

École Pour l'Informatique et les Techniques Avancées – EPITA

BSc L1 – 16 May 2024

Course: Introduction to Computer Networks

Introduction to Computer Networks

Date & Time	No.	Topics	Duration (hours)
Fri 19/04/24 – 10:00–13:00	1	Primer, Network protocols, types, topology, architecture	3
Fri 26/04/24 – 10:00–13:00	2	Network models, TCP/IP model, Packet switching	3
Sat 27/04/24 – 10:00–13:00	3	Physical Layer (Function, Signals, Modulation, Multiplexing, Transmission media & Hardware, Optical networks)	3
Sat 27/04/24 – 14:00–17:00	4	Data Link Layer (Function, Framing, Protocols, Flow control, Access control, Error correction, Hardware)	3
Fri 03/05/24 – 14:30–17:30	5	Network Layer (Function, IP addressing and subnets)	3
Sat 04/05/24 – 10:00–13:00	6	Network Layer (Routing algorithms and protocols), Internet Control Message Protocol	3
Tue 14/05/24 – 16:30–19:30	7	Network Layer (IGP & EGP), Autonomous System, Border Gateway Protocol	3
Wed 15/05/24 – 14:30–17:30	8	Transport Layer (Function, Flow and congestion controls, Protocols)	3
Thu 16/05/24 – 11:15–13:15	9	Cross-layer process: Access Control Lists	2

Introduction to Computer Networks

Date & Time	No.	Topics	Duration (hours)
Fri 17/05/24 – 14:00–17:00	10	Application Layer (Function, Protocols)	3
Sat 18/05/24 – 14:00–17:00	11	Cross-layer process: Network Address Translation	3
Fri 24/05/24 – 10:00–13:00	12	Review / Open-session	3
<i>Total</i>			<i>35</i>
Fri 31/05/24 – 14:30–15:30		EXAM	1

GRADING criteria :

- Class participation comprising **attendance & reactivity**): 10%
- **Exercises** (practical work): 40%
- Final evaluation (**Quiz & Exercises**): 50%

i Check policies in the course outline

Lecture 9 Outline

- ▶ **Router ACLs**
 - Operations
 - Application
 - Cisco Syntax
 - Class exercise 13

Router ACLs (operations)


- ▶ Access Control List (ACL):
 - ▶ List of Conditions → Actions: Permit/Deny
 - ▶ To control traffic flow
- ▶ Usually, network traffic goes through conditions from top to down until a match is found
 - ▶ Every ACL has an implicit DENY at the end!
- ▶ Two main types of ACLs:
 - ▶ **Standard**: Filter traffic based on **source** IP address
 - ▶ **Extended**: Filter traffic based on **both** source and destination IP addresses, **as well as other criteria** (e.g., protocol and port number)

Router ACLs (application)

- ▶ Depending on the direction of traffic (source and destination) that needs to be controlled:
 - ▶ You can apply an ACL on either an inbound or outbound interface (based on 'where you stand')
 - ▶ The 'in' direction filters traffic as it enters the interface, 'out' direction filters traffic as it leaves the interface
- ▶ ACLs are applied to traffic in a specific order, based on their number or name:
 - ▶ If Multiple entries in an ACL applied to an interface, traffic will be processed by the ACL with the lowest number or alphabetical name first, and then by the next lowest number or alphabetical name, and so on

Cisco router ACLs (syntax)

- ▶ **Standard access-list (classify traffic based on source IP): IDs 1 – 99 or 1300–1999, Names**

 Apply close to destination

Configure (modern syntax)

Rx(config)# ip access-list standard {ACL_No./Name}

Rx(config-std-nacl)# {permit/deny} X.X.X.X Z.Z.Z.Z //X: host ip, Z: wildcard

Apply, optional: sequence no. behind permit/deny to change filter order

Rx(config)# interface z/z

Rx(config-if)#ip access-group {ACL_No./Name} in/out

- ▶ **Extended access lists (classify traffic based on source IP, destination IP, Protocol, Port no.): IDs 100–199 or 2000–2699, Names**

Configure (modern syntax)

 Apply close to Source

Rx(config)# ip access-list extended {ACL_No./Name}

Rx(config-ext-nacl)# {permit/deny} <Protocol> <Source_IP> <

Source_Wildcard> [Protocol: port no.] <Destination_IP>

<Destination_Wildcard> [Protocol: port no.]

Apply, optional: sequence no. behind permit/deny to change filter order

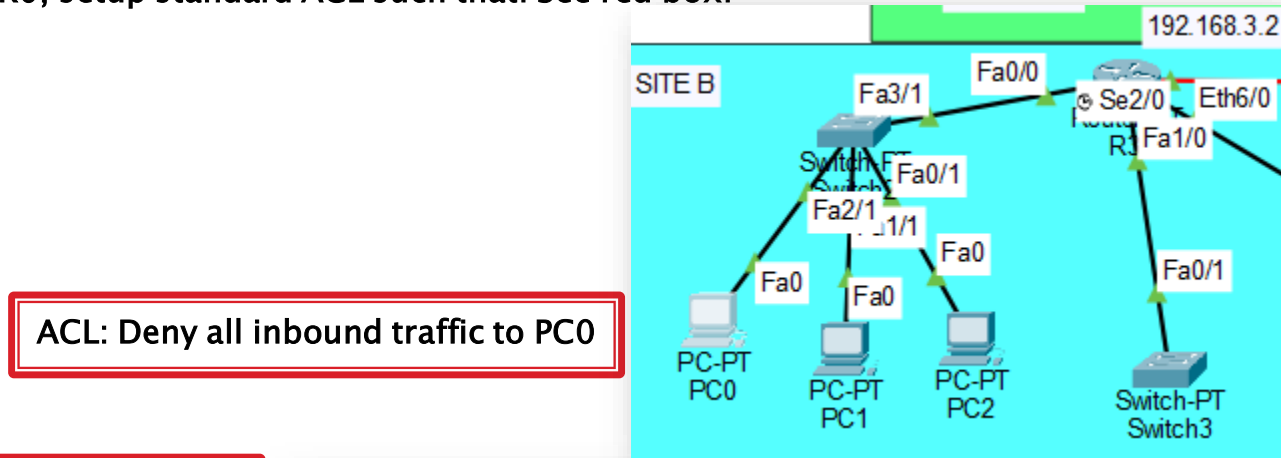
Rx(config)# interface z/z

Rx(config-if)#ip access-group {ACL_No./Name} in/out

 Using aforementioned syntax, instead of the classic 'ip access-group' syntax, lets you define order easily

Exercise 14: Practical work

- ▶ Use your existing cisco packet tracer file (from last class exercise):
 - On R0, setup standard ACL such that: See red box:



R3 should:

The device sends back an ICMP Administratively Prohibited Unreachable message.

- ▶ **Commands (classic syntax):**
 - *R0(config)#access-list* Number? *deny ip any host* IP?
 - *R0(config)#int* Fa0/0
 - *R0(config-if)#ip access-group* Number? *in/out*?

Deadline: See 'Teams' Assignment section

Lecture 9 ends here

- ▶ Course Slides: Go to MS Teams:
'Introduction to Computer Networks – Spring 2024 | BSc'
-> Files section
- ▶ Send your questions by email:
mohammad-salman.nadeem@epita.fr
OR via direct message using MS Teams
- ▶ Thank You!