Basics of Switched Networks

SWITCH Module 1, 8

Agenda

- **Cisco Documentation**
- **Network Design**
- **Switches**
- **Ethernet**
- **Layer 2 Switching Concepts**
- **Power Over Ethernet**
- **Neighbor Discovery Protocols**
  - CDP
  - LLDP
- **Switch Port Analyzer**

Absolute Mandatory Commands Minimum

- To alleviate and ease your work with Cisco boxes in labs:

```
(conf)# line console 0
(conf-line)# logging synchronous
(conf)# line vty 0 15
(conf-line)# logging synchronous
(conf-line)# no login
(conf-line)# privilege exec level 15
(conf)# no ip domain-lookup
(conf)# ip host NAME IP
(conf)# terminal monitor
```

Course Recommendation

```
DLS1(config)# line vty 0 15
DLS1(config-line)# no login
DLS1(config-line)# privilege level 15
```

```
DLS1# terminal monitor
```

```
DLS1(config)# ip host als2 10.1.1.104
DLS1# als2
Trying als2 (10.1.1.104)... Open
ALS2#
ALS2# conf t

! Ctrl+Shift+6 and then x which simulates Ctrl^x

DLS1# show sessions
Conn Host                Address             Byte  Idle Conn
Name
   1 DLS2                10.1.1.102           671     0 DLS2
   2 ALS1                10.1.1.103             0     0 ALS1
*  3 ALS2                10.1.1.104             0     0 ALS2
DLS1# 3
[Resuming connection 3 to als2 ... ]

ALS2#
```

Cisco Web Documentation

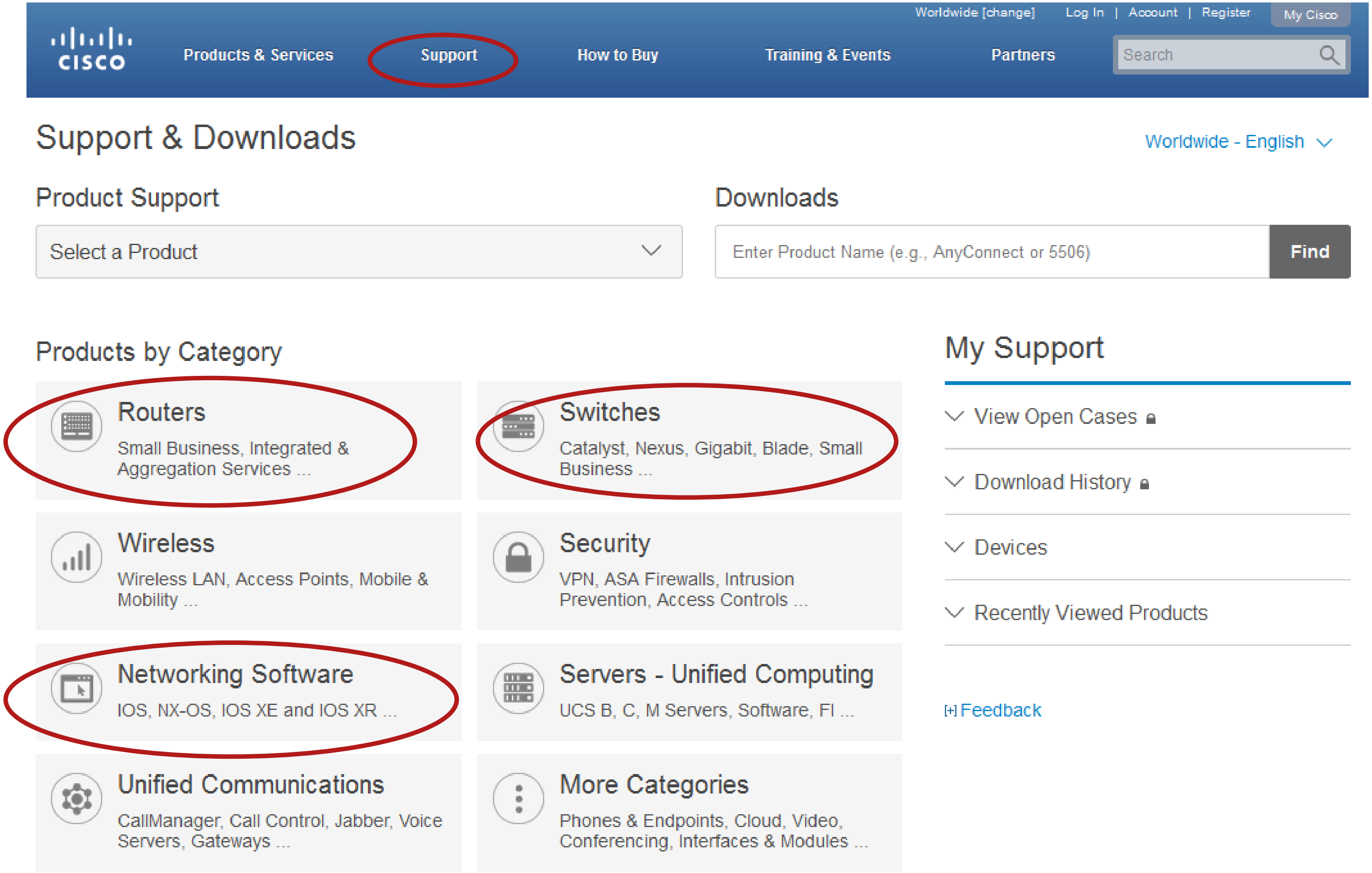
Cisco Web Documentation ①

- *No web curriculums at all!!!*
- cisco.com is your best friend
- Orientation on web pages are crucial for all IT networkers
  - *…and they are trying to sabotage it all the time ☺*
  - Huge knowledgebase

Cisco Web Documentation ②

- Products documentation available
  - by HW platforms
  - by IOS versions
- Experience learn us that IOS commands…
  - for routers are best to find directly in relevant IOS documentation
  - for switches are best to find directly in relevant switch product documentation
- *Hence it is usually good to know exact IOS and HW version*

http://cisco.com/go/support



Worldwide [change] Log In | Account | Register My Cisco

Products & Services | Support | How to Buy | Training & Events | Partners | Search

Support & Downloads

Worldwide - English

Product Support

Select a Product

Downloads

Enter Product Name (e.g., AnyConnect or 5506) Find

Products by Category

Routers
Small Business, Integrated & Aggregation Services ...

Switches
Catalyst, Nexus, Gigabit, Blade, Small Business ...

Wireless
Wireless LAN, Access Points, Mobile & Mobility ...

Security
VPN, ASA Firewalls, Intrusion Prevention, Access Controls ...

Networking Software
IOS, NX-OS, IOS XE and IOS XR ...

Servers - Unified Computing
UCS B, C, M Servers, Software, FI ...

Unified Communications
CallManager, Call Control, Jabber, Voice Servers, Gateways ...

More Categories
Phones & Endpoints, Cloud, Video, Conferencing, Interfaces & Modules ...

My Support

- View Open Cases
- Download History
- Devices
- Recently Viewed Products

[+] Feedback

IOS Documentation

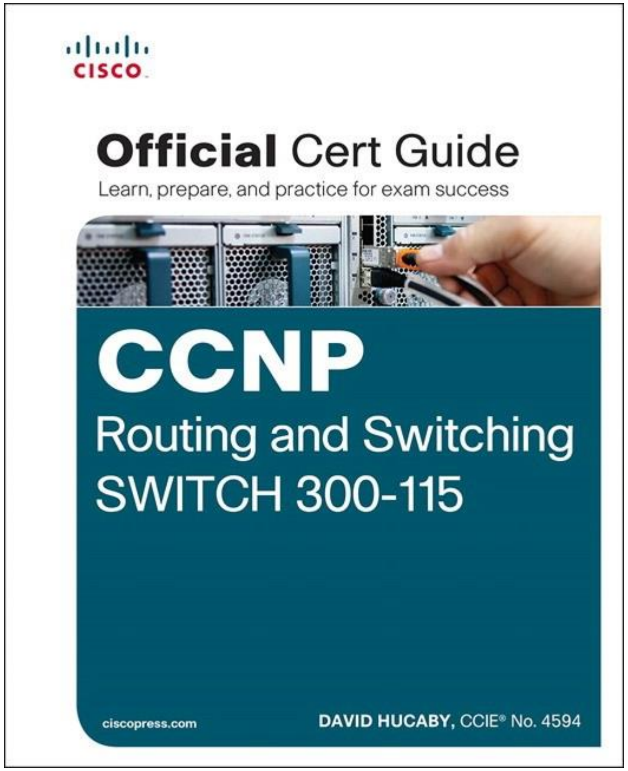
- Most important/interesting are following parts:
  - Configuration Guides consists of thorough description of technologies or protocols and ways how to configure them
  - Command References consists of commands descriptions, syntax and semantics
  - Master Index is alphabet index of commands with references to Command Reference
  - Error and System Messages consists of lists of IOS messages and theirs explanations
- Alternatively it’s possible to use Command Lookup Tool to find Command Reference to appropriate command
  - CCO account needed!

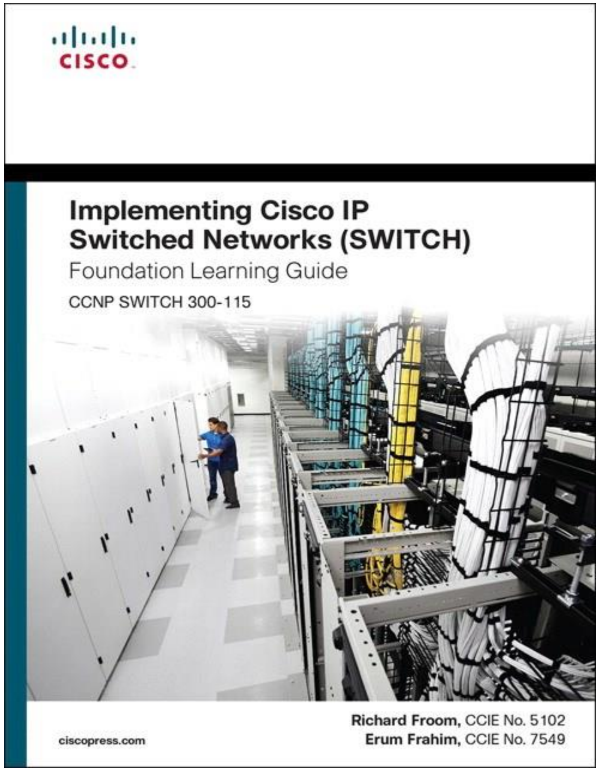
Supporting Documentation

- Case-studies, principle descriptions, configuration examples, technologies reviews
- Many of them have **Document ID** *NUMBER*
- How to search for them
  - „Configuring ...“
  - „Understanding ...“
  - „Troubleshooting ...“
  - „How to ...“
  - Support → Cisco IOS and NX-OS Software → Technology
- Cross-referencing between documents hence it’s necessary to make bookmarks

Self-study Literature

- CCNP R&S: SWITCH 300-115 official certification guide
- CCNP R&S: SWITCH 300-115 Foundation Learning Guide



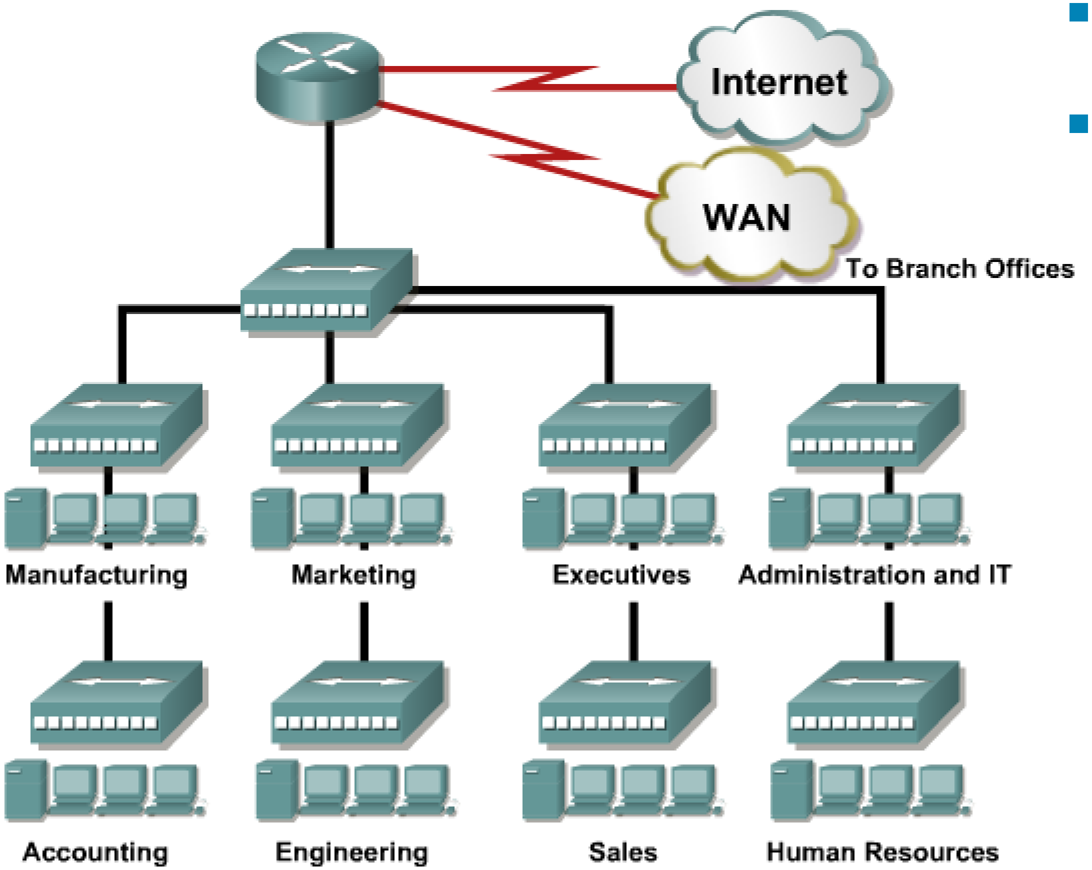

cisco
Implementing Cisco IP
Switched Networks (SWITCH)
Foundation Learning Guide
CCNP SWITCH 300-115
Richard Froom, CCIE No. 5102
Erum Frahim, CCIE No. 7549
ciscopress.com

Campus Network Structure

Multilayer Switching?

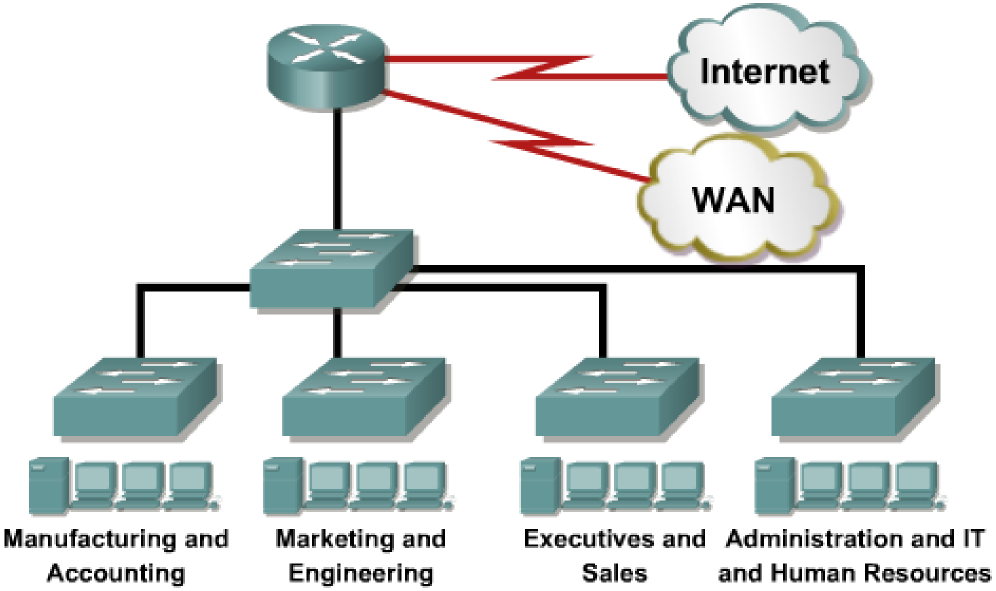
- **Multilayer Switching** is term referring to datagram switching on different layers of ISO/OSI model:
  - Layer 1 switching: Signal transmission and amplification
  - Layer 2 switching: Frame transmission (according to L2 header)
  - Layer 3 switching: Packet transmission (according to L3 header)
  - Layer 4 switching: Segment transmission (according to L4 header)
  - Layer 7 switching: Aplication data transmission (according to content)
- *What is difference between L3 switching and routing?*
  - Today it is usually the same process:
    - Routing is usually done by SW – CPU processed
    - Switching is accelerated by HW – ASIC processed
- **Multilayer switches**
  - Switches with datagram switching support on multiple layers at the same time
  - TCAM for fast lookup of RIB

Network without Hierarchy ①



- *Notice HUBs*
- Disadvantages:
  - Large collision domains
  - Large broadcast domains
  - No working groups separations
  - Nearly none security
  - Very hard to troubleshoot

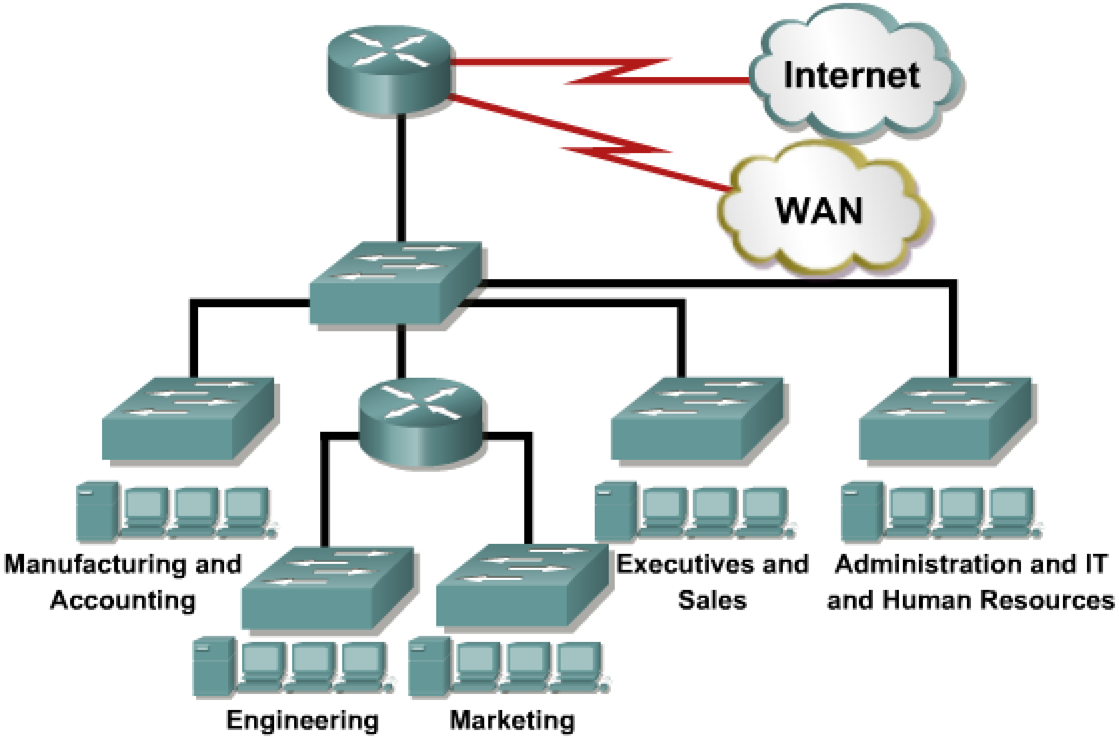
Network without Hierarchy ②



Internet
WAN
Manufacturing and Accounting
Marketing and Engineering
Executives and Sales
Administration and IT and Human Resources

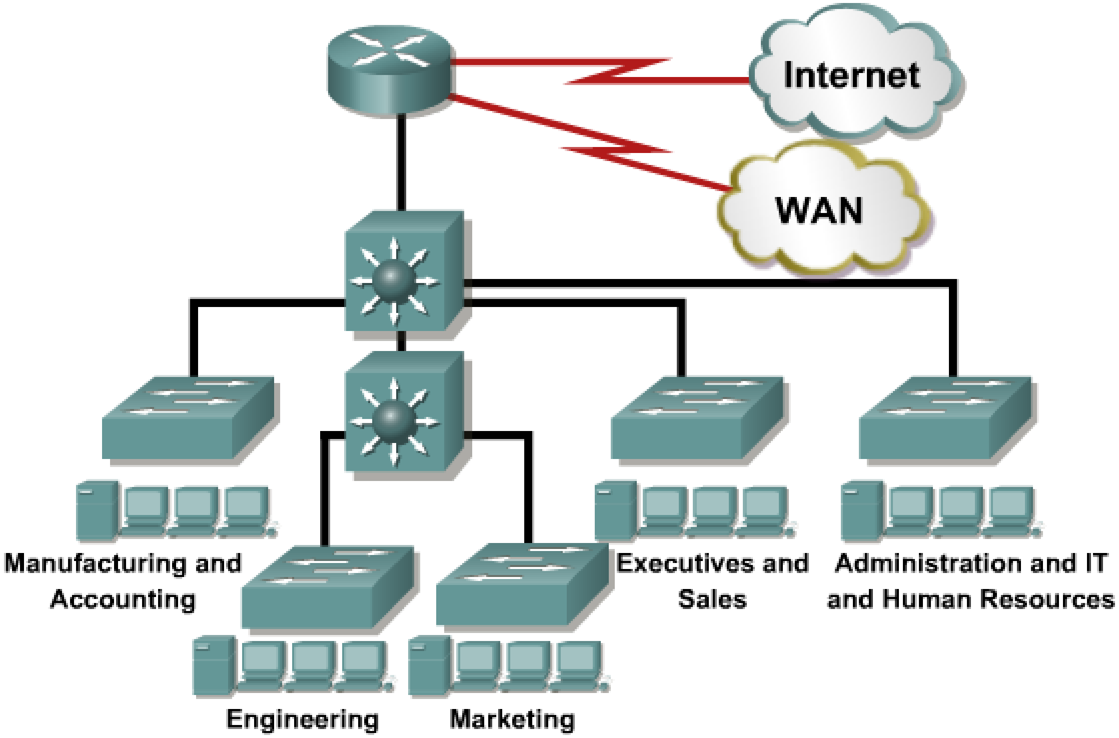
- *What if we replace hubs with switches – what is corrected and what is still missing?*
  - Bandwidth is not shared anymore
  - Large broadcast domains stays
  - Working groups are still not separated
  - No central point for sharing network resources

Introducing Hierarchy to Network


Internet
WAN
Manufacturing and Accounting
Executives and Sales
Administration and IT and Human Resources
Engineering
Marketing

- With help of router
  - Smaller broadcast domains
  - More control over transferred traffic
- *Unfortunately routers are quite expensive*
  - Price for port is high
  - Number of ports on usual router is limited

Introducing Multilayer Switching


Internet
WAN
Manufacturing and Accounting
Executives and Sales
Administration and IT and Human Resources
Engineering
Marketing

- Multilayer switches replace routers as integrated devices
- Combine features of
  - Layer 2 switching
  - Layer 3 routing
  - Layer 4 balancing
- Low latency
- High switching throughput

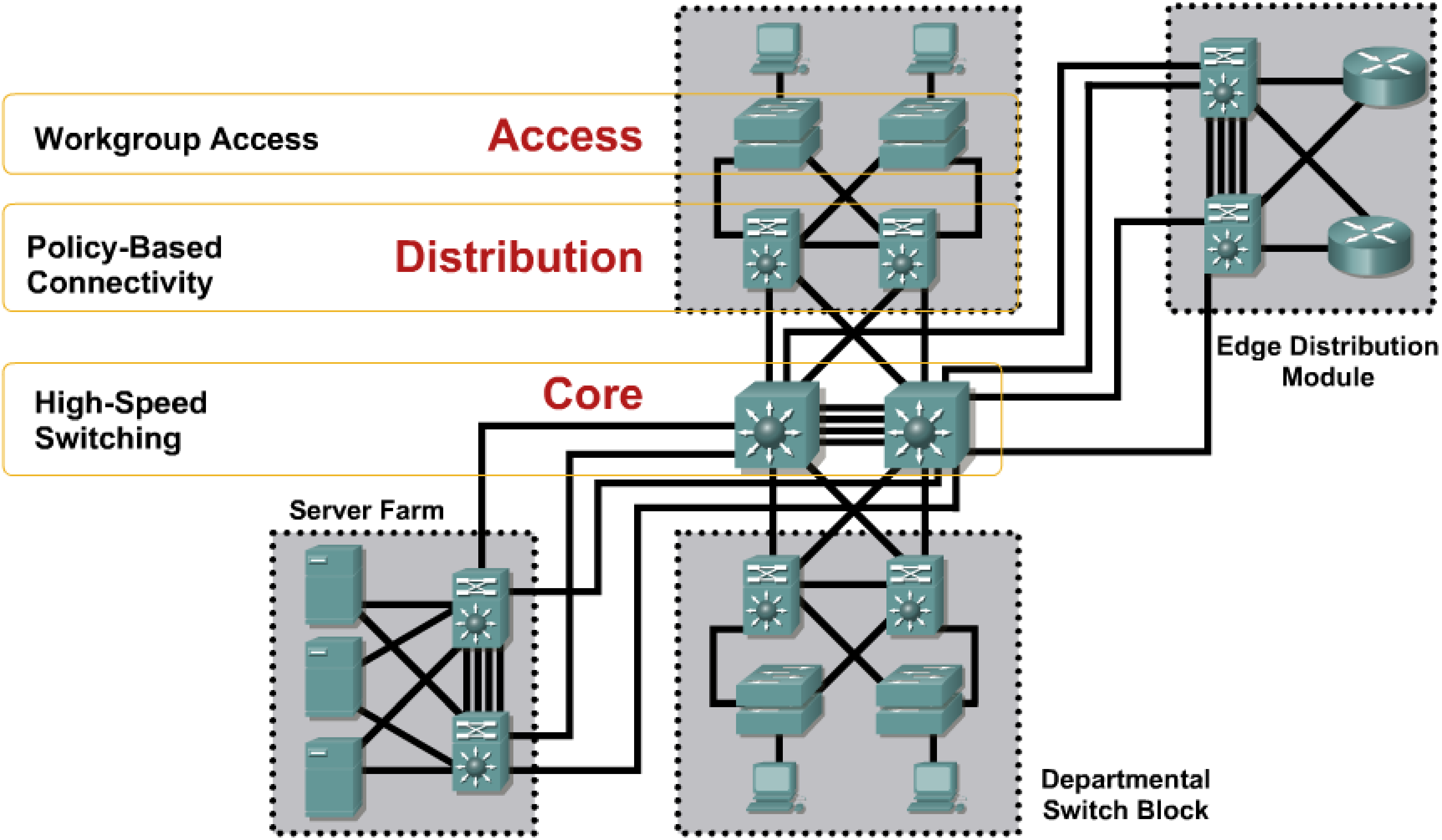
Features of Good Design

- Ad-hoc approach and design *leads you to hell and further!!!*
- Hierarchically designed network:
  - Has well-known borders of collision, broadcast and error domains
  - Has positive impact on operation
  - Scalable assignment of addresses together with their summarization
  - Transparent network flows
  - Divides L2 and L3 functionality

3Layered Network Design ①

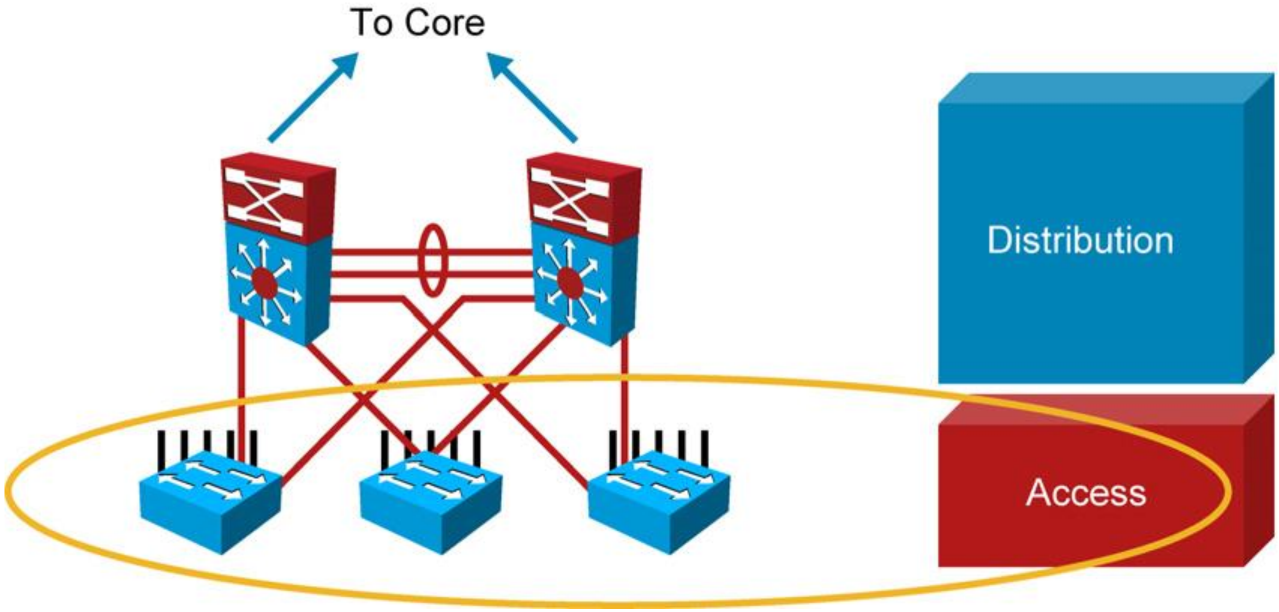
- *Bigger network means more attached devices*
- It’s favorable to divide them according to theirs network function thereby organize them into layers
  - End-to-end connectivity
  - Policy-based routing
  - Fast backbone switching
- System of those three layers (**access**, **distribution**, **core**) is old, traditional but still working

3Layered Network Design ②



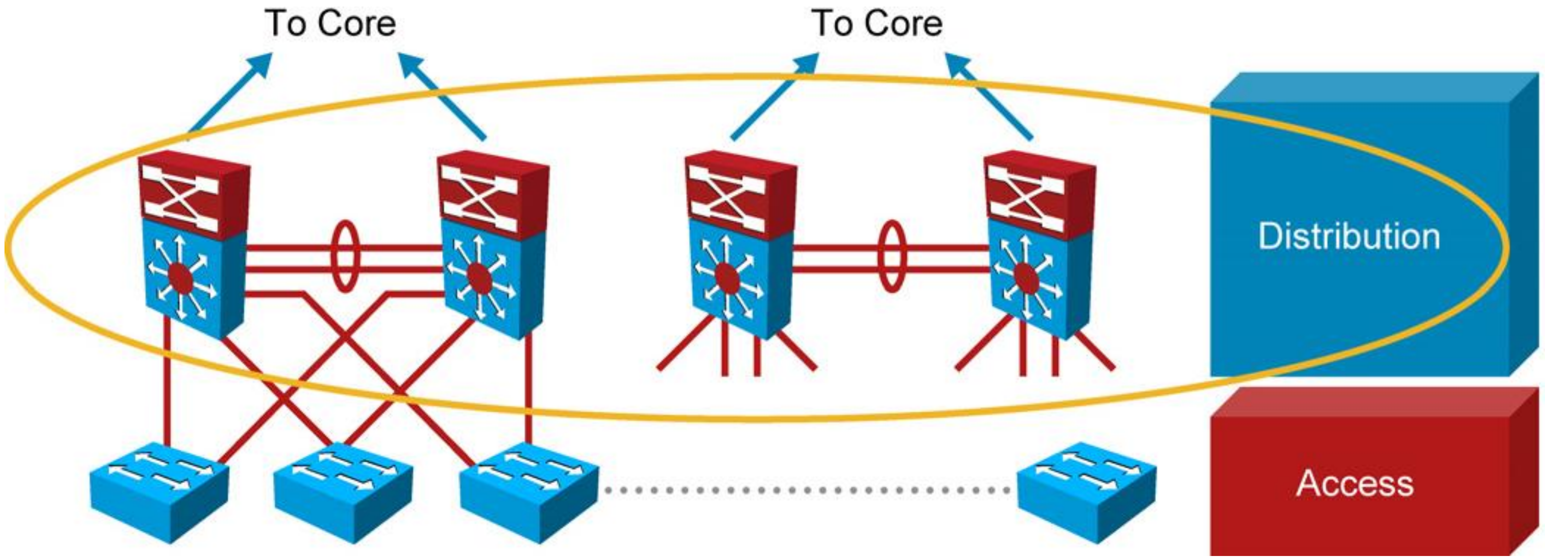
Access Layer

- Provides access and aggregation for users in a feature-rich environment
- Provides high availability through software attributes and redundancy
- Supports convergence for voice, wireless, and data
- Provides security services to help control network access
- Offers QoS services including traffic classification and queuing
- Supports IP multicast traffic for efficient network use



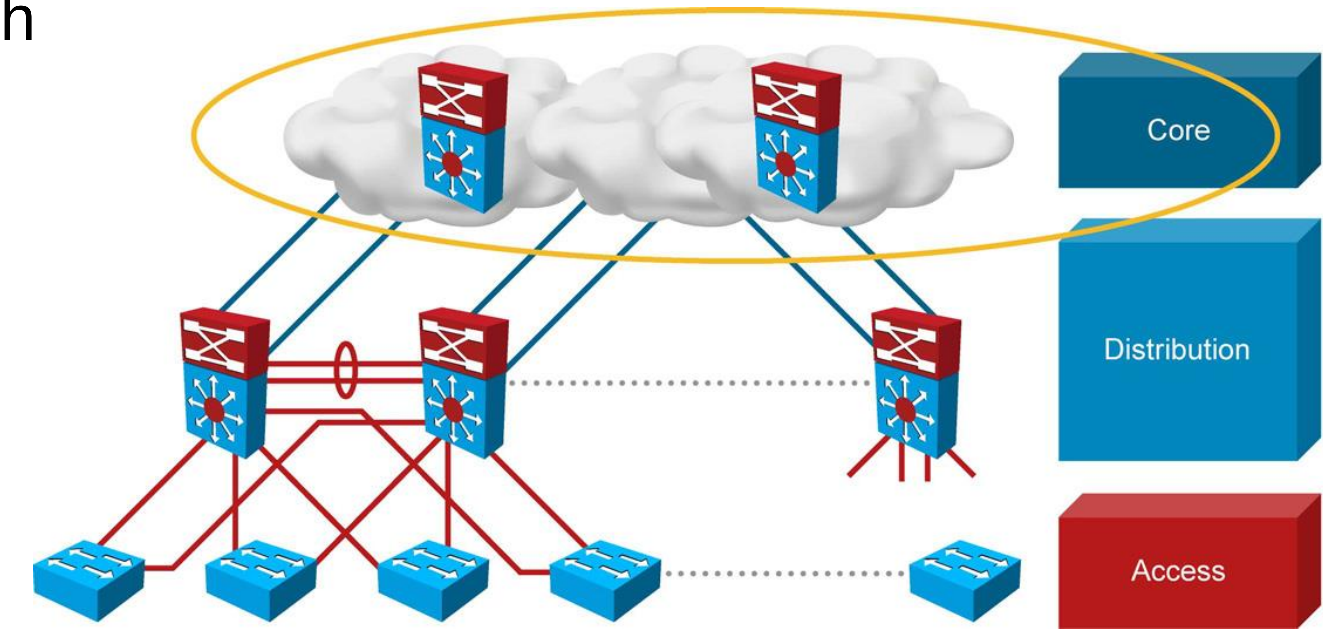
Distribution Layer

- Aggregates access nodes and uplinks
- Provides redundant connections and devices for high availability
- Offers routing services such as summarization, redistribution, and default gateways
- Implements policies including filtering, security, and QoS mechanisms
- Segments workgroups and isolates problems

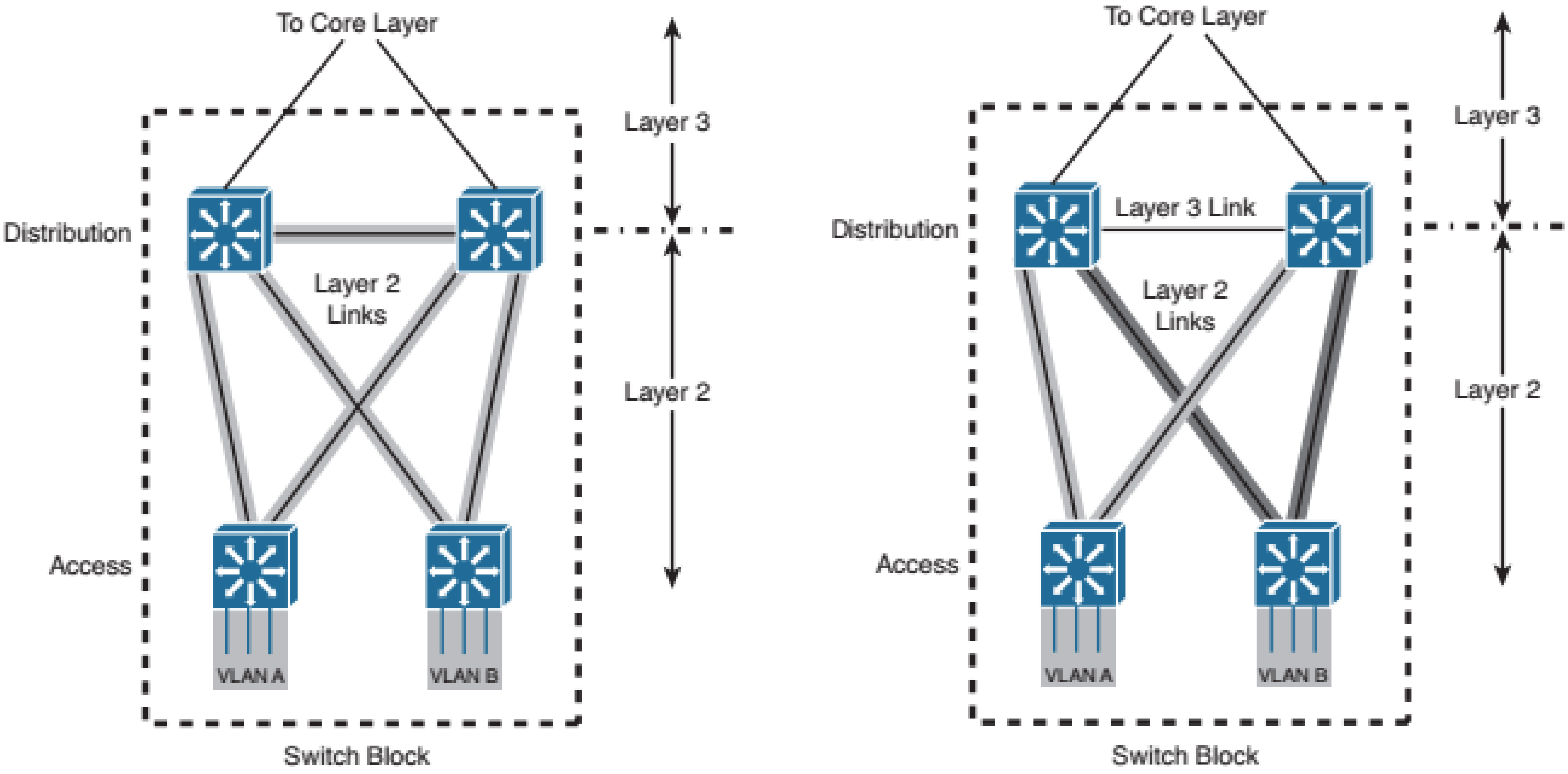


Core Layer (Backbone)

- The core layer is a high-speed backbone and aggregation point for the enterprise.
- It provides reliability through redundancy and fast convergence.
- The separate core layer helps in scalability during future growth

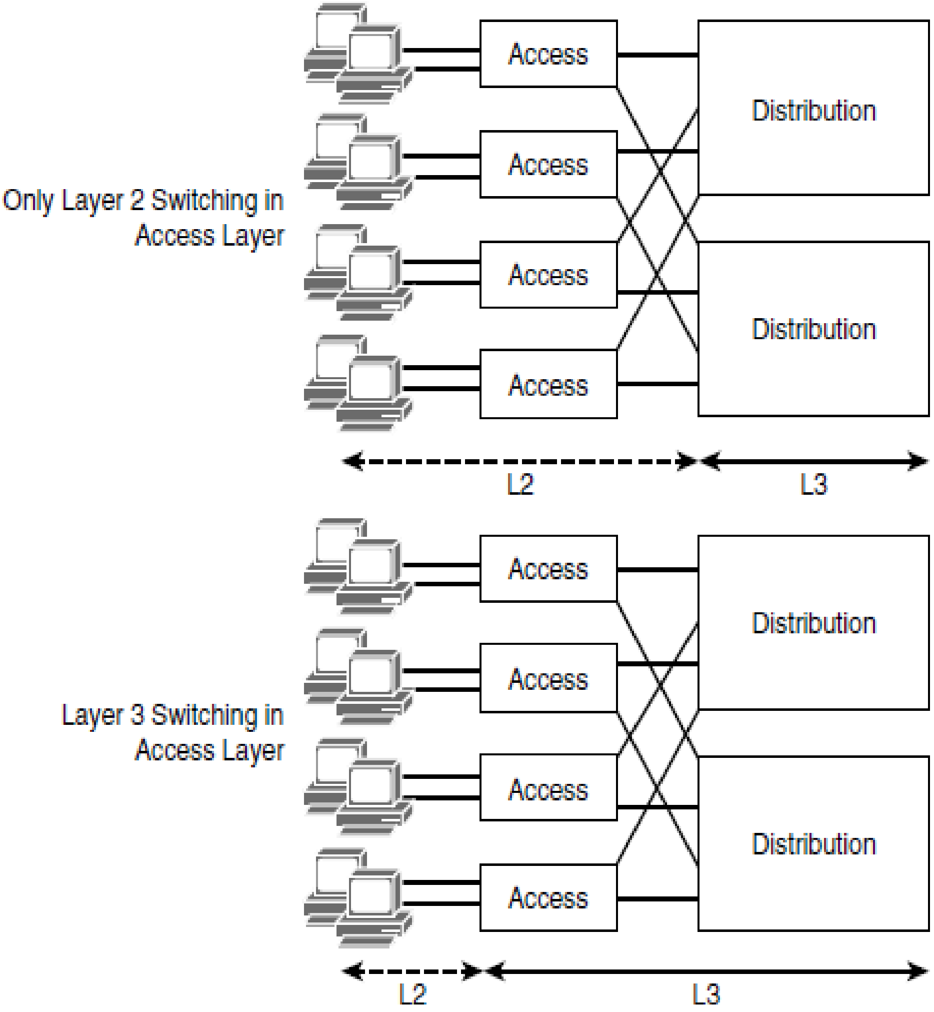


Redundancy in the network design



Layer 3 in the Access Layer

- Because of the reduced cost and a few inherit benefits, Layer 3 switching in the access layer has become more common over typical Layer 2 switching in the access layer.
- Using Layer 3 switching or traditional Layer 2 switching in the access layer has benefits and drawbacks.



Layer 3 in the Access Layer

- **Benefits**
  - Using a design that leverages Layer 3 switching to the access layer VLANs scales better than Layer 2 switching designs because VLANs get terminated on the access layer devices.
  - Specifically, the links between the distribution and access layer switches are routed links; all access and distribution devices would participate in the routing scheme.
  - The Layer 2-only access design is a traditional, slightly cheaper solution, but it suffers from optimal use of links between access and distribution due to spanning tree
- **Drawbacks**
  - Layer 3 designs introduce the challenge of how to separate traffic.
  - Layer 3 designs also require careful planning with respect to IP addressing.
  - A VLAN on one Layer 3 access device cannot be on another access layer switch in a different part of your network because each VLAN is globally significant.
  - Traditionally, mobility of devices is limited in the campus network of the enterprise in Layer 3 access layer networks. without using an advanced mobility networking features .

Best practices for hierarchical design

- Design each layer with pairs of switches.
- Connect each switch to the next higher layer with two links for redundancy
- Connect each pair of distribution switches with a link
- Do not connect the access layer switches to each other (unless logical stack).
- Do not extend VLANs beyond distribution switches. The distribution layer should always be the boundary of VLANs, subnets, and broadcasts.
- VLAN traffic should not traverse the network core.

Switches

Switch Properties ①

- **Form factor (size)**
  - Number of rack units (R or RU)
  - 1 RU = 1,75” = 44,45 mm
- **Configuration**
  - Fixed
  - Modular
    - Supervisors and link cards
    - ASICs
    - Power supply
- **Stackable**
  - Stacking of routers which from outside behave as one switch

1 rack unit (1U)

Switch Properties ②

- **Port density**
  - Number of available ports on device
- **Forwarding rate (overall bandwidth)**
  - Efficiency of device datagram switching in bps resp. pps
- **Link aggregation**
  - Option to combine multiple ports to one logical interconnection
- **Power over Ethernet (PoE)**
  - To provide power for IP phones, wireless Aps or CATV
  - Increasing cost of devices
- **Multilayer capabilities**
  - L3 routing, load-balancing

Switches for 3Layered Network Design

- Access layer
  - Catalyst 2960X (L2 switch)
  - Catalyst 3650, 3850, 4500 (L3 switch)
  - Wifi Aps
- Distribution layer
  - Catalyst 4500-X, 4500-E, 6800
- Core
  - Catalyst 4500, 6800

Access layer

	Catalyst Model	Max Port Density	Uplinks	Max Backplane	Other Features
	2960-X	384 (Up to 8 48-port switches in a stack)	2 10GE or 4 1 Gigabit Ethernet per switch	80 Gbps	RIP, OSPF available for routed access layer; PoE+
	3650	432 (Up to 9 48-port switches in a stack)	2 Gigabit Ethernet or 4 10GE	160 Gbps	Full-featured routing available, integrated wireless controller, PoE+
	3850	432 (Up to 9 48-port switches in a stack)	4 Gigabit Ethernet, 4 10GE	480 Gbps	Full-featured routing available, integrated wireless controller, PoE+, UPoE

Distribution layer

	Catalyst Model	Max Port Density	Max Backplane	Other Features
	4500-X	80 10GE	1.6 Tbps	Dual-chassis Virtual Switching System (VSS) redundancy
	4500E	96 10GE or 384 Gigabit Ethernet	928 Gbps	Dual supervisors

Core layer

Catalyst Model	Max Port Density	Max Backplane	Other Features
6807-XL	40 40Gbps, 160 Gigabit Ethernet, 480 Gigabit Ethernet	22.8 Tbps	Dual supervisor, dual-chassis VSS redundancy

Ethernet

A Brief Introduction

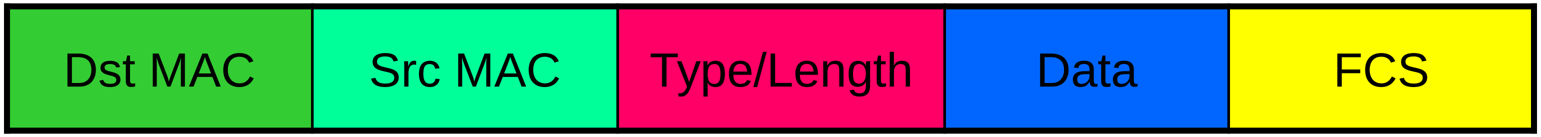
- Ethernet was invented in the first half of 70s in XEROX Inc.
- One of inventors was Robert Metcalf, founder of 3Com
- *It is cheap, undemanding, best-effort technology*
- Currently is wide-spread dominant L2 technology for LANs which targets also SANs, MANs and even WANs
  - Carrier Ethernet
  - Data Center Bridging
  - Synchronous Ethernet
- Speeds from 10 Mbps up to 100 Gbps

Questions FYI and Discussion

- What is collision and broadcast domain?
- Why has frame set minimum and maximum length?
- What is slot time?
- How does CSMA/CD work?
- How does full-duplex work on TP cabling? How is it related with CSMA/CD?
- What is collision? What kind of collision types do exist?
- What types of active network devices are/were usually used in Ethernet?
- Is there any limit for number of devices in cascade?
- How does auto-negotiation operate? What if it does not work?
- What is Auto-MDIX and when does it work properly?
- Is Ethernet synchronous technology?
- How many Ethernet frame types actually do exist?

Ethernet Frame Format ①

- Multiple types of Ethernet frame exists and all of them has same base structure:

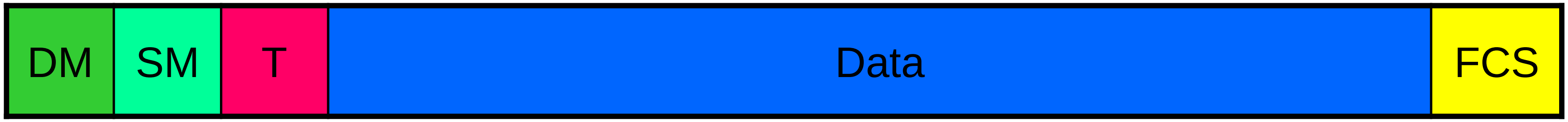


Dst MAC	Src MAC	Type/Length	Data	FCS

- Currently known variants:
  - Ethernet II (aka DIX)
  - 802.3 (sometimes referred as 802.2 because of LLC header)
  - SNAP (aka 802.3 SNAP)
  - Novell Raw (IPX run over it)

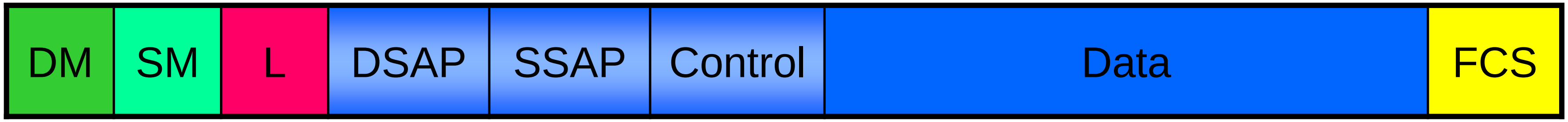
Ethernet Frame Format ②

Ethernet II



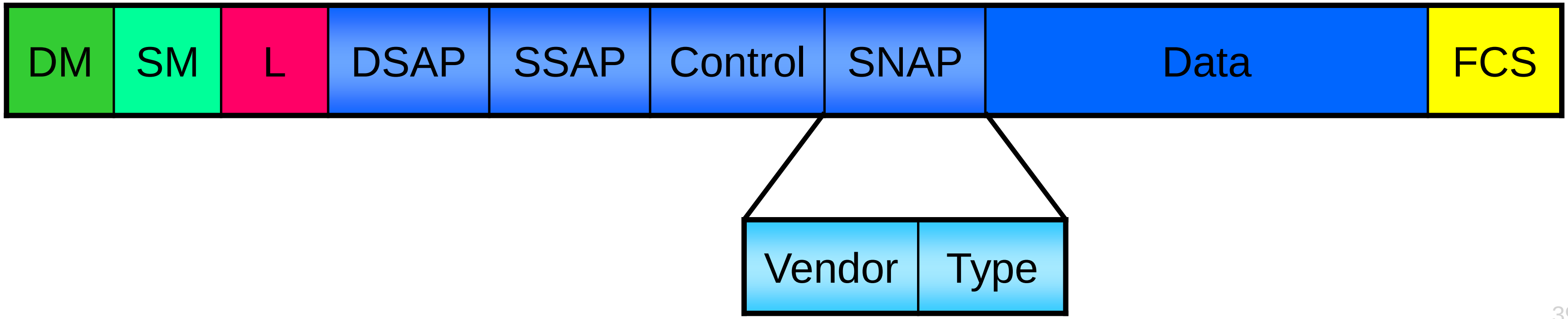
DM	SM	T	Data	FCS

Ethernet 802.2 LLC



DM	SM	L	DSAP	SSAP	Control	Data	FCS

Ethernet 802.3 SNAP



DM	SM	L	DSAP	SSAP	Control	SNAP	Data	FCS

Vendor	Type

Layer 2 Switch Operation

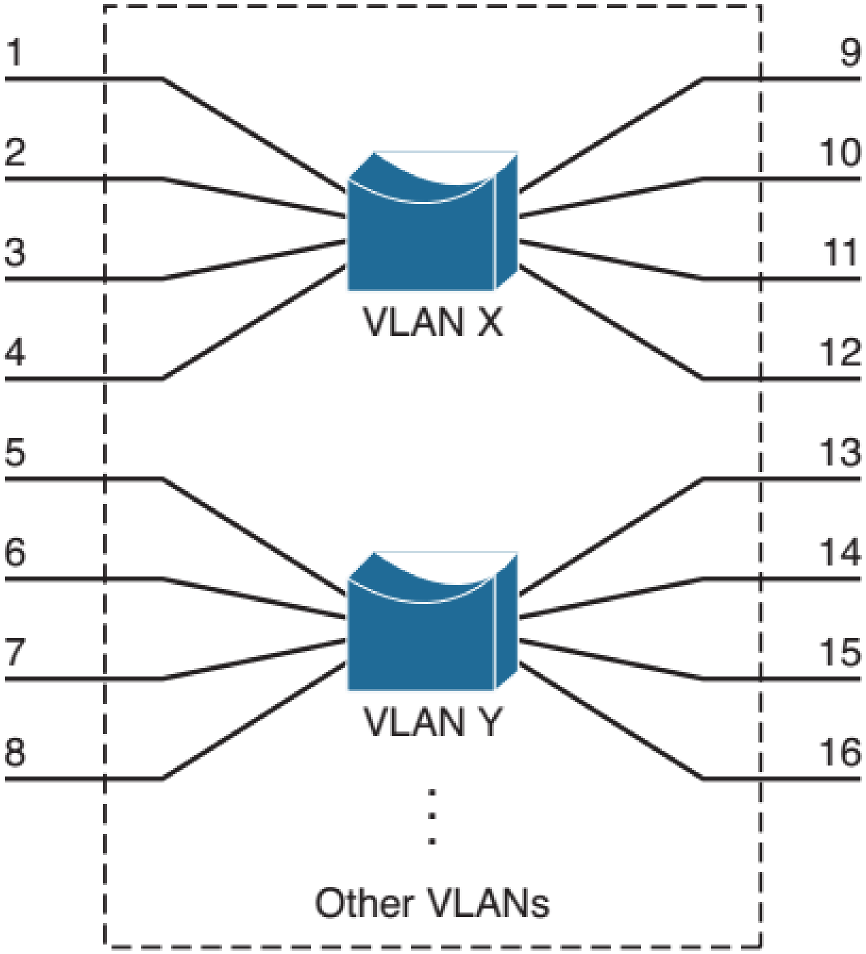
Basic switch operation

- Ethernet switch operates at L2, making decisions based on the destination MAC addresses found within the frames
- Provides isolation between connected host
  - Host connections can operate in full-duplex mode
  - On each switch port, the collision domain consists of the switch port itself and the devices directly connected to that port
  - Errors in frames are not propagated
  - You can limit broadcast traffic to a volume threshold

Comparing Layer 2 and Multilayer Switches

- L2 switches make decisions about forwarding frames based on the destination MAC addresses found within the frame.
- When a switch receives in **store-n-forward mode**, the frame is checked for errors, and frames with a valid cyclic redundancy check (CRC) are regenerated and transmitted.
- Some models of switches, mostly Nexus switches, opt to switch frames based only on reading the Layer 2 information and bypassing the CRC check.
- This bypass, referred to as **cut-through switching**, lowers the latency of the frame transmission as the entire frame is not stored before transmission to another port.
- Lower switching latency is beneficial for low-latency applications such as algorithm trading programs found in the data center. The assumption is that the end device network interface card (NIC) or an upper-level protocol will eventually discard the bad frame.
- Most Catalyst switches are store-n-forward.

L2 Switching



Forwarding Table

0000.1111.1111: port 11, vlan X
0000.2222.2222: port 6, vlan Y
0000.3333.3333: port 1, vlan X
0000.4444.4444: port 9, vlan X
0000.5555.5555: port 8, vlan Y
0000.6666.6666: port 14, vlan Y
0000.7777.7777: port 3, vlan X
0000.8888.8888: port 16, vlan Y

Broadcast: VLAN X: all VLAN X ports
Broadcast: VLAN Y: all VLAN Y ports

Content-Addressable Memory (CAM)

- A CAM table is used for Layer 2 switching
- Switch stores the source MAC address, port of arrival, VLAN and timestamp
- By default, CAM table entries are kept for 300 seconds

```
Switch(config)# mac address-table aging-time seconds
```

- MAC addresses are learned dynamically from incoming frames

```
Switch(config)# mac address-table static mac-address
   vlan vlan-id interface type mod/num
```

Ternary Content-Addressable Memory (TCAM)

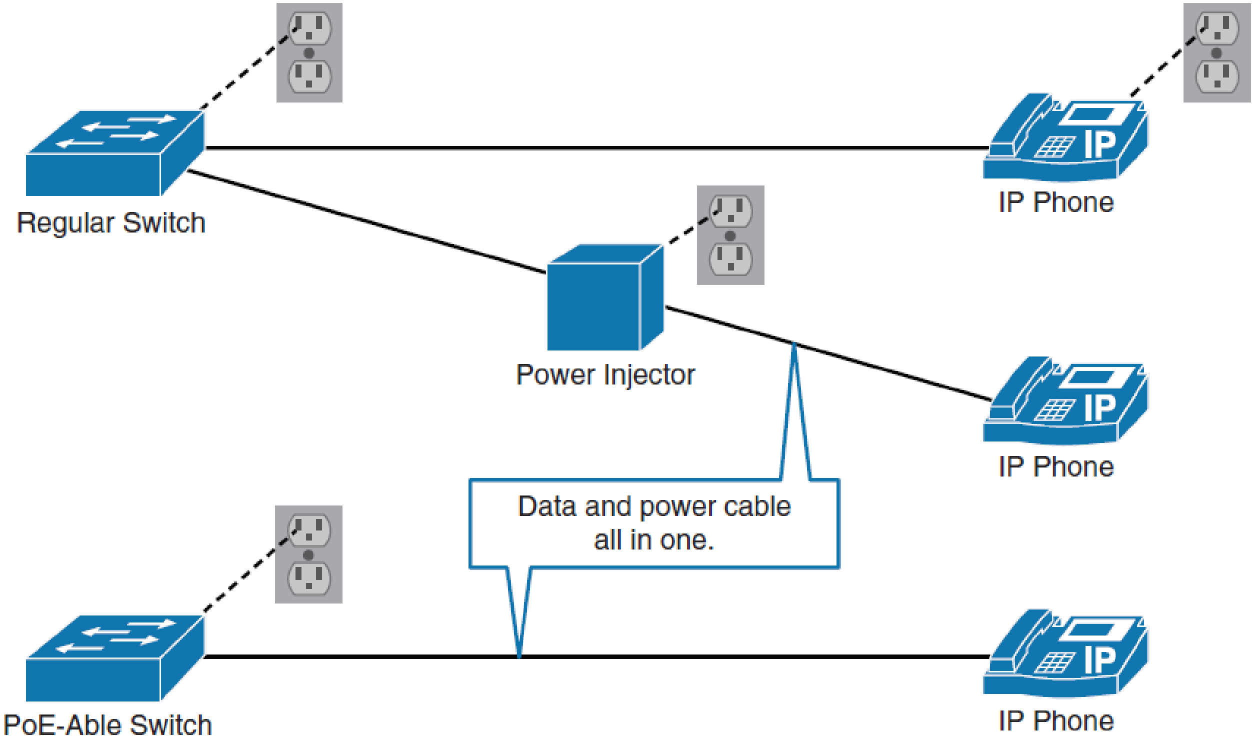
- a packet can be evaluated against an entire access list within a single table lookup
- Most switches have multiple TCAMs
  - inbound and outbound security and QoS ACLs, forwarding L3 decision
- Feature Manager (FM):
  - Compiles and merges ACLs into entries in the TCAM table
- Switching Database Manager (SDM):
  - the TCAM is partitioned into several areas that support different functions
  - configures or tunes the TCAM partitions

```
Switch(config)# show platform tcam utilization
```

Power over Ethernet

Power over Ethernet

- http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/troubleshooting/g_power_over_ethernet.html
- Power over Ethernet (PoE) supplies power through the same cable as data.



PoE Components

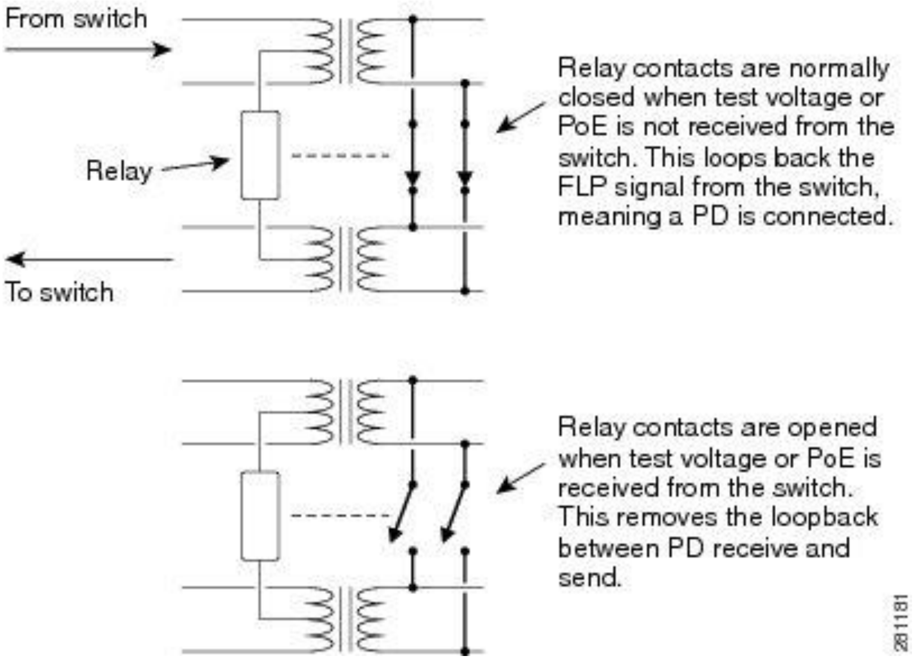
- PoE terminology refers to three types of components:
  - **Power-sourcing devices**
    - Cisco Catalyst switches and power injectors
  - **Powered devices**
    - Access points, IP phones, and IP cameras.
    - Thin clients, sensors, wall clocks, and so on.
    - Even switches can be powered through PoE itself.
  - **Ethernet cabling**
    - As with standard Ethernet, the distance of PoE is limited to 100 meters with Category 5 cabling.

PoE Standards

- **IEEE 802.3af (ratified 2003)**
  - This standard provides interoperability between different vendors.
  - Up to 15.4 W of DC power is available for each powered device.
- **IEEE 802.3at (ratified 2009)**
  - This standard is an improvement over the 802.3af standard, and can provide powered devices with up to 25.5 W of power.
  - This number can be increased to 50 W and more with implementations that are outside the standard.
  - This standard is also known as PoE+ or PoE Plus.

PoE Detection

- The switch sends a special Fast Link Pulse (FLP) signal to any device connected to the port
- The switch port determines if the special FLP signal is looped back by the powered device receive pair to the send pair. The only devices that loop back the FLP signal are those that would use inline power
- When the switch detects the looped-back FLP signal and determines that it should provide inline power to the port, the switch determines if there is power available for the connected device. The switch might use a default power allocation to check available power. It can then adjust this allocation based on CDP information from a Cisco powered device.
- The switch port then applies power to the connected device, and the relay inside the phone releases the loopback
- If the powered device is a Cisco device, it boots, and CDP becomes active. The power budget in the switch can be adjusted by power requirement information in CDP messages from the powered device.



Relay contacts are normally closed when test voltage or PoE is not received from the switch. This loops back the FLP signal from the switch, meaning a PD is connected.

Relay contacts are opened when test voltage or PoE is received from the switch. This removes the loopback between PD receive and send.

PoE Power Classes

- When the switch detects a powered device and grants a power request, the switch can adjust the power budget (available power) according to the IEEE classification.
- The powered device can provide the switch with a power class information.
  - The default class of 0 is used if either the switch or the powered device does not support power class discovery

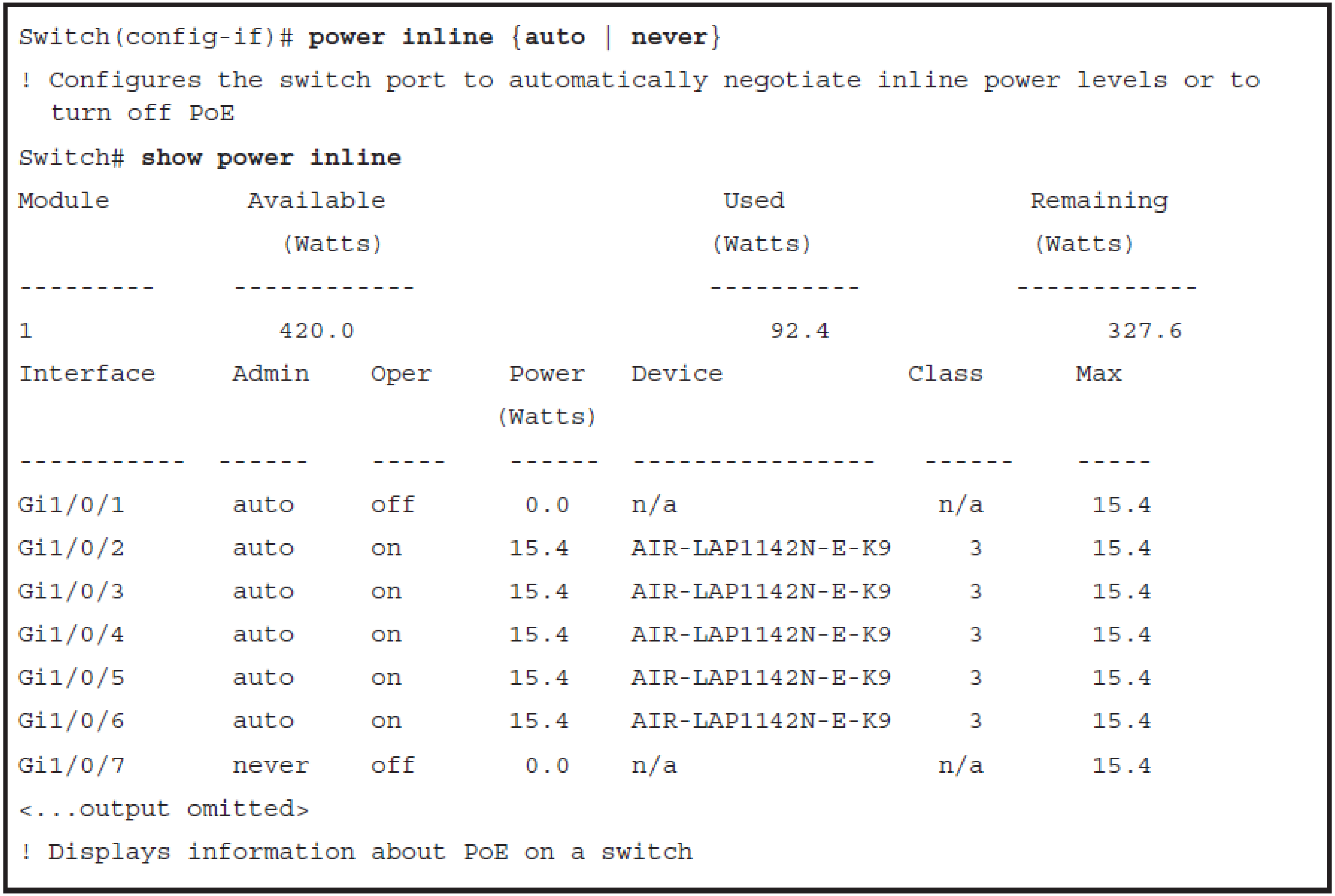
IEEE 802.3af Power class	Power delivered by switch port	Maximum power used by powered device	Class signature current (typical and maximum)
0	15.4 W	12.95 W	0-4 mA, 6 mA max.
1	4 W	3.84 W	9-12 mA, 14.5 mA max.
2	7 W	6.4 9W	17-20 mA, 23 mA max.
3	15.4 W	12.95 W	26-30 mA, 33 mA max.
4	-	-	36-44 mA, 48 mA max.

Configuring PoE

- When powered devices are locally powered (no PoE), it might be appropriate in some cases to disable it:

```
Switch(config)# int gi0/1
Switch(config-if)# power inline {never|auto}
```

Configuring and Verifying PoE

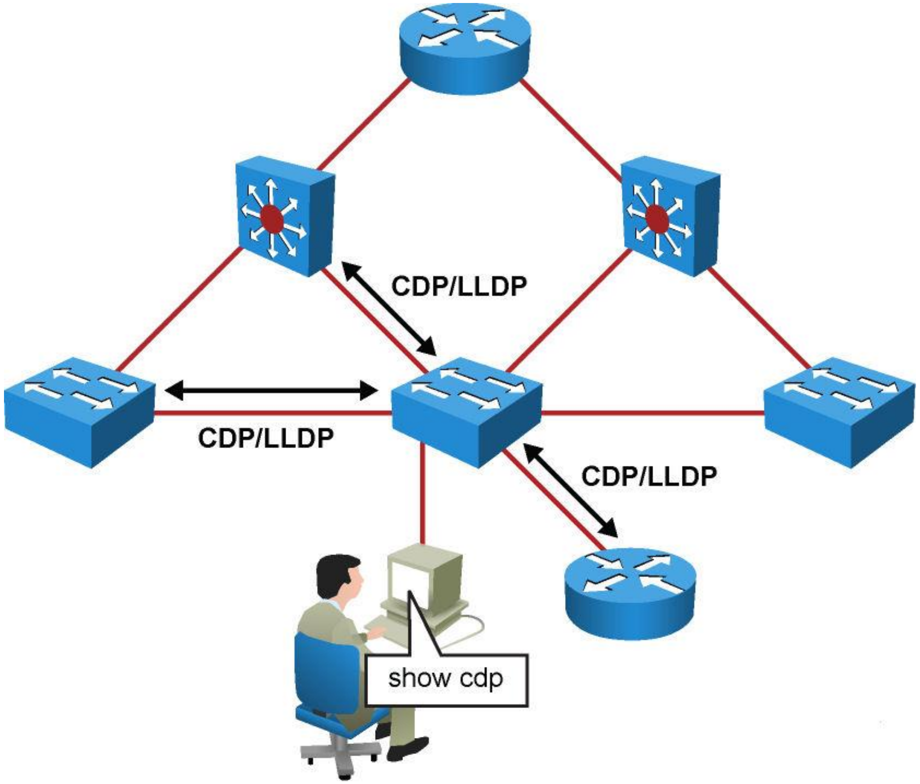


```
Switch(config-if)# power inline {auto | never}
! Configures the switch port to automatically negotiate inline power levels or to
  turn off PoE
Switch# show power inline
Module          Available                          Used                 Remaining
                  (Watts)                         (Watts)               (Watts)
---------      ------------                     ----------           ------------
1                 420.0                               92.4                  327.6
Interface      Admin     Oper      Power   Device                Class       Max
                                  (Watts)
-----------  ------     -----     ------   ----------------    ------     -----
Gi1/0/1        auto      off        0.0    n/a                    n/a        15.4
Gi1/0/2        auto      on        15.4    AIR-LAP1142N-E-K9        3        15.4
Gi1/0/3        auto      on        15.4    AIR-LAP1142N-E-K9        3        15.4
Gi1/0/4        auto      on        15.4    AIR-LAP1142N-E-K9        3        15.4
Gi1/0/5        auto      on        15.4    AIR-LAP1142N-E-K9        3        15.4
Gi1/0/6        auto      on        15.4    AIR-LAP1142N-E-K9        3        15.4
Gi1/0/7        never     off        0.0    n/a                    n/a        15.4
<...output omitted>
! Displays information about PoE on a switch
```

Neighbor Discovery Protocols

Neighbor Discovery Protocols

- **Neighbor Discovery Protocols (NDP)** provide a summary of directly connected switches, routers and other Cisco devices
- CDP is Cisco proprietary
- LLDP is vendor-neutral IEEE 802.1ab standard



Cisco Discovery Protocol

- **Cisco Discovery Protocol (CDP)** is multicast hello-based protocol periodically advertising device’s attributes
- Uses TTL value in seconds to indicate freshness of information
- Cached CDP information are available to network management
- CDP is enabled by default with 60 s gap between consecutive messages
- Configuration:

```
Switch(config)# cdp timer seconds
Switch(config)# [no] cdp run
Switch(config-if)# [no] cdp enable
```

Displaying CDP Intel

```
switch# show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID      Local Intrfce   Holdtme   Capability   Platform   Port ID
c2960-8        Fas 0/8         168       S I          WS-C2960-  Fas 0/8
```

```
4506# show cdp neighbor detail
-----------------------
Device ID: TBA03501074(SwitchA-6500)
Entry address(es):
IP address: 10.18.2.137
Platform: WS-C6506, Capabilities: Trans-Bridge Switch IGMP
Interface: FastEthernet3/21, Port ID (outgoing port): 3/36
Holdtime : 170 sec
Version :
WS-C6506 Software, Version McpSW: 7.6(1) NmpSW: 7.6(1)
Copyright © 1995-2003 by Cisco Systems
advertisement version: 2
VTP Management Domain: ‘0’
Native VLAN: 1
Duplex: full

<output omitted>
```

Link Layer Discovery Protocol

- **Link Layer Discovery Protocol (LLDP)** is open-standard clone of CDP
- Supported by HP, Juniper and other vendors as unified solution
- LLDP allows more features to be announced
- LLDP is disabled by default on Cisco boxes
- Configuration

```
Switch(config)# lldp timer seconds
Switch(config)# [no] lldp run
Switch(config-if)# [no] lldp enable
```

Introduction to LLDP

- This protocol can advertise details such as configuration information, device capabilities, IP address, hostname, and device identity.
- LLDP is used for a plethora of information sharing, it is not architected to send out real-time information such as performance data or counter data.
- An advantage of LLDP over CDP is that it allows for customization. LLDP can carry a lot of information that is relevant to your network.
- One drawback of LLDP in comparison to CDP is that it is not very lightweight.

Introduction to LLDP

The following list captures a few important implementation properties of LLDP:

- LLDP is unidirectional.
- LLDP operates only in an advertising mode.
- LLDP does not solicit for information or monitor state changes between LLDP nodes.
- LLDP leverages a Layer 2 multicast frame to notify neighbors of itself and its properties.
- LLDP will receive and record all information it receives about its neighbors.
- LLDP uses 01:80:c2:00:00:0e, 01:80:c2:00:00:03, or 01:80:c2:00:00:00 as the destination multicast MAC address.

Displaying LLDP Intel

```
switch(config)# lldp run
switch(config)# end
switch# show lldp neighbor
Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID      Local Intf      Hold-time      Capability     Port ID
c2960-8        Fa0/8           120            B              Fa0/8
Total entries displayed: 1
```

Configuration
Tips&Tricks

Interface Default Configuration

- *How to set interface to default configuration state?*

```
Switch(config)# default interface interface-id
E.g.:
Switch(config)# default interface fa 0/1
```

- *How to accomplish same thing with multiple interfaces?*

```
Switch(config)# default interface range fa 0/1 – 24
```

Resetting Switch

- Catalyst switches do not have NVRAM
  - NVRAM is just emulated in FLASH memory
  - Hence, startup configuration is stored in file **`flash:config.text`**
- Along with startup configuration is also VLAN and VTP configuration (**`vlan.dat`**) stored in FLASH
- Resetting switch means deleting “NVRAM” and also VLAN configuration:

```
Switch# erase startup-config
!or alternatively
Switch# write erase

Switch# delete vlan.dat !not necessary to write flash:vlan.dat
Switch# reload
```

Large Topology Reset

- Systematic approach is needed when resetting lab without breaking the interconnections
  - VTP is capable to renew current VLAN database configuration after reloading switch to blank state
- Recommended procedure:

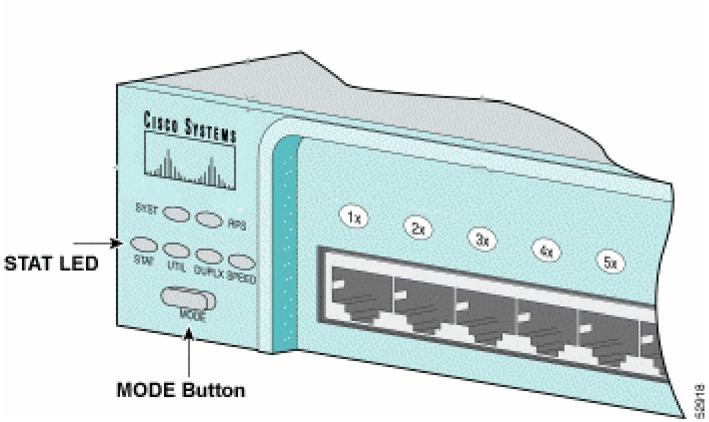
1. On all switches issue:

```
Switch(config)# interface range fa0/1 – 24 , gi0/1 – 2
Switch(config-if)# shutdown
```

2. Only after completing previous step we can start to clear configurations and restart switches

Password Recovery Procedure

1) Unplug switch - Push and hold MODE - Plug switch again
2) Hold MODE button until amber blinking SYST turns to be solid green



3) Enter following commands:

```
switch: flash_init
switch: load_helper !not necessary with newer IOS

switch: delete flash:config.text
!or alternatively
switch: rename flash:config.text flash:config.old

switch: boot
```

IOS Restoration

- Be aware of confusing **erase startup-config** resp. **delete flash:vlan.dat** with the command **erase flash:**
- Catalyst switch could upload IOS only through COM port (XMODEM protocol) – unfortunately not through Ethernet
- After getting to bootloader following must be issued:

```
switch: flash_init
switch: load_helper !not necessary with newer IOSes
switch: set BAUD 115200 !speed up console speed to 115.2 kbps
switch: format flash: !not mandatory
switch: copy xmodem:IOS_name flash:IOS_name
switch: unset BAUD !set console speed back to 9.6 kbps
switch: boot
```

Treacherousness of Port Speed and Duplex ①

- Speed and duplex are configured in following manner:

```
Switch(config-if)# speed { 10 | 100 | 1000 | auto }
Switch(config-if)# duplex { half | full | auto }
```

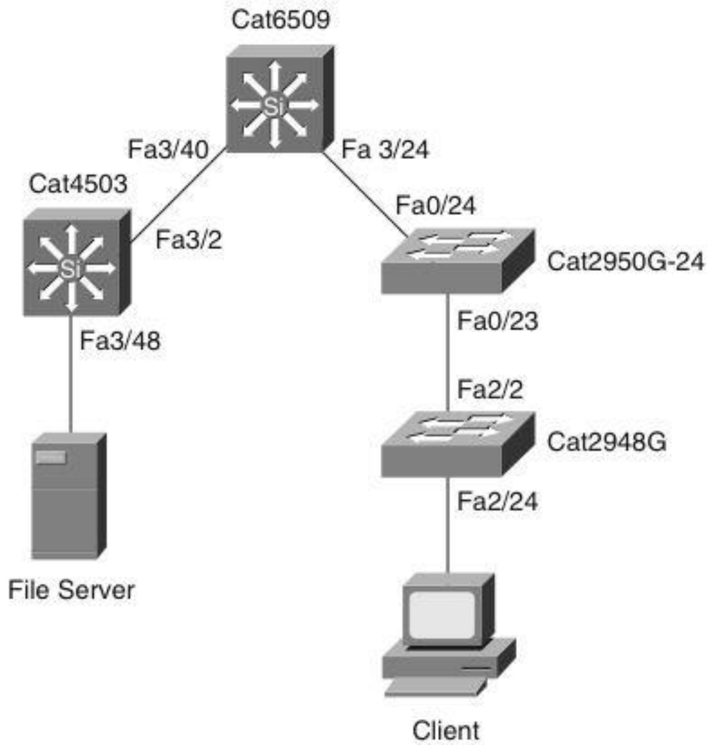
- IF at least one of those parameters is set to auto THEN port has auto-negotiation ENABLED
  - In port "capabilities" are shown only alternatives according to fixed set parameter
- IF both parameters are set fixed THEN port has auto-negotiation DISABLED only whenever
  - As a consequence switch guess speed (from channel coding) but set half-duplex as a fallback parameter
  - Possible cause of severe troubles because of duplex mismatch!
- *Hence there is strong difference between „auto-negotiation turned off" and „auto-negotiation advertising only one alternative"!!!*

Treacherousness of Port Speed and Duplex ①

- `IF` auto-negotiation is turned off `THEN` auto-MDIX is not working!
- From praxis: Cat3560v2 turns auto-negotiation off but Cat2960 not
- Hence following principle:
  - `IF` *speed and duplex must be fixedly configured* `THEN` *do it on both ends of link simultaneously*
- *Enforcing speed or duplex is in general not a very good idea!*

L2 Traceroute

- Use-case – A administrator needs to identify the performance and path on a hop-by-hop basis for a specific server and client exhibiting slow file-transfer performance
- To perform an L2 traceroute, administrator can choose any switch in the network as long as that switch has both the source and destination MAC addresses in the MAC address table



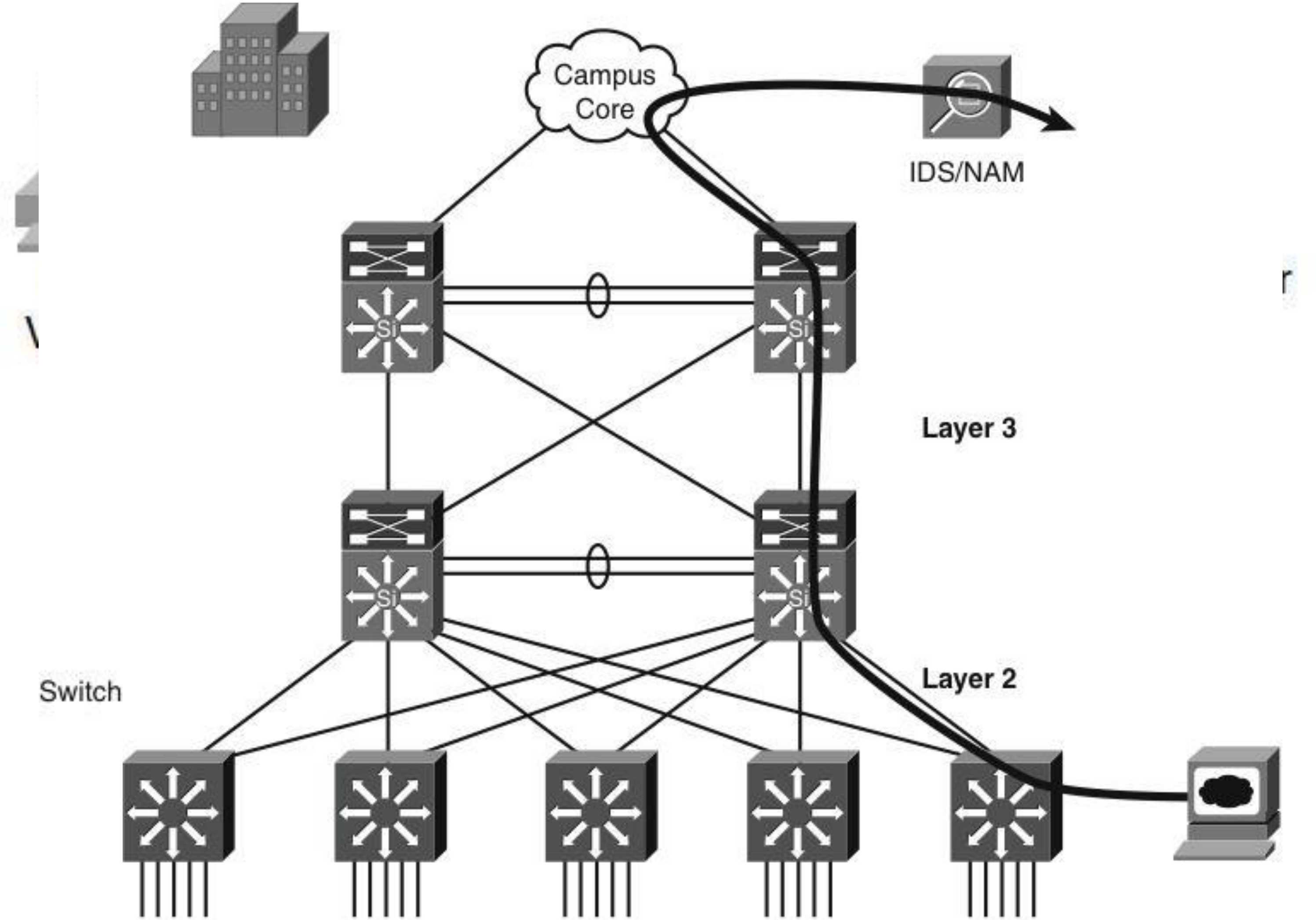
```
2950G# traceroute mac 0000.0000.0007 0000.0000.0011
Source 0000.0000.0007 found on 4503
4503 (14.18.2.132) : Fa3/48 => Fa3/2
6500 (14.18.2.145) : 3/40 => 3/24
2950G (14.18.2.176) : Fa0/24 => Fa0/23
2948G (14.18.2.91) : 2/2 => 2/24
Destination 0000.0000.0011 found on 2948G Layer 2 trace completed
```

Traffic Monitoring

Traffic Monitoring

- Many times it is useful to monitor traffic on some ports
- Cisco introduces following monitoring feature
  - **(VLAN) Switched Port Analyzer** a.k.a. **(V)SPAN**
  - **Remote SPAN (RSPAN)**
  - **Enhanced RSPAN (ERSPAN)**
- Basic idea is that monitoring session is configured which consists of
  - Definition on which port (or VLAN) sniffing occurs
  - Definition to which port (or VLAN) is sniffed traffic sent

SPAN Variants



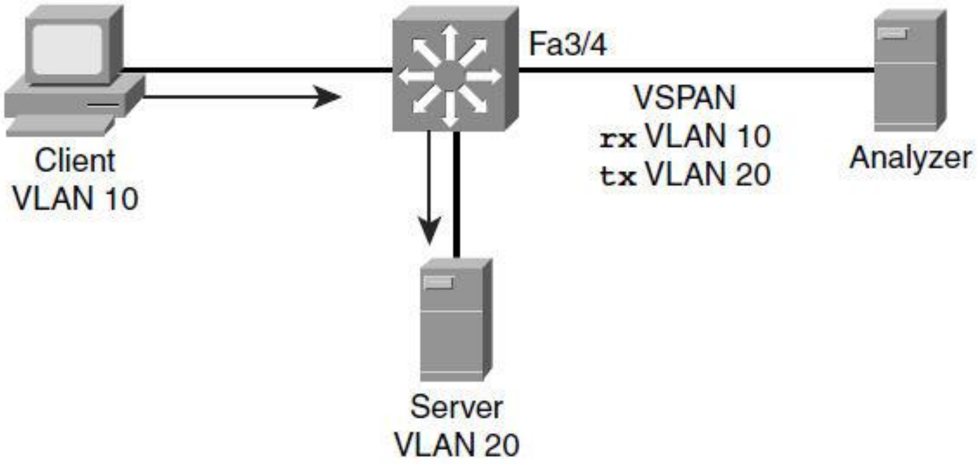
Configuring (V)SPAN

- SPAN is relation in which traffic from local ports or VLANs is replicated on concrete interface

```
Switch(config)# monitor session session-id source {interface
IFACE | vlan vlan-id [,][-] {rx | tx | both}
Switch(config)# monitor session session-id destination interface
IFACE [encapsulation {dot1q | isl}] [ingress vlan vlan-id]
```

- By default destination port is no longer capable of switching – incoming frames are discarded
  - But it is possible to overcome this behavior by appending command `ingress`
- By default command `encapsulation replicate` bellow is needed whenever we want to monitor L2 protocols (e.g. CDP, DTP, VTP, STP, PAgP, LACP, ...) and keep original VLAN tags
  - Without this command all frames will be marked as „untagged“ and service L2 protocols won’t be captured

Example: VSPAN



```
cat4k(config)# monitor session 1 source vlan 10 rx
cat4k(config)# monitor session 1 source vlan 20 tx
cat4k(config)# monitor session 1 destination interface FastEthernet 3/4
cat4k# show monitor session 1
Session 1
-----
Type                   : Local Session
Source VLANs    :
  RX Only       : 10
  TX Only       : 20
Destination Ports : Fa3/4
  Encapsulation : Native
  Ingress              : Disabled
```

Configuring RSPAN

- **Remote SPAN** is pair of relation where
  - Traffic is catch on source ports or VLAN(s) and sent to special RSPAN VLAN
  - Traffic inside RSPAN VLAN is then replicated to destination port on target switch
  - RSPAN VLAN could be used only for purpose of RSPAN
- Dedicate one VLAN as RSPAN VLAN:

```
Switch(config-vlan)# remote-span
```

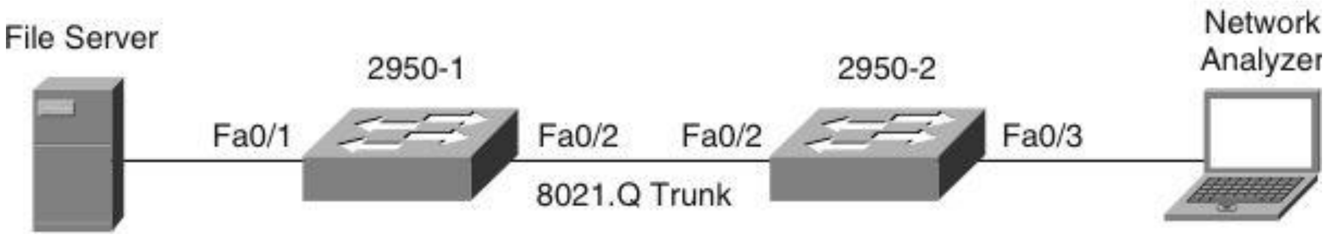
- On the source switch:

```
Switch(config)# monitor session session-id source {interface
IFACE | vlan vlan-id} [,][-] {rx | tx | both}
Switch(config)# monitor session session-id destination remote
vlan vlan-id
```

- On the destination switch:

```
Switch(config)# monitor session session-id source {interface
IFACE | vlan vlan-id [,][-] {rx | tx | both}
Switch(config)# monitor session session-id destination interface
IFACE [encapsulation {dot1q | isl}] [ingress vlan vlan-id]
```

Example: RSPAN



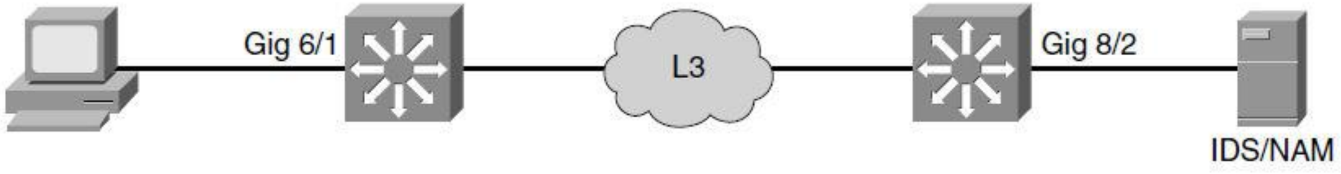
```
2950-1(config)# vlan 100
2950-1(config-vlan)# remote-span
2950-1(config)# monitor session 1 source interface Fa 0/1
2950-1(config)# monitor session 1 destination remote vlan 100
reflector-port Fa0/24
2950-1(config)# interface Fa0/2
2950-1(config-if)# switchport mode trunk

2950-2(config)# monitor session 2 source remote vlan 100
2950-2(config)# monitor session 2 destination interface Fa0/3
2950-2(config)# interface Fa0/2
2950-2(config-if)# switchport mode trunk
```

Enhanced RSPAN

- **Enhanced Remote SPAN (ERSPAN)** is similar to RSPAN, but it supports source ports, source VLANs, and destination ports on different switches, even across the Layer 3 boundary
  - The payload of a Layer 3 ERSPAN packet is a copied Layer 2 Ethernet frame, excluding any ISL or 802.1Q tags
  - ERSPAN adds a 50-byte header to each copied Layer 2 Ethernet frame and replaces the 4-byte cyclic redundancy check (CRC) trailer
  - ERSPAN session carries SPAN traffic in GRE tunnel
  - Only for Catalyst6500
- ERSPAN supports jumbo frames that contain Layer 3 packets of up to 9202 bytes
  - `IF` the length of the copied Layer 2 Ethernet frame is greater than 9170 bytes (9152-byte Layer 3 packet) `THEN` ERSPAN truncates the copied Layer 2 Ethernet frame to 9202-byte

Example: ERSPAN



```
Switch1(config)# monitor session 66 type erspan-source
Switch1(config-mon-erspan-src)# source interface gigabitethernet 6/1
Switch1(config-mon-erspan-src)# destination
Switch1(config-mon-erspan-src-dst)# ip address 10.10.10.10
Switch1(config-mon-erspan-src-dst)# origin ip address 20.20.20.200
Switch1(config-mon-erspan-src-dst)# erspan-id 111

Switch2(config)# monitor session 60 type erspan-destination
Switch2(config-erspan-dst)# destination interface Gi8/2
Switch2(config-erspan-dst)# source
Switch2(config-erspan-dst-src)# ip address 10.10.10.10
Switch2(config-erspan-dst-src)# erspan-id 111
```

Useful Commands

```
show interfaces [IFACE]

show interfaces status

show interfaces description

show interfaces counters [errors]

show interfaces capabilities

test cable-diagnostics tdr

show cable-diagnostics tdr
```

The show interface capabilities Command

```
Router# show interfaces fastethernet 4/1 capabilities

FastEthernet4/1
Model: WS-X6348-RJ-45
Type: 10/100BaseTX
Speed: 10,100,auto
Duplex: half,full
Trunk encap. type: 802.1Q,ISL
Trunk mode: on,off,desirable,nonegotiate
Channel: yes
Broadcast suppression: percentage(0-100)
Flowcontrol: rx-(off,on),tx-(none)
Fast Start: yes
QOS scheduling: rx-(1q4t), tx-(2q2t)
CoS rewrite: yes
ToS rewrite: yes
Inline power: no
SPAN: source/destination
```

The test cable-diagnostics tdr Command

```
Router> test cable-diagnostics tdr interface gi8/1

Router> show cable-diagnostics tdr interface gi8/1
TDR test last run on: February 25 11:18:31
Interface Speed Pair Cable length    DistanceToFault Channel Pair status
--------- ----- ---- ----- --------  --------------- ------- -----------
Gi8/1     1000  1-2  1     +/- 6 m   N/A             Pair B  Terminated
                3-4  1     +/- 6 m   N/A             Pair A  Terminated
                5-6  1     +/- 6 m   N/A             Pair C  Terminated
                7-8  1     +/- 6 m   N/A             Pair D  Terminated
Router>
```

Slides adapted by Vladimír Veselý and Matěj Grégr partially from official course materials but the most of the credit goes to CCIE#23527 Ing. Peter Palúch, Ph.D.

The last update: 2016-11-03