Network Technology 2 –

Lennart Franked
email:lennart.franked@miun.se
Tel:060- 148683

Informationsteknologi och medier / Informations- och Kommunikationssystem (ITM/IKS)
Mittuniversitetet

15/03-2013

Background

Back in the days

- Coaxial network, one long yellow garden hose.
  - Everyone that were sitting physically together belonged to the same network.
- Introduction to hubs and switches.
  - Made it easier (cheaper) to divide the organisation into multiple LANs
  - K LAN, K switches

Purpose of VLAN

Why separate Local Area Networks?

- Performance,
- limit broadcast traffic,
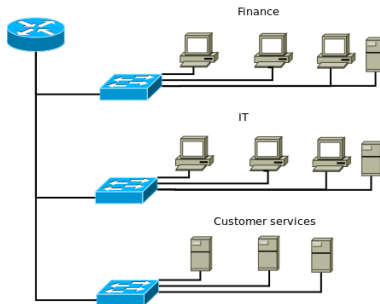- Security, physically restrict access to some networks.

Figure 1 : physically separated networks

Purpose of VLAN

Will this scale?

- Organisations grow and new offices, buildings, location will be added.
- expensive, difficult to administer by separating the departments in physically different networks.
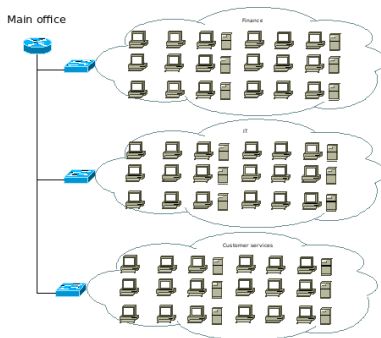

Figure 2 : Expanding organisation

Purpose of VLAN

Virtual LAN allows us to separate networks logically instead.
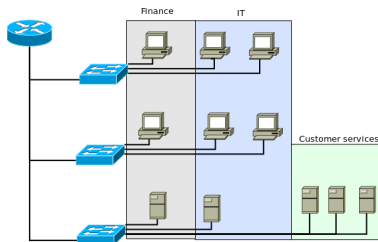

Figure 3 : Expanding organisation
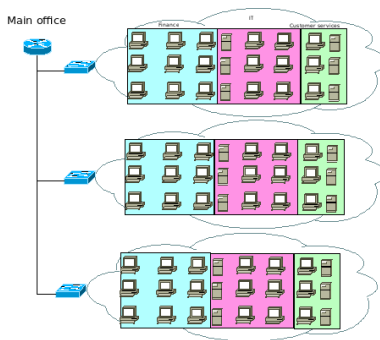
Purpose of VLAN

Figure 4 : Expanding organisation with VLAN

Different types of VLAN

Different types of VLAN that are defined by type or function.

- Default VLAN
    - The VLAN all ports are members of by default.
    - VLAN1, not possible to modify.
- Black Hole VLAN
    - Dummy VLAN for unused ports.
- Data VLAN
    - User-generated traffic
    - Voice, data
- Management VLAN
    - Used to manage network equipment.
- Native VLAN
    - Used for backwards compatibility in trunk-links
    - Only needed if switches that don't support VLANs are present in the network.

VLAN identification

VLAN ID
- Normal range
  - 1 to 1005
  - 1002 to 1005 reserved for Token Ring and FDDI
  - VLAN 1, 1002-1005 are created by default and cannot be removed.

- Extended range
  - 1006 to 4094
  - Only fully supported in VTPv3.
  - VTPv1 and v2 Switches only support extended range vlan if they are set in transparent mode.

Assigning VLAN

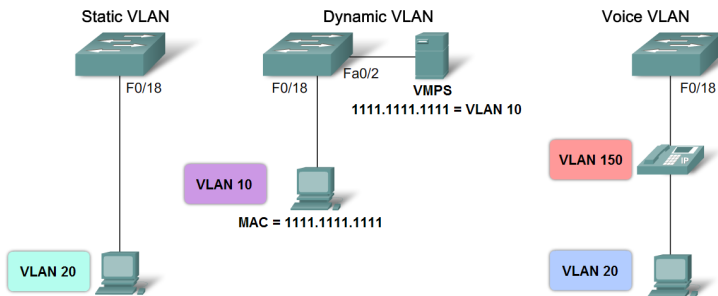
Figure 5 : Assigning VLAN membership

VoIP

- mls qos – Enable QoS for the switch
- mls qos trust cos – trust the Class of Service values.
- switchport voice vlan # – Set voice VLAN ID
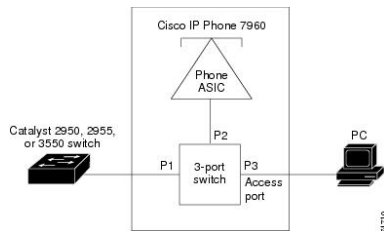- switchport access vlan # – Set data VLAN ID

Figure 6 : VLAN tagging within a Cisco phone

VLANs in a multiswitch network

- VLAN within one switch is simple.
- How about between two switches?
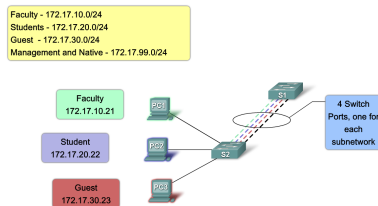

Figure 7 : One link per VLAN

Trunk

- Share a common link between all VLAN
- Need a way to mark which VLAN a frame belongs to.
- Tunneling – Inter-switch Link (ISL)
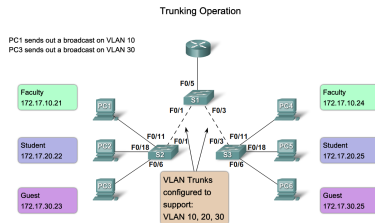- New ethernet header – IEEE 802.1Q

Figure 8 : VLAN trunking

Inter-switch link

- DA - Destination Multicast address.
- Type - Type of datalink protocol encapsulated.
- User - Priority setting.
- SA - MAC source address of the transmitting switch port.
- LEN - Length of the encapsulated package.
- SNAP - Contains information about the type of frame.
- HSA - High Bits of Source Address. Manufacturer of the source Interface. Must be Cisco Systems, Inc.
- VLAN - Contains the VLAN ID number.
- BPDU - Indicates if the encapsulated package is a BPDU or CDP frame.
- Index - Source port Index (Unique ID of the port).
- Reserved - Reserved 16 bit field, used for carrying extra information when encapsulating Token Ring and FDDI.
- Encapsulated frame.
- Frame Check Sequence.

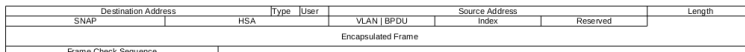| Destination Address		Type	User	Source Address			Length
SNAP	HSA		VLAN | BPDU	Index	Reserved		
Encapsulated Frame							
Frame Check Sequence							

Figure 9 : VLAN tagging within a Cisco phone

IEEE 802.1Q

- How to squeeze in VLAN information in the Ethernet header without having to replace all the Ethernet NIC?
- 1998 IEEE did the unthinkable and changed the Ethernet header.
- Only needed to be supported by the switches and not the end hosts.
- Priority field – 3 bit field, allow prioritizing frames.
- Canonical Format Indicator – Originally to indicate if MAC address are given in big endian or little endian.
- Used to allow forwarding Token Ring traffic.
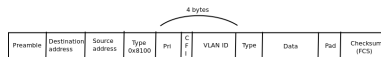- VLAN ID – Contains the VLAN ID number.

Figure 10 : IEEE 802.1Q header

Switchport types

- Access port
  - A switchport that belongs to a single VLAN
- Trunk port
  - A port that supports multiple VLAN

Dynamic Trunking Protocol (DTP)

- Cisco proprietary protocol
- Sends periodic DTP frames to the neighbouring port.
- Each interface can be in one out of four states
    - Dynamic Auto
    - Dynamic Desirable
    - Trunk
    - Access
- Turn off DTP using the `switchport nonegotiate`
- To show which mode an interface is in, use the `show dtp interface`

Dynamic Trunking Protocol (DTP)

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	–
Access	Access	Access	–	Access

DTP Switchport Mode Interactions

Port F0/1 is configured with
`switchport mode trunk`

Port F0/3 is configured with
`switchport mode dynamic auto`

S1

F0/1   F0/3

Port F0/1 is configured with
`switchport mode trunk`

Port F0/3 is configured with
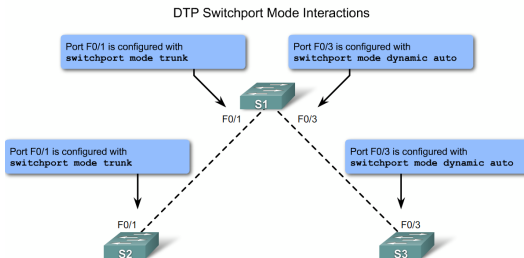`switchport mode dynamic auto`

F0/1

S2

F0/3

S3

Figure 11 : Trunking modes in DTP

Create a VLAN
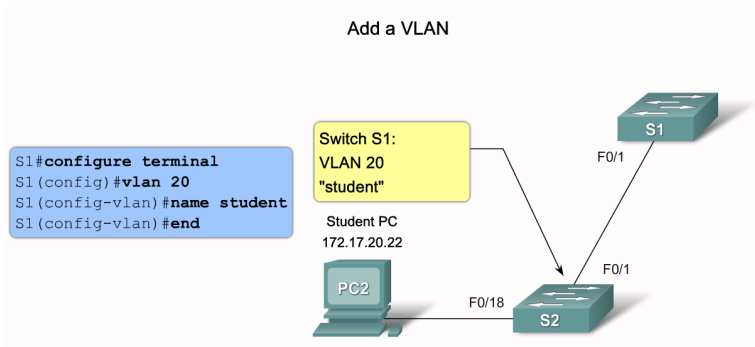
Figure 12 : Creating VLAN

Verify VLANs and Port Memberships

Show VLAN Command

Cisco IOS CLI Command Syntax	
`show vlan [brief	id ` *`vlan-id`* `	name ` *`vlan-name`* `	summary].`	
Display one line for each VLAN with the VLAN name, status, and its ports.	`brief`
Display information about a single VLAN identified by VLAN ID number. For vlan-id, the range is 1 to 4094.	`id ` *`vlan-id`*
Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.	`name ` *`vlan-name`*
Display VLAN summary information.	`summary`

Show Interfaces Command

Cisco IOS CLI Command Syntax	
`show interfaces ` *`[interface-id`* `	vlan ` *`vlan-id`* `]	switchport`	
Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 6.	*`interface-id`*
VLAN identification. The range is 1 to 4094.	`vlan ` *`vlan-id`*
Display the administrative and operational status of a switching port, including port blocking and port protection settings.	`switchport`

Figure 13 : Verifying VLAN

Configure switchports

Configure trunk port

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 1
```

Configure access port

```
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
```

VLAN troubleshoot

Common Problems with VLANs and Trunks

Problem	Result	Example
Native VLAN mismatches	Pose a security risks and create unintended results.	For example one port has defined as VLAN 99, the other defined as VLAN 100.
Trunk mode mismatches	Causes loss of network connectivity.	For example on port configured as trunk mode "off" and the other as trunk mode "on".
VLANs and IP Subnets	Causes loss of network connectivity.	For example user computers may have been configured with the incorrect IP addresses.
Allowed VLANs on Trunks	Causes unexpected traffic or no traffic is being sent over the trunk.	The list of allowed VLANs does not support current VLAN trunking requirements.

Figure 14 : Common problems

Introduction to VTP

What is VTP?

- To be able to use VLAN across multiple switches, each switch must have the same VLAN information.
- Manually configure each switch
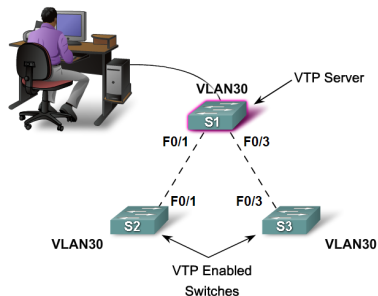- Use some sort of protocol that will fix this for us.

Figure 15 : VLAN Trunking Protocol

Purpose of VTP

- Allows for VLAN configuration consistency across the network.
- Accurate tracking and monitoring of VLANs.
- Dynamic reporting of added VLANs across the network.

VTP Components

- VTP domain.
- VTP modes.
  - VTP Server.
  - VTP client.
  - VTP transparent.
- VTP pruning
- VTP advertisements.
  - Summary advertisements.
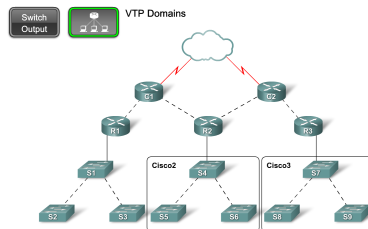 - Subset advertisements.
  - Request advertisements.

Figure 16 : Separating network into VTP domains

VTP roles - Server

- VTP server – Administers the VTP-domain
  - Stores VLAN information in vlan.dat
  - Supports adding, deleting and modifying VLAN.
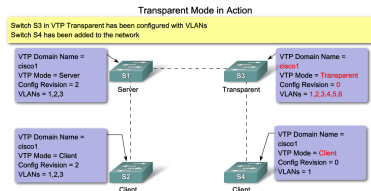 - Default VTP mode.

Figure 17 : VTP Modes

VTP roles - Client

- VTP Client
  - Stores VLAN information in running-config
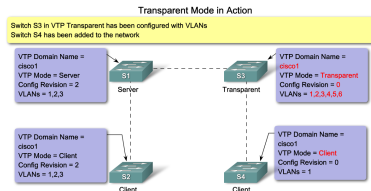 - Unable to add, delete or modify VLAN.

Figure 18 : VTP Modes

VTP roles - Transparent

- VTP transparent
  - Forwards VTP advertisements
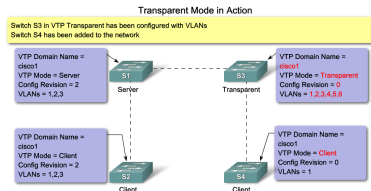 - Don't process them.
  - VLANs are local only.

Figure 19 :   VTP Modes

VTP Pruning

- VTP Pruning
  - Negotiate which VLANs are accessible per port.
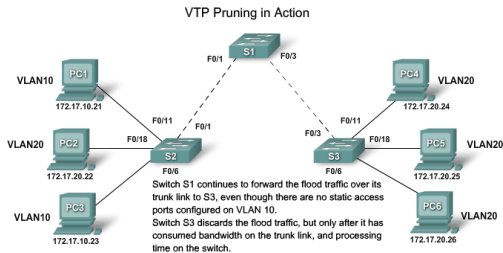 - `vtp pruning`

Figure 20 : VTP pruning

VTP Advertisement types

- Summary Advertisements
    - Sent every 5 minutes from a VTP server.
    - or when a change have occurred
    - Contains VTP domain name, revision number et cetera.
    - Informs about which VTP revision is the latest.

- Subset Advertisements
    - Contains information about the available VLANs
    - Sent from VTP-server when new vlan information has been added.

VTP Advertisement types

- Request advertisements
  - Sent to a VTP-server
  - sent when the domain name of the switch has been changed,
  - the switch receives a summary advertisement with a higher configuration value or
  - when a subset advertisement is missing.

Questions?