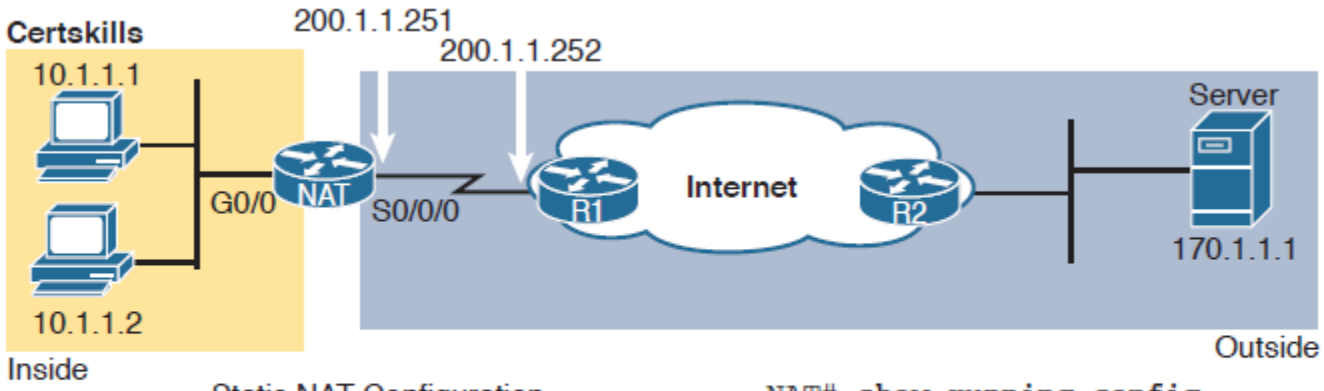
Static NAT


Inside
Outside
10.1.1.1
10.1.1.2
NAT
Internet
Server
170.1.1.1
SA = 10.1.1.1
SA = 200.1.1.1
Inside Local
Inside Global
10.1.1.1
10.1.1.2
200.1.1.1
200.1.1.2
Legend
SA: Source Address

Static NAT (from the reference)

Term	Values in Figures	Meaning
Inside local	10.1.1.1	**Inside:** Refers to the permanent location of the host, from the enterprise's perspective: it is inside the enterprise. **Local:** Means not global; that is, local. It is the address used for that host while the packet flows in the local enterprise rather than the global Internet. **Alternative:** Think of it as inside private, because this address is typically a private address.
Inside global	200.1.1.1	**Inside:** Refers to the permanent location of the host, from the enterprise's perspective. **Global:** Means global as in the global Internet. It is the address used for that host while the packet flows in the Internet. **Alternative:** Think of it as inside public, because the address is typically a public IPv4 address.
Outside global	170.1.1.1	With source NAT, the one address used by the host that resides outside the enterprise, which NAT does not change, so there is no need for a contrasting term. **Alternative:** Think of it as outside public, because the address is typically a public IPv4 address.
Outside local	—	This term is not used with source NAT. With destination NAT, the address would represent a host that resides outside the enterprise, but the address used to represent that host as packets pass through the local enterprise.

Example (static)

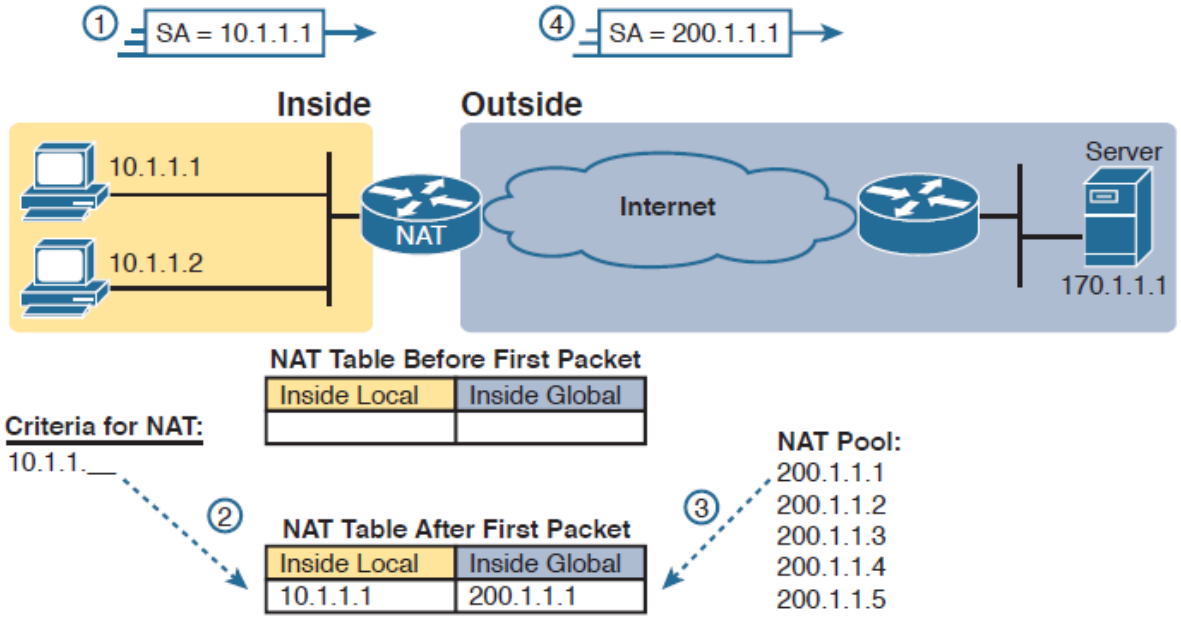


Static NAT Configuration

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

```
NAT# show running-config
!
! Lines omitted for brevity
!
interface GigabitEthernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip nat inside
!
interface Serial0/0/0
 ip address 200.1.1.251 255.255.255.0
 ip nat outside
!
ip nat inside source static 10.1.1.2 200.1.1.2
ip nat inside source static 10.1.1.1 200.1.1.1
```

Dynamic NAT



1. Host 10.1.1.1 sends its first packet to the server at 170.1.1.1.
2. As the packet enters the NAT router, the router applies some matching logic to decide whether the packet should have NAT applied. Because the logic has been configured to match source IP addresses that begin with 10.1.1, the router adds an entry in the NAT table for 10.1.1.1 as an inside local address.
3. The NAT router needs to allocate an IP address from the pool of valid inside global addresses. It picks the first one available (200.1.1.1, in this case) and adds it to the NAT table to complete the entry.
4. The NAT router translates the source IP address and forwards the packet.

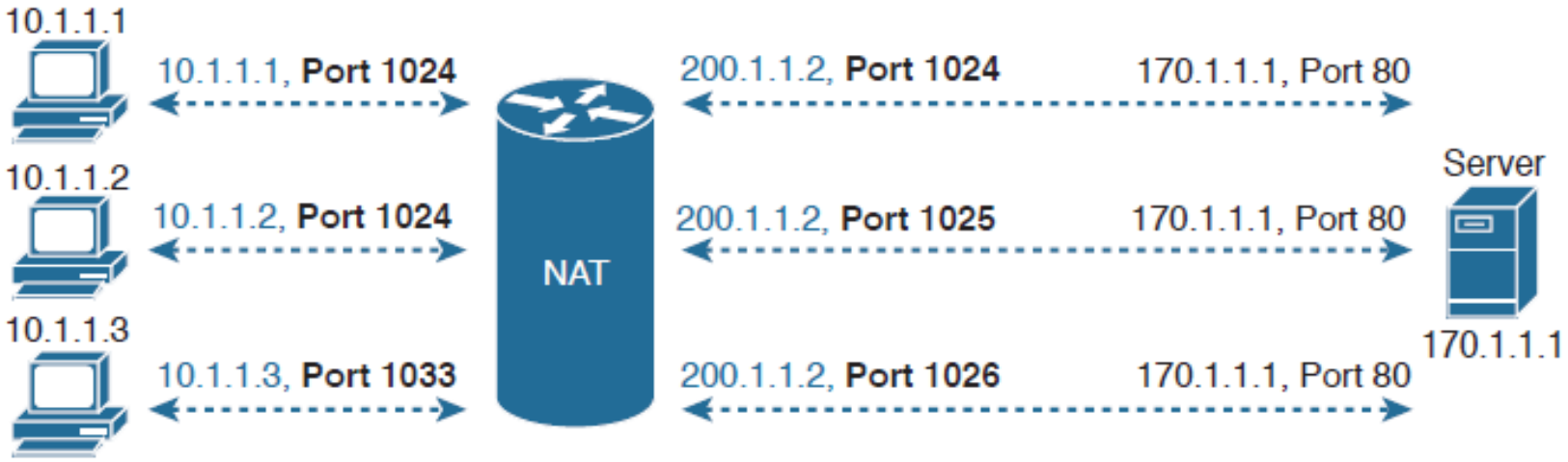
Example (dynamic)

```
NAT# show running-config
!
! Lines omitted for brevity
!
interface GigabitEthernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip nat inside
!
interface Serial0/0/0
 ip address 200.1.1.251 255.255.255.0
 ip nat outside
!
ip nat pool fred 200.1.1.1 200.1.1.2 netmask 255.255.255.252
ip nat inside source list 1 pool fred
!
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.1
```

PAT

- Port Address Translation
  - 1 public address with several private addresses
  - Translation: global IP + port#
- Port
  - 16 bits (max. 65536)
  - In practice ~4000 inside address
  - If it is possible, use the original port number

PAT concept



Inside Local	Inside Global
10.1.1.1: **1024**	200.1.1.2: **1024**
10.1.1.2: **1024**	200.1.1.2: **1025**
10.1.1.3: **1033**	200.1.1.2: **1026**

Dynamic NAT Table, With Overloading

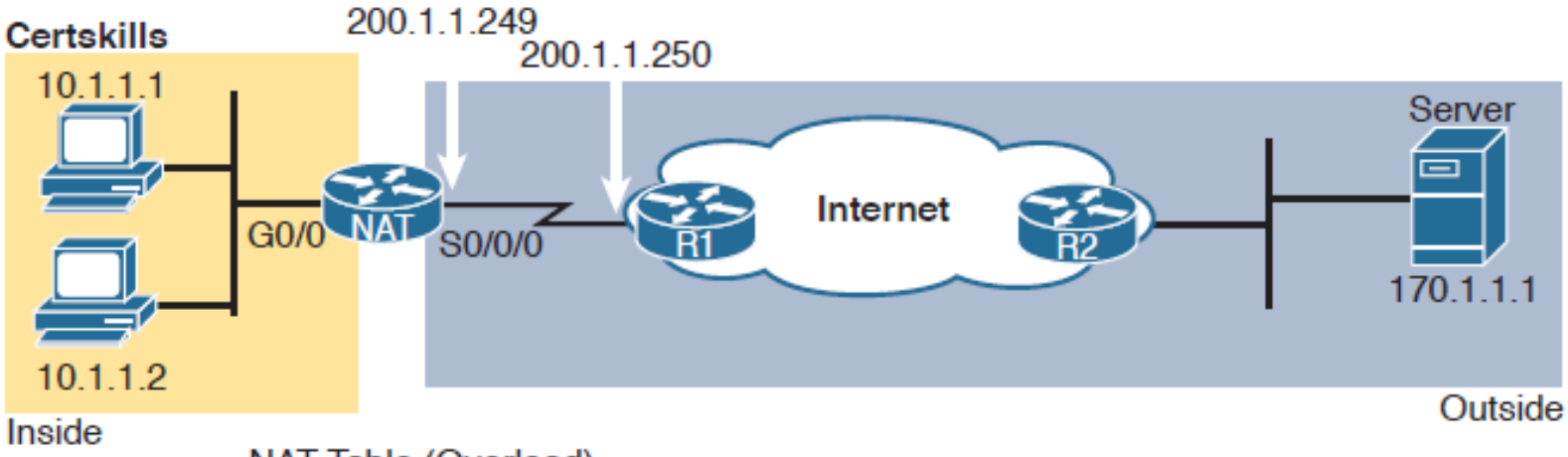
PAT configuration

- Two possible configuration

  - **Case A**
    We have only 1 public address, PAT overloads one address (or interface)

  - **Case B**
    We have more public IP addresses, so PAT overloads a public IP pool

PAT example



NAT Table (Overload)

Inside Local	Inside Global
10.1.1.1: 3212	200.1.1.249: 3212
10.1.1.2: 3213	200.1.1.249: 3213
10.1.1.2: 38913	200.1.1.249: 38913

PAT example

```
NAT# show running-config
!
! Lines Omitted for Brevity
!
interface GigabitEthernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip nat inside
!
interface Serial0/0/0
 ip address 200.1.1.249 255.255.255.252
 ip nat outside
!
ip nat inside source list 1 interface Serial0/0/0 overload
!
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.1
!
```

Check settings

Router# **show ip nat translations**

```
NAT# show ip nat translations
Pro Inside global         Inside local       Outside local      Outside global
--- 200.1.1.1             10.1.1.1           ---                ---
--- 200.1.1.2             10.1.1.2           ---                ---
```

```
NAT# show ip nat translations
Pro Inside global         Inside local       Outside local      Outside global
tcp 200.1.1.249:3212      10.1.1.1:3212      170.1.1.1:23       170.1.1.1:23
tcp 200.1.1.249:3213      10.1.1.2:3213      170.1.1.1:23       170.1.1.1:23
tcp 200.1.1.249:38913     10.1.1.2:38913     170.1.1.1:23       170.1.1.1:23
```

Reuse addresses

```
Router# clear ip nat translation *
```

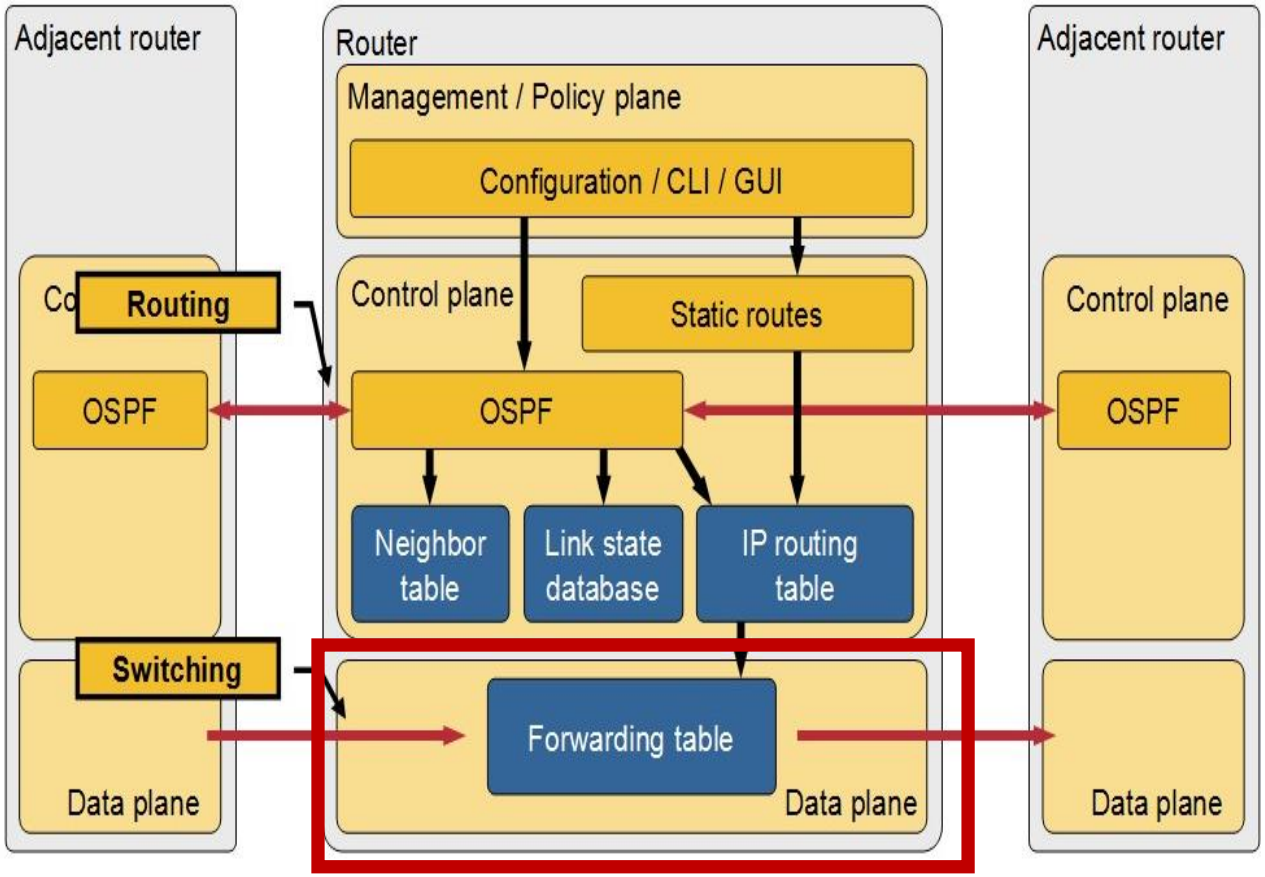
```
! Host 10.1.1.1 currently uses inside global 200.1.1.1
NAT# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 200.1.1.1          10.1.1.1           ---                ---
NAT# clear ip nat translation *
```

Chapter 06

ACL service

NFP framework

- Network Foundation Protection framework



Firewall definition

- „A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules”

Type of firewalls

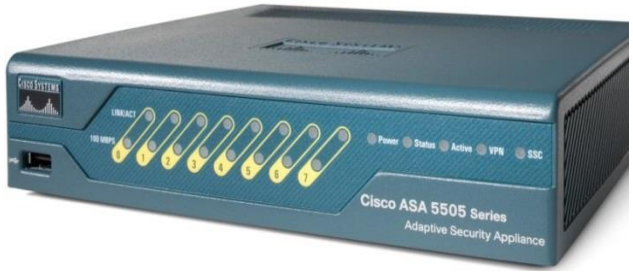
- Packet filtering firewall
- Stateful packet filtering firewall
- Proxy firewall
  - Application layer gateway
- NAT firewall

Packet filtering firewall

- Rules for
  - Outgoing packets
  - Incoming packets
- Decision
  - Permit packets
  - Deny packets

Locating firewalls

- Network
  - Router packet filtering module
    - E.g. Cisco ACL
  - Hardware firewall
    - E.g. Cisco ASA (Adaptive Security Appliance)
- Endpoint firewall
  - Enterprise
    - E.g. iptables
  - Personal
    - E.g. Kaspersky firewall

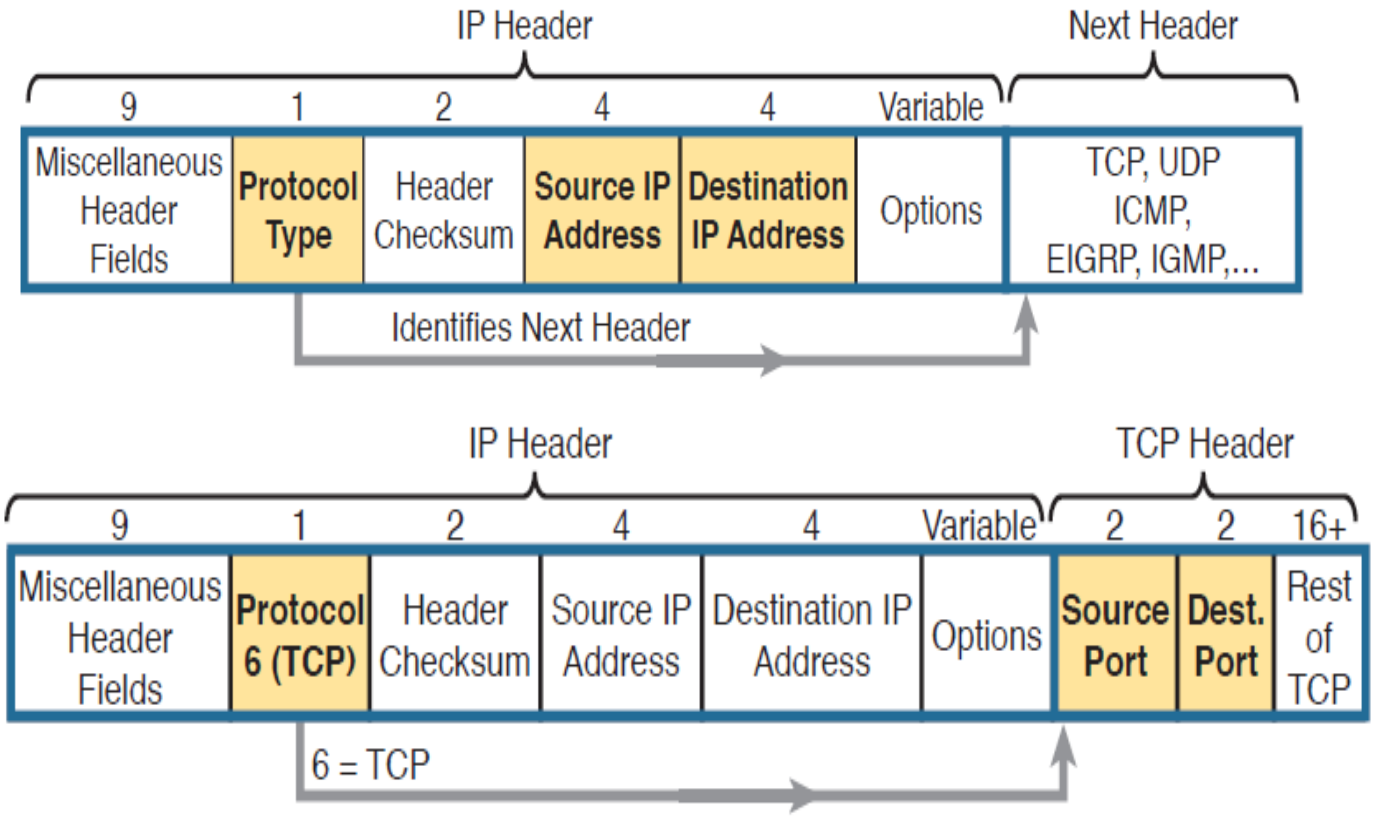


ACL

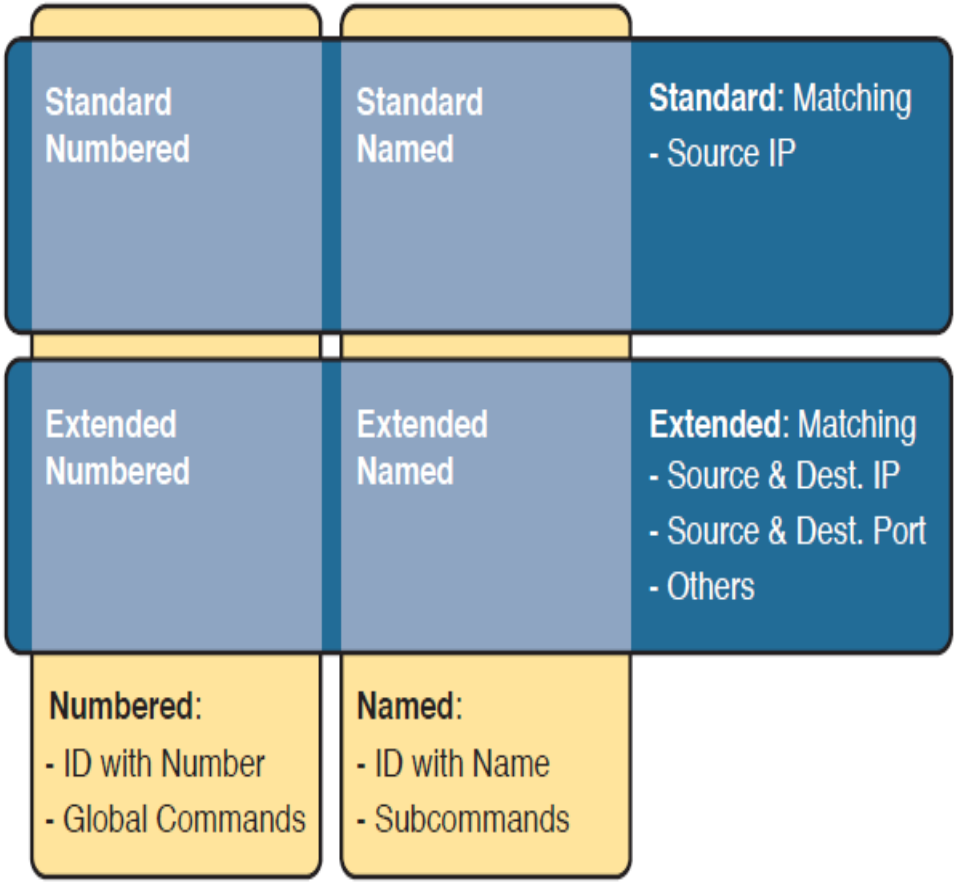
- **A**ccess **C**ontrol **L**ist
- Cisco IOS devices
- packet filtering firewall

Packet filtering

- L3 and L4 parameters



ACL types



Standard Numbered ACL

- Most simple one
- Filltering based on
  - Only the source IP address
- ACL ID
  - **1-99**
  - 1300-1999
- deny any

Configuring

- Create ACL

```
(config)#access-list access_list_number
                    {permit|deny} matching_parameter
```

- Attach to an interface

```
(config)#interface gigabitEthernet 0/0
(config-if)#ip access-group access_list_number {in|out}
```

Matching logic

- Matching
  - Group of IP addresses (IP+wildcard)
  - Only one IP address (host+IP)
  - Every IP addresses (any)

Group of addresses

- Matching parameter
  - IP address
  - Wildcard mask

- E.g. **192.168.1.0 0.0.0.255**

Wildcard mask

- Wildcard mask (WC mask)
  - **0** bits
    - Matching required
  - **1** bits
    - Matching not required

Example

`192.168.1.4 0.0.0.255`

192	168	1	4
0	0	0	255
192	168	1	x

- Does this IP address match?
  - 192.168.1.56
  - 192.168.2.1

Example

192.168.1.4 0.0.0.255

11000000	10101000	00000001	00000100
00000000	00000000	00000000	11111111
11000000	10101000	00000001	xxxxxxxx

- Does this IP address match?
  - 192.168.1.56
  - 192.168.2.1

Matching only one IP address

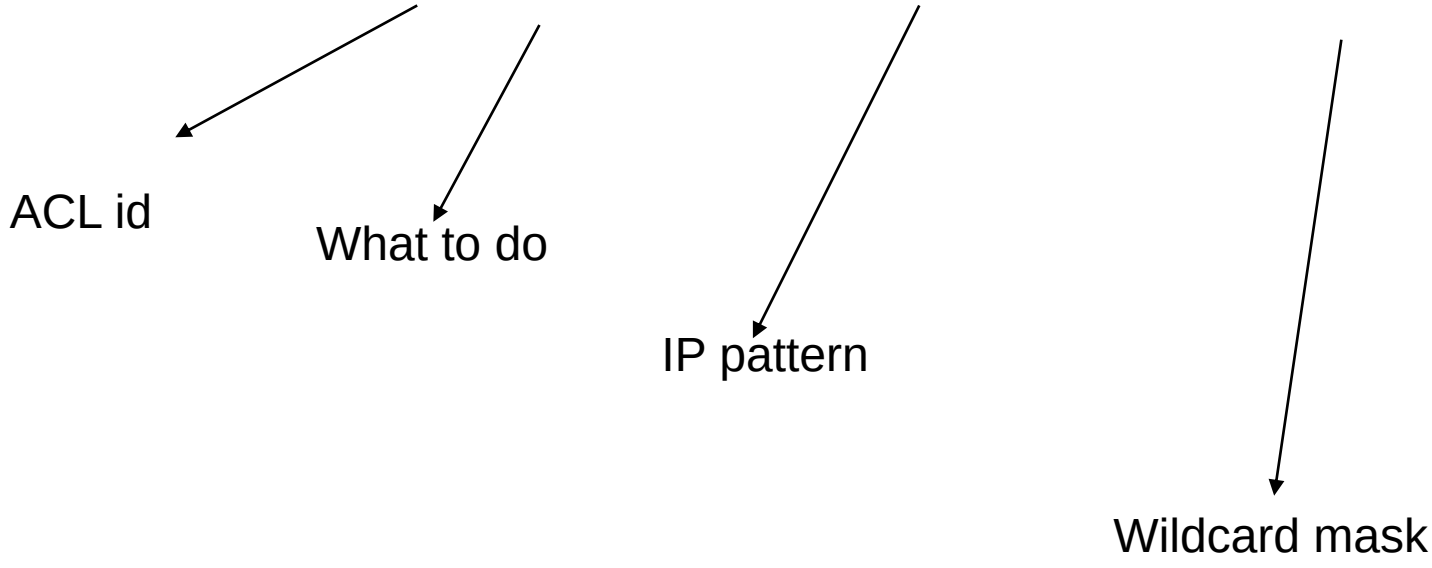
- Matching parameter
  - IP address and wildcard mask **0.0.0.0**
  - or **host** word before the IP address
  - or only the IP address→ only latest IOS versions
- Example (different syntax but same operation)
  - #accsess-list 33 deny 192.168.1.55 0.0.0.0
  - #accsess-list 33 deny host 192.168.1.55
  - #accsess-list 33 deny 192.168.1.55

Matching every IP addresses

- Matching parameter
  - IP address and **255.255.255.255** WC mask
  - or the word **any**
- Example (the two solutions are equivalent)
  - #accsess-list 33 deny 192.168.1.55 255.255.255.255
  - #accsess-list 33 deny any

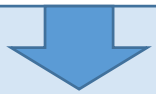
Standard ACL example

```
#access-list 7 permit 172.16.0.0 0.0.255.255
```



Standard ACL config example

ACL with two rules



```
Make a list
R(config)#access-list 8 deny host 192.168.1.55
R(config)#access-list 8 permit any
```

(DENY ANY) ←Don't forget! Deny any is always there.

```
Attache the list to an interface
R(config-if)#ip access-group 8 in
```

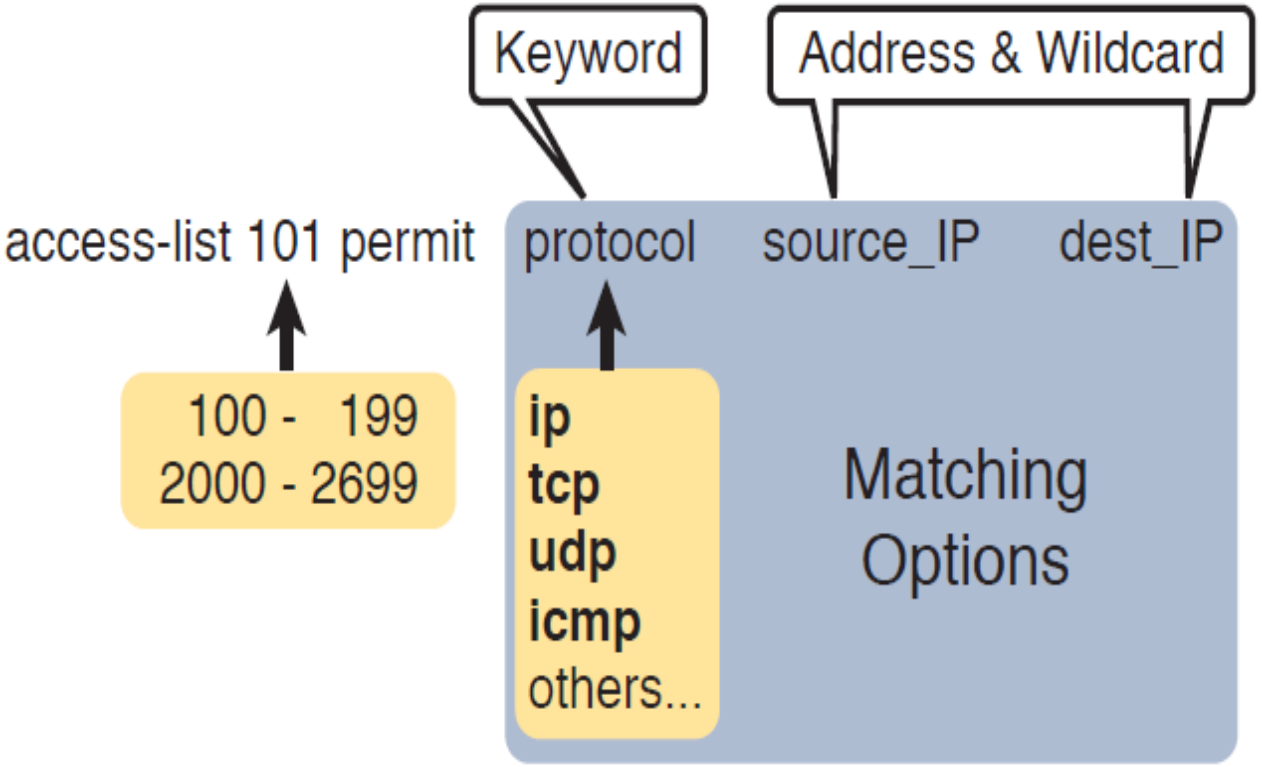
Standard ACL location

- Standard ACL's are always has to be configured nearest to the **destination**.

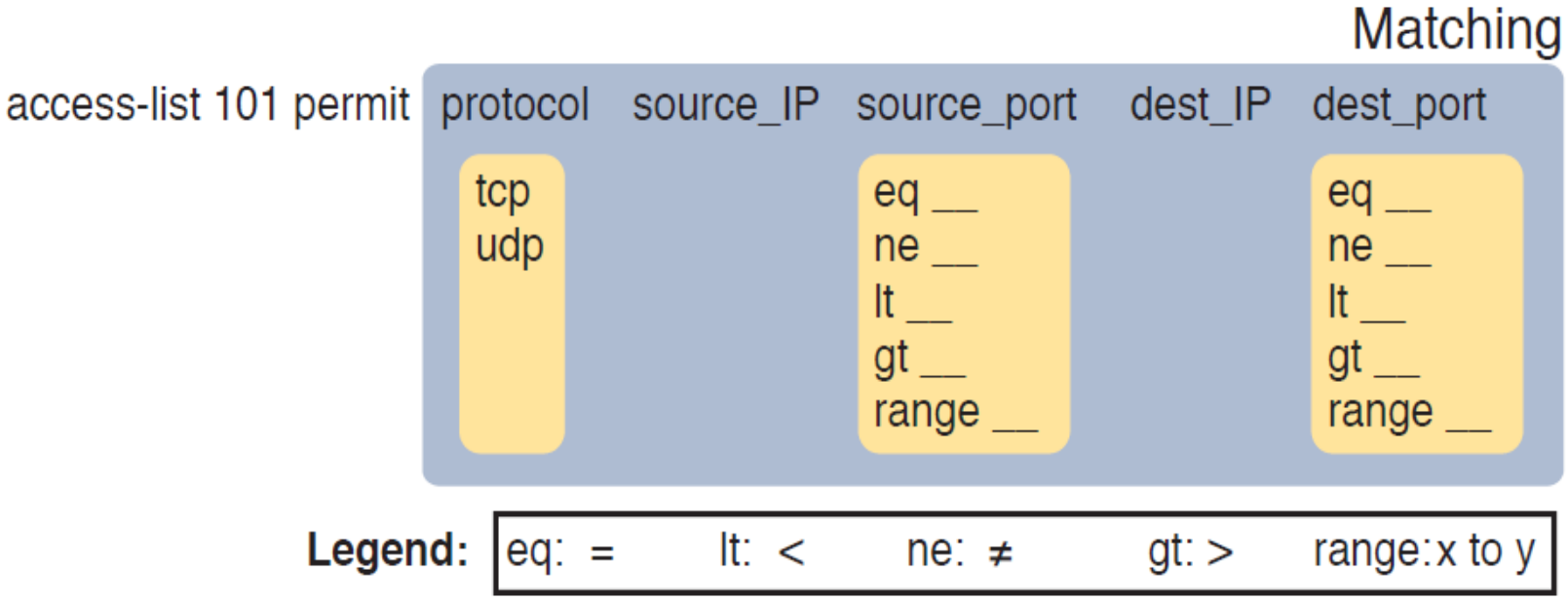
Extended ACL

- Extended ACL
- More complex than standard
- Filtering based on
  - Source IP address
  - Destination IP address
  - Protocol
  - Port number
- ACL ID
  - **100-199**
  - 2000-2699
- Implicit deny any

Extended ACL



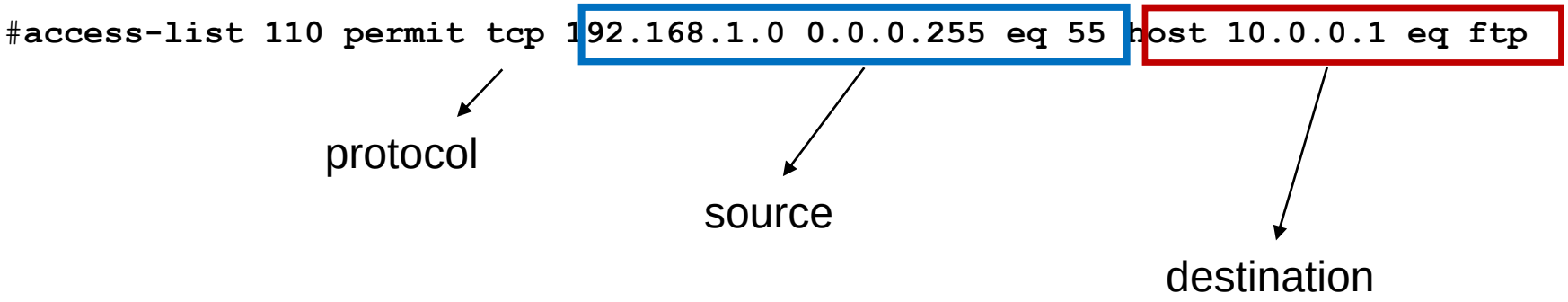
Matching parameters



Protocol numbers and keywords

Port Number(s)	Protocol	Application	access-list Command Keyword
20	TCP	FTP data	ftp-data
21	TCP	FTP control	ftp
22	TCP	SSH	—
23	TCP	Telnet	telnet
25	TCP	SMTP	smtp
53	UDP, TCP	DNS	domain
67	UDP	DHCP Server	—
68	UDP	DHCP Client	—
69	UDP	TFTP	tftp
80	TCP	HTTP (WWW)	www
110	TCP	POP3	pop3
161	UDP	SNMP	snmp
443	TCP	SSL	—
514	UDP	Syslog	—
16,384 – 32,767	UDP	RTP (voice, video)	—

Extended ACL example



Extended ACL location

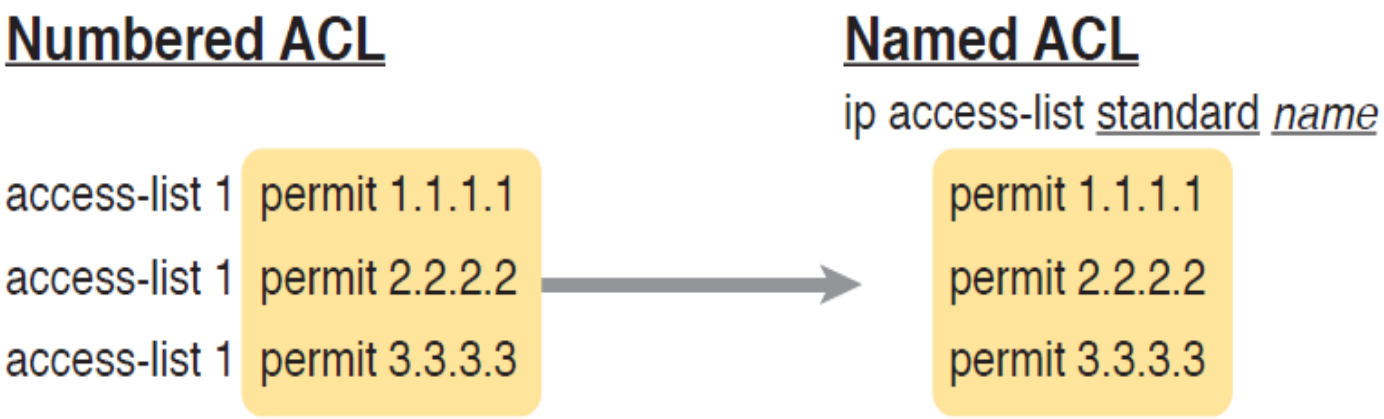
- Extended ACL's are always has to be configured nearest to the **source**.

NACL

- **N**amed **ACL**
- Use a name to identify an ACL (instead of a number)
- Difference only in syntax

NACL

- Different syntax



NACL example

- Standard NACL

```
Router(config)#ip access-list standard Proba
Router(config-std-nacl)#deny host 192.168.1.5
Router(config-std-nacl)#deny host 192.168.1.6
Router(config-std-nacl)#permit any
```

- Extended NACL

```
Router(config)#ip access-list extended Proba_kiterjesztett
Router(config-ext-nacl)#deny tcp host 10.0.0.1 any eq www
Router(config-ext-nacl)#deny tcp host 10.0.0.1 any eq 21
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#
Router(config-ext-nacl)#
```

Show command

```
Router#show access-lists
Standard IP access list Proba
    10 deny host 192.168.1.5
    20 deny host 192.168.1.6
    30 permit any
Extended IP access list Proba_kiterjesztett
    10 deny tcp host 10.0.0.1 any eq www
    20 deny tcp host 10.0.0.1 any eq ftp
    30 permit ip any any
Standard IP access list 1
    deny host 192.168.1.1
    permit any
Extended IP access list 155
    permit ip host 10.0.0.1 any
    permit ip host 10.0.0.2 any
```

PÉCSI TUDOMÁNYEGYETEM
MŰSZAKI ÉS INFORMATIKAI KAR

Chapter 07

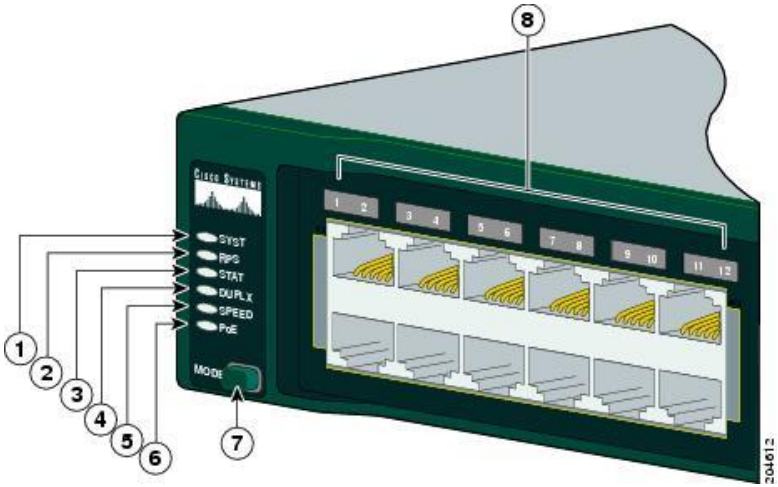
Switches and VLAN

L2 switches

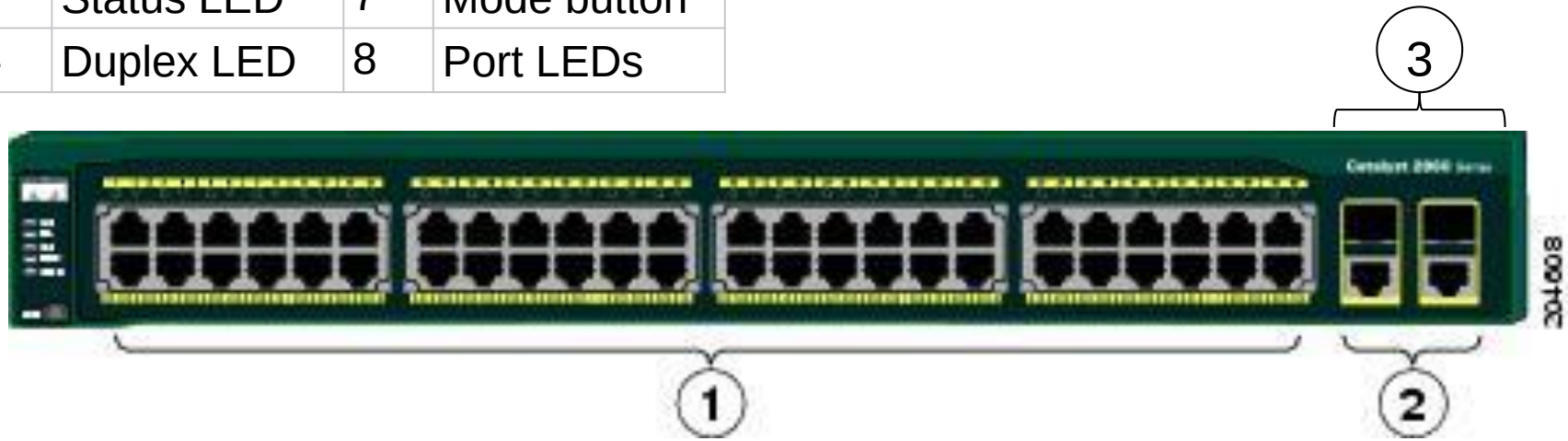
- Central elements of the star topology
- Basic elements of LANs

Cisco Catalyst 2960 family

Forward plane



1	SYST LED	5	Speed LED
2	RPS LED	6	PoE LED
3	Status LED	7	Mode button
4	Duplex LED	8	Port LEDs

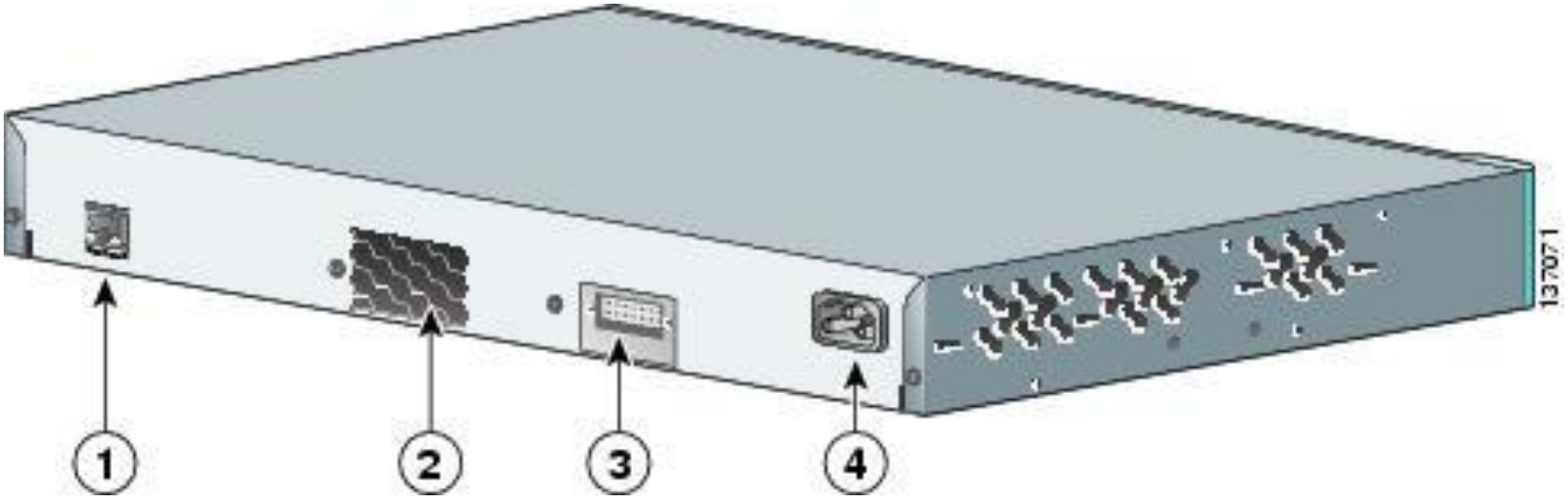


1	Standard ports	3	SFP module slot
2	Uplink ports		

SFP module

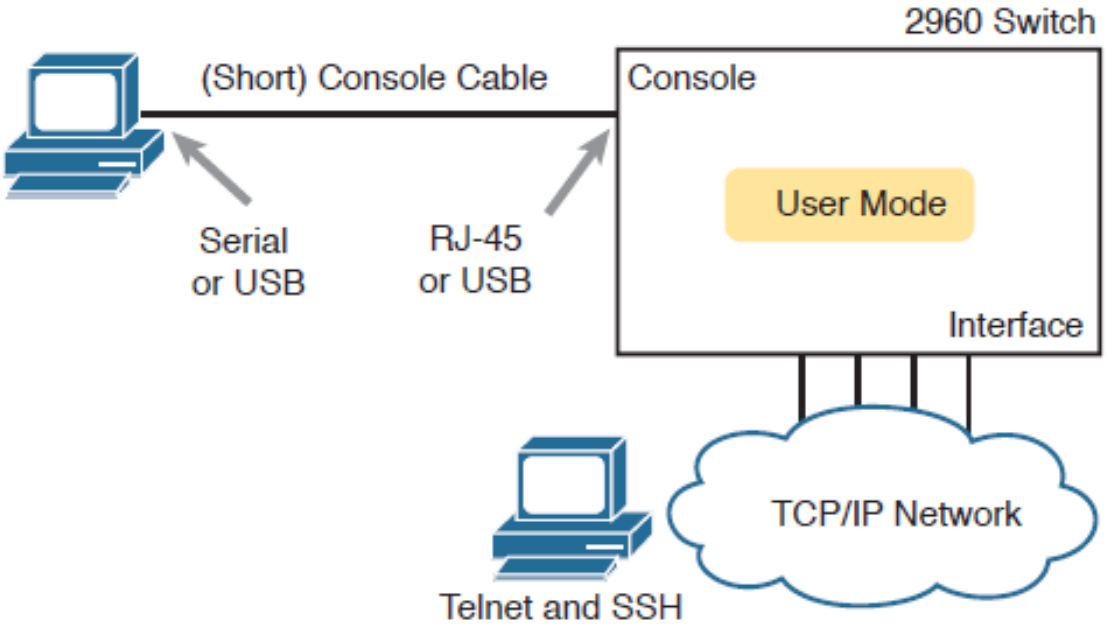

GLC-SX-MM
30-1301-01
Class 1 21CFR1040.10
MADE IN MALAYSIA
SN: FNS0839P1WV
COM

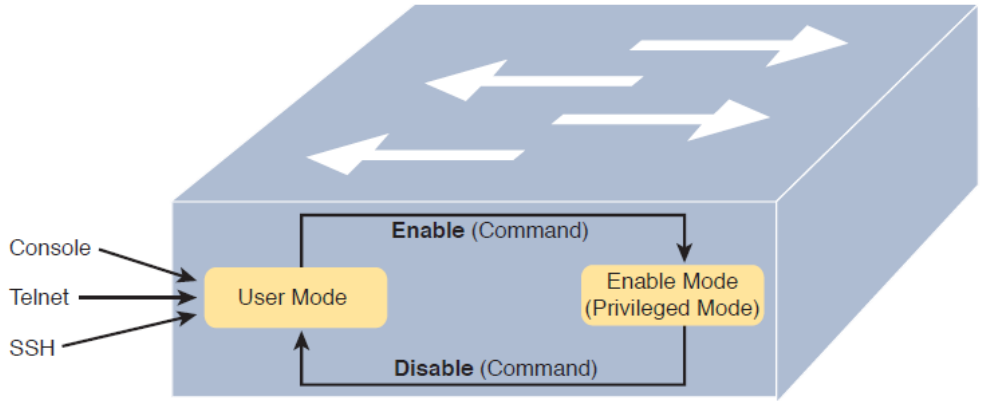
Backplane



1	RJ-45 console port	3	RPS connector
2	Fan exhaust	4	AC power connector

Access





Cisco IOS®
SOFTWARE

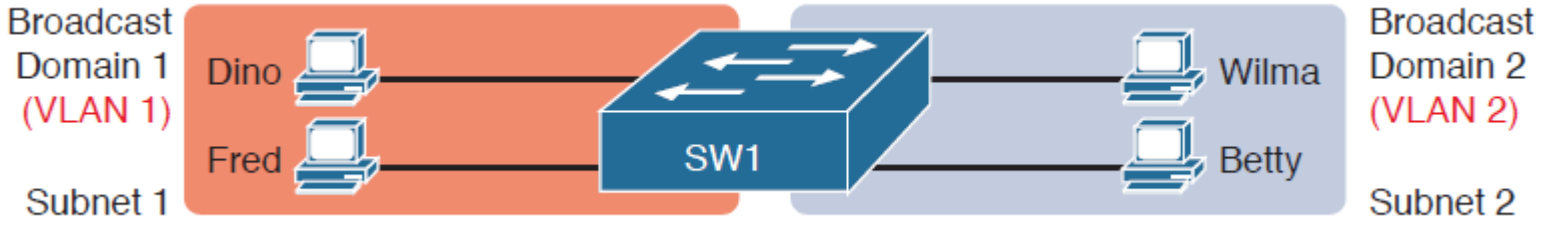
Switches

- Every switch make an independent broadcast domain

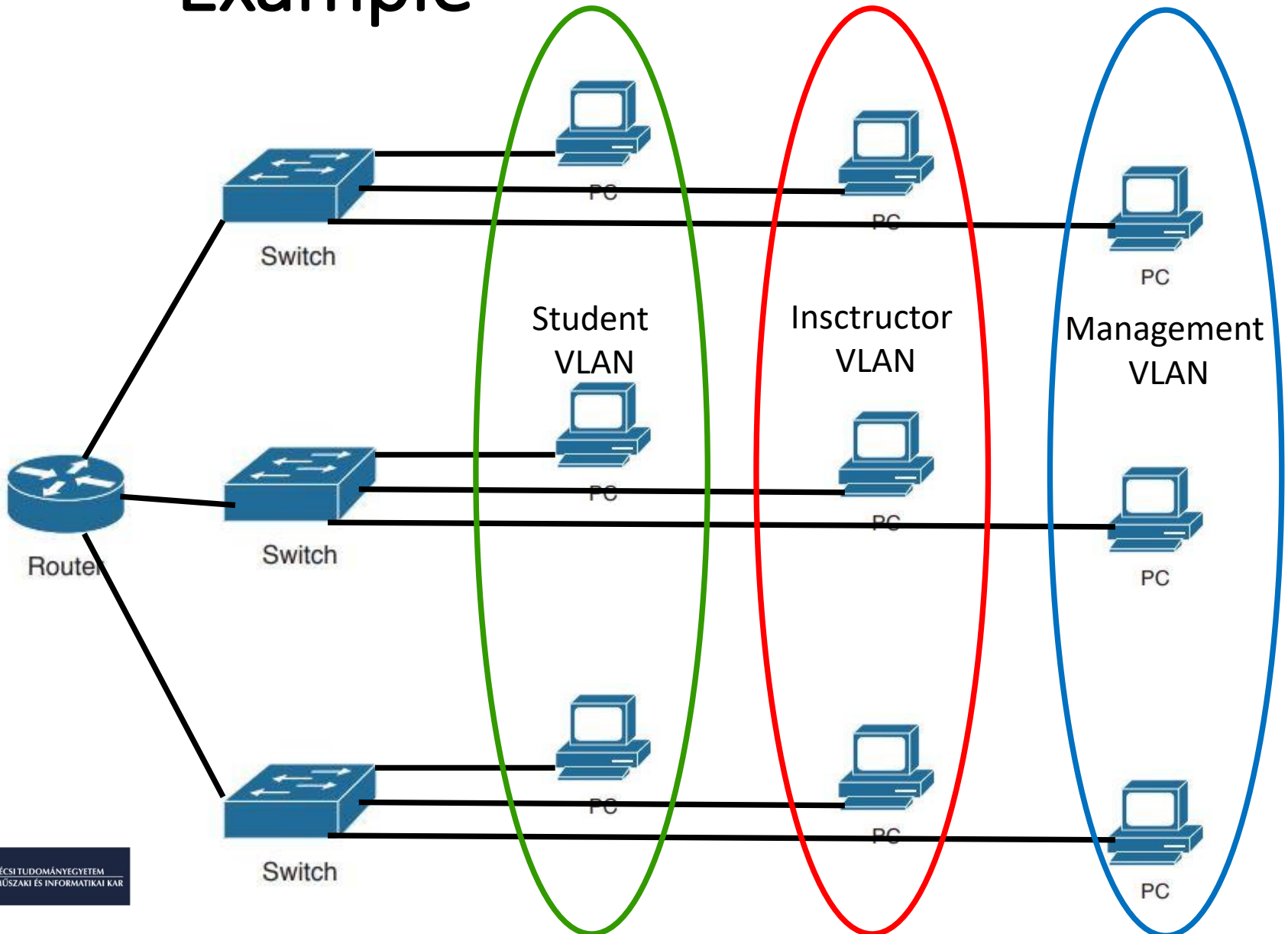
VLAN

- VLAN (Virtual Local Area Network)

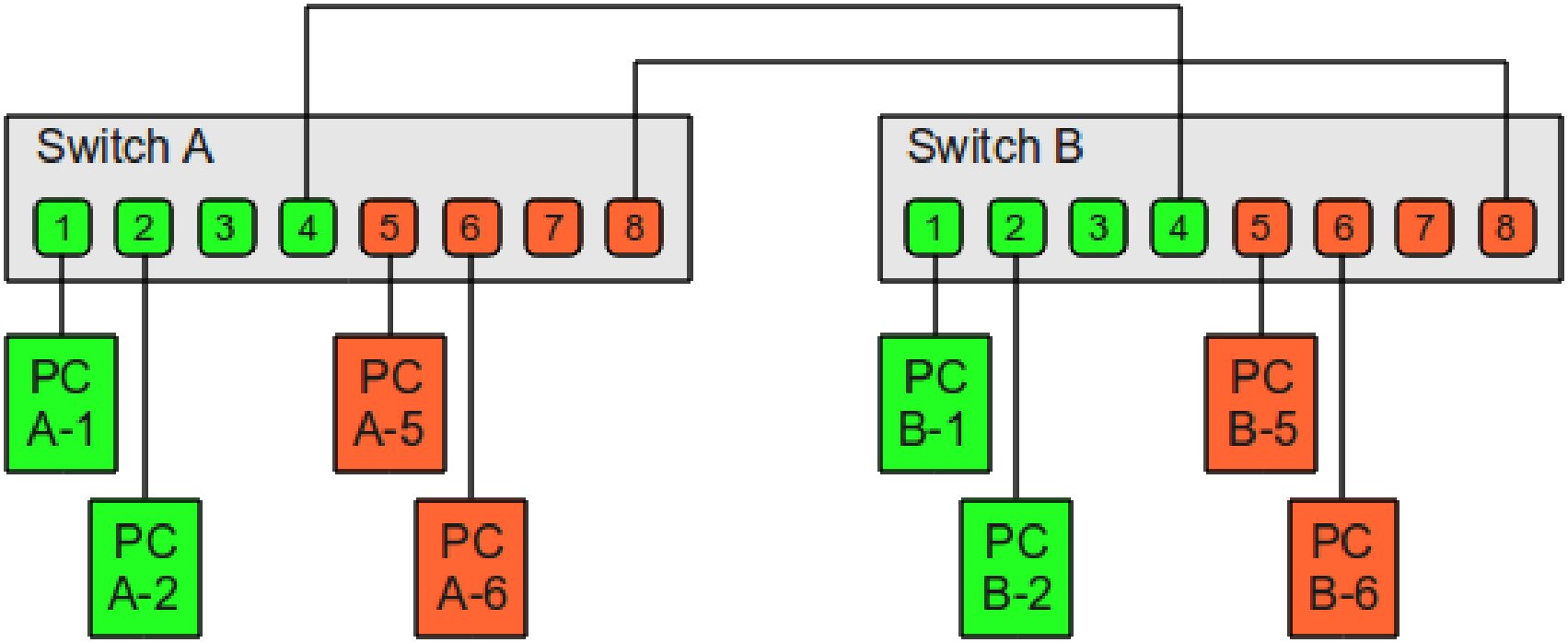
- Purpose
  - Making independent broadcast domains on one physical device
  - Logical grouping of hosts
    - irrespective of their physical location



Example


Switch
PC
PC
PC
Student
VLAN
Insctructor
VLAN
Management
VLAN
Router
Switch
PC
PC
PC
Switch
PC
PC
PC

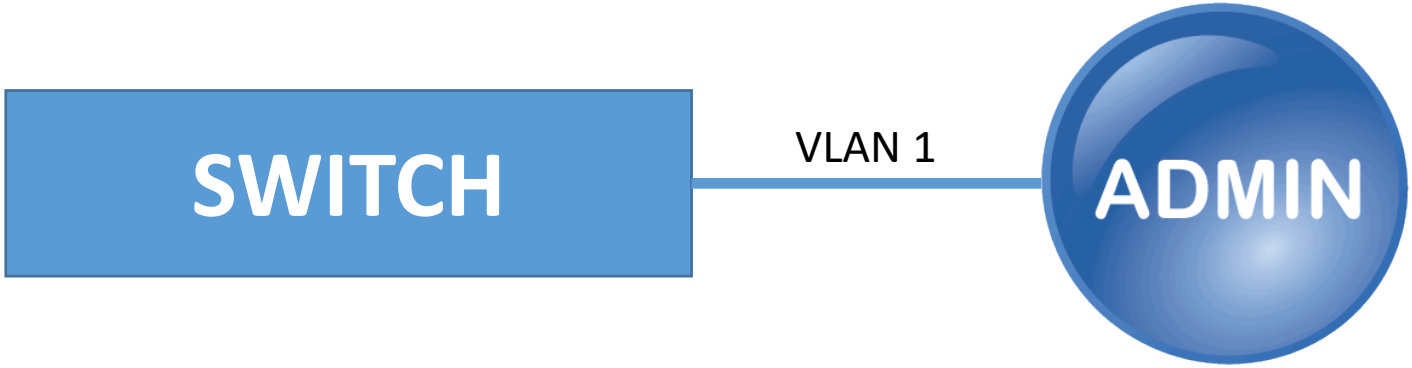
Port based VLAN



Different ports belongs to different virtual networks.

Administrative VLAN

- **VLAN id is 1**
- also known as the Management VLAN
- Default VLAN (all ports assigned to this VLAN)



Advantages of VLANs

- Limit the size of broadcast domains
- Keeps the hosts separated
- Limiting what device can talk ot other device
- Cost efficient
- Less complex to manage

Disadvantages of VLANs

- Complex management
- Possible interoperability
- VLAN cannot forward traffic to another VLAN
  - Solution:
    - Router
    - Layer 3 switch

VLAN configuration

- VLAN ID and name settings
  - `Switch(config)#vlan vlan_id`
  - `Switch(config-vlan)#name vlan_name`
  - `Switch(config-vlan)#exit`

- Assign ports to VLANs
  - `Switch(config)#interface fa0/1`
  - `Switch(config-if)#switchport access vlan vlan_id`
  - `Switch(config-if)#exit`

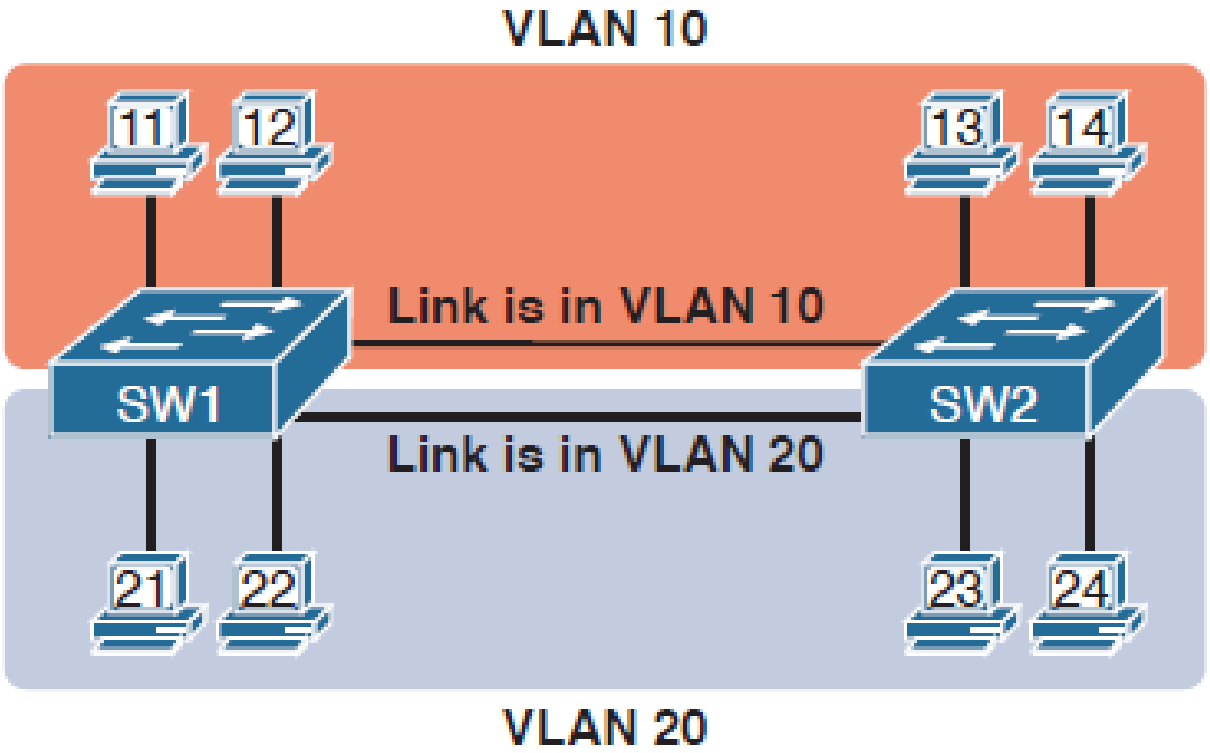
VLAN settings check

```
Switch#show vlan
```

```
VLAN  Name                             Status    Ports
----- -------------------------------- --------- -------------------------------
1     default                          active    Fa0/1, Fa0/4, Fa0/5
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
27    accounting                       active    Fa0/13
28    engineering                      active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12
1002  fddi-default                     active
1003  token-ring-default               active
1004  fddinet-default                  active
1005  trnet-default                    active
```

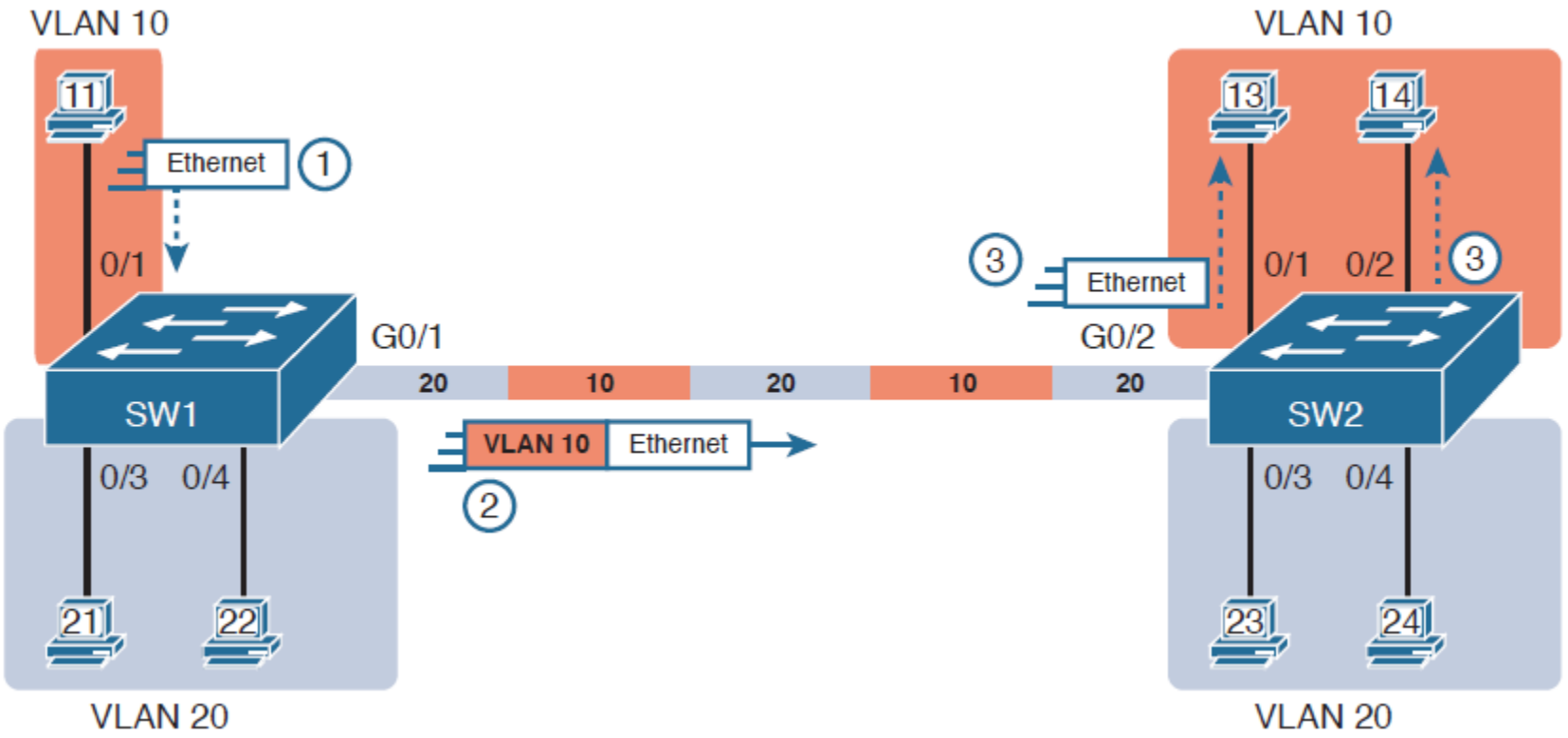
Multiswitch VLAN

- VLANs extended to more switches



Trunking

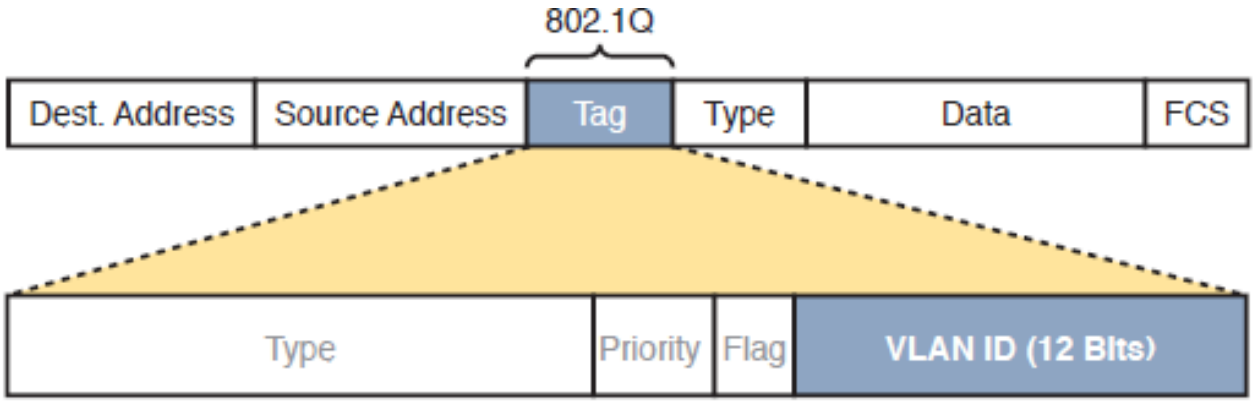
- Multiswitch connection with trunking



Terms

- Access port
  - Only one VLAN traffic
- Trunk port
  - Transfer two or more VLANs traffic

- Trunk protocol
  - IEEE 802.1q (dot1q)



VLAN tagging

- VLAN frame tagging place an unique identifier in the header of each frame
- The identifier can recognize where to forward the package

- The most common tagging schemes
  - ISL (Inter-Switch Link)
  - 802.1Q – An IEEE standard

VLAN tagging

- Inter-Switch Link
  - The ethernet frame is encapsulated with a header, which contains the VLAN ID
  - ISL added by the switch before sending across the trunk and removes before sending it out a non trunk link
  - Adds overhead to the frame 26 byte header containing a 10 bit VLAN ID
- 802.1Q
  - Less overhead than ISL, using only 4 bytes
  - The switch inserts the 802.1Q tag before sending across the trunk, and removes it before sending out a non trunk link

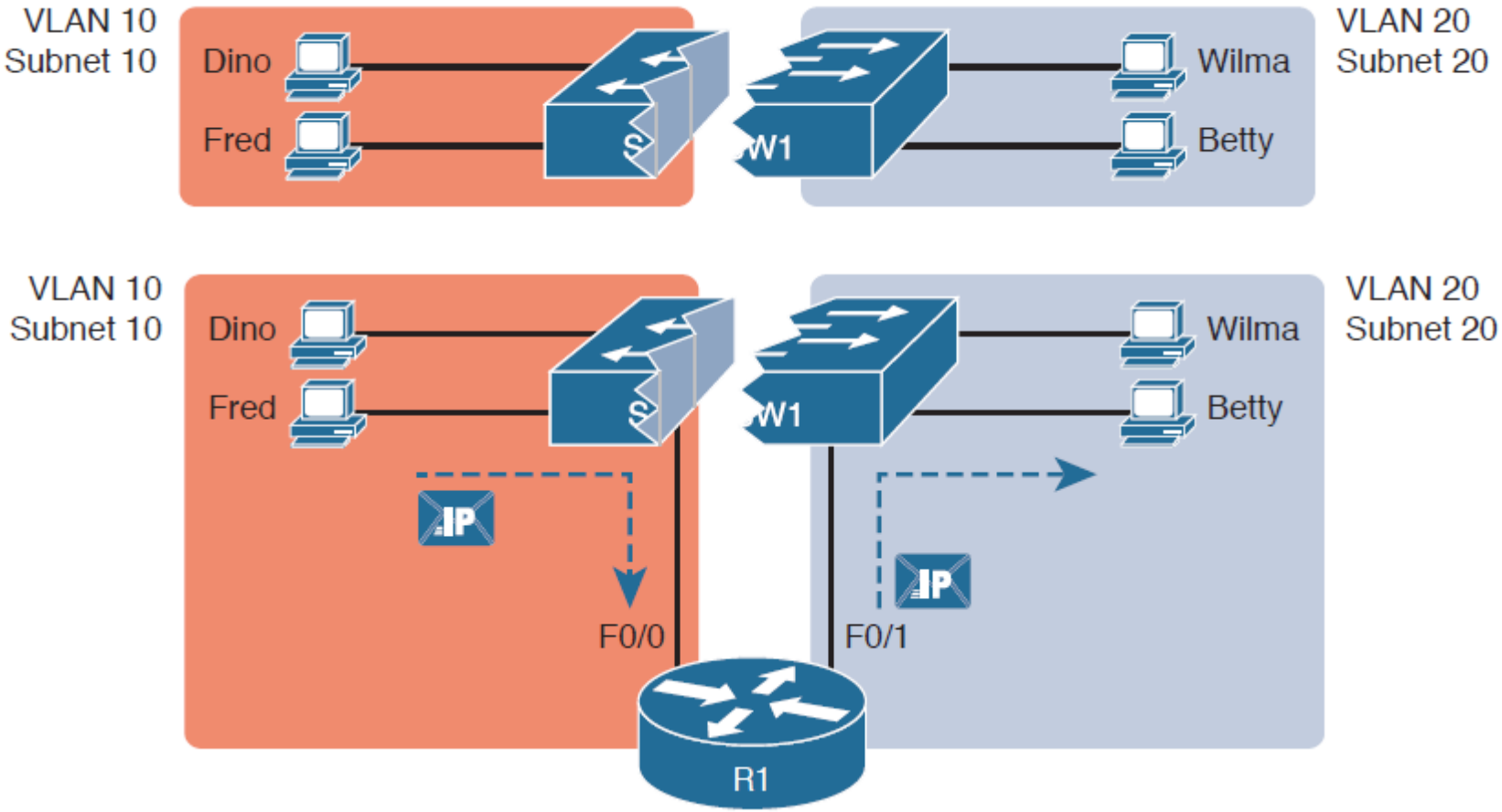
Trunk configuration

```
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
```

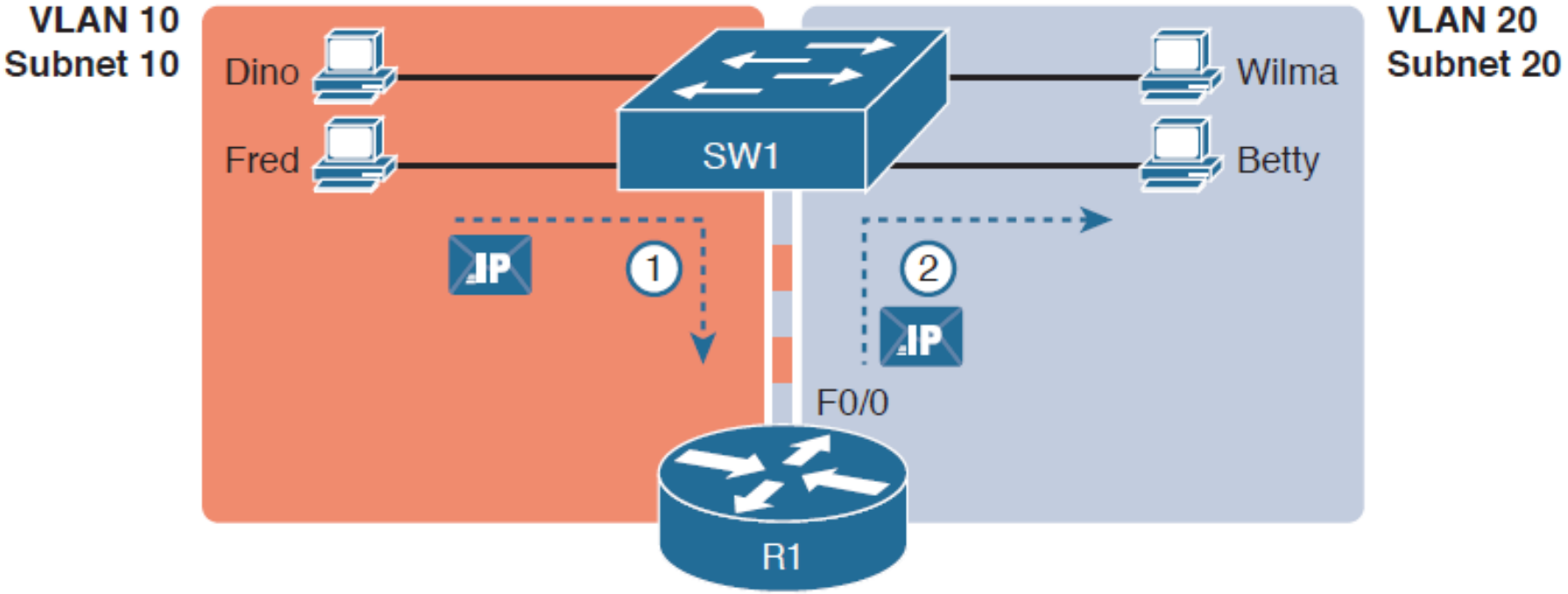
Cisco: **VTP** (Virtual Trunking Protocol)

VLAN connections

- Direct communication only inside VLAN
- Need L3 device (router) between VLANs



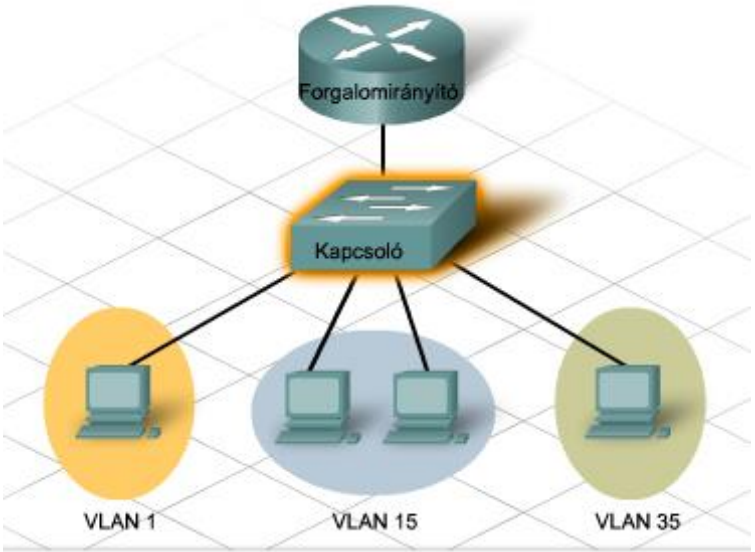
Router side


VLAN 10
Subnet 10
Dino
Fred
SW1
Wilma
Betty
VLAN 20
Subnet 20
IP
1
2
IP
F0/0
R1

Subinterface configuration

- Switch
  - `interface fa2/0`
  - `switchport mode trunk`
- Router
  - `interface fa0/0.10`
  - **`encapsulation dot1q`** *`10`*
  - `ip address …`

Vlan id



L3 switch devices