

# Interconnexion des réseaux

Mohammed EL KOUTBI

2024-2025

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

1

## Plan du cours

- **Introduction**
- **Part I : LAN interconnexion**
  - Configuration des Switchs
  - VLAN
  - STP
- **Part II: WAN interconnexion**
  - Protocoles WAN
  - Technologies WAN (ppp, Frame Relay)
- **Gestion, virtualisation et Automatisation**
- **Labs, Projet**

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

2

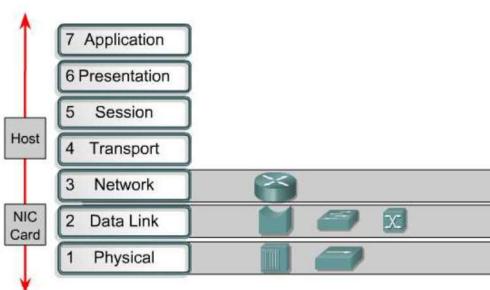
3

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

SupMTI.ma

## Part I : Switching

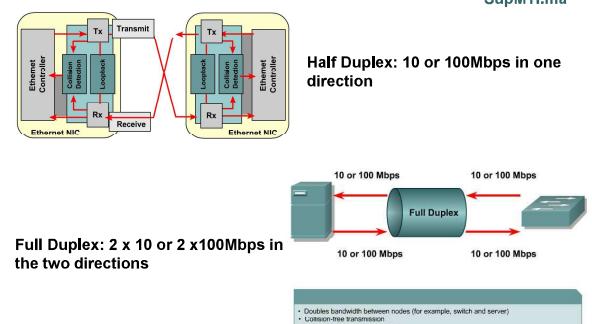
### Devices Function at Layers



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

5

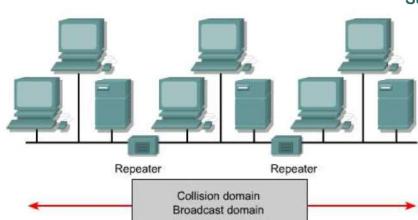
### Half-Duplex vs Full-Duplex Transmitting



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

7

### Benefits of Using Repeaters

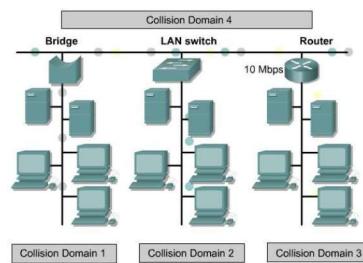


- Repeaters are Layer 1 device that regenerate the signal, and pass it on
- Repeaters allow a longer end-to-end distance
- Repeaters increase the collision domain size
- Repeaters increase the broadcast domain size

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

6

### LAN Segmentation



Segmentation allows network congestion to be significantly reduced within each segment.

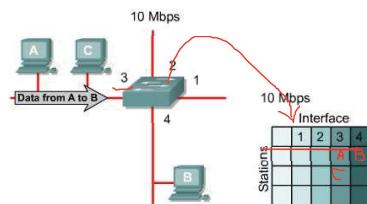
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

8

## LAN Switch Operation

SupMTI.ma

- Forward packets based on forwarding table
- Fowards based on the MAC (Layer 2) address
- Operates at OSI Layer 2
- Learns a station's location by examining source address
- Sends out all ports when destination address is broadcast, multicast, or unknown address
- Forwards when destination is located on different interface

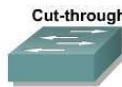


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

9

## Two Switching Methods

SupMTI.ma



Switch checks destination address and immediately begins forwarding frame



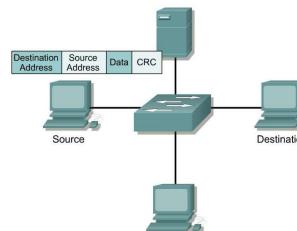
Complete frame is received before forwarding

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

16

## Store and Forward

SupMTI.ma



- The complete frame is received at the switch's end before being forwarded to the proper port.
- This will ensure that an invalid frame will not be forwarded.

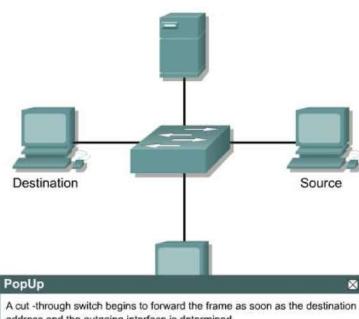
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

17

## Cut Through

SupMTI.ma

- Fast Forward:** Read Destination and immediately send. Lowest latency.
- Fragment Free:** Read Destination and bytes up to 64 then send. Better error handling.

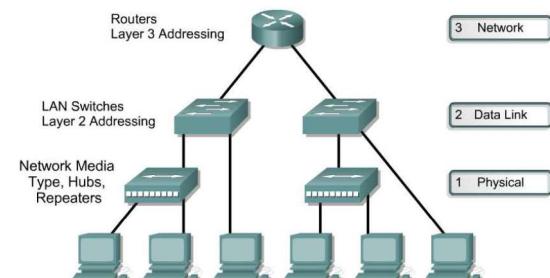


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

18

## Three-Layers Design

SupMTI.ma

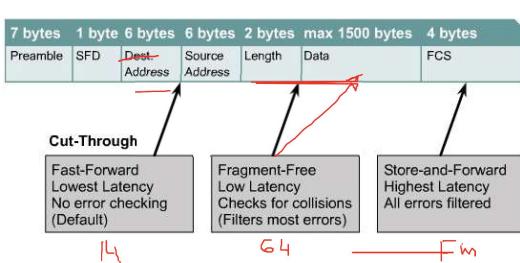


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

20

## Frame Transmission Modes

SupMTI.ma

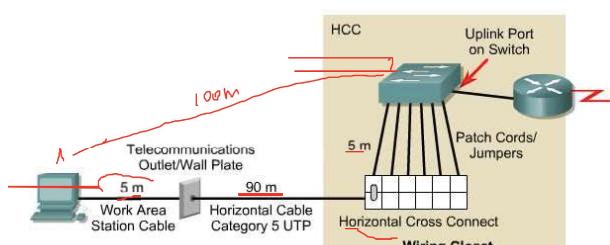


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

19

## Typical MDF in Star Topology

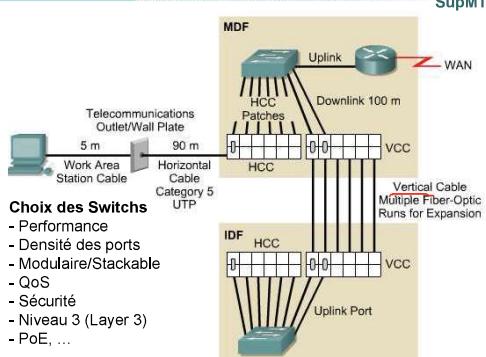
SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

21

## Extended Star Topology in a Multi-Building Campus



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

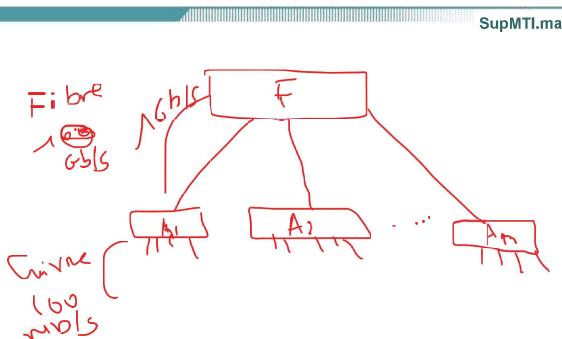
22

## Architecture de Câblage



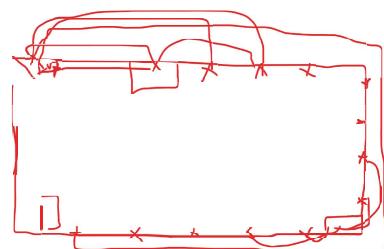
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

24



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

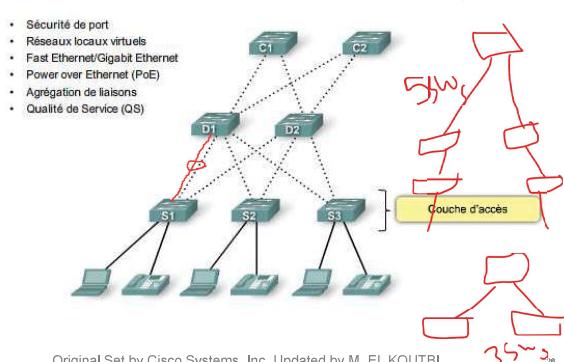
23



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

25

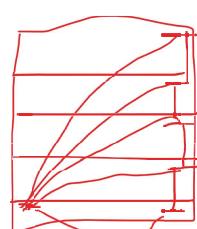
## Switched LAN Architecture



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

SupMTI.ma

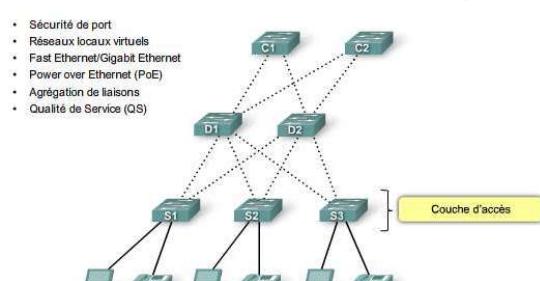
SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

27

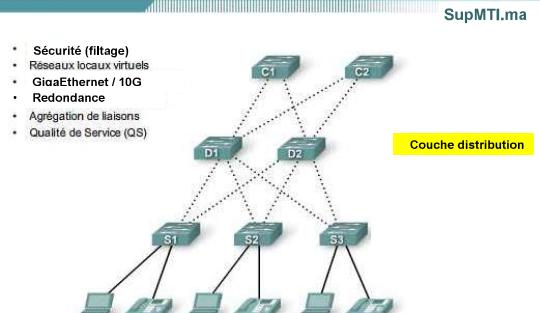
## Switched LAN Architecture



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

28

## Switched LAN Architecture

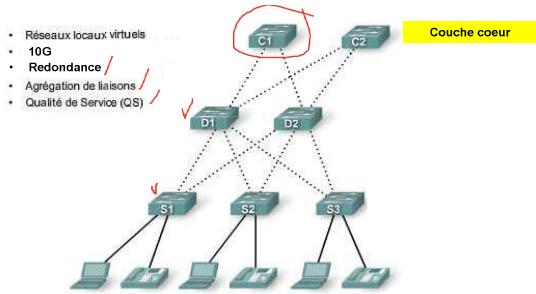


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

29

## Switched LAN Architecture

SupMTI.ma

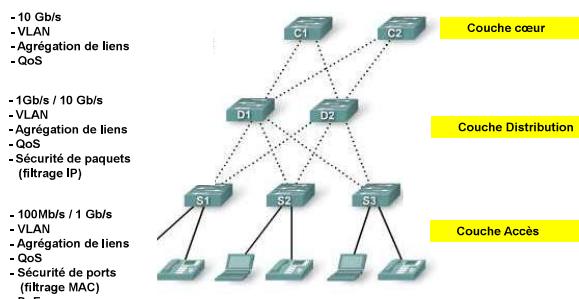


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

30

## Switched LAN Architecture

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

31

## Connecting a Switch to a PC

SupMTI.ma

Device with Console



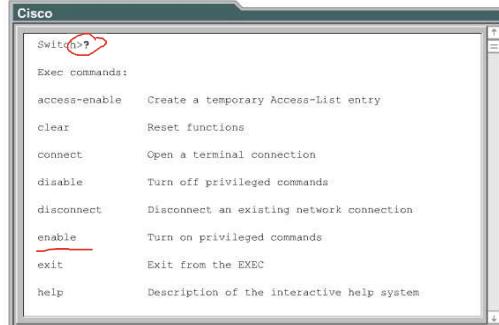
- PCs require an RJ-45 to DB-9 or RJ-45 to DB-25 adapter.
- COM port settings are 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control.
- This provides out-of-band console access.
- AUX switch port may be used for a modem-connected console.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

32

## Examining Help in the Switch CLI

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

33

## Show Commands in User EXEC Mode

SupMTI.ma

Commands	Description
show version	Gives version information for software and hardware. Used to see exactly which modules and software are in use.
show running-config	Displays the current configuration file of the switch.
show interface	Displays the administrative and operational status of a switching port, packets in/out and errors.
show interface status	Display the operational mode of the port.
show controllers ethernet-controller	Gives discarded frames, deferred frames, alignment errors, collisions, and so on.
show post	Tells if the switch passed the Power-On Self Test (POST).

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

34

## Configuring the Catalyst Switch

SupMTI.ma

```

Switch(config)#hostname ALSwitch
ALSwitch(config)#line con 0
ALSwitch(config-line)#password <your-choice>
ALSwitch(config-line)#login
ALSwitch(config-line)#line vty 0 4
ALSwitch(config-line)#password <your-choice>
ALSwitch(config-line)#login

Catalyst 2950
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat! [confirm]
Switch#erase startup-config
<output omitted>
Switch#reload

ALSwitch(config)#interface VLAN1
ALSwitch(config-if)#ip address 192.168.1.2
255.255.255.0
ALSwitch(config)#ip default-gateway 192.168.1.1

```

**Web Management Interface**

The screenshot shows the Web Management Interface for the Catalyst 2950 switch. It displays the Cluster System Device Port VLAN Security Help page. Key information shown includes:

- Switch Information: Host Name: ALSwitch, Switch IP Address: 192.168.1.2, Location: The Player, Contact: Paul Gormley, Software Version: 12.05(5.3)WC1 Enterprise Edition.
- Port Status: Shows 8 ports, all in a 'Normal' state.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

35

## Configuring Static MAC Addresses

SupMTI.ma

```

Switch(config)#mac-address-table ?
  aging-time      Set MAC address table entry maximum age
  notification    Enable/Disable MAC Notification on the
  switch
  static          static keyword

Switch(config)#mac-address-table static 00b0.d0cd.8e1d
  vlan 1 interface FastEthernet 0/5
Switch(config)#exit
Switch#
00:30:01: %SYS-5-CONFIG_I: Configured from console by
console

```

Set the Interface FastEthernet 0/5 to allow the MAC address 00b0.d0cd.8e1d only and be part of VLAN 1

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

36

## Configuring Port Security

SupMTI.ma

### Attaques sur les switches :

- Debordement de la table de commutation
  - MAC Spoofing
  - Racine STP
  - ....
- ```
Switch(config)#interface fast ethethernet 0/2
Switch(config-if)#switchport port-security ?
  aging      Port-security aging commands
  mac-address Secure mac address
  maximum    Max secure addrs
  violation   Security Violation Mode
<cr>
```

**Hint:** Set the Maximum to 1, this will allow the first learned MAC address to use the port only.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

38

## Secure telnet = SSH

SupMTI.ma

```
(config)#ip domain-name mydomain.com
(config)#crypto key generate rsa
(config)#ip ssh version 2
(config)#line vty 0 15
(config-line)#transport input SSH
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

40

## Port security (sticky option)

SupMTI.ma

| Script de configuration de la sécurité des ports                    |                                                              |
|---------------------------------------------------------------------|--------------------------------------------------------------|
| Syntaxe de commande de l'interface de ligne de commande Cisco IOS   | Comm1#configure terminal                                     |
| Passez en mode de configuration globale.                            | Comm1(config)#                                               |
| Utilisez la commande Cisco IOS                                      | config terminal                                              |
| Précisez le type et le numéro de l'interface physique à configurer. | Comm1(config)#interface fastethernet 0/18                    |
| Utilisez la commande Cisco IOS                                      | config-if                                                    |
| Définissez le mode d'interface en accès.                            | Comm1(config-if)#switchport mode access                      |
| Utilisez la commande Cisco IOS                                      | config-if                                                    |
| Activez la sécurité des ports sur l'interface.                      | Comm1(config-if)#switchport port-security                    |
| Utilisez la commande Cisco IOS                                      | config-if                                                    |
| Définissez le nombre maximal d'adresses sécurisées à 50.            | Comm1(config-if)#switchport port-security maximum 50         |
| Utilisez la commande Cisco IOS :                                    | config-if                                                    |
| Activez l'apprentissage rémanent.                                   | Comm1(config-if)#switchport port-security mac-address sticky |
| Utilisez la commande Cisco IOS :                                    | config-if                                                    |
| Revenez au mode d'exécution privilégié.                             | Comm1 (config-if) #end                                       |
| Utilisez la commande Cisco IOS :                                    |                                                              |

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

39

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

41

## Virtual LANs

## Switching

SupMTI.ma

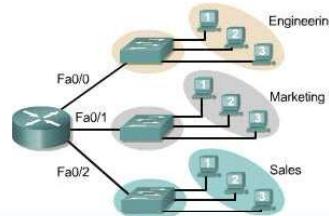
- VLAN concepts
- VLAN configuration

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

42

## Broadcast Domains (without VLANs)

SupMTI.ma



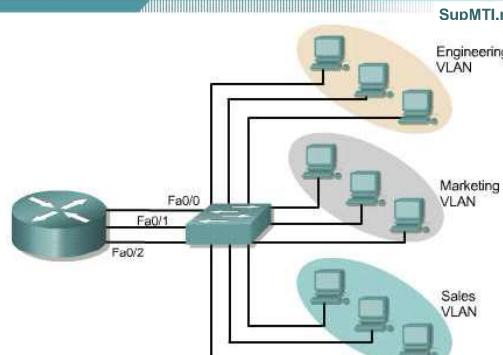
- In this scenario 3 switches & 1 router could be used. No VLANs are used.
- Switch for Engineering.
- Switch for Sales.
- Switch for Marketing.
- Each switch treats all ports as members of one broadcast domain.
- Router is used to route packets among the three broadcast domains.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

44

## Example with 3 Broadcast Domains, 3 VLANs

SupMTI.ma

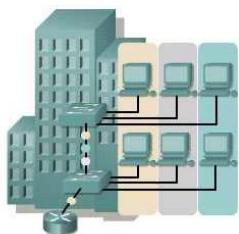


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

45

## Introduction to VLANs

SupMTI.ma



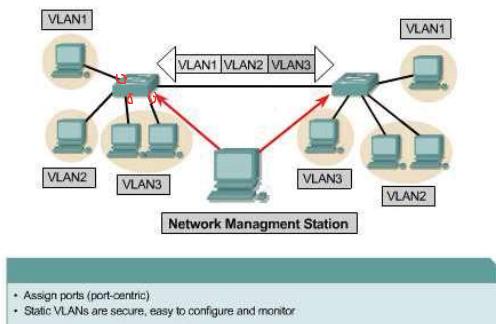
- A group of ports or users in same broadcast domain
- Can be based on port ID, MAC address, protocol, or application
- LAN switches and network management software provide a mechanism to create VLANs
- Frame tagged with VLAN ID

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

43

## Static VLANs

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

48

## VLAN Types

SupMTI.ma

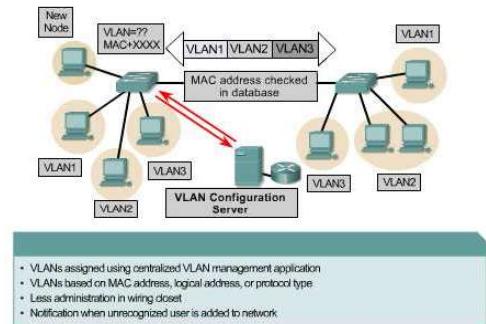
| VLAN Types     | Description                                                                                                                                                                                                                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port-based     | <ul style="list-style-type: none"> <li>Most common configuration method</li> <li>Ports assigned individually, in groups, in rows, or across 2 or more switches</li> <li>Simple to use</li> <li>Often implemented where Dynamic Host Control Protocol (DHCP) is used to assign IP addresses to network hosts</li> </ul> |
| MAC address    | <ul style="list-style-type: none"> <li>Rarely implemented today</li> <li>Each address must be entered into the switch and configured individually</li> <li>Users find it useful</li> <li>Difficult to administer, troubleshoot, and manage</li> </ul>                                                                  |
| Protocol-based | <ul style="list-style-type: none"> <li>Configured like MAC addresses, but instead uses a logical or IP address</li> <li>No longer common because of DHCP</li> </ul>                                                                                                                                                    |

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

48

## Dynamic VLANs

SupMTI.ma



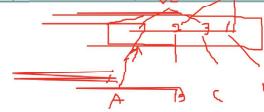
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

47

## Frame Tagging / Interswitch Linking

SupMTI.ma

| Tagging                 | Method        | Media                                                                                | Description                          |
|-------------------------|---------------|--------------------------------------------------------------------------------------|--------------------------------------|
| Inter-Switch Link (ISL) | Fast Ethernet | ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header | Frame is lengthened                  |
| 802.1Q                  | Fast Ethernet | IEEE defined Ethernet VLAN protocol                                                  | Header is modified                   |
| LAN Emulation (LANE)    | ATM           | No tagging                                                                           | Virtual connection implies a VLAN ID |

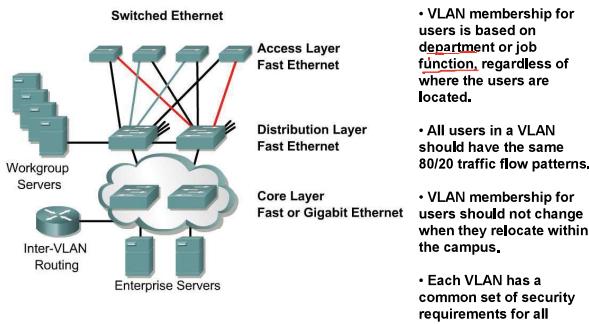


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

49

## End-to-End VLANs

SupMTI.ma

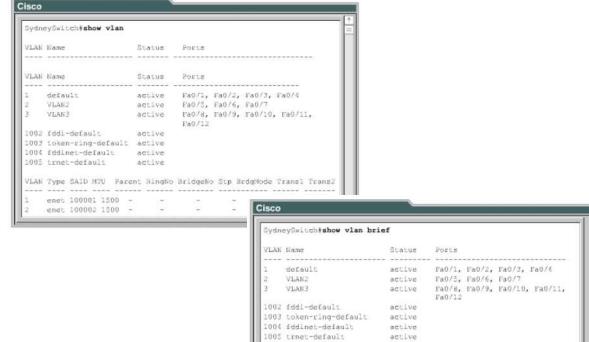


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

50

## Verifying VLAN Configuration

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

52

## Creating VLANs Statics

SupMTI.ma

### Add a VLAN to the VLAN database

```
# vlan database
(vlan) # vlan vlan_number
(vlan) # exit
```

### Assign switch ports to VLANs

```
(config)# interface interface_info
(config-if) # switchport access vlan vlan_number
(config-if) # exit
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

51

## Deleting VLANs

SupMTI.ma

### Deleting VLAN association

```
(config) # interface interface_info
(config-if) # no switchport access vlan vlan_number
(config-if) # exit
```

### Deleting VLANs

```
# vlan database
(vlan) # no vlan vlan_number
Deleting VLAN vlan_number
(vlan) # exit
```

When a VLAN is deleted any ports assigned to that VLAN become inactive. The ports will, however, remain associated with the deleted VLAN until assigned to a new VLAN.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

53

## Creating VLANs Statically

SupMTI.ma

- Add a VLAN to the VLAN database

```
# vlan database  
(vlan) # vlan vlan_number  
(vlan) # exit
```

- Assign switch ports to VLANs

```
(config)# interface interface_info  
(config-if)# switchport access vlan vlan_number  
(config-if)# exit
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

51

## Deleting VLANs

SupMTI.ma

- Deleting VLAN association

```
(config)# interface interface_info  
(config-if)# no switchport access vlan vlan_number  
(config-if)# exit
```

- Deleting VLANs

```
# vlan database  
(vlan) # no vlan vlan_number  
Deleting VLAN vlan_number  
(vlan) # exit
```

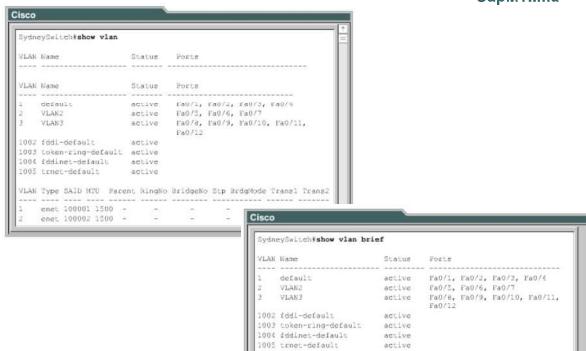
When a VLAN is deleted any ports assigned to that VLAN become inactive. The ports will, however, remain associated with the deleted VLAN until assigned to a new VLAN.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

53

## Verifying VLAN Configuration

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

52

## Catalyst IOS show vlan Command

SupMTI.ma

| VLAN Name               | Status | IfIndex | Mod/Ports |
|-------------------------|--------|---------|-----------|
| 1 default               | active | 45      | 1/1-2     |
| 100 VLAN0100            | active | 53      | 2/4-5     |
| 200 VLAN0200            | active | 54      | 2/6-7     |
| 300 VLAN0300            | active | 56      | 2/3,2/30  |
| 1002 fddi-default       | active | 46      |           |
| 1003 token-ring-default | active | 49      |           |
| 1004 fddinet-default    | active | 47      |           |
| 1005 trnet-default      | active | 48      |           |

| VLAN Type | SAID   | MTU  | Parent RingNo | BrdgNo | Stp | BrdgMode | Transl Trans2 |
|-----------|--------|------|---------------|--------|-----|----------|---------------|
| 1 enet    | 100001 | 1500 | -             | -      | -   | -        | 0             |
| 0         |        |      |               |        |     |          |               |

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

54

## Trunking Concepts

SupMTI.ma

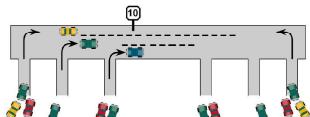
- A 1 to 1 ratio between switches does not scale well! Why?



- Channel all VLAN information into one or more TRUNKs



The Highway distributor model:



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

55

## Trunking Configuration

SupMTI.ma

- Check the switch port capabilities first

```
#show port capabilities portinfo
```

- Set the switch port to Trunk mode

```
(config-if)#switchport mode trunk
```

- Now, use IEEE 802.1q's encapsulation (or any other one)

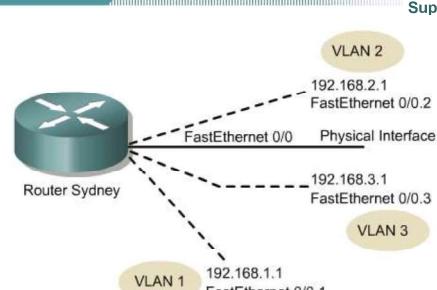
```
(config-if)#switchport trunk encapsulation { dot1q | isl }
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

56

## Dividing Physical Interfaces into Subinterfaces

SupMTI.ma

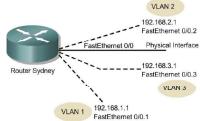


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

58

## Configuring Inter-VLAN Routing

SupMTI.ma



- Since the Switch will be sending trunking information to the router, it's up to the router's interface to "decode" this tag:

```
(config)# interface fa 0/0
(config-if)# full duplex
(config-if)# no shut
(config-if)# interface fa 0/0.1
(config-subif)# encapsulation dot.1q 1
(config-subif)# ip address 192.168.1.1 255.255.255.0
```

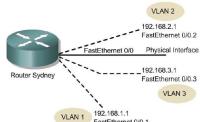
Note the 'subif'

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

59

## Configuring Inter-VLAN Routing - Cont'd

SupMTI.ma



```
(config-subif)# interface fa 0/0.2
(config-subif)# encapsulation dot.1q 2
(config-subif)# ip address 192.168.2.1 255.255.255.0
(config-subif)# interface fa 0/0.3
(config-subif)# encapsulation dot.1q 3
(config-subif)# ip address 192.168.3.1 255.255.255.0
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

60

## Configuring Inter-VLAN Routing – Switch L3

SupMTI.ma

- Configurer les interfaces VLANs sur le Switch L3
- Activer le routage sur le Switch L3
- Configurer des ports routés pour se connecter à l'extérieur
- Ajouter les routes ou configurer le routage dynamique

```
(config)# int vlan 1
(config-if)# ip address 192.168.2.1 255.255.255.0
(config-if)# no shutdown
(config)# int vlan 2
(config-if)# ip address 192.168.2.1 255.255.255.0
(config-if)# no shutdown
(config)# int vlan 3
(config-if)# ip address 192.168.3.1 255.255.255.0
(config-if)# no shutdown
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

61

## Configuring Inter-VLAN Routing – Switch L3

SupMTI.ma

- Configurer les interfaces VLANs sur le Switch L3
- Activer le routage sur le Switch L3
- Configurer des ports routés pour se connecter à l'extérieur
- Ajouter les routes ou configurer le routage dynamique

```
(config)# int gigabitethernet 0/1
(config-if)# no switchport
(config-if)# ip address 192.168.4.2 255.255.255.0
(config-if)# no shutdown

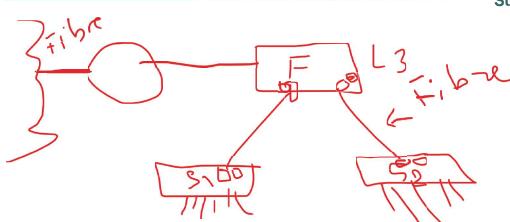
(config)# ip routing

(config)# ip route 0.0.0.0 0.0.0.0 192.168.4.1
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

62

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

63

63

SupMTI.ma

## Redundancy Spanning Tree Protocol

## Redundancy

SupMTI.ma

Redundant networking topologies are designed to ensure that networks continue to function in the presence of single points of failure.

Securing a 99.999% or **five nines** uptime is a goal that organizations set.  
99.999% = 5.25 minutes/Year!!!



There is one car, can I drive to work?

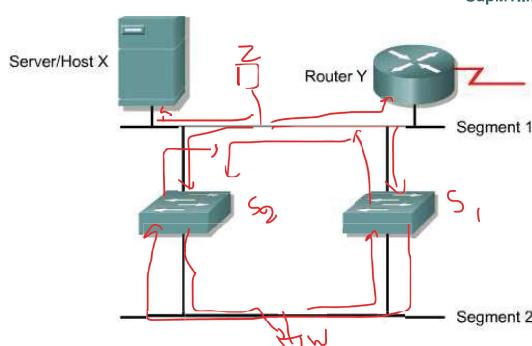
There are two cars, can I drive to work?

64

64

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

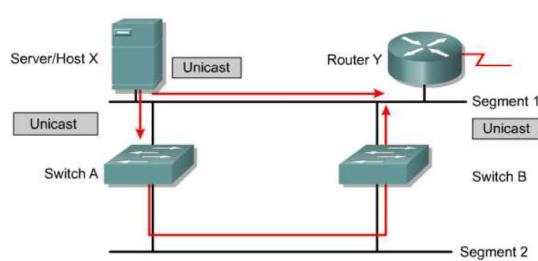
## Simple Redundant Switched Topology



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

65

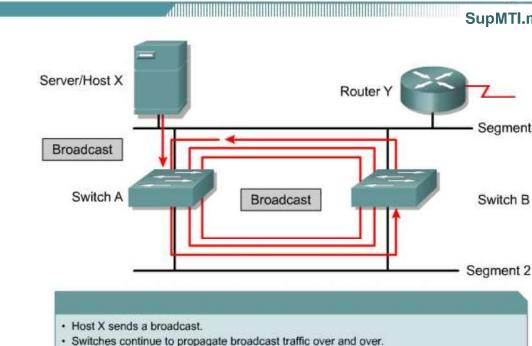
## Multiple Frame Transmissions



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

67

## Broadcast Storm

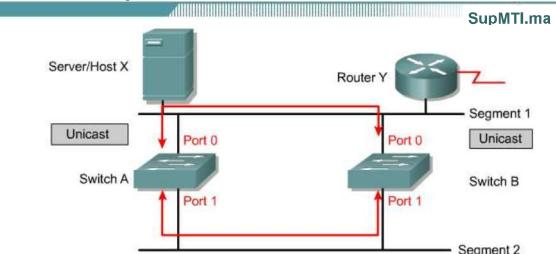


- Host X sends a broadcast.
- Switches continue to propagate broadcast traffic over and over.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

68

## Media Access Control Database Instability

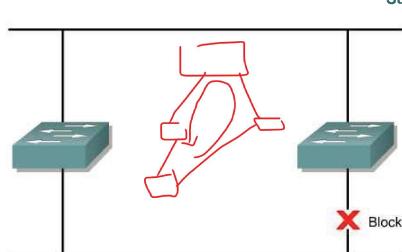


In a redundant switched network, it is possible for switches to learn the wrong information. A switch can learn that a MAC address is on a port when it is not.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

69

## Spanning-Tree Protocol

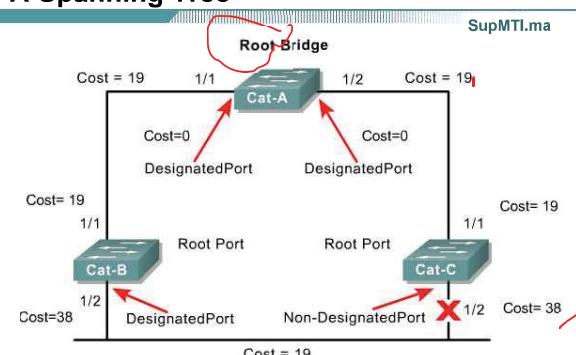


Provides a loop-free redundant network topology by placing certain ports in the blocking state.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

69

## A Spanning Tree



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

71

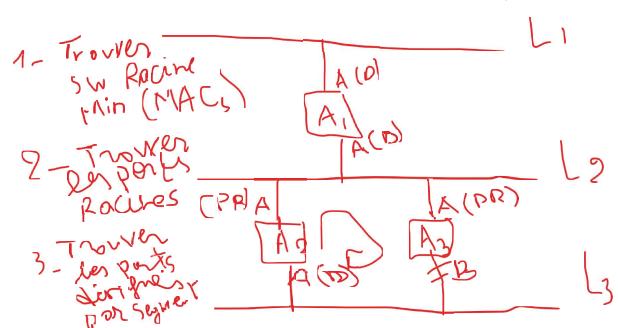
## Spanning Tree Link Costs

SupMTI.ma

| Link Speed | Cost(Revised IEEE Spec) | Cost (Previous IEEE Spec) |
|------------|-------------------------|---------------------------|
| 10 Gbps    | 2                       | 1                         |
| 1 Gbps     | 4                       | 1                         |
| 100 Mbps   | 19                      | 10                        |
| 10 Mbps    | 100                     | 100                       |

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

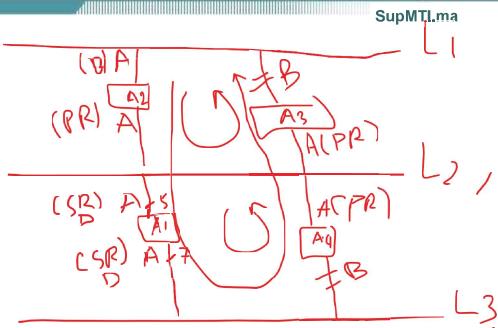
70



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

72

À coût égal, on le port qui est connecté au port le plus petit du switch racine



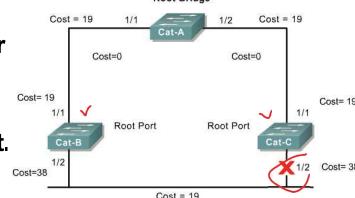
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

73

## Spanning-Tree Operation

SupMTI.ma

- 1. One root bridge per network.
- 2. One root port per nonroot bridge.
- 3. One designated port per segment.
- 4. Nondesignated ports are unused.

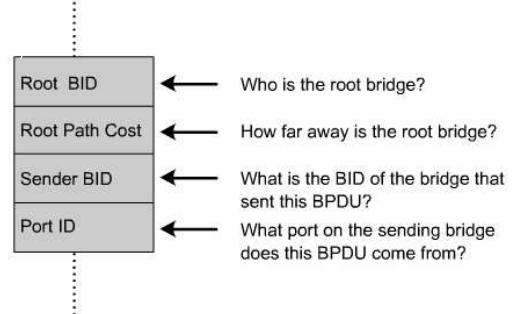


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

74

## Bridge Protocol Data Unit

SupMTI.ma

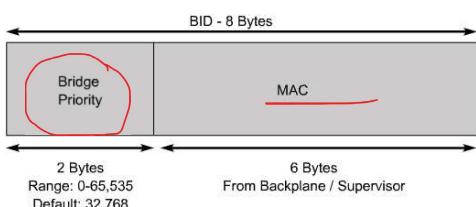


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

75

## Bridge IDs

SupMTI.ma



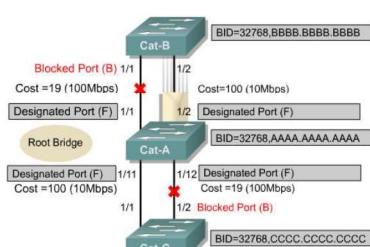
- Bridge ID (BID) is used to identify each bridge/switch.
- The BID is used in determining the center of the network, in respect to STP, known as the root bridge.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

77

## Spanning-Tree Recalculation

SupMTI.ma



A switched internetwork has converged when all the switch and bridge ports are in either the forwarding or blocked state.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

78

## Versions STP Standard / Cisco

SupMTI.ma

| Protocol    | Standard | Resources Needed | Convergence    | Tree Calculation |              |
|-------------|----------|------------------|----------------|------------------|--------------|
| STP         | 802.1D   | Low              | Slow           | All VLANs        |              |
| PVST+       | Cisco    | High             | Slow           | Per VLAN         |              |
| RSTP        | 802.1w   | Medium           | Fast           | All VLANs        |              |
| Rapid PVST+ | Cisco    | Very high        | Fast           | Per VLAN         |              |
| MSTP        | 802.1s   | Cisco            | Medium or high | Fast             | Per Instance |

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

80

## Configuration STP

SupMTI.ma

```
S1# configure terminal  
S1(config)# spanning-tree mode rapid-pvst  
S1(config)# interface f0/2  
S1(config-if)# spanning-tree link-type point-to-point  
S1(config-if)# end  
S1# clear spanning-tree detected-protocols
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

81

## Configuration STP

SupMTI.ma

```
S3(config)# spanning-tree vlan 20 root primary
```

This command forces S3 to be the primary root for VLAN 20.

```
S3(config)# spanning-tree vlan 10 root secondary
```

This command forces S3 to be the secondary root for VLAN 10.

```
S1(config)# spanning-tree vlan 10 root primary
```

This command forces S1 to be the primary root for VLAN 10.

```
S1(config)# spanning-tree vlan 20 root secondary
```

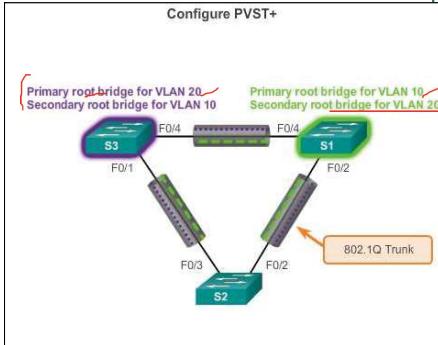
This command forces S1 to be the secondary root for VLAN 20.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

83

## Configuration STP

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

82

## Configuration STP

SupMTI.ma

```
S3# show spanning-tree  
VLAN0001  
Spanning tree enabled protocol ieee  
Root ID Priority 24577  
Address 00A.0033.3333  
This bridge is the root  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Bridge ID Priority 24577 (priority 24576 sys-id-ext 1)  
Address 00A.0033.3333  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Aging Time 300  
Interface Role Sts Cost Prio.Nbr Type  
-----  
Fa0/1 Desg FWD 4 128.1 p2p  
Fa0/2 Desg FWD 4 128.2 p2p  
S3#
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

84

Ne désactivez jamais STP, même si votre architecture est un arbre



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

85

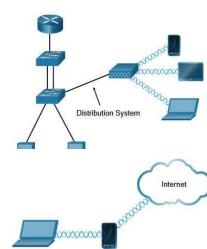
## Modes de topologie sans fil 802.11

SupMTI.ma

**Mode ad hoc** - Utilisé pour connecter les clients de manière poste à poste sans point d'accès.



**Mode infrastructure** - Utilisé pour connecter les clients au réseau à l'aide d'un AP.



**Partage de connexion** - La variation de la topologie ad hoc se produit lorsqu'un téléphone intelligent ou une tablette avec accès aux données cellulaires est activé pour créer un point d'accès personnel.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

86

## Wireless LAN

### BSS et ESS

SupMTI.ma

**Le mode infrastructure définit deux blocs de topologie:**

**Ensemble de services de base (BSS)**



- Un BSS consiste en un seul AP interconnectant tous les clients sans fil associés.
- Les clients de différents BSS ne peuvent pas communiquer.

**Ensemble de service étendu (ESS)**



- Union de deux ou plusieurs BSS interconnectés par un système de distribution câblé.
- Les clients de chaque BSS peuvent communiquer via l'ESS.

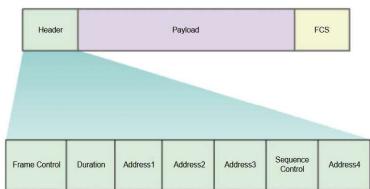
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

88

## Structure de trame 802.11

SupMTI.ma

Le format de trame 802.11 est similaire au format de trame Ethernet, sauf qu'il contient plus de champs.



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

89

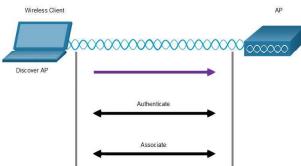
## Clients et Association des point d'accès

SupMTI.ma

Pour que les périphériques sans fil puissent communiquer sur le réseau, ils doivent tout d'abord être associés à un point d'accès ou à un routeur sans fil.

Les appareils sans fil effectuent le processus en trois étapes suivant:

- Découvrir de nouveaux points d'accès sans fil
- S'authentifier auprès du point d'accès
- S'associer au point d'accès



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

90

## WLAN technologies

SupMTI.ma

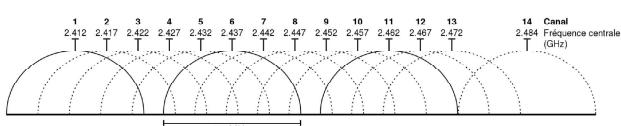
|                   | 802.11a                                   | 802.11b                            | 802.11g                                                            | 802.11n                                           |
|-------------------|-------------------------------------------|------------------------------------|--------------------------------------------------------------------|---------------------------------------------------|
| Bande             | 5,7 GHz                                   | 2,4 GHz                            | 2,4 GHz                                                            | A confirmer<br>Bandes 2,4 et 5 GHz (probablement) |
| Canaux*           | Jusqu'à 23                                | 3                                  | 3                                                                  |                                                   |
| Modulation        | OFDM                                      | DSSS                               | OFDM                                                               | MIMO-OFDM                                         |
| Débits de données | Jusqu'à 54 Mbit/s                         | Jusqu'à 11 Mbit/s                  | Jusqu'à 54 Mbit/s                                                  | 248 Mbit/s supposés pour deux flux MIMO           |
| Avantages         | ~35 mètres                                | ~35 mètres                         | ~35 mètres                                                         | ~70 mètres                                        |
| Inconvénients     | Octobre 1999                              | Octobre 1999                       | Juin 2003                                                          | Ratification attendue en 2008                     |
| Avantages         | Rapidité, moins sujette aux interférences | Faible coût, bonne portée          | Rapidité, bonne portée, peu sensible aux obstacles                 | Excellent débits de données, portée accrue        |
| Inconvénients     | Coût plus élevé, portée inférieure        | Lenteur, sujette aux interférences | Sujette aux interférences des appareils utilisant la bande 2,4 GHz |                                                   |

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

93

## Designing WLAN Canaux sans interférences

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

94

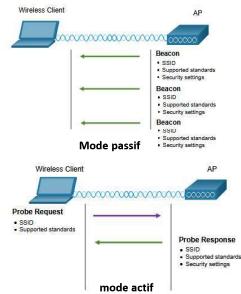
## Mode découverte passif et actif

SupMTI.ma

Les clients sans fil se connectent à l'AP à l'aide d'un processus de balayage (sondage) passif ou actif.

• **Mode passif** - AP annonce ouvertement son service en envoyant périodiquement des trames de balise de diffusion contenant le SSID, les normes prises en charge et les paramètres de sécurité.

• **Mode actif** - Les clients sans fil doivent connaître le nom du SSID. Le client sans fil lance le processus en diffusant une trame de demande d'enquête sur plusieurs canaux.

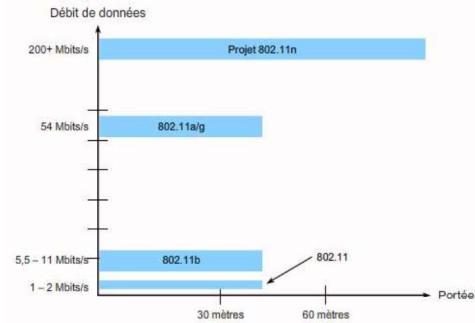


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

91

## WLAN technologies

SupMTI.ma

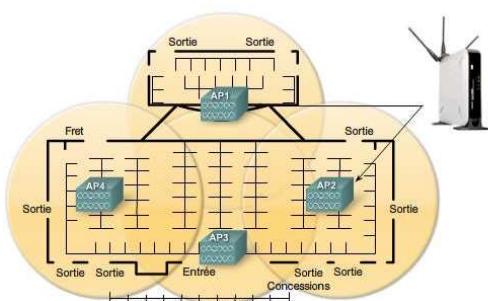


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

92

## Designing WLAN

SupMTI.ma

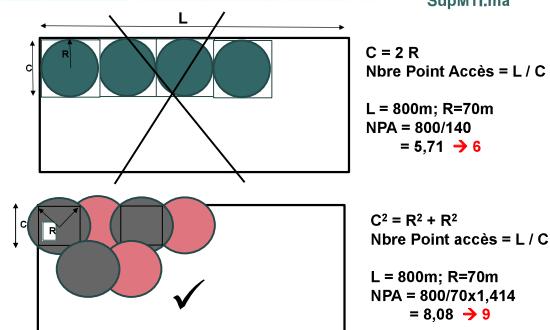


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

95

## Designing WLAN

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

96

## Securing WLAN

| Accès ouvert                                                                                                                                       | Chiffrement de première génération                                                                                                       | Provisoire                                                                                                                                                               | Présent                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSID                                                                                                                                               | WEP                                                                                                                                      | WPA                                                                                                                                                                      | 802.11i/WPA2                                                                                                                                                                                                                    |
| <ul style="list-style-type: none"> <li>Aucun chiffrement</li> <li>Authentification de base</li> <li>N'est pas un dispositif de sécurité</li> </ul> | <ul style="list-style-type: none"> <li>Authentification non efficace</li> <li>Cles statiques, cassables</li> <li>Non évolutif</li> </ul> | <ul style="list-style-type: none"> <li>Standardisé</li> <li>Chiffrement amélioré</li> <li>Authentification utilisateur efficace (p.ex., LEAP, PEAP, EAP-FAST)</li> </ul> | <ul style="list-style-type: none"> <li>Chiffrement AES</li> <li>Authentification : 802.1X</li> <li>Gestion des clés dynamiques</li> <li>WPA2 correspond à la mise en œuvre de la norme 802.11i par la Wi-Fi Alliance</li> </ul> |

Méthodes de contrôle d'accès au périphérique local sans fil :

- Les diffusions de SSID par les points d'accès sont désactivées.
- Le filtrage d'adresses MAC est activé.
- Sécurité WPA2 mise en œuvre.

ATTENTION : les points 1 et 2 ne sont pas considérés comme des mesures de sécurité valables.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

97

## Contrôleur Wireless (WLC)

- Le point d'accès (AP) est un AP basé sur un contrôleur par opposition à un **AP autonome**, il ne nécessite donc aucune configuration initiale et est souvent appelé AP léger (LAP).
- Les LAP utilisent le Lightweight Access Point Protocol (**LWAPP**) pour communiquer avec un contrôleur WLAN (WLC).
- Les points d'accès basés sur un contrôleur sont utiles dans les situations où de nombreux points d'accès sont requis dans le réseau.
- Comme plus d'AP sont ajoutés, chaque AP est automatiquement configuré et géré par le WLC.



| Appareil                     | Interface    | Adresse IP        | Masque de sous-réseau |
|------------------------------|--------------|-------------------|-----------------------|
| R1                           | F0/0         | 172.16.1.1        | 255.255.255.0         |
| R1                           | F0/1.1       | 192.168.200.1     | 255.255.255.0         |
| S1                           | VLAN 1       | DHC               |                       |
| WLC                          | Gestion      | 192.168.200.254   | 255.255.255.0         |
| AP1                          | Filaire 0    | 192.168.200.3     | 255.255.255.0         |
| PCA                          | Carte réseau | 172.16.1.254      | 255.255.255.0         |
| PC-B                         | Carte réseau | Le protocole DHCP |                       |
| Ordinateur portable sans fil | Carte réseau | Le protocole DHCP |                       |

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

98

## Configurer un WLAN avec un WLC

SupMTI.ma  
Les contrôleurs LAN sans fil ont des ports de commutation de couche 2 et des interfaces virtuelles qui sont créées dans le logiciel et sont très similaires aux interfaces VLAN.

- Chaque port physique peut prendre en charge de nombreux points d'accès et WLANs.
- Les ports sur le WLC sont essentiellement des ports de jonction qui peuvent transporter le trafic de plusieurs VLAN vers un commutateur pour la distribution vers plusieurs AP.
- Chaque AP peut prendre en charge plusieurs WLAN.



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

101

## Configurer un WLAN (suite)

SupMTI.ma

La configuration de base du WLAN sur le WLC comprend les étapes suivantes:

- Créez le WLAN
- Appliquez et activez le WLAN
- Choisissez l'interface
- Sécurisez le WLAN
- Vérifiez que le WLAN est opérationnel
- Surveillez le WLAN
- Affichez les informations du client sans fil

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

102

## Protocole CAPWAP

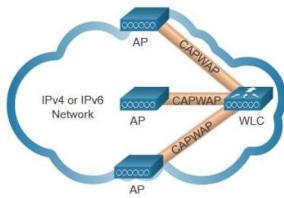
SupMTI.ma

CAPWAP est un protocole standard IEEE qui permet à un WLC de gérer plusieurs AP et WLAN.

CAPWAP est basé sur LWAPP mais ajoute une sécurité supplémentaire avec Datagram Transport Layer Security (DTLS).

Encapsule et transfère le trafic client WLAN entre un AP et un WLC sur des tunnels en utilisant les ports UDP 5246 et 5247.

Fonctionne sur IPv4 et IPv6.



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

99

## WLC et Architecture MAC divisée

SupMTI.ma

Le concept de MAC divisé du **CAPWAP** remplit toutes les fonctions normalement remplies par les AP individuels et les répartit entre deux composantes fonctionnelles :

### - Fonctions MAC AP

### - Fonctions MAC WLC

| Fonctions MAC AP                                              | Fonctions MAC WLC                                  |
|---------------------------------------------------------------|----------------------------------------------------|
| Balises et réponses des sondes                                | Authentification                                   |
| Accusé de réception et retransmissions de paquets             | Association et réassociation de clients itinérants |
| Mise en file d'attente des trames et priorisation des paquets | Traduction de trame vers d'autres protocoles       |
| Cryptage et décryptage des données de la couche MAC           | Arrêt du trafic 802.11 sur une interface filaire   |

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

100

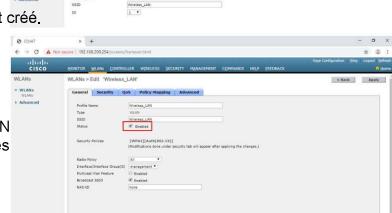
## Configurer un WLAN (suite)

SupMTI.ma

- Créer le WLAN: Dans la figure, un nouveau WLAN avec un nom SSID **Wireless\_LAN** est créé.

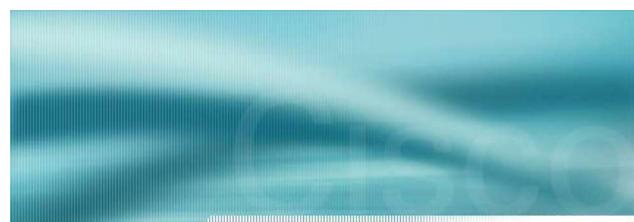


- Appliquer et activer le WLAN: Ensuite, le WLAN est activé, les paramètres WLAN sont configurés.



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

103



SupMTI.ma

## Liens d'agrégation

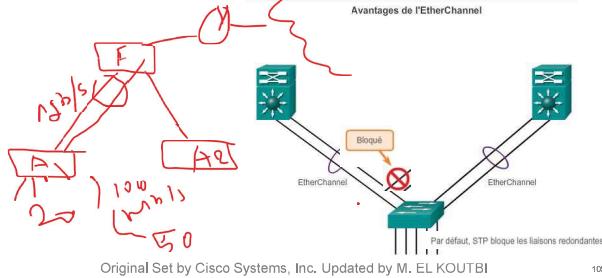
## Etherchannel

104

## Introduction à l'agrégation de liaisons

SupMTI.ma

- L'agrégation de lien permet la création des liens logiques composés de plusieurs liens physiques.
- EtherChannel est une forme d'agrégation de lien utilisée dans les réseaux commutés.



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

105

## Exemple de dimensionnement

SupMTI.ma

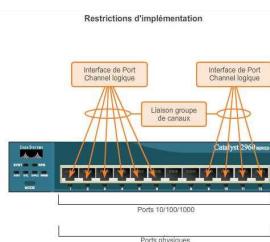
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

107

## Considération d'implémentation

SupMTI.ma

- EtherChannel peut être implémenté en regroupant plusieurs ports physiques sur une ou plusieurs liaisons logiques EtherChannel.
- L'EtherChannel offre une bande passante bidirectionnelle simultanée jusqu'à 800 Mb/s (Fast EtherChannel) ou 8 Gb/s (Gigabit EtherChannel).
- Le commutateur Cisco IOS peut actuellement prendre en charge six EtherChannel.
- Le groupe de port est vu en tant qu'un lien logique par STP



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

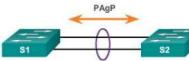
106

## Protocol Aggregation Port (PAgP) CISCO

Protocole PAgP

SupMTI.ma

| Modes PAgP :                                                                                      |  |  |
|---------------------------------------------------------------------------------------------------|--|--|
| Activé : membre de canal sans négociation (pas de protocole)                                      |  |  |
| Auto-Désirable (Souhaitable) : demande activement si l'autre côté peut participer ou participera. |  |  |
| Auto : attend passivement l'autre côté.                                                           |  |  |



| S1                                  | S2            | Établissement de canal |
|-------------------------------------|---------------|------------------------|
| Activé                              | Activé        | Oui                    |
| Auto-Désirable (Souhaitable)        | Souhaitable   | Oui                    |
| On/Off/Auto-Désirable (Souhaitable) | Non configuré | Non                    |
| Activé                              | Souhaitable   | Non                    |
| Passive (Passif)/On (Activé)        | Auto          | Non                    |

PAgP permet de créer la liaison EtherChannel en détectant la configuration de chaque côté et en assurant la compatibilité des liaisons, afin que la liaison EtherChannel puisse être activée si besoin.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

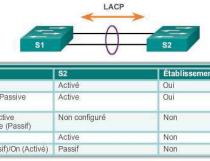
108

## Protocol Liens Aggregation Port (LACP) Non Cisco

Protocole LACP

SupMTI.ma

| Modes LACP :                                                                                |  |  |
|---------------------------------------------------------------------------------------------|--|--|
| Activé : membre de canal sans négociation (pas de protocole)                                |  |  |
| Activé/Passif (Passif) : demande activement si l'autre côté peut participer ou participera. |  |  |
| Passif (Passif)/Activé : attend passivement l'autre côté.                                   |  |  |



| S1            | S2            | Établissement de canal |
|---------------|---------------|------------------------|
| Activé        | Activé        | Oui                    |
| Activé/Passif | Activé        | Oui                    |
| On/Off/Activé | Non configuré | Non                    |
| Activé        | Activé        | Non                    |
| Passif/Activé | Passif        | Non                    |

LACP offre les mêmes avantages en matière de négociation que PAgP. LACP permet de créer la liaison EtherChannel en détectant les configurations de chacun des côtés et en assurant leur compatibilité, afin que la liaison EtherChannel puisse être activée au besoin.

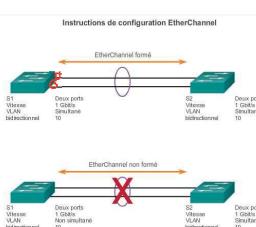
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

109

## Directives de configuration

SupMTI.ma

- Prise en charge d'EtherChannel sur tous les modules.
- Vitesse et mode duplex doit être compatible sur toutes les interfaces.
- Vlan doit être compatible – Toutes les interfaces sont sur le même VLAN.
- Plage de VLAN – Même plage sur toutes les interfaces.



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

110

## Verification de EtherChannel

SupMTI.ma

- show interface Port-channel - affiche l'état général de l'interface de port-channel..
- show etherchannel summary - pour afficher une ligne d'informations unique par canal de port.
- show etherchannel port-channel - pour afficher des informations concernant une interface port-channel spécifique.
- show interfaces etherchannel - peut fournir des informations sur le rôle de l'interface dans l'EtherChannel

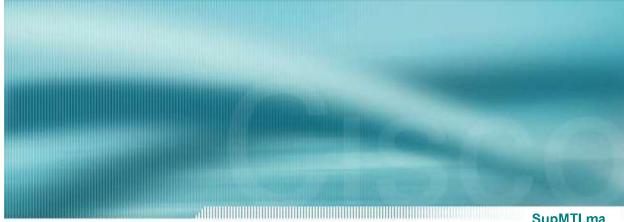
Si# show interface port-channel  
Port-channel-1 is up, line protocol is up (connected).  
Hardware is EtherChannel, address is 00d9.36e8.8a02 (bia  
00d9.36e8.8a02).  
Internet address is 192.168.1.10, subnet mask is 255.255.255.0.  
MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 100 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
encapsulation ARPA, loopback not set  
(output omitted)

Vérifie l'état de l'interface.



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

112



## Protocoles FHRP (First Hop Redundancy Protocols)

SupMTI.ma

| Options FHRP                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hot Standby Router Protocol (HSRP)                               | Le Protocole HSRP (Hot Standby Router Protocol) est un protocole FHRP propriétaire de Cisco, conçu pour permettre le basculement transparent d'un routeur actif vers un routeur de secours. Il fournit une adresse IP unique pour un groupe de routeurs actifs et un périphérique en veille. Le dispositif actif est celui qui est utilisé pour l'échangeement des renvois. Le dispositif de réserve est le dispositif qui prend le relais lorsque le dispositif actif tombe en panne, ou lorsque des conditions préétablies sont remplies.  |
| HSRP pour IPv6                                                   | Il s'agit d'un FHRP propriétaire de Cisco qui offre les mêmes fonctionnalités que le HSRP, mais dans un environnement IPv6. Un groupe IPv6 du HSRP a une adresse MAC virtuelle dérivée du numéro de groupe du HSRP et une adresse IPv6 locale de liaison virtuelle dérivée de l'adresse MAC virtuelle du HSRP. Des annonces périodiques de routeurs (RAs) sont envoyées pour l'adresse IPv6 virtuelle du local du HSRP lorsque le groupe HSRP est actif. Lorsque le groupe devient inactif, ces RAs cessent après l'envoi d'une dernière RA. |
| Protocole de redondance des routeurs virtuels version 2 (VRRPv2) | Il s'agit d'un protocole d'élection non propriétaire qui attribue dynamiquement la responsabilité d'un ou plusieurs routeurs virtuels aux routeurs VRRP sur une interface local IPv4. Cela permet à plusieurs routeurs sur un lien multi-sécurité d'utiliser la même adresse IPv4 virtuelle. Dans une configuration VRRP, un routeur est élu en tant que routeur maître virtuel. Les autres routeurs servent de secours en cas de défaillance du routier maître virtuel.                                                                     |
| VRRPv3                                                           | Cela permet de prendre en charge les adresses IPv4 et IPv6. Le VRRPv3 fonctionne dans des environnements multi-fournisseurs et est plus évolutif que le VRRPv2.                                                                                                                                                                                                                                                                                                                                                                              |
| Protocole d'équilibrage de charge de la passerelle (GLBP)        | Il s'agit d'un FHRP propriétaire de Cisco qui protège le trafic de données d'un routeur ou d'un circuit défaillant, comme le HSRP et le VRRP, tout en permettant l'équilibrage de la charge (également appelé partage de la charge) entre un groupe de routeurs redondants.                                                                                                                                                                                                                                                                  |
| GLBP pour IPv6                                                   | Il s'agit d'un protocole GLBP pour IPv6 qui offre les mêmes fonctionnalités que le GLBP pour IPv4, mais dans un environnement IPv6. Le protocole GLBP pour IPv6 offre un mode de secours automatique pour les hôtes IPv6 connectés avec une passerelle par défaut unique sur un LAN. Plusieurs routeurs de premier saut se combinent dans le réseau local pour offrir un routeur de premier saut IPv6 virtuel unique, tout en partageant la charge de réacheminement des paquets IPv6.                                                       |
| ICMP Router Discovery Protocol (IRDP)                            | Spécifié dans la RFC 1256, IRDP est une solution FHRP héritée. Le protocole IRDP permet aux hôtes IPv4 de localiser les routeurs offrant une connectivité IPv4 à d'autres réseaux IP (non locaux).                                                                                                                                                                                                                                                                                                                                           |

## Passerelles Redondantes

### FHRP

113

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

115

## Redondance des routeurs

SupMTI.ma

Pour éviter tout risque de point de défaillance unique au niveau de la passerelle par défaut, il est possible d'implémenter un routeur virtuel. Pour mettre en œuvre ce type de redondance des routeurs, plusieurs routeurs sont configurés pour fonctionner ensemble afin de présenter l'illusion d'un seul routeur aux hôtes du réseau local. En partageant une adresse IP et une adresse MAC, plusieurs routeurs peuvent jouer le rôle d'un routeur virtuel unique.

- L'adresse IPv4 du routeur virtuel est configurée en tant que passerelle par défaut pour les postes de travail sur un segment IPv4 donné.
- Lorsque des trames sont envoyées à la passerelle par défaut par des périphériques hôtes, les hôtes utilisent le processus ARP pour résoudre l'adresse MAC associée à l'adresse IPv4 de la passerelle par défaut. La résolution ARP renvoie l'adresse MAC du routeur virtuel. Les trames envoyées à l'adresse MAC du routeur virtuel peuvent alors être traitées physiquement par le routeur actif, au sein du groupe de routeurs virtuel.
- Un protocole est utilisé pour identifier au moins deux routeurs comme périphériques chargés de traiter les trames envoyées à l'adresse MAC ou à l'adresse IP d'un routeur virtuel unique. Les périphériques hôtes transmettent le trafic à l'adresse du routeur virtuel. Le routeur physique qui achemine ce trafic est transparent pour les appareils hôtes.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

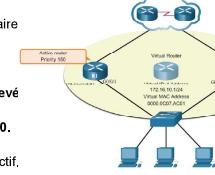
114

## Priorité et préemption HSRP

SupMTI.ma

Le rôle des routeurs actifs et de secours est déterminé lors du processus de sélection de HSRP. Par défaut, le routeur avec l'adresse IPv4 la plus élevée devient le routeur actif. Cependant, il est toujours plus judicieux d'avoir le contrôle de la manière dont votre réseau fonctionne en conditions normales plutôt que de laisser le hasard faire des choses.

- Il est possible d'utiliser la priorité HSRP pour déterminer le routeur actif.
- Le routeur associé à la priorité HSRP la plus élevée devient le routeur actif.
- La valeur par défaut de la priorité HSRP est 100.
- Si les priorités sont identiques, le routeur avec l'adresse IPv4 la plus élevée devient le routeur actif.
- Pour configurer un routeur comme étant le routeur actif, utilisez la commande `standby priority`. La plage de priorité HSRP va de 0 à 255.
- Pour forcer un nouveau processus d'élection du HSRP à avoir lieu lorsqu'un routeur de plus haute priorité est mis en ligne, la préemption doit être activée à l'aide de la commande `interface standby preempt`.



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

116

## Configuration du protocole HSRP

SupMTI.ma

### Configuration de R1

```
R1(config)#int fa0/0
R1(config-if)#ip address 192.168.0.3 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
R1(config-if)#standby 1 ip 192.168.0.1
R1(config-if)#standby 1 preempt
R1(config-if)#end
R1#
```

### Configuration de R2

```
R2(config)#int fa0/0
R2(config-if)#ip address 192.168.0.2 255.255.255.0
R2(config-if)#standby 1 ip 192.168.0.1
R2(config-if)#standby 1 priority 110
R2(config-if)#standby 1 preempt
R2(config-if)#end
R2#
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

117

## NAT & PAT

SupMTI.ma

## Private Addressing

SupMTI.ma

| Class | RFC 1918 Internal Address Range | CIDR Prefix      |
|-------|---------------------------------|------------------|
| A     | 10.0.0.0 - 10.255.255.255       | 10.0.0.0 / 8     |
| B     | 172.16.0.0 - 172.31.255.255     | 172.16.0.0 / 12  |
| C     | 192.168.0.0 - 192.168.255.255   | 192.168.0.0 / 16 |

## WAN interconnexion

118

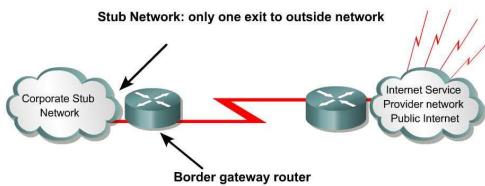
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

120

## NAT

SupMTI.ma

- A NAT-enabled device typically operates at the border of a stub network.



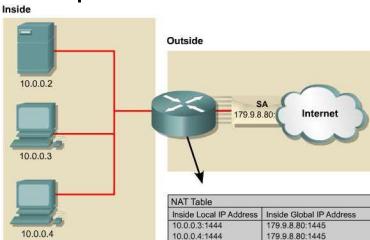
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

121

## NAT Features

SupMTI.ma

- Static NAT is designed to allow one-to-one mapping of local and global addresses.
- Dynamic NAT is designed to map a private IP address to a public address.



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

122

## NAT and PAT Benefits

SupMTI.ma

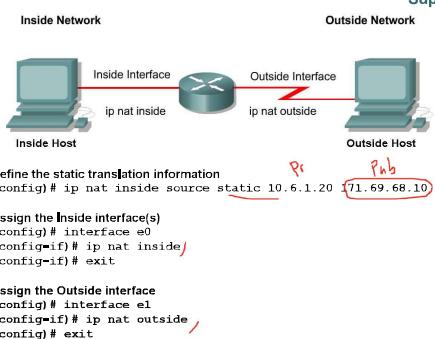
- Eliminates re-assigning each host a new IP address when changing to a new ISP
- Eliminates the need to re-address all hosts that require external access, saving time and money
- Conserves addresses through application port-level multiplexing
- Protects network security

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

125

## Configuring Static Translation

SupMTI.ma

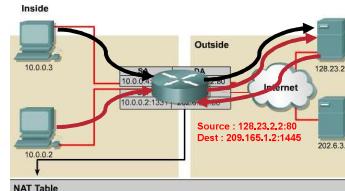


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

126

## PAT Features

SupMTI.ma

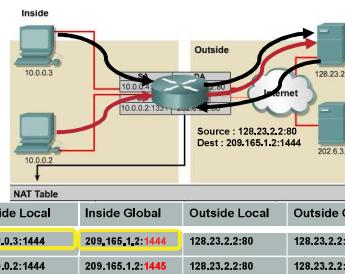


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

123

## PAT Features

SupMTI.ma

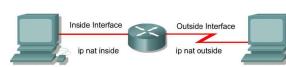


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

124

## Configuring Dynamic Translation

Inside Network      Outside Network      SupMTI.ma



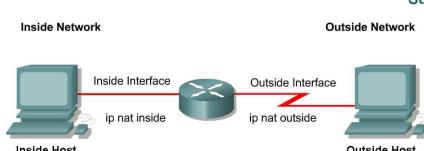
Define the NAT IP "pool"  
(config) # ip nat pool mypool 179.1.1.1 179.1.1.254 netmask 255.255.255.0  
Define the allowed internal IPs that can perform the NAT operation  
(config) # access-list 1 permit 10.0.0.0 0.0.0.255  
Define the dynamic translation information  
(config) # ip nat inside source list 1 pool mypool  
Assign the Inside interface(s)  
(config) # interface e0  
(config-if) # ip nat inside  
(config-if) # exit  
Assign the Outside interface  
(config) # interface e1  
(config-if) # ip nat outside  
(config-if) # exit

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

127

## Configuring PAT

SupMTI.ma

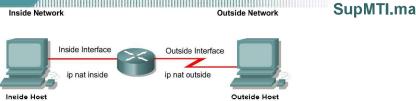


Same as NAT, simply add the keyword OVERLOAD at the end of the NAT translation line  
(config) # ip nat inside source list 1 pool mypool overload  
Another possible way to do it: Bind it to the external interface  
(config) # ip nat inside source list 1 interface e1 overload

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

128

## Configuring Dynamic Translation



- 1 Define the allowed internal IPs that can perform the NAT operation  
(config)# access-list 1 permit 10.0.0.0 0.0.0.255
- 2 Define the dynamic translation information  
(config)# ip nat inside source list 1 interface e1 overload
- 3 Assign the Inside interface(s)  
(config)# interface e0  
(config-if)# ip nat inside  
(config-if)# exit
- 4 Assign the Outside interface  
(config)# interface e1  
(config-if)# ip nat outside  
(config)# exit

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

129

## Issues With NAT

SupMTI.ma

NAT has several advantages, including the following:  
• NAT conserves the legally registered addressing scheme by allowing the privatization of intranets.  
• NAT allows the existing scheme to remain, and it still supports the new assigned addressing scheme outside the private network.

Cisco IOS NAT does support the following traffic types although they carry IP addresses in the application data stream:

- ICMP
- File Transfer Protocol (FTP), including PORT and PASV commands
- NetBIOS over TCP/IP, datagram, name, and session service
- Progressive Networks' RealAudio
- White Pines' CuSeMe
- DNS "A" and "PTR" queries
- H.223/NetMeeting, versions 12.0(1)/12.0(1)T and later
- VDO/LIVE, version 11.3(0)(1)T and later
- Xtreme, versions 11.3(4)(1)T and later
- IP Broadcast, version 12.0(1)T, the source address translation only

Cisco IOS NAT does not support the following traffic types:  
• Routing table updates  
• DNS zone transfers  
• BOOTP  
• talk, talkt  
• Simple Network Management Protocol (SNMP)

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

131

## Verifying NAT and PAT Configuration

SupMTI.ma

```
Router#show ip nat translations [verbose]
  • Displays active translation

Router#show ip nat translation
Pro Inside global   Inside local   Outside local   Outside global
172.16.131.1        10.10.10.1    ---           ---
Router#show ip nat statistics
  • Displays translation statistics

Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Serial0
Inside interfaces:
Ethernet0, Ethernet1
Hits: 5 Misses:0



Command	Description
show ip nat translations	Displays active translations
show ip nat statistics	Displays translation statistics

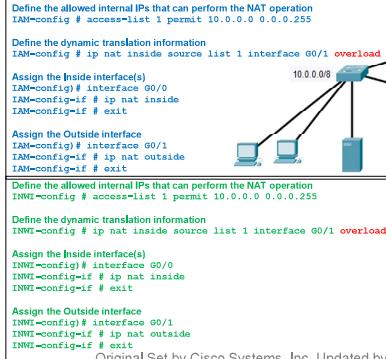

```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

130

## Cas de plusieurs connexions Internet

SupMTI.ma



On doit également configurer HSRP  
IAM-config# standby 1 ip 10.0.0.254  
IAM-config# standby 1 priority 110  
IAM-config# standby 1 preempt  
  
INWI-config# standby 1 ip 10.0.0.254  
  
Dans cette config, le routeur IAM sera le routeur actif et celui de INWI sera le routeur de backup

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

132



SupMTI.ma

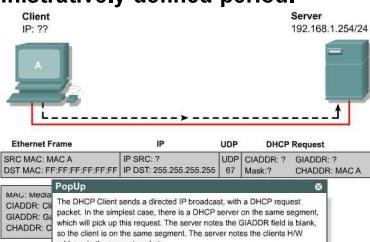
## DHCP Server over Cisco

133

## DHCP

SupMTI.ma

- DHCP works by providing a process for a server to allocate the IP information to clients. Clients lease the information from the server for an administratively defined period.



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

134

## Configuring DHCP

SupMTI.ma

Enable the DHCP Service  
(config)# service DHCP

Define a DHCP pool  
(config)# ip dhcp pool mypool

Define the range of "leasable" IP  
(dhcp-config)# network 172.16.10.0 255.255.255.0

Define the lease parameters  
(dhcp-config)# default-router 172.16.10.1  
(dhcp-config)# dns-server 172.16.10.1  
(dhcp-config)# domain-name cisco.com  
Etc...

(Optional) Define an Exclusion "aka UNWANTED" range  
(config)# ip dhcp excluded-address low [hi]

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

135

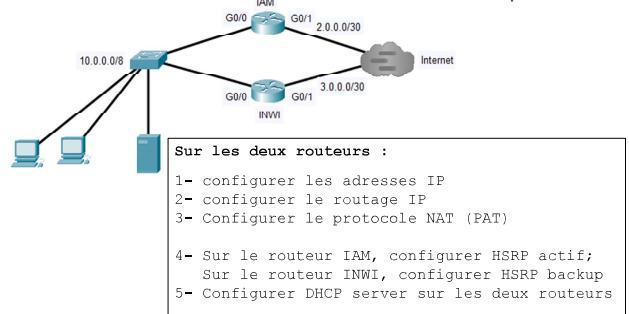
## Verifying DHCP

```
Router#show ip dhcp binding
Router#show ip dhcp binding
IP address      Hardware address    Lease expiration     Type
172.16.12.11   0100.10a4.97f4.6d Mar 02 1993 12:38 AM Automatic
Router#
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

137

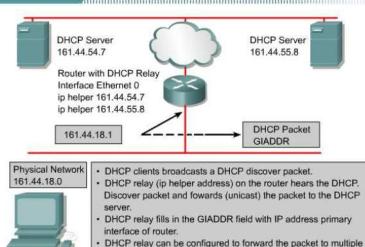
## TP : HSRP + NAT +DHCP



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

138

## DHCP Relay



Define one or more "helper address"  
(config) # ip helper-address 161.44.54.7  
...

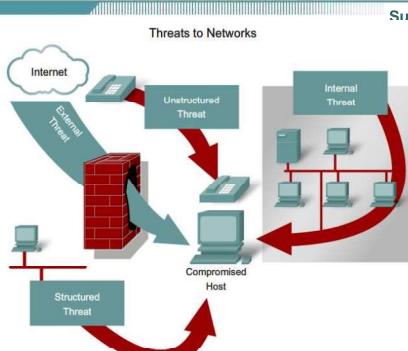
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

138

140

## Network security Access Control List: ACL

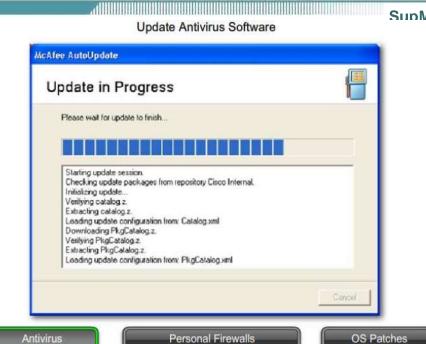
## ACL (Access Control List)



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

141

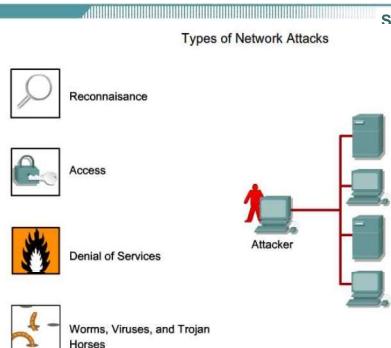
## ACL (Access Control List)



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

143

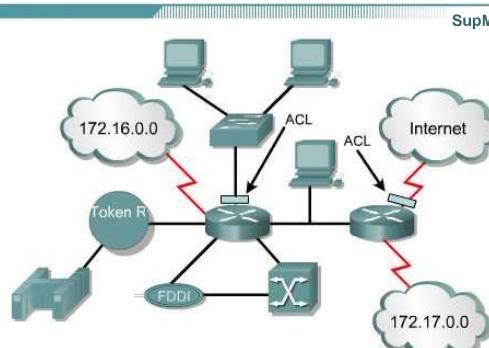
## ACL (Access Control List)



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

142

## ACL (Access Control List)

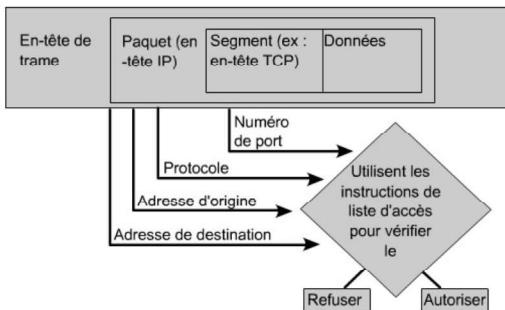


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

144

## ACL (Access Control List)

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

145

## ACL (Access Control List)

SupMTI.ma

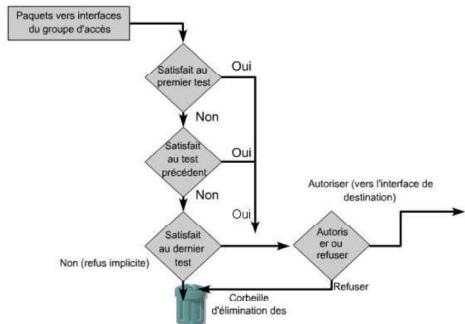
| Protocole                         | Plage              |
|-----------------------------------|--------------------|
| IP standard                       | 1-99, 1300-1999    |
| IP étendu                         | 100-199, 2000-2699 |
| AppleTalk                         | 600-699            |
| IPX                               | 800-899            |
| IPX étendu                        | 900-999            |
| Protocole IPX Service Advertising | 1000-1099          |

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

147

## ACL (Access Control List)

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

148

## ACL (Access Control List)

SupMTI.ma

```

Router(config)#access-list 2 deny 172.16.1.1
Router(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 2 deny 172.16.0.0 0.0.255.255
Router(config)#access-list 2 permit 172.0.0.0
0.255.255.255
Router(config)#interface e0
Router(config-if)#ip access-group 2 in
    
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

148

## Secure telnet: SSH

SupMTI.ma

```

R1# conf t
1. Configure the IP domain
R1(config)# ip domain-name span.com name of the network
R1(config)# crypto key generate rsa general-keys
2. Generate one way secret key
modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

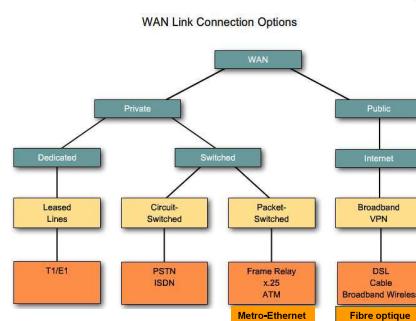
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
3. Verify or create a local database entry
R1(config) # username Bob secret cisco
R1(config) # line vty 0 4
R1(config-line) # login local
R1(config-line) # transport input ssh
R1(config-line) # exit
4. Enable VTY inbound SSH sessions
    
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

148

## WAN Technologies

SupMTI.ma

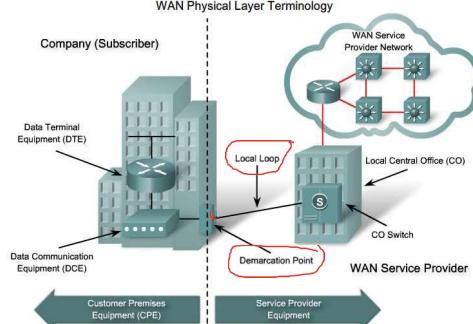


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

150

## WAN Technologies

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

151

## Lignes téléphoniques et le protocole PPP

149

## Commutation de circuits

SupMTI.ma

Les connexions à commutation de circuits sont fournies par les entreprises de réseau téléphonique de service public (PSTN). La boucle locale reliant le CPE au CO est un support cuivre.

Il existe deux options traditionnelles de commutation de circuits:

Réseau téléphonique public commuté (RTPC) *analogique*

- L'accès WAN à distance utilise le RTPC comme connexion WAN. Les boucles locales classiques peuvent transporter des données informatiques binaires sur le réseau téléphonique à l'aide d'un modem.

RNIS (Réseau Numérique à Intégration de Services) *Numerique*

- Les caractéristiques physiques de la boucle locale et sa connexion au réseau téléphonique public commuté (RTPC) limitent le débit signal à moins de 65 kbit/s.
- Le ISDN est une technologie de commutation de circuit qui permet à la boucle locale du RTPC de transporter des signaux numériques. Cela a permis d'obtenir des connexions communiquées de plus grande capacité que l'accès par ligne commutée. ISDN fournit des débits de données de 45 Kbit/s à 2.048 Mbit/s.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

152

## Configuring HDLC Encapsulation

SupMTI.ma

### Enable HDLC encapsulation on a serial interface

```
(config) # interface s0/0  
(config-if) # encapsulation hdlc
```

#### Caution:

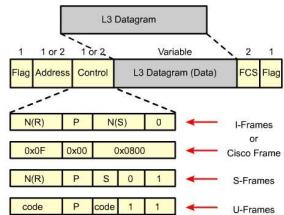
- HDLC is the default encapsulation on CISCO devices
- The HDLC implementation is CISCO proprietary, you need to use PPP when communicating with non-CISCO devices on serial links

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

154

## Protocole HDLC

SupMTI.ma



- Defined in 1979 by ISO, gave birth to a multitude of Link Access Protocols (LAP): LAPB (X.25), LAPD (ISDN), LAPM (Modem), LAPF (Frame Relay).
- Vendors offer proprietary versions of HDLC.
- CISCO HDLC supports multi-protocol on the same serial link.
- HDLC is the default Layer 2 encapsulation on CISCO serial links.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

153

## Troubleshooting a Serial Interface

SupMTI.ma

Several states can be identified in the interface status line when you issue the show interfaces serial command:

- Serial x is down, line protocol is down denotes a Layer 1 fault
- Serial x is up, line protocol is down denotes a Layer 2 fault
- Serial x is up, line protocol is up/down denotes a Layer 2 fault
- Serial x is up, line protocol is up denotes that the connection is Ok.
- Serial x is administratively down, line protocol is down denotes a user manual shutdown of the interface

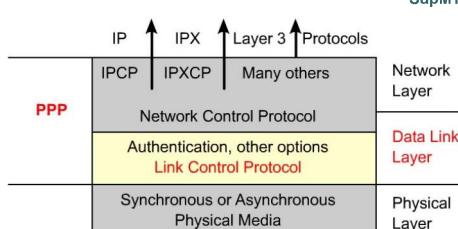
Use the show controllers command to check on the DCE/DTE cable states and clockrate

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

155

## PPP and the Data Link Layer

SupMTI.ma



LCP is in charge of the following:

- Authentication
- Compression
- Error detection
- Multilink and Callback

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

156

## PAP and CHAP

SupMTI.ma

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

158

## PPP Configuration Options

SupMTI.ma

| Features        | How It Operates                                        | Protocol                                |
|-----------------|--------------------------------------------------------|-----------------------------------------|
| Authentication  | Require a password and Perform Challenge Handshake     | PAP ✓<br>CHAP ✓                         |
| Compression     | Compress data at source; reproduce data at destination | Stacker, Predictor, TCP Header, or MPPC |
| Error Detection | Monitor data dropped on link<br>Avoid frame looping    | Quality Magic Number                    |
| Multilink       | Load balancing across multiple links                   | Multilink Protocol (MP)                 |

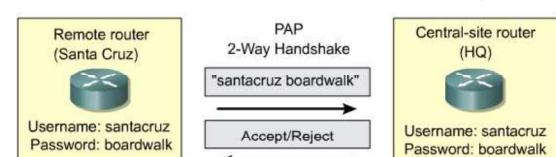
Cisco routers that use PPP encapsulation may include the LCP options shown in this table.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

157

## PPP Authentication - Password Authentication Protocol (PAP)

SupMTI.ma

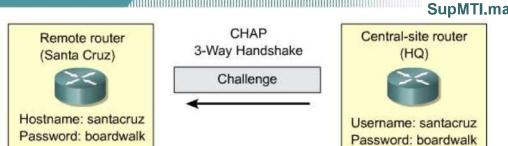


- Passwords sent in clear text
- Peer in control of attempts

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

159

## PPP Authentication - Challenge Handshake Authentication Protocol (CHAP)



Uses a secret password known only to authenticator and peer.

**CHAP provides protection against playback attack through the use of a variable challenge value that is unique and unpredictable.**

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

160

## Configuring PPP

SupMTI.ma

Router(config-if)#compress [predictor | stac]

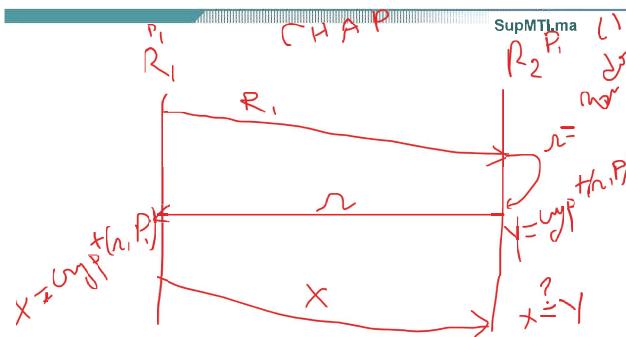
| Keyword   | Description                                                                   |
|-----------|-------------------------------------------------------------------------------|
| Predictor | (Optional) Specifies that a predictor compression algorithm will be used.     |
| Stac      | (Optional) Specifies that a Stacker (LZS) compression algorithm will be used. |

Router(config-if)#ppp quality percentage

| Keyword    | Description                                              |
|------------|----------------------------------------------------------|
| Percentage | Specifies the link quality threshold. Range is 1 to 100. |

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

162

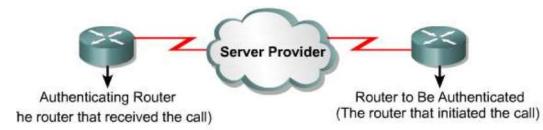


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

161

## Configuring PPP Authentication

SupMTI.ma



### Enabling PPP

ppp encapsulation

### Enabling PPP Authentication

hostname

username/password

ppp authentication

### Enabling PPP

ppp encapsulation

### Enabling PPP Authentication

hostname

username/password

ppp authentication

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

163

## PAP Configuration

SupMTI.ma



```
hostname Left
username Right password
someone
!
int serial 0/0
ip address 128.0.1.1
255.255.255.0
encapsulation ppp
ppp authentication pap
ppp pap sent-username
Left
password someone
```

```
hostname Right
username Left password
someone
!
int serial 0/0
ip address 128.0.1.2
255.255.255.0
encapsulation ppp
ppp authentication pap
ppp pap sent-username
Right
password someone
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

164

## Verifying PPP

SupMTI.ma

```
Router#show interfaces serial0/0
Serial0/0 is up, line protocol is up
  Hardware is HD6457
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive
    set (10 sec)
    LCP Open
    Open: IPCP, CDP/CP
    Last input 00:00:05, output 00:00:05, output
      hang never
    Last clearing of "show interface" counters never
    Queueing strategy: fifo
    Output queue 0/40, 0 drops; input queue 0/75, 0
      drops
    5 minute input rate 0 bits/sec, 0 packets/sec
      5 minute output rate 0 bits/sec, 0 packets/sec
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

165

## CHAP Configuration

SupMTI.ma



```
hostname Left
username Right password
someone
!
int serial 0/0
ip address 128.0.1.1
255.255.255.0
encapsulation ppp
ppp authentication CHAP
```

```
hostname Right
username Left password
someone
!
int serial 0/0
ip address 128.0.1.2
255.255.255.0
encapsulation ppp
ppp authentication CHAP
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

166

## PPP Configuration Commands

SupMTI.ma

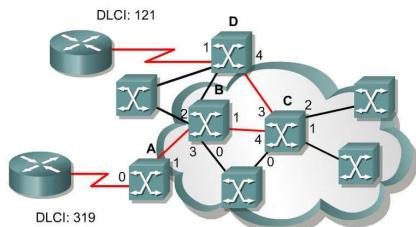
| Command                  | Description                                                                      |
|--------------------------|----------------------------------------------------------------------------------|
| encapsulation ppp        | Enables PPP on an interface                                                      |
| ppp authentication pap   | Enables PAP authentication on an interface                                       |
| ppp authentication chap  | Enables CHAP authentication on an interface                                      |
| username username        | Establishes a username-based authentication system                               |
| password password        | Displays statistics for all interfaces configured on the router or access server |
| show interfaces          | Displays statistics for all interfaces configured on the router or access server |
| debug ppp authentication | Debugs the PAP or CHAP authentication process                                    |
| undebug all              | TURNS OFF ALL DEBUGGING DISPLAYS                                                 |

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

167

## Frame Relay, Concepts

SupMTI.ma



La connexion entre deux DTE est appelée circuit virtuel (VC)

- Établi dynamiquement : SVC (Switched Virtual Circuits)
- Établi statiquement : PVC (Circuits Virtuels Permanents)

Frame Relay ne fournit aucun mécanisme de détection d'erreur.

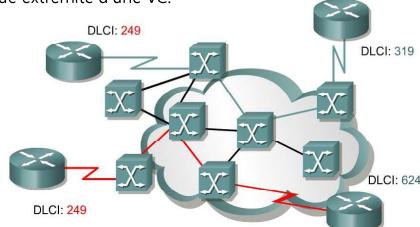
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

190

## Adresses Frame Relay : DLCIs

SupMTI.ma

L'identificateur de connexion de liaison de données (DLCI) est stocké dans le champ Adresse de chaque trame transmise. Le DLCI n'a généralement qu'une signification locale et peut être différent à chaque extrémité d'une VC.

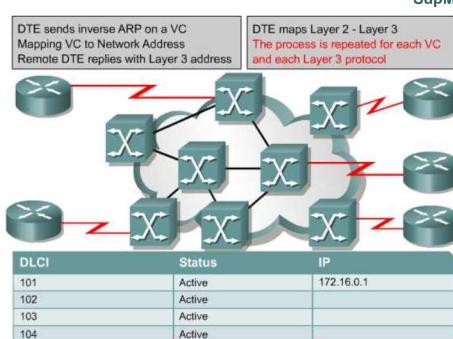


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

191

## Mappage, Inverse ARP - LMI2

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

194

## Frame Relay Configuration

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

195

## Interface locale de Management

SupMTI.ma

- Des extensions LMI ont été ajoutées pour permettre l'acquisition dynamique d'informations sur l'état du réseau.

• DLCI autorise les numéros VC allant de 0 à 1023 (10 bits). Les extensions de l'IMT réservent une partie de ces numéros

- LMI ajoute les fonctionnalités suivantes :

- Mécanisme de maintien en vie
- Prise en charge de la multidiffusion
- Contrôle de flux
- Importance mondiale pour DLCI
- Informations sur l'état

• Types d'IMT :

- CISCO, ANSI, q933a

| VC Identifiers | VC Types                                 |
|----------------|------------------------------------------|
| 0              | LM (ANSI/ITU)<br>Reserved for future use |
| 1..15          |                                          |
| 992..1007      | CLLM<br>Reserved for future use          |
| 1008..1022     |                                          |
| 1019..1022     | MultiLink (Cisco)<br>LM (Cisco)          |
| 1023           |                                          |

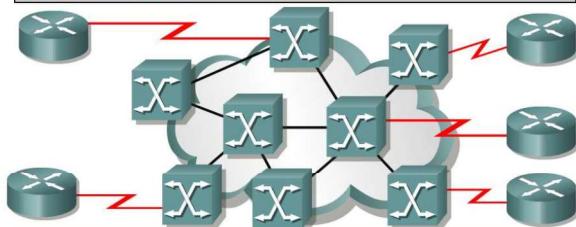
Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

192

## Apprentissage VC - LMI1

SupMTI.ma

DTE sends Status Enquiry Message (75) to DCE  
DCE responds with Status Message (7D) - includes configured DLCIs  
DTE learns what VCs it has

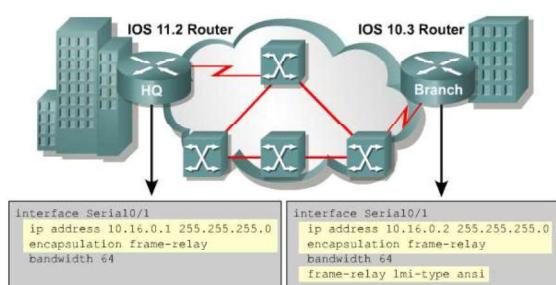


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

193

## Configuration Frame Relay avec LMI

SupMTI.ma

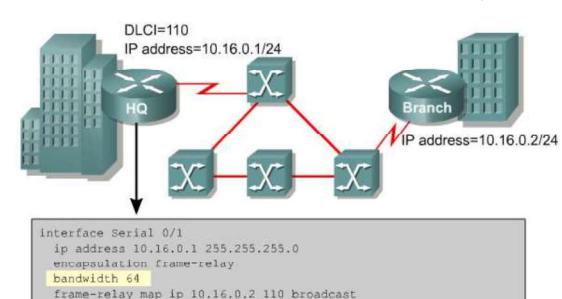


Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

196

## Mappage statique IP, DLCI (sans LMI)

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

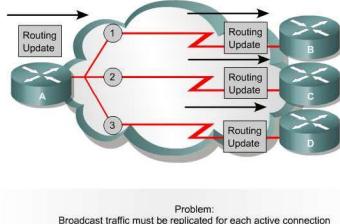
197

## Problème de routage dynamique

### RIP

SupMTI.ma

Par défaut, un réseau Frame Relay fournit une connectivité NBMA (Nonbroadcast MultiAccess) entre des sites distants. Un environnement NBMA est traité comme d'autres environnements multimédias multiaccès, où tous les routeurs se trouvent sur le même sous-réseau.



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

198

## Vérification Frame Relay

SupMTI.ma

```
Router#show frame-relay pvc 100
PVC Statistics for interface Serial0/0 (Frame Relay DTE)
  DLCI - 100, DLCI USAGE - LOCAL, PVC STATUS - ACTIVE,
  INTERFACE - Serial0/0

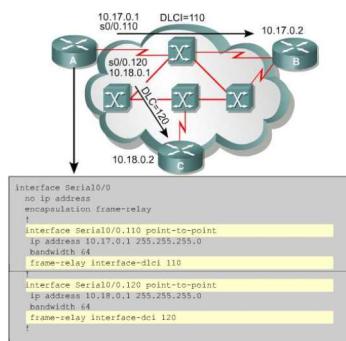
  input pkts 28      output pkts 10      in bytes 8398
  out bytes 1198     dropped pkts 0      in FECN pkts 0
  in BECN pkts 0    out FECN pkts 0     out DE pkts 0
  in DE pkts 0      out DE pkts 0      out bcast pkts 0
  out bcast pkts 10 out bcast bytes 1198
  pvc create time 00:03:46, last time pvc status changed
  00:03:47
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

200

## Configuration de Sous-interfaces

SupMTI.ma



Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

199

## Vérification Frame Relay

SupMTI.ma

```
Router#show frame-relay map
Serial0/0 (up): ip 10.40.1.1 dcli 100 (0x64,0x1840),
dynamic, broadcast, status defined, active
Router#clear frame-relay-inarp
Router#show frame map
Router#
```

Le réseau Frame Relay ne supporte pas les broadcasts.  
Si on configure le routage OSPF, il faut donc ajouter la ligne suivante sur les Interfaces Frame Relay :

**ip ospf network point-to-point**

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

201

## Gestion des Configs et IOSs

SupMTI.ma



### Maintenance des fichiers de routeurs et de commutateurs

#### Systèmes de fichiers de routeurs

SupMTI.ma

Le Cisco IFS (IOS File System) permet à l'administrateur de naviguer dans différents répertoires et d'établir la liste des fichiers d'un répertoire. L'administrateur peut également créer des sous-répertoires en mémoire flash ou sur un disque. Les répertoires disponibles dépendent du périphérique.

L'exemple affiche la sortie de la commande **show file systems**, qui répertorie tous les systèmes de fichiers disponibles sur un routeur Cisco 4221.

```
Router# show file systems
File Systems:
  Size(b)  Free(b)   Type  Flags  Prefixes
  -        -         opaque  rw    system:
  * 7194652672 6294822932 disk   rw    bootflash:; flash:
  256589324 256573440 disk   rw    usb0:
  1804488224 1/23/89312 disk   ro    webui:
  -        -         opaque  rw    null:
  -        -         opaque  rw    priv:
  -        -         opaque  rw    tftp:
  -        -         network rw    https:
  -        -         opaque  ro    syslog:
  3355432 33539983 nvram  iw    nvram:
  -        -         network rw    rcp:
  -        -         network rw    rsh:
  -        -         network rw    http:
  -        -         network rw    scp:
  -        -         network rw    sftp:
  -        -         opaque  ro    cns:
```

Router#
Il indique qu'il s'agit du système de fichiers par défaut actuel. Le signe dièse (#) indique un disque de démarrage. Les deux sont assignés au système de fichiers flash par défaut

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

202

### Maintenance des fichiers de routeurs et de commutateurs

#### Systèmes de fichiers de routeurs (suite)

SupMTI.ma

Comme flash est le système de fichiers par défaut, la commande **dir** liste le contenu de flash. La dernière liste présente un intérêt particulier. Il s'agit du nom de l'image en cours des fichiers Cisco IOS qui s'exécute dans la mémoire vive.

```
Router# dir
Directory of bootflash:/          10/15/14 Aug 2 2019 04:15:11 00:00
37094 drwx 4096 Aug 2 2019 04:15:10 +00:00 1flasher
338689 drwx 4096 Aug 2 2019 04:15:10 +00:00 .ash
217739 drwx 4096 Aug 2 2019 04:15:10 +00:00 core
337990 drwx 4096 Aug 2 2019 04:15:10 +00:00 .psync
86441 drwx 4096 Aug 2 2019 04:15:10 +00:00 1black_tuner
161281 drwx 4096 Aug 2 2019 04:16:11 +00:00 qm_script
112897 drwx 102400 Oct 2 2019 05:23:07 +00:00 traceilog
363890 drwx 4096 Aug 23 2019 04:15:41 +00:00 .dpmtest
298359 drwx 4096 Aug 23 2019 04:15:41 +00:00 .dpmtest-instance
12  -rw- 30 Oct 3 2019 05:14:41 +00:00 throughput_monitor_params
8055 drwx 4096 Aug 2 2019 04:17:55 +00:00 otep
13  -rw- 34 Oct 3 2019 05:14:41 +00:00 .ospf
248985 drwx 4096 Aug 20 2019 17:40:11 +00:00 archives
14  -rw- 65037 Oct 3 2019 15:19:41 +00:00 png-tech-discovery-summary
17  -rw- 5032908 Sep 19 2019 04:14:02 +00:00 .dpmtest
18  -rw- 817513193 Sep 21 2019 04:24:04 +00:00 iqr4200-
universalrpk_iqr4200_rpm.bak
7194652672 bytes total (6294822932 bytes free)
Router#
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

204

### Maintenance des fichiers de routeurs et de commutateurs

#### Systèmes de fichiers de routeurs (suite)

SupMTI.ma

Pour visualiser le contenu de la NVRAM, vous devez modifier le système de fichiers actuel par défaut en utilisant la commande **cd** (change directory), comme indiqué dans l'exemple.

La commande actuelle du répertoire de travail est **pwd**. Cette commande vérifie que nous affichons le répertoire NVRAM. Enfin, la commande **dir** affiche la liste du contenu de la mémoire non volatile NVRAM. Parmi les différents fichiers affichés, le seul qui présente un intérêt pour nous est le fichier nommé **start-up-config** qui définit la configuration de démarrage.

```
Router# cd nvram:
Router# pwd
nvram:
Router# dir
Directory of nvram:/          1024
32769  -rw- 1024 Aug 2 2019 04:15:12 00:00 startup-config
32770  -rw- 61 Aug 2 2019 04:15:10 00:00 private-config
32771  -rw- 1024 underlying-config
32772  -rw- 447 Aug 2 2019 04:15:10 00:00 private-vrf
6  -rw- 1237 Aug 2 2019 04:15:10 00:00 comp_invenctory
5  -rw- 0 Aug 2 2019 04:15:10 00:00 persistant-data
ISRA221-2xGIG_0_0_0_d
ecfm_ieee_mib
ifindex-table
10M-2x1G-4x1G
10G-SFP-Sig1.cer
10G-SFP-Sig2.cer
10G-Self-Sig1.cer
10G-Self-Sig2.cer
33554432 bytes total (35539983 bytes free)
Router#
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

205

## Maintenance des fichiers de routeurs et de commutateurs sauvegarder et restaurer une configuration

SupMTI.ma

Procédez comme suit pour sauvegarder la configuration en cours sur un serveur TFTP:  
Étape 1. Saisissez la commande `copy running-config tftp`.  
Étape 2. Entrez l'adresse IP de l'hôte sur lequel le fichier de configuration sera stocké.  
Étape 3. Entrez le nom à attribuer au fichier de configuration.  
Étape 4. Appuyez sur Entrée pour confirmer chaque choix.

Procédez comme suit pour restaurer la configuration en cours à partir d'un serveur TFTP:  
Étape 1. Saisissez la commande `copy tftp running-config`.  
Étape 2. Saisissez l'adresse IP de l'hôte sur lequel le fichier de configuration est stocké.  
Étape 3. Entrez le nom à attribuer au fichier de configuration.  
Étape 4. Appuyez sur Enter pour confirmer chaque choix.

```
R1# copy running-config tftp
Remote host [!]192.168.10.254
Destination filename [running-config]? R1-Jan-2019
Write file R1-Jan-2019 to 192.168.10.254? [confirm]
Writing R1-Jan-2019 !!!!! [OK]
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

206

## Maintenance des fichiers de routeurs et de commutateurs sauvegarder et restaurer une configuration

SupMTI.ma

- Exécutez la commande `show file systems` pour vérifier que le lecteur USB est là et confirmer son nom. Dans cet exemple, le système de fichiers USB est nommé `usbflash0`.
- Utilisez la commande `copy run usbflash0:/` pour copier le fichier de configuration vers la clé USB. Veuillez à utiliser le nom du disque Flash tel qu'il apparaît dans le système de fichiers. La barre oblique est facultative et indique le répertoire racine du disque Flash USB.
- LIOS vous invite à indiquer le nom du fichier. Si le fichier existe déjà sur le lecteur Flash USB, le routeur demande s'il peut le remplacer

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Avertissement : Il existe déjà un fichier portant ce nom
Vous voulez sur-écrire ? [confirm]

5024 bytes copied in 1.796 secs (2797 bytes/sec)
R1#
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

207

## Maintenance des fichiers de routeurs et de commutateurs Exemple de récupération de mot de passe

SupMTI.ma

```
Router# copy startup-config running-config
Destination filename [running-config]?

1450 bytes copied in 0.156 secs (9295 bytes/sec)
R1#

R1# configure terminal
Entrez les commandes de configuration, une par ligne. End with
CTRL/Z.
R1(config)# enable secret cisco

R1(config)# config-register 0x2102
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]? Building
configuration... [OK]
R1#
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

210

## Gestion des images IOS Sauvegarde d'une image IOS sur un serveur TFTP

SupMTI.ma

Pour gérer les opérations réseau avec un temps d'in disponibilité minimum, il est nécessaire de mettre en place des procédures de sauvegarde des images Cisco IOS. Ainsi, l'administrateur réseau peut rapidement copier une image sur un routeur en cas d'image corrompue ou effacée. Procédez comme suit :

- Envoyez une requête ping au serveur TFTP. Ping sur le serveur TFTP pour tester la connectivité.
- Vérifiez la taille de l'image en flash. Vérifiez que le serveur TFTP possède un espace disque suffisant pour accueillir l'image du logiciel Cisco IOS. Utilisez la commande `show flash0:` sur le routeur pour déterminer la taille du fichier image Cisco IOS.
- Copiez l'image sur le serveur TFTP. Copiez l'image sur le serveur TFTP en utilisant la commande `copy source-url destination- url`. Une fois la commande exécutée à l'aide des URL source et de destination spécifiées, l'utilisateur est invité à indiquer le nom du fichier source, l'adresse IP de l'hôte distant et le nom du fichier de destination. Le transfert commence.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

211

## Maintenance des fichiers de routeurs et de commutateurs Procédures de récupération des mots de passe

SupMTI.ma

Les mots de passe des périphériques permettent d'empêcher les accès non autorisés. Les mots de passe chiffrés, tels que les mots de passe secrets chiffrés, doivent être remplacés après la récupération. Selon l'appareil, la procédure détaillée de récupération de mot de passe varie.

Cependant, toutes les procédures de récupération des mots de passe pour les périphériques Cisco suivent le même principe :

- Activez le mode ROMMON.
- Modifiez le registre de configuration.
- Copiez la configuration de démarrage dans la configuration d'exécution.
- Changez le mot de passe.
- Enregistrez le running-config comme nouveau startup-config.
- Rechargez l'appareil.

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

208

## Maintenance des fichiers de routeurs et de commutateurs Exemple de récupération de mot de passe

SupMTI.ma

Étape 1. Activez le mode ROMMON. La console d'accès permet à l'utilisateur d'accéder au mode ROMMON au moyen d'une séquence de pause pendant le processus de démarrage ou en retirant la mémoire flash externe au moment de la mise hors tension du périphérique.

En cas de succès, l'invite `rommon 1 >` s'affiche, comme indiqué dans l'exemple.

```
Readonly ROMMON initialized
monitor: command "boot" aborted due to user interrupt
rommon 1 >

rommon 1 > confreg 0x2142
rommon 2 > reset

System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
(output omitted)
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

209

## Gestion des images IOS Restaurer une image IOS sur un appareil

SupMTI.ma

```
R1# copy tftp: flash:
Address or name of remote host []? 2001:DB8:CAFE:100::99
Source filename []? isr4200-universalk9 ias.16.09.04.SPA.bin
Destination filename [isr4200-universalk9 ias.16.09.04.SPA.bin]?
Accessing tftp://2001:DB8:CAFE:100::99/ isr4200-
universalk9 ias.16.09.04.SPA.bin... Loading isr4200-
universalk9 ias.16.09.04.SPA.bin from 2001:DB8:CAFE:100::99 (via
GigabitEthernet0/0/0): !!!!!!!!!

[OK - 517153193 bytes]
517153193 bytes copied in 868.128 secs (265652 bytes/sec)
```

```
R1(config)# config-register 0x2102
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]? Building configuration... [OK]
R1#
```

Original Set by Cisco Systems, Inc. Updated by M. EL KOUTBI

212

## Fin du cours

SupMTI.ma

213