17. Port security on access layer switchport

Port security is feature that enable permit or deny traffic for end user PCs connected to access layer switch. Port security enable specify a group of valid MAC address on port. If maximum secure MAC address is reached then security violation modes lead to protect, restrict or shutdown of port.

There are 3 ways how to configure port security:

1) Static secure MAC addresses - manually configured with

switchport port-security mac-address MAC_ADDRESS

2) Dynamic secure MAC address - dynamic learned and stored only in address table (after restart cleared)

3) Sticky secure MAC address – mac address are learned dynamically and saved in running config (next can be merged with startup config).

Default port security:

- disabled on port -> switchport port-security
- maximum nr. of secure MAC: 1
- violation mode: shutdown
- sticky address learning: disabled

Sample configs:

A) Dynamic port security configuration

sl#configure terminal

s1(C)# interface FastEthernet0 0/10

s1(c-if)#switchport mode access

s1(c-if)#switchport port-security

s1(c-if)#end

B) **Sticky port security** – can configure max. nr. of secure mac address, in this example we configure shutdown as the violation mode

sl#configure terminal

s1(C)# interface FastEthernet0 0/10

s1(c-if)#switchport mode access

s1(c-if)#switchport port-security (enable port security)

s1(c-if)#switchport port-security maximum 20 (maximum nr. of secure address)

sl(c-if)#switchport port-security mac-address sticky
 (enable sticky learning)

sl(c-if)#end

Table: Security violation modes

Violation mode	Forward traffic	Send syslog message	Display error message	Increase violation counter	Shuts down port
protect	no	no	no	no	no
restrict	no	yes	no	yes	no
shutdown	no	yes	no	yes	yes

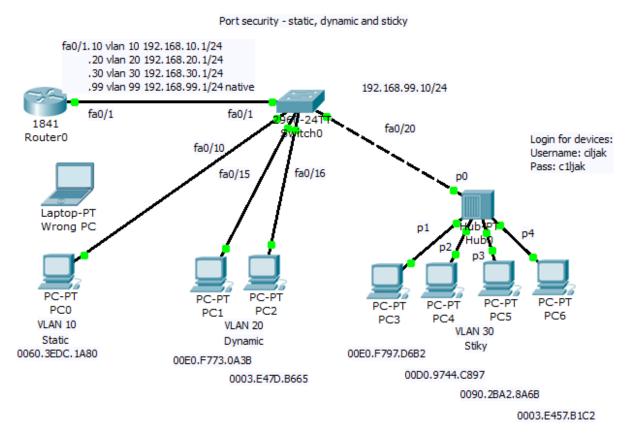
Verification commands:

• show port-security [interface interface-id]

Switch#show port-security	interface fa0/10
Port Security	: Disabled
Port Status	: Secure-down
Violation Mode	: Shutdown
Aging Time	: 0 mins
Aging Type	: Absolute
SecureStatic Address Aging	: Disabled
Maximum MAC Addresses	: 1
Total MAC Addresses	: 1
Configured MAC Addresses	: 1
Sticky MAC Addresses	: 0
Last Source Address:Vlan	: 0000.0000.0000:0
Security Violation Count	: 0

show port-security [interface interface-id] address

Our training scenario focused on port-security can be obtained from here (Packet tracer 5.2 or above you will need).



Network topology consist of router acting on stick and switch. Port security is configured sticky for 10 mac address for port 20 to 24 with commands:

```
interface FastEthernet0/20
switchport access vlan 30
switchport port-security maximum 10
switchport port-security mac-address sticky
!
```

```
interface FastEthernet0/21
switchport access vlan 30
switchport port-security maximum 10
switchport port-security mac-address sticky
I.
interface FastEthernet0/22
switchport access vlan 30
switchport port-security maximum 10
switchport port-security mac-address sticky
L
interface FastEthernet0/23
switchport access vlan 30
switchport port-security maximum 10
 switchport port-security mac-address sticky
L
interface FastEthernet0/24
switchport access vlan 30
switchport port-security maximum 10
 switchport port-security mac-address sticky
```

```
You are strongly encouraged to try
```

1) Static port security for PC on vlan 10 on port fa0/10 with mac 0060.3EDC.1A80 — then disconnect device with mentioned mac and attach device with wrong mac (examine shuting down state of port), then correct port state and enable traffic forwarding.

```
interface FastEthernet0/10
switchport access vlan 10
switchport port-security mac-address 0060.3EDC.1A80
!
```

2) Enable dynamic learning for PC on ports fa0/15 and fa0/16.

As example, output from show mac-address-table of switch

	#sh mac-address-ta Mac Address Ta	able		
Vlan	Mac Address	Type	Ports	
10	0060.2fcc.9102	DYNAMIC	Fa0/1	
10	0060.3edc.1a80	DYNAMIC	Fa0/10	
20	0003.e47d.b665	DYNAMIC	Fa0/16	
20	0060.2fcc.9102	DYNAMIC	Fa0/1	
20	00e0.f773.0a3b	DYNAMIC	Fa0/15	
30	0003.e457.b1c2	DYNAMIC	Fa0/20	
30	0060.2fcc.9102	DYNAMIC	Fa0/1	
30	0090.2ba2.8a6b	DYNAMIC	Fa0/20	
30	00d0.9744.c897	DYNAMIC	Fa0/20	
30	00e0.f797.d6b2	DYNAMIC	Fa0/20	
99	0060.2fcc.9102	DYNAMIC	Fa0/1	
Switch	<pre>#show interface tr</pre>	runk		
	Mode	-		
Fa0/1	on	802.1q	trunking	99
-				
	Vlans allowe	ed on trunk		
Fa0/1	1-1005			
Port	Vlans allowe	d and active :	in management (domain
	1,10,20,30,9		in managemento .	
240/1	1,10,20,00,5	-		
Port	Vlans in spa	nning tree for	warding state	and not pruned
Fa0/1	-	-		
	//-			

On port fa0/20 can be spot shared network segment (in our case it is hub interconnected segment).

16. Administrative Distance and route source preference

In environment with 2 or more enabled routing protocols must be present mechanism for selection of routing sources that are learned. What routing protocol obtained routes for remote network will be introduced to routers routing table? That is a big question.

Administrative Distance in short AD is considered parameter that will break the tie and say about trustworthiness of routing source.

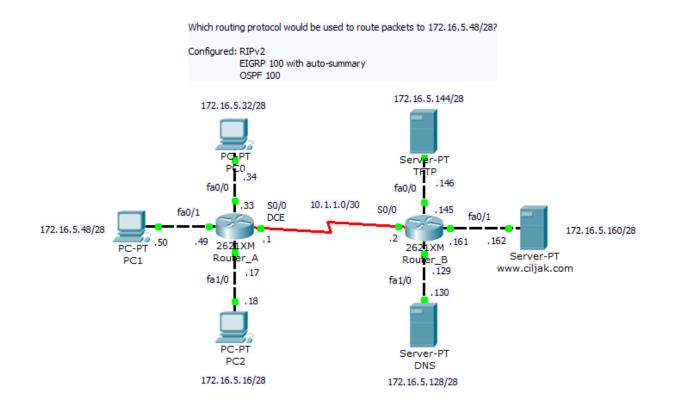
Routing source	AD (administrative distance)
connected	0
static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
0SPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Table of administrative distance of routing protocols

Say in other words – AD is number from interval <0, 255>. And lower is better that mean static route (AD=1) is preferred over OSPF learned route (AD=110).

Training scenario focus on introduction routing sources (learned route) from RIP, EIGRP and OSPF routing protocols.

Fully configured lab. scenario for Cisco Packet Tracer 5.2 or above can be obtained from here. Topology diagram show next picture.



Routing protocols configuration is

Router_A	Router_B

router eigrp 100 passive-interface FastEthernet0/0 passive-interface FastEthernet0/1 passive-interface FastEthernet1/0 network 172.16.5.0 0.0.0.63 network 10.1.1.0 0.0.0.3 auto-summary router ospf 100 log-adjacency-changes passive-interface FastEthernet0/0 passive-interface FastEthernet0/1 passive-interface FastEthernet1/0 network 172.16.5.0 0.0.0.63 area 0 network 10.1.1.0 0.0.0.3 area 0 router rip version 2 passive-interface FastEthernet0/0 passive-interface FastEthernet0/1 passive-interface FastEthernet1/0 network 10.0.0.0 network 172.16.0.0 ip classless

router eigrp 100 passive-interface FastEthernet0/0 passive-interface FastEthernet0/1 passive-interface FastEthernet1/0 network 172.16.5.128 0.0.0.63 network 10.1.1.0 0.0.0.3 auto-summary router ospf 100 log-adjacency-changes passive-interface FastEthernet0/0 passive-interface FastEthernet0/1 passive-interface FastEthernet1/0 network 172.16.5.128 0.0.0.63 area 0 network 10.1.1.0 0.0.0.3 area 0 router rip version 2 passive-interface FastEthernet0/0 passive-interface FastEthernet0/1 passive-interface FastEthernet1/0 network 10.0.0.0 network 172.16.0.0 L ip classless

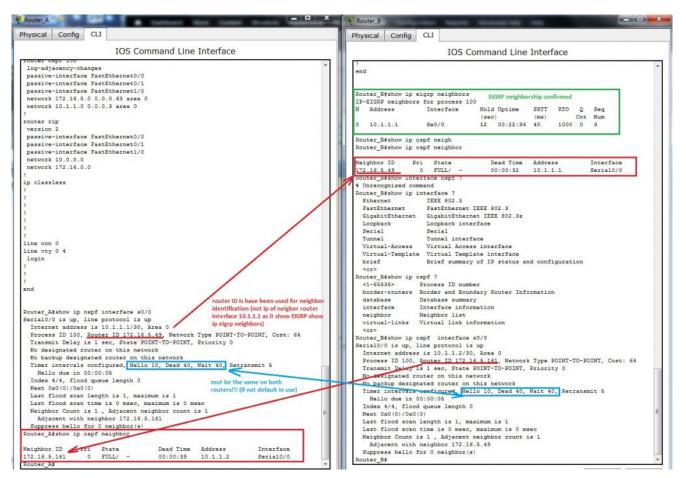
EIGRP and OSPF routing protocols will create neighborship relation between facing interfaces. This mechanism is important for generate triggers after breaking relationship after topology change in network and cause generating and spreading routing protocols PDU, algorithm recalculation and rearrangement in routing table.

If routing table is missing expected route please take a look at creation of neighbor relation and verify appropriate timers that trigger sending hallo packet or define time for detaching route from table after their potential error.

Important commands for troubleshooting at CCNA level are:

- show ip eigrp neighbors
- show ip ospf neighbor
- show ip ospf interface INTERFACE
- show ip route
- show ip protocols

Output from neighborship verification commands are

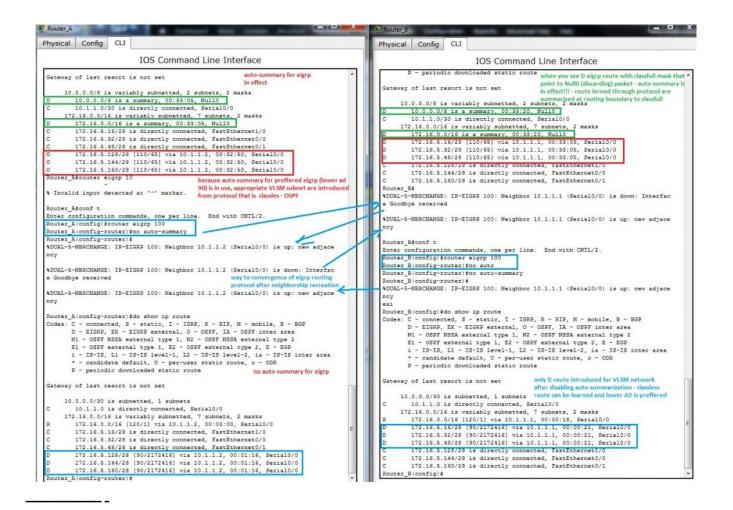


Now we can look at routing table both router A and B. What we can to expect? Which routing protocol introduce their route to routing table? Lower AD is preferred and lowest AD has EIGRP!

But what is wrong, routing table show only classfull D (Duall EIGRP route) that point nowhere (NullO)? Can you mentally answer why it is so? What is wrong in our config? Classless VLSM route (network mask is longer as appropriate classfull mask) are introduced by OSPF because OSPF is inherently classless routing protocol.

Please remember that *null0* classfull route introduced to routing table by EIGRP protocol (leading D for that route) *is because auto-summary was not suppressed and is in use.* For correcting this behavior on our network we must type *no autosummary* on router-config command prompt of router eigrp 100.

All that was we describe is recorded from output of CLI Router_A and Router_B on next picture.



One of many processes that run on our router is mapping L3 address to L2 mac address on Ethernet interfaces. Info about learned relationship between L3 and L2 address offer ARP table of router. Their output can be visible after typing show arp on privileged exec of CLI (output depend on previews communication, arp cache is dynamic table that is aged after appropriate time non use of connection. That mean, if you will have all mac in table you must make ping sweep).

Router_A#	show arp					
Protocol	Address	Age	(min)	Hardware Addr	Type	Interface
Internet	172.16.5.17		-	0060.7038.CD01	ARPA	FastEthernet1/0
Internet	172.16.5.18		2	0090.2193.645C	ARPA	FastEthernet1/0
Internet	172.16.5.33		-	000C.85D9.5D01	ARPA	FastEthernet0/0
Internet	172.16.5.34		3	00D0.BAE7.3634	ARPA	FastEthernet0/0
Internet	172.16.5.49		-	000C.85D9.5D02	ARPA	FastEthernet0/1
Internet	172.16.5.50		2	0090.0C1B.3E57	ARPA	FastEthernet0/1

Records with character — in Age column is local interface of device. These records are excluded from aging mechanism! (- mean local interface on device, other are learned through ARP protocol)

15 DDD and Erama rolaw i

15. PPP and Frame relay in small network

PPP and Frame relay are protocols operating at data link layer used in segment of private WAN connection. PPP enable establish communication through serial link between cisco and noncisco device where can not be used proprietary HDLC cisco encapsulation. Frame relay networks offer packet switched technology in providers network. This article will focus on simple implementation of PPP serial link and Frame relay link in office environment.

About PPP (basics)

Is nonproprietary data link protocol carefully designed for compatibility with common HW devices. Enabled are these connection establishments:

- serial cables
- phone lines
- trunk lines
- cellular telephones
- fiber optic links

Extend features supported on serial links as quality management and PAP or CHAP authentication mechanism.

Main components of protocol are:

- 1. HDLC protocol for encapsulation over point to point link
- 2. Link control protocol establish link connection
- 3. Network control protocols (NCPs) for establishing and configuration different network layer protocol

PPP configuration step by step

- 1) Enable PPP on interface
- R #config t
- R(config)#interface serial 0/0/0

R(config-if)#encapsulation ppp

- 2) Configure authentication
 - PAP older and unsecure, password is send as clear text ppp authentication pap ppp pap sent-username My name password PSWD
 - CHAP based on 3 way handshake mechanism using message digest – preferred if can be used ppp authentication chap
- 3) Optionally configure compression with compress command
- 4) Optionally enable link quality monitoring

ppp quality 80 (1 to 100) — if link does not meet quality requirements then goes down

5) Optionally enable load balancing across link with ppp multilink

About Frame relay

All frame relay networks are build on 3 main components: DTE equipment at each end of connection (FRAD device of user), DCE (telephony company CO) and middle components (frame relay switches in operator network).

In frame relay networks our routers act as DTE devices and

serial connection T1/E1 leased lines connect router to FR switch in POP (point of presence) our ISP (internet service provider). Frame relay switches on other end act as DCE devices.

DLCI – *is local meaning number that identify link connection* (but in opposite of IP address have only local meaning).

Frame relay address mapping is important for knowing how map which DLCI map to L3 address of remote destination. Mapping can be configured as dynamic or static. (for beginners is it a bit confusing in configuration and in CCNA eLearning materials). For configuration easier way is relay on dynamic mapping that use inverse arp. For static mapping must be used frame-relay map command.

Frame relay configuration step by step

1) Enable frame relay on interface

encapsulation frame-relay

and set encapsulation options cisco /ietf, cisco is on cisco devices default. IETF use only in multivendor environment when second end is non cisco device.

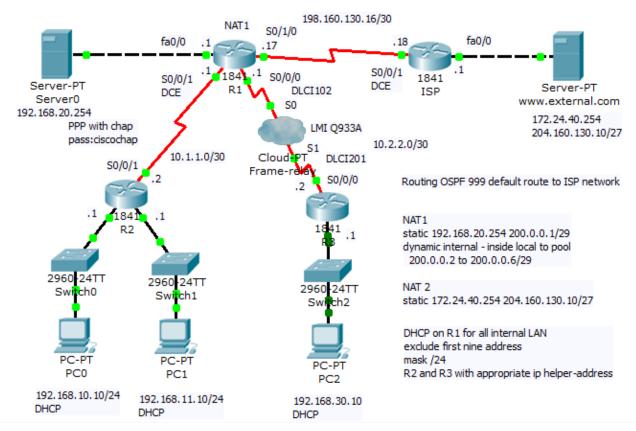
2) Configure bandwidth (does not affect real bandwidth) that is important for EIGRP and OSPF metric calculation

3) Set appropriateLMI type (cisco, q933a or ansi)

4) Optionally disable inverse arp for frame-relay DLCI mapping and configure appropriate static frame-relay map commands (important in end-to-end reachability in hub and spoke networks when spoke to spoke reachability is expected).

For training and hardening skills before CCNA examination we introduce next configuration scenario that can be

as preconfigured downloaded from here.



Small topology with PPP and FR interconnections

Scenario include PPP and frame relay configuration, subnetting and dynamic routing using OSPF routing protocol with ID 999. Office network use private addressing space with subnets 192.168.10.0/24, 192.168.11.0/24, 192.168.30.10 and 10.0.0.0/8 (10.1.1.0/30 and 10.2.2.0/30 VLSM subnets). On router R1 is configured NAT with PAT for private client address space and static nat translation for remote access to internal servers.

For PPP link configuration on R2 and R1 router we use

username R1 password 0	username R2 password 0
ciscochap	ciscochap

interface Serial0/0/1
ip address 10.1.1.2
255.255.255.252
encapsulation ppp
ppp authentication chap

interface Serial0/0/1
 bandwidth 2048
ip address 10.1.1.1
 255.255.255.252
 encapsulation ppp
ppp authentication chap
 ip nat inside
 clock rate 2000000

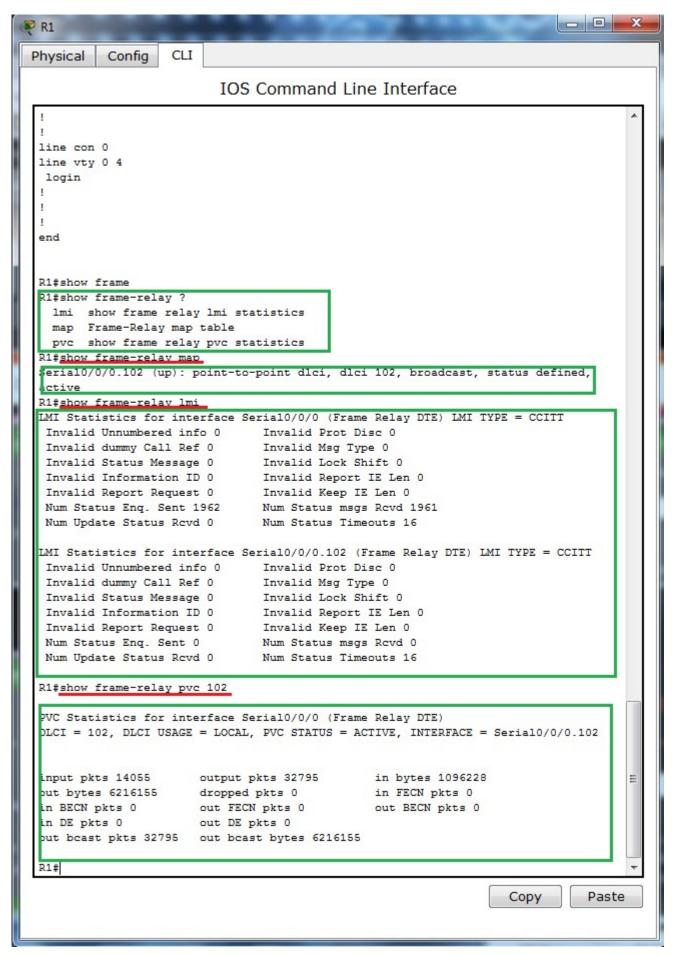
For Frame relay configuration at R1 FRAD and R3 FRAD we used (configuration of FR switch is beyond scope of our training but Packet Tracer offer Cloud-PT simulation object that we will introduce in one of our next article).

R1	R3
<pre>interface Serial0/0/0.102 point-to-point ip address 10.2.2.1 255.255.255.252 frame-relay interface-dlci 102 ip nat inside clock rate 2000000</pre>	interface Serial0/0/0.201 point-to-point ip address 10.2.2.2 255.255.255.252 frame-relay interface-dlci 201 clock rate 2000000

For examination of frame-relay open state and mapping remote address to local DLCI can be used this show commands:

- show frame-relay pvc
- show frame-relay map
- show frame-relay lmi
- show interface

Output from this commands show next pictures



Output from show frame-relay lmi supply us with statistic information about link. LMI as management build in mechanism

can be used for link state monitoring. As frame relay lmi standard can be selected cisco, q933a and ansi. As it is discussed in this topics http://www.tek-tips.com/viewthread.cfm?qid=402209, 21.3.2012 most important thing to consider is that both end must support apropriate type of LMI.

Output from show ip interface brief contain physical link and data link up state. If link state is down you need check clock rate command on DCE end of link, encapsulation command and authentication mechanism if used (optionally compression and other optional config).

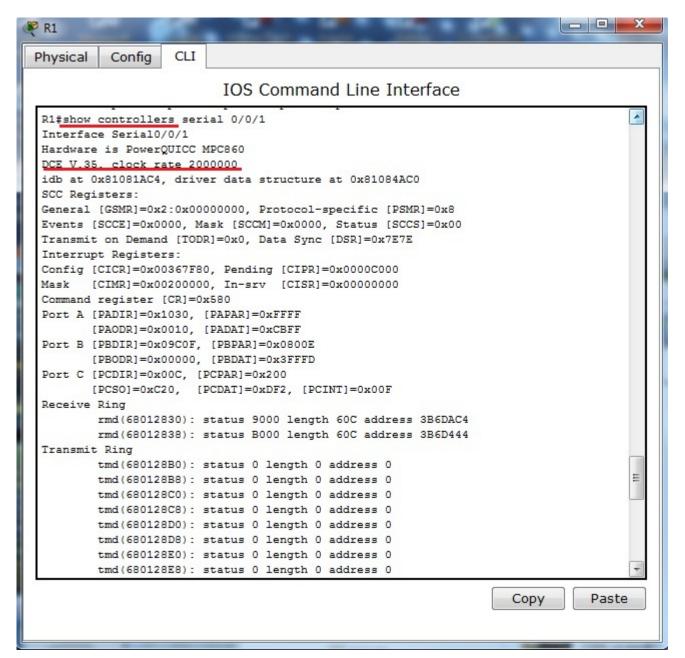
Rl#show ip int brief Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.20.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	n down
Serial0/0/0	unassigned	YES	unset	up	up
Serial0/0/0.102	10.2.2.1	YES	manual	up	up
Serial0/0/1	10.1.1.1	YES	manual	up	up
Serial0/1/0	198.160.130.17	YES	manual	up	up
Serial0/1/1	unassigned	YES	unset	administratively down	n down
Vlan1 R1#show interface s0/0	-	YES	unset	administratively down	n down
Serial0/0/0.102 is up, Hardware is HD64570 Internet address is MTU 1500 bytes, BW 1 reliability 255/2 Encapsulation FRAME- Last clearing of "sh	10.2.2.1/30 544 Kbit, DLY 20 55, txload 1/255 RELAY	000 , гж	usec, load 1/3	255	

IO	S Command Line Interface
-	Comparts 0 Out BACM parts 0
out beast pkts 32795 out be	
Cat Deast pros 02,50 Cat De	
R1#show frame-relay lmi	
the second se	Serial0/0/0 (Frame Relay DTE) LMI TYPE = CCITT
Invalid Unnumbered info 0	Invalid Prot Disc 0
Invalid dummy Call Ref 0	Invalid Msg Type 0
Invalid Status Message 0	Invalid Lock Shift 0
Invalid Information ID 0	Invalid Report IE Len 0
Invalid Report Request 0	Invalid Keep IE Len 0
Num Status Enq. Sent 718	Num Status msgs Revd 717
Num Update Status Revd 0	Num Status Timeouts 16
LMI Statistics for interface	Serial0/0/0.102 (Frame Relay DTE) LMI TYPE = CCITT
Invalid Unnumbered info 0	Invalid Prot Disc 0
Invalid dummy Call Ref 0	Invalid Msg Type 0
Invalid Status Message 0	Invalid Lock Shift 0
Invalid Information ID 0	Invalid Report IE Len 0
Invalid Report Request 0	Invalid Keep IE Len 0
Num Status Enq. Sent 0	Num Status msgs Revd 0
Num Update Status Rovd 0	Num Status Timeouts 16
R1#	
274	*
	Copy Paste

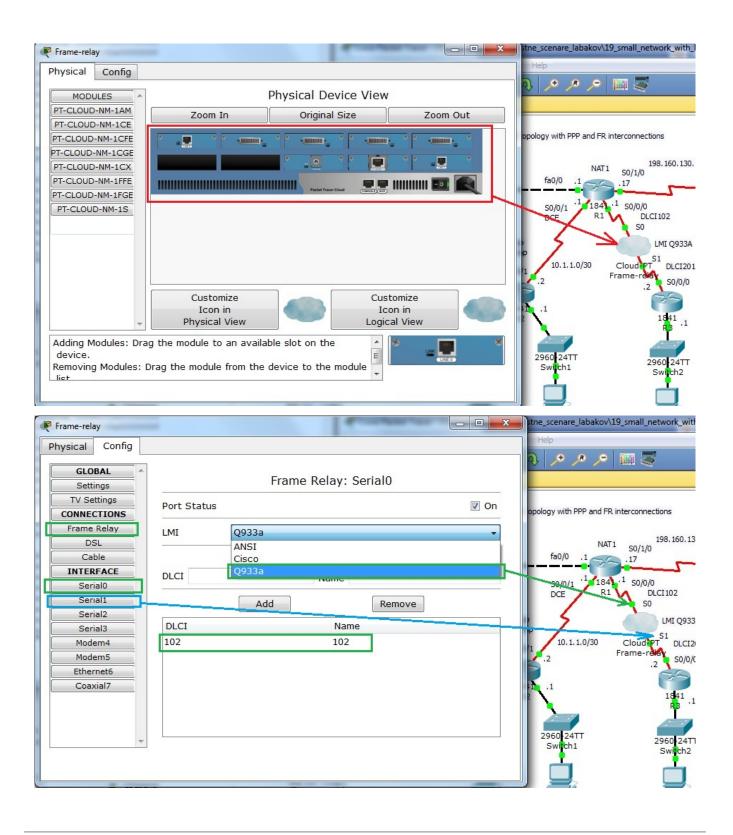
Next pictures show output from show interface on interfaces participating in PPP encapsulation. As you can see from output of command encapsulation is PPP and both LCP and appropriate NCP (IPCM and CDPCP) are in open state.

🤾 R1 📃 🗖 🖉
Physical Config CLI
IOS Command Line Interface
· · ·
Num Status Enq. Sent 0 Num Status msgs Rcvd 0
Num Update Status Rovd 0 Num Status Timeouts 16
R1#show interface s0/0/1
Serial0/0/1 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 10.1.1.1/30
MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open LCP open state
Open: IPCP, CDPCP Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1536 kilobits/sec
5 minute input rate 58 bits/sec, 0 packets/sec
5 minute output rate 56 bits/sec, 0 packets/sec
411 packets input, 28264 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort 404 packets output, 28156 bytes, 0 underruns
Doutput errors. O collisions, O interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
R1#
Copy Paste

For further reference about connected serial cable and clocking of link you can use show controllers serial – interface s0/0/1 on R1 router act as DCE end with configured clock rate command.



Last two pictures show Frame-relay simulation device available in Cisco Packet tracer.



14. Wrong default route

propagation in OSPF enabled network

Default route introduce ultimate outgoing interface for L3 PDU from our network. Most common use is in stub-networks where is only one interface pointing to outside network (in this case is no need for load balancing between two or among ISPs interfaces). Instead of routers having to store routes for all of the networks in the internet, they can share a single default route to represent any network that is not in the routing table.

In small office networks is static routing and manual default route settings in use but in large network or in much more flexible network scenarios are dynamic routing protocol introduced.

Static default route can be propagated from router where command *ip route 0.0.0.0 0.0.0.0 interface/IP_of_next_hop* to all other routers in network.

How to enable default route distribution to network with most common IPv4 routing protocols?

1) Configure static default route on router that act as network boundary to ISP network with command:

ip route 0.0.0.0 0.0.0.0 interface/IP_of_next_hop

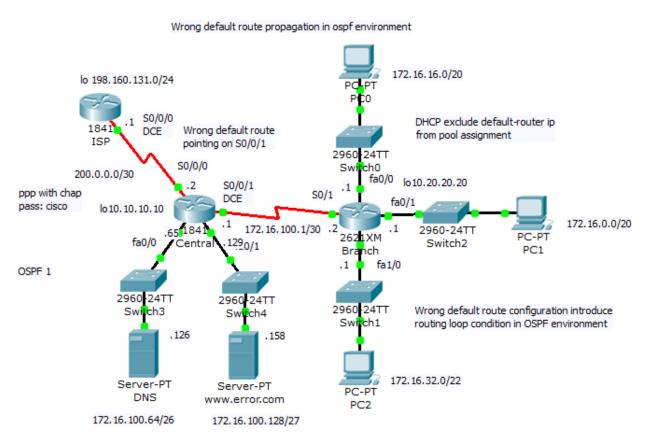
2) Default static route needs to be advertised to all others routers that use dynamic routing protocols

- for RIP1/2 use router command: default-information originate
- for EIGRP use router command: redistribute static
- for OSPF use router command: default-information originate

But what is happen when wrong default route is introduced in

network topology? How troubleshoot problem with wrong default static route? We going to explore how this condition affect our production network and how to fix it.

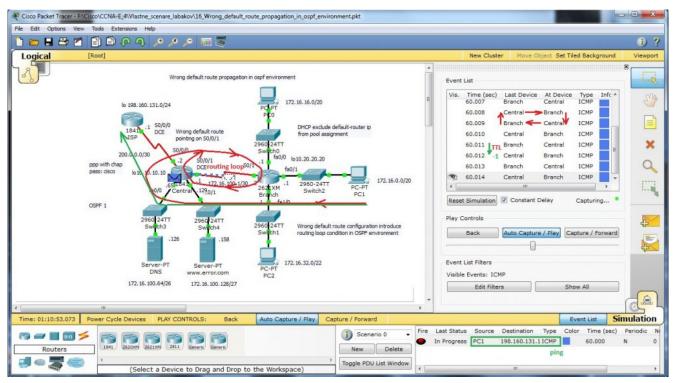
Preconfigured scenario in cisco packet tracer 5.2 or above can be obtained from here. Small office network in this scenario look like this



Network topology consist of central router (act as boundary between office network and WAN) and one branch router (for simplicity is there only one branch router). All end devices are on separate networks and private address space is in use in internal network. Wrong default route

ip route 0.0.0.0 0.0.0.0 serial0/0/1 (correct it is serial0/0/0) introduce in network routing loop that we will examine.

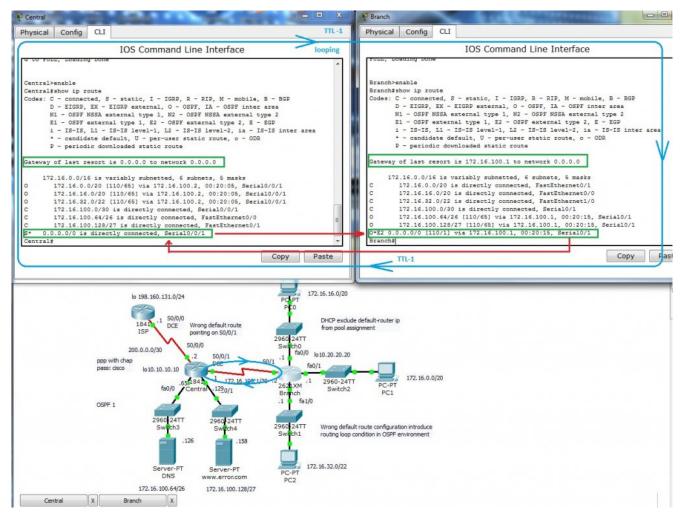
Our lab include option for sending ping and follow what is happen. Toggle to simulation mode and Auto capture/play.



Wrong default route lead PDU to its origin and Branch router loop back to central router with default route. L3 PDU contain mechanism how to break endless looping of PDU – TTL in data packet header is decreased after L3 routing to appropriate interface as you can see on next picture (PDU examination in cisco packet tracer – simulation mode).

SI Model	Inbound	PDU Details	Outbou	and PDU Deta	ails				
PDU Form	ats		1	TTL=1 de routing to					
HDLC	- 1			when 0 r				1	
0 8	16	32	/	be drop	324	-v	48	+x 56+x	Bi
FLG: 0111 1110	ADR: C	ONTROL: 0x0		VARIABLE NGTH)		FCS: 0x0		FLG: 0111 1110	
<u>IP</u> 0	4	./	16	19			31	Bits	
4	THL	DSCP: 0x0	D	TL: 28					
	Y 10.	0x4	0x0		0x0)			
C	TL: 2	PRO: 0x1		CHKS	SUM				
		SRC I	P: 172.16	.0.2					
		DST IP:	198.160.	131.1					
		OPT: 0x0	0			0x0			
		DATA (VA	ARIABLE L	ENGTH)					
ICMP	8	16			31	Bits			
		ODE: 0x0	CHE	CKSUM	Ĩ	5105			
	ID: 0x2		SEQ N	JMBER: 1					
4									•

Output from most common troubleshooting command show ip route that output from routers routing table issued on both routers is:



Now is time correct our mistake. What we need to do? At first you must remove wrong default route. There is no way how to change existing static route. First remove wrong route with command

no ip route 0.0.0.0 0.0.0.0 serial0/0/1

that point not to ISP router but back to internal Branch router and cause routing loop. Next step is introduce appropriate (correct) default route this way:

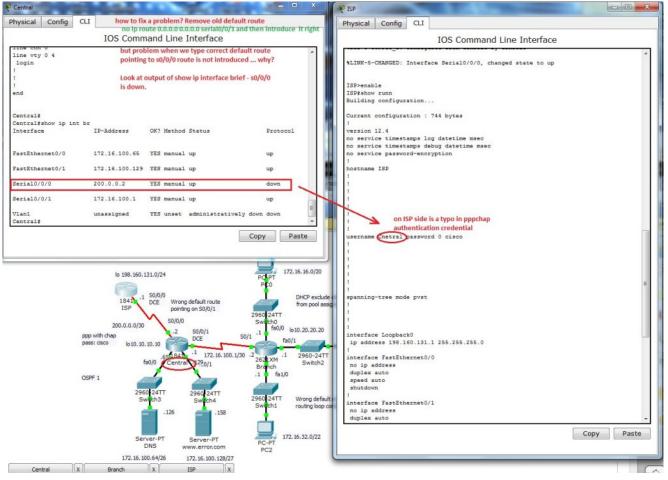
ip route 0.0.0.0 0.0.0.0 serial0/0/0

and now we going to examine output from show ip route. But you will obtain problem that is cause of my mistake. In routing table is not default route introduced. Keep in mind that static route (but all routes) is in output only when appropriate outgoing interface is on. Then we will examine up state of s0/0/0 interface. As you can see physical layer is Up

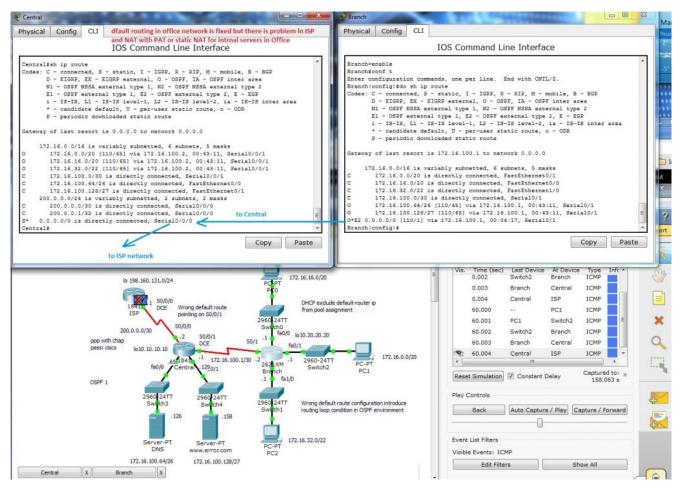
but protocol is down.

S0/0/0 interface on Central router is connected to ISP with PPP link that use chap as authentication protocol. We need examine clock command on DCE end of serial link and then authentication credential on bot end of link.

And there is the problem, ISP side is supplied wit incorrect name of Central router. there is a typo Cnetral and correct it may state Central.



Default route is now correct but can we establish a connection between end devices on office network and ISP? Fire ICMP packet to destination nework 198.160.131.1. Packet can reach ISP router but then is discarded because no translation to public network have not been made. We are closer to our goal, data re well routed but address translation on private network boundary must be established.



For ISP (internet access – now without security configuration) connection in network with many clients I decided for NAT (network address translation) with PAT (port address translation) on interface s0/0/0.

At first we must create standard access list (i use named but also can be used numbered)

ip access-list standard NAT

permit 172.16.0.0 0.0.15.255

- permit 172.16.16.0 0.0.15.255
- permit 172.16.32.0 0.0.15.255

permit 172.16.100.0 0.0.0.3

and then enable nat translation with command

ip nat inside source list NAT interface s0/0/0 overload

most common beginners (also me) mistake is forget mark appropriate interface as ip nat inside and outside. in our case it is:

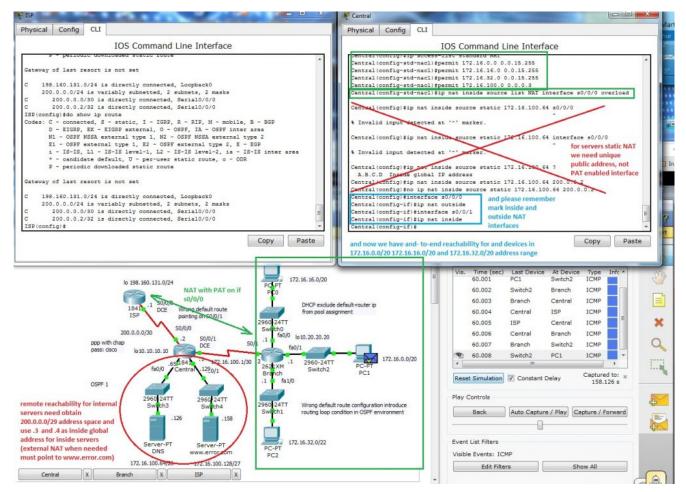
interface s0/0/0

ip nat outside

interface s0/0/1

ip nat inside.

Now we can place simple PDU between appropriate ends.



As "how to?" training you can establish connection for inside servers and enable reach them from ISP side. There must be used static nat and address range for inside global must increase from 200.0.0.0/30 to minimal 200.0.0.0/29 as it state previews picture.

Final and fixed packet tracer lab is on next picture and for

your training can be obtained from here (PKT 5.2 or above).

Logical	[Root]	New Cluste		Set Tiled Background	Viewport
L.	Wrong default route propagation in ospfenvironment				
	Io 198.160.131.0/24 PC PT 172.16.16.0/20 IVE NAT with PAT on interface PC PT 172.16.16.0/20 ISA 1 50/0/0 DHCP exclude default-router p from pool assignment DHCP exclude default-router p from pool assignment 2960/24TT 2960/24TT 2960/24TT 2960/24TT 1 200.0.0.0/30 50/0/0 Switch0 50/1 1 ppss:: cace Io1.10.10 172.16.100.1/30 7 266/24TT PC-PT fa0/0 Central 1172.16.100.1/30 7 266/24TT PC-PT 172.16.00.0/20	Time (sec) 60.001 60.002 60.003 60.004 60.005 60.006 60.006 60.007 60.008	PC1 Sw Switch2 Bra Branch Cer Central ISF ISP Cer Central Bra	ntral ICMP nch ICMP tch2 ICMP I ICMP	* C
		Reset Simulation Image: Constant Delay Captured to: * 158.126 s Play Controls			
need public address for remote reachability and DNS records How to do It is for your personal training. 172: 16. 100.64/26 172: 16. 100.128/27		Event List Filters Visible Events: ICMP			
•	I 72.10.100.120/27	Edit Filter	3	Show All	
Time: 01:41:26.556	Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward			Event List	imulation
Routers	Fire Last State	Contract of the owner	Destination Typ 198.160.131.1 ICM		N Periodic Ni N O
		was our goal	:-) m		,

13. STP port roles selection

For port roles selection is important which switch is selected as root bridge. That mean after root bridge selection process (in fact during this process) are port roles determined. (we will discus 802.1d STP, difference in 802.1w rapid STP will be explicit marked in document).

In stable converged L2 topology with STP support are there these types of ports:

- 1. Root ports exist on non- root bridges and are switch ports with best cost path to root bridge.
- 2. Designated ports exist on root and non-root bridges. For root bridge all ports are designated ports!!! (quick examination but there can be confusion if root-bridge role is distributed among VLANs or when there is default VLAN root bridge selected with other mechanism as other VLANs). Please keep in mind that on segment is allowed

only one designated port!!!. Designate ports also as root ports are capable populate mac-address-table (CAM table of switch).

- 3. Non-designated ports switchport that is blocked (in 802.1W rapid STP is used term alternate ports in discarding state).
- Disabled port is administratively down (has no function or does not participate in STP).

STA (spanning tree algorithm) determines which port role is assigned to each switchport:

- switch port with lowest overall path cost to root bridge is root port
- in network topology all switches except root bridge have a single root port
- if 2 ports have same port cost switches uses customizable port priority value or lowest port ID if both port priority value are same (*if cost is same – > lowest port ID – > if equal port ID break the tie*, that mean Fa0/1 < Fa0/2 < Fa0/3 As example port fa0/0 default priority is 128.1 configurable_priority.portID). As configurable priority can be used number from 0 to 240 with increment 16, and lower priority is better/ preferred.

Example of port priority configuration:

S#configure terminal

S(configure)#interface fa0/1

S(decision-if)#spanning-tree port-priority 112 (0 - 240 increment 16)

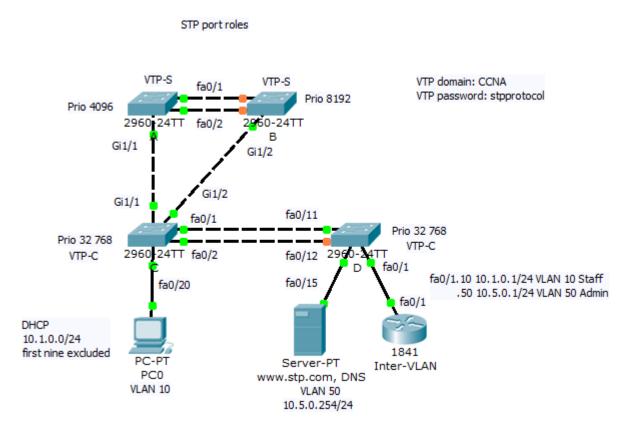
How is port role lowest made?

1. Switch with lowest bridge priority (if equal lowest MAC

address) is selected as root bridge.

- Root bridge set all its port as designated (in stable topology are in forwarding state).
- 3. Other, non-root bridge switches set one port with lowest cost to root-bridge as root ports.
- 4. In shared segment are determined port roles way that set one port as designated per shared segment and all other set as non-designated (prevent L2 loops and broadcast storm arisen). Keep in mind that lowest priority is first, only if equal then port priority or portID is used for tie breaking!!!

When we repeat basic theory, now we can prepare our PKT simulation lab. Preconfigured scenario in Cisco Packet Tracer 5.2 or above can be obtained from here._



Scenario consist of 4 switches. Root bridge role is determined by spanning-tree vlan 1, 10, 50 priority 4096 command for switch A. For VLAN information consistency is used proprietary VTP protocol with VTP domain: CCNA and password: stpprotocol. For redundancy of server roles in VTP two switches A and B are configured as VTP servers. Inter VLAN communication establish router on a stick Inter-VLAN.

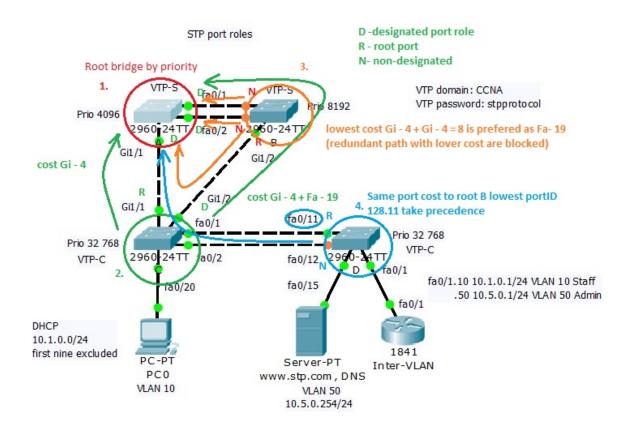
Staff PCs are on VLAN 10 and office web and DNS server is on VLAN 50 and use IP address 10.5.0.254/24.

Host Staff PCs obtain address automatically by DHCP that exclude first nine IP address from address pool.

As it was mentioned earlier root bridge can be noticed by two way from show spanning-tree command – explicit marking themselves as root bridge: "This bridge is root bridge". Second way how to examine root bridge from output of show spanning-tree command is by fact that all port of root bride are set as designated. Next picture show output from switch A

A# show spanning-tree VLAN0001 Obvious mistake in port role examination in PKT is omited existence of Spanning treefautbyea wightool with make all clear for lerning set priority for all Root ID configured VLANS but also default VLAN 1 equal - only for learning - in real Address 000D.BD79.C1B0 environment is load diversity required and for security reason can be This bridge is the root YLAN Irdisabled after moving to anoter sumber) Delay 15 sec Bridge ID Priority 4097 (priority 4096 sys-id-ext 1) 000D.BD79.C1B0 Address Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 20 Interface Role Sts Cost Prio.Nbr Type _____ _____ Fa0/2 Fa0/1 128.2 P2p Desg FWD 19 Desg FWD 19 128.1 P2p Desg FWD 4 128.25 P2p Gi1/1 VLAN0010 Spanning tree enabled protocol ieee Root ID Priority 4106 Address 000D.BD79.C1B0 This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 4106 (priority 4096 sys-id-ext 10) 000D.BD79.C1B0 Address Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 20 Role Sts Cost Prio.Nbr Type Interface ------128.2 P2p Fa0/2 Desg FWD 19 128.1 P2p 128.25 P2p Fa0/1 Desg FWD 19 Gi1/1 Desg FWD 4 VLAN0050 Spanning tree enabled protocol ieee Root ID Priority 4146 000D.BD79.C1B0 Address This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 4146 (priority 4096 sys-id-ext 50) 000D.BD79.C1B0 Address Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 20 Prio.Nbr Type Interface Role Sts Cost Desg FWD 19 Fa0/2 128.2 P2p Desg FWD 19 Fa0/1 128.1 P2p Desg FWD 4 Gi1/1 128.25 P2p

Now we will take closer look on port role selection in training environment

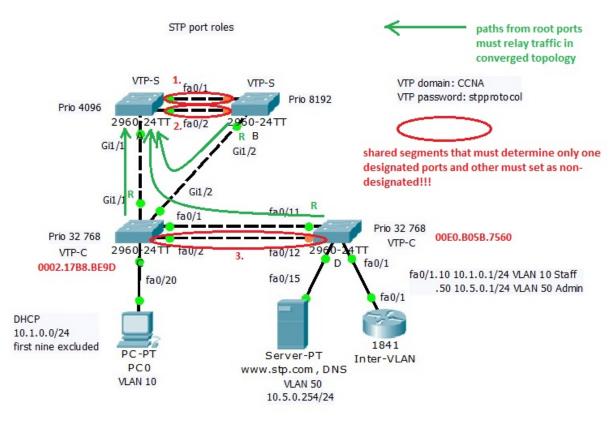




- Root bridge was elected because their lowest spaningtree vlan 1, 10, 50 priority 4096
- 2. Root bridge mark all its port as designated for all VLAN for which is root bridge (for simplicity our lab set root bridge role for all VLAN the same)
- 3. Election of root ports on all non root bridge switches select root ports. Root ports has lowest cost to rood bridge and only one root port per switch is selected. For switch marked with nr. 2 (green) is lowest cost port Gil/1 because port cost is 4 (Gil/1 cost), Gil/2 has cost (4+19 Fa of orange switch B). For orange switch with nr. 3 is as root port selected port Gil/2 because its cost to root bridge is 8 (4 Gi + 4second gigabit link from green to red switch) that is lower than 19 and 19 (costs of fa0/1 and fa0/2 ports). Blue switch with nr. 4 has two equal path cost (blue arrow in picture). If port cost are equal then port priority configured by

user or port ID (128.11 and 128.12 – only port ID are different if configurable port priority is default 128 as in our case). Lower portID 11 (port 11 – 128.11) determine role of root port. Now we know which ports are designated on root bridge (all) and which are root ports on all non- root bridge.

4. Elect designated and non-designated ports per segment. Each segment can have only one designated port, other is non-designated (prevent L2 loop creation). Next picture mark shared segment where must be selected designated and non designated role. Keep in mind that path from root ports with lowest cost to rood bridge must be open. Now we must examine only segment that does not participate in forwarding data from root ports to root-bridge (are not best path to root bridge). Final step that lead to converged L2 topology is on next picture



1) 2) Because root bridge set its por as designated other ends of links must be set as non-designated if we will have only one designated port per shared segment after root port selection process

3) Because cost to rootbridge from switch C is lower as from switch D (+19 added by outgoing port fa0/12) port fa0/2 will remain open and fa0/12 will close

12. Examination of VTP modes

VTP as Vlan trunking protocol make management of VLAN database across network simply but is proprietary. VTP allows configure appropriate VLANs on one switch (VTP server) and then propagate these VLANs to whole network (Other VTP server with lover revision number or other VTP clients).

But be careful when adding preconfigured switch – higher revision number take precedents and will populate preconfigured VLANs to entire network. Possibly best thing that you can du is change VTP domain name to another and then to expected because change in VTP domain name reset revision number to zero. Higher revision number mean "I have more accurate information about what is in network expected to do".

Benefits of use VTP are:

- consistency in VLAN across network
- dynamic trunk configuration when VLANs are introduced to network

In VTP terminology we must concern with these terms

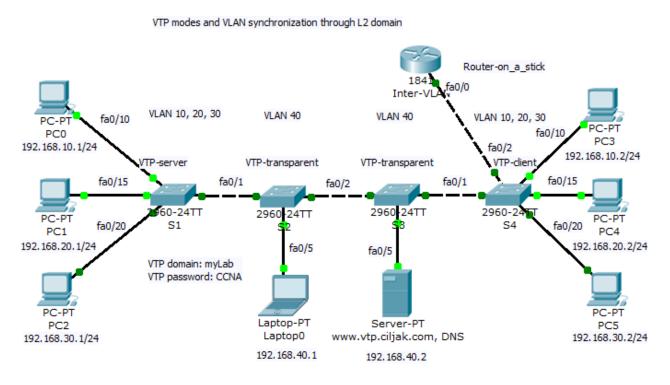
- VTP domain one or more interconnecting switch same VLAN configured. L3 devices dictate domain boundary.
- VTP advertisements distribute and synchronize VLANs
- VTP modes defines interaction with spread advertisements of VTP protocol across network
- VTP pruning restrict flooding traffic to switches where are not appropriate VLANs. Help save available bandwidth on network trunks.

VTP modes are:

- VTP Server (default mode) advertise VTP domain VLAN information to other enabled SW in same VTP domain (store VLAN info in NVRAM!!!). From server can be VLAN created, renamed or deleted.
- 2. VTP client only stores VLAN info. Is not default vtp mode client CLI command must be configured. can not any way change configured VLANs as server mode can, but accept server made changes (exception is higher revision number that can harm whole network – please before adding used switch to existing network reset revision number!!!!).

 VTP transparent – forward VTP advertisement but do not participate on VTP.

Now we can take closer look at our training lab. Preconfigured scenario can be obtained from here (PKT 5.2 or above).



All switches participate on same VTP domain with name: myLab (please remember that names are case sensitive!!!). Switch S1 act as VTP server and can introduce and change VLAN to network. S4 is client switch that will accept VLANs modified by VTP server S1. Storage and administrative devices are connected to two switches S2 and S3. These are VTP transparent and contain only private VLAN 40 but trunk link between S1-S2-S3-S4-Inter VLAN router must be allowed for all VLAN (is default but show interface trunk and per trunk configured switchport trunk allowed vlan nr.nr, .. can help correct errors wen occur.).

Inter VLAN communication (reachability is enabled by router on a stick Inter VLAN router. If some access are expected be prohibited (access from clients to administrative VLAN with other ports as 80 and 443or 53 then appropriate access list must be created and assigned on appropriate interface to take effect.)

Now we can examine our topology:

 Status of VTP enabled protocol on S1 is displayed after typing command show vtp status under privileged exec mode or after do under other config modes

Physical Config CLI	Physical Config CLI
IOS Command Line Interface	IOS Command Line Interface
VIDERFORM Like proceeded on interface FastEthernet0/20, changed state to up %LINK-5-CRANGED: Interface FastEthernet0/20, changed state to up %LINK-5-CRANGED: Interface FastEthernet0/20, changed state spreading VLANs among servers and clients %LINK-5-CRANGED: Interface FastEthernet0/20, changed state spreading VLANs among servers and clients %LINK-5-CRANGED: Interface FastEthernet0/20, changed state spreading VLANs among servers and clients %Ilenable VTP Server spreading VLANs among servers and clients %Ilenable : 2 must be same on all sw in domain Configuration Revision : 4 must be same on all sw in domain WTP Persiting Mode : Disabled must be same on all sw in domain WTP Promain Name : Disabled must be same on all sw in domain WTP Yrung Mode : Disabled must be same on all sw in domain WTP Yrung Generation : Disabled must be same on all sw in domain WTP Yrung Generation : Disabled must be same on all sw in domain WTP Yrung Generation : Disabled must be same on all sw in domain WTP Yrung Generation : Disabled must be same on all sw in domain WTP Yrung Generation : Disabled must be sam	<pre>\$LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/20, changed state to up \$LINEFROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up \$LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state t o up YTP Client \$45#ahow vtp status YTP Version : 2 Configuration Revision : 4 Maximum VLAMs supported locally: 255 Number of existing VLAMs : 9 YTP Operating Mode : Client YTP Pruning Mode : Disabled YTP Yruning Mode : 0x95 0x85 0x85 0x1C 0xFF 0xF5 Configuration last modified by 0.0.0 at 3-1-93 00:25:54 Stg Yanter Yruning Yruning</pre>
Messages pass through but non intact tra	statent III IIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
Physical Config CLI mode switches!!!	Physical Config CLI
IOS Command Line Interface	IOS Command Line Interface
<pre>\$LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state t o up \$LINE-5-CHANGED: Interface FastEthernet0/5, changed state to up \$LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state t o up</pre>	<pre>\$LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state t o up \$LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up \$LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state t o up</pre>
S2>enable S2>enable S2>show vtp status VTP Version : 2 Configuration Revision : 0 Maximum VLAMs supported locally : 255 number have been not altering Number of existing VLAMs : 9 VTP Operating Mode : Transparent VTP Domain Name : myLab VTP Druning Mode : Disabled VTP V2 Mode : Disabled VTP V2 Mode : Disabled VTP Trans Generation : Disabled VTP Signes Centration : Disabled ND5 digest : 0x41 0x08 0x06 0x98 0xDD 0x68 0x67 0x57 Configuration last modified by 0.0.0.0 at 3-1-93 00:25:54 S2#	S3>enable S3#ahow vtp status VTP Version : 2 Configuration Revision : 0 Maximum VLAMs supported locally : 255 Number of existing VLAMs : 9 VTP Optiming Mode : Transparent VTP Preasing Mode : Disabled VTP VI Mode : Disabled VTP VI Mode : Disabled VTP Traps Generation : Disabled VTP Traps Generation : Disabled VTP Traps Generation : Disabled VTP State Section : Disabled VTP State S

- 2. VLANs spread from S1 to S4 does not alter config on S3 and S2 in transparent mode.
- 3. Examination of allowed VLANs on trunk link among switches – show interface trunk

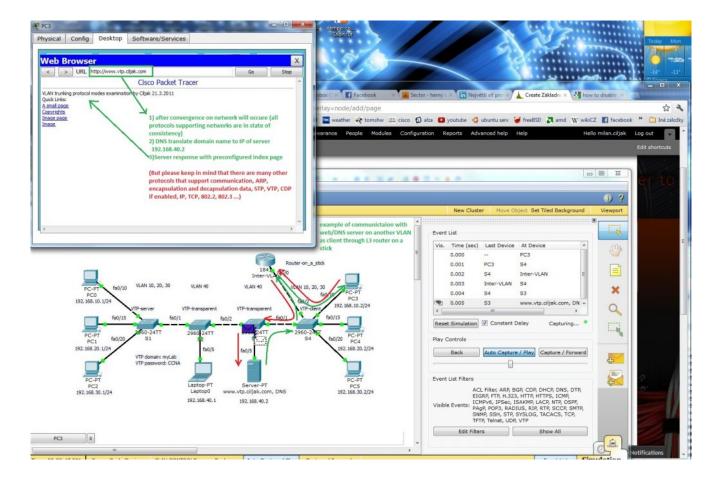
IOS	Command Line Interface	IOS Command Line Interface
ULAN0020	active Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19	40 VLAN0040 active Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9
VLAN0030	active Fa0/20, Fa0/21, Fa0/22, Fa0/23	1002 fddi-default active
VLAN0040	Fa0/24 active Fa0/5, Fa0/6, Fa0/7, Fa0/8	1003 token-ring-default active 1004 fddinet-default active
02 fddi-default	Fa0/9 active	1005 trnet-default active
3 token-ring-default	active	S4#show int trunk Port Mode Encapsulation Status Native vlan
4 fddinet-default	active	Fa0/1 on B02.1q trunking 1
5 trnet-default	active	Fa0/2 on 802.1q trunking 1
show interface trunk t Mode Encapsy	Ilation Status Native vian enumeration of true	nk Port Vlans allowed on trunk
/1 on 802.1q	trunking 1 configured	Fa0/1 1-1005
t Vlans allowed on tru	switchports	Fa0/2 1-1005
/1 1-1005		Port Vlans allowed and active in management domain
		Fa0/1 1,10,20,30,40
	ctive in management domain	Fa0/2 1,10,20,30,40
/1 1,10,20,30,40 enu	meration of allowed VLANs propagated on trunk - default all	Port Vlans in spanning tree forwarding state and not pruned
	ree forwarding state and not pruned	Fa0/1 1,10,20,30,40
/1 1,10,20,30,40		Fa0/2 1,10,20,30,40
(Produced)		
		₹ \$3
sical Config CLI		Physical Config CLI
sical Config CLI	Command Line Interface	₹ \$3
sical Config CLI	Command Line Interface	Physical Config CLI IOS Command Line Interface
Sical Config CLI IOS	Command Line Interface	S3 Physical Config CLI IOS Command Line Interface ZaU/24 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/5
Sical Config CLI IOS VLAN0040 12 fddi-default 13 token-ring-default	Command Line Interface revize active Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9 active active	S3 Physical Config CLI IOS Command Line Interface IOV VLAN0040
Sical Config CLI IOS VLAN0040 2 fddi-default 3 token-ring-default 4 fddine-default	Command Line Interface Tau/2* active Ta0/5, Fa0/5, Fa0/7, Fa0/8 Ta0/9 active active active	S3 Physical Config CLI IOS Command Line Interface ZaU/24 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/5
VLANO040 VLANO040 12 fddi-default 13 token-ring-default 14 fddinet-default 15 trnet-default	Command Line Interface revize active Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9 active active	S3 Physical Config CLI IOS Command Line Interface IOV Fa0/6, Fa0/7, Fa0/8 Fa0/5 fa0/6, Fa0/7, Fa0/8 Fa0/5 fa0/9 1002 fddi-default active 1004 fddinet-default active 1004 fddinet-default active softwe
Sical Config CLI IOS VLAN0040 22 fddi-default 33 token-ring-default 34 fddinet-default 55 trnet-default 56 trnet-default 56 trnet-default	Command Line Interface Tau/2* active Ta0/5, Fa0/5, Fa0/7, Fa0/8 Ta0/9 active active active	<pre>\$3 Physical Config CLI IOS Command Line Interface xau/iv IOS Command Line Interface xau/iv IOS fddi-default 1002 fddi-default active 1003 token-ring-default 1004 fddinet-default 1005 time-default 3 active 3 active</pre>
Sical Config CLI IOS VLAN0040 2 fddi-default 3 token-fing-default 4 fddinet-default 5 trut-default 5 tint truk t Mode Encaps 7/1 on 802.1q	Command Line Interface Tav/2* active Fa0/5, Fa0/6, Fa0/7, Fa0/8 active act	S3 Physical Config CLI IOS Command Line Interface IOV/A VLAN0040
Sical Config CLI IOS VLAN0040 2 fddi-default 3 token-fing-default 4 fddinet-default 5 trut-default 5 hint truk t Mode Enceps V/1 on 802.1q	Command Line Interface Tav/2* active Fa0/5, Fa0/6, Fa0/7, Fa0/8 active act	<pre>\$3 Physical Config CLI IOS Command Line Interface xau/iv IOS Command Line Interface xau/iv IOS fddi-default 1002 fddi-default active 1003 token-ring-default 1004 fddinet-default 1005 time-default 3 active 3 active</pre>
Sical Config CLI IOS VLAN0040 22 fddi-default 35 token-ring-default 34 fddinet-default 54 int trunk tt Mode Encaps 7/1 on 802.1q 7/2 on 802.1q	Command Line Interface active Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9 active active active active ulation Status Native vlan trunking 1 trunking 1	S3 Physical Config CLI IOS Command Line Interface Iavra Fav/s
Sical Config CLI IOS VLAN0040 D2 fddi-default D3 token-ring-default D4 fddinet-default D4 fddinet-default D4 fddinet-default D5 trnet-default D4 fddinet-default D4 fddinet-defa	Command Line Interface active Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9 active active active active ulation Status Native vlan trunking 1 trunking 1	S3 Physical Config CLI IOS Command Line Interface IOV/5 IO2 fddi-default active IO3 token-ring-default IO4 token-ring-default IO5 token-ring-defa
Sical Config CLI IOS VLAN0040 22 fddi-default 35 token-ring-default 44 fddinet-default 54 int trunk tt Mode Encaps 5/1 on 802.1q 7/2 on 802.1q 7/2 on 802.1q 7/2 on 802.1q	Command Line Interface active Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9 active active active active ulation Status Native vlan trunking 1 trunking 1	S3 Physical Config CLI IOS Command Line Interface Iavra Fav/s
Sical Config CLI IOS VLAN0040 02 fddi-default 03 token-ring-default 04 fddine-default 05 trnet-default 05 trnet-default 05 trnet-default 04 ddine-default 05 trnet-default 07 on 802.1q 07 on 802.1q 07 on 802.1q 07 1-1005	Command Line Interface active Fa0/6, Fa0/6, Fa0/7, Fa0/8 Fa0/9 active active active active ulation Status Native vlan trunking 1 trunking 1 unk	Physical Config CLI IOS Command Line Interface 1002 fddi-default 1003 tdke-ring-default 1004 fddinet-default 1004 fddinet-default 1005 trnet-default 1005 trnet-default 1005 trnet-default 1005 trnet-default 1005 trnet-default 1005 trnet-default 1005 trnet-default 1007 truk 1007 truk
Sical Config CLI IOS VLAN0040 VLAN0040 VLAN0040 VLAN040 VLAN040 VLAN040 VLAN040 VLAN040 VLAN040 Stoken-ring-default Stoken-	Command Line Interface active Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9 active active active active ulation Status Native vlan trunking 1 trunking 1	S3 Physical Config CLI IOS Command Line Interface INUTAL IOS Command Line Interface INUTAL IOS fddi-default active IOS token-ring-default active IOS token-ring-default active IOS tract-default active Sisshow int trunk Port Node Encapsulation Status Native vian Fa0/1 on 802.1q trunking 1 Fa0/2 on 802.1q trunking 1 Port Vians allowed on trunk Fa0/1 1-1005 Port Vians allowed and active in management domain Port Vians allowed and active in management domain
Sical Config CLI IOS VLAN0040 12 fddi-default 13 token-ring-default 14 fddinet-default 15 trunk-tefault 15 trunk-tefault 15 trunk tt Mode Encaps 1/1 on 802.1q 1/2 on 802.1q 1	Command Line Interface TRO/2* active TRO/5, FRO/6, FRO/7, FRO/8 active active active active ulation Status Native Vian trunking 1 trunking 1 trunking 1 trunking 1	S3 Physical Config CLI IOS Command Line Interface IOV/A IOS Command Line Interface IOV/A IOS Command Line Interface IOV/A IOS Command Line Interface IOS command Line Interfa
Sical Config CLI IOS VLAN0040 02 fddin=-default 03 token=ring-default 04 fddin=-default 05 trne=-default 94 hint trunk tt Mode Encappe 0/1 on 802.1q 0/2 on 802.1q 0/1 1-1005 rt vlans allowed on tr 0/1 1-1005 vt Vlans allowed and a 0/1 1,10,20,30,40 0/1 1,10,20,30,40 0/2 1	Command Line Interface Fau/a active Fau/5, Fau/6, Fau/7, Fau/8 Fau/5 active active active active active ulation Status Native vlan trunking 1 trunking 1 unk ctive in management domain tran for pass through communication S1-S4 - Inter VLAN rout	S3 Physical Config CLI IOS Command Line Interface IOV/A IOS Command Line Interface IOV/A IOS Command Line Interface IOV/A IOS Command Line Interface IOS command Line Interfa
VLAN0040 VLAN0040 22 fddi-default 03 token-ring-default 04 fddinet-default 55 trnet-default 56 trnet-default 56 trnet-default 57 Mode Encaps 0/1 on 802.1q 0/2 on 802.1q 0/2 on 802.1q 1.1005 rt Vlans allowed on tr 0/1 1.10,20,30,40 0/2 1.100,20,30,40 0/2 1.10,20,30,40 0/2 1.10,20,30,40 Vlans an spanning t	Command Line Interface TRO/2* active TRO/5, FRO/6, FRO/7, FRO/8 active active active active ulation Status Native Vian trunking 1 trunking 1 trunking 1 trunking 1	Physical Config CLI IOS Command Line Interface 1002 fddi-default active 1003 fddi-default active 1004 fddinet-default active 1004 fddinet-default active 1005 trnet-default active 1005 trnet-default active S38ahow int trunk Pao/1 on 802.1q trunking 1 Pao/2 on 802.1q trunking 1 Pao/2 on 802.1q trunking 1 Pao/2 in 1005 Pao/2 in 1005 Pao/2 in 1, 10, 20, 30, 40 Port Vians in spanning tree forwarding state and not pruned
vsical Config CLI IOS 00 VLAN0040 002 fddi-default 003 tokkn-ring-default 004 fddina-default 005 trans-default 128 hint trunk Encaps 00/1 on 802.1q 00/2 on 802.1q 00/1 1-1005 ort 00/2 1 100 00/1 1,10,20,30,40 mport	Command Line Interface Fau/a active Fau/5, Fau/6, Fau/7, Fau/8 Fau/5 active active active active active ulation Status Native vlan trunking 1 trunking 1 unk ctive in management domain tran for pass through communication S1-S4 - Inter VLAN rout	<pre>\$3 Physical Config CLI IOS Command Line Interface 40 VLAN0040 setive Fa0/5, Fa0/6, Fa0/7, Fa0/8 1002 fddi-default active 1003 token-ring-default active 1004 fddinet-default active 1005 trnet-default active \$3\$\$\$ anow int trunk \$3\$\$\$ mode Incorporation Status Native vlan Fa0/1 on 802.1q trunking 1 Fa0/2 on 802.1q trunking 1 Fa0/2 1-1005 Port Vlans allowed and active in management domain Fa0/1 1,10,20,30,40 Fa0/2 1,10,20,30,40 </pre>

Because default are allowed all VLANs to propagate across trunk, no additional commands are necessary – but keep in mind that they must be allowed or somebody for security reasons can enable only appropriate VLANs.

4. A bit confusing *output from show running-config*. You would by surprised where are all VTP config commands and VLANs that you created. But no worry, they are stored in vlan.dat in router flash. Vtp config can be examined with earlier mentioned commands. But next figure will explain something that you can be interested in.

Physical Config	ash: of flash:/ of flash:/ firmware of switch w- 4414921 <no date=""> c2960-lanbase-mz.122-25.FX.bin w- 796 <no date=""> vlan.dat bytes total (59600667 bytes free) VTP server switch store its VLAN configs in vlan.dat - client only in running-config in RAM</no></no>	
inysical coming	CLI My VTP co	mmands and VLAN are missing from running-config?
	CLI My VTP commands and VLAN are missing from running-config Where are the? IOS Command Line Interface in show running-config you cann not spot VTP configuration commands and commands creating VLANs - VLANs are stored in vlan.dat file on flas along firmware of switch ash:/ firmware of switch ash:/ firmware of switch ash:/ firmware of switch ash:/ firmware of switch ash:/ firmware of switch total (59600667 bytes free) VTP server switch store its VLAN configs in vlan.dat - client only in running-config in RAM detected at '^' marker. Lan.dat unix like command integrated in IFS (integrated file system) of IOS is in PKT environment not suppoted (simulated) - but on real device it will work Copy Paste De CLI IOS Command Line Interface a cli supporterston status nature vian sol.lq trunking 1 ns allowed on trunk 005 ns allowed and active in management domain 0,20,30,40 0,20,30,40	
Physical Config CLI My VTP commands and VLAN are missing from running-config? Where are they? IOS Command Line Interface Inter Conrol in show running-config you cann not spot VTP configuration commands and commands creating line vry 5 15 login in show running-config you cann not spot VTP configuration commands and commands reating line vry 5 15 login in show running-config you cann not spot VTP configuration commands and commands reating line vry 5 15 login in show running-config you cann not spot VTP configuration commands and commands reating line vry 5 15 login Sigidiz flash: firmware of Switch 1 end Sigidiz flash: for date> c2960-lanbase-mz.122-25.FX.bin crow date> vlan.dat Config Line Add the spot of		
Directory of fla 1 -rw-	4414921 <no date<="" td=""><td><pre>c2960-lanbase-mz.122-25.FX.bin</pre></td></no>	<pre>c2960-lanbase-mz.122-25.FX.bin</pre>
S1‡cd flash:		in vlan.dat - client only in running-config
	is in PKT environme	ent not suppoted (simulated) - but on real
3 52		
	J CLI	
Physical Config	IOS Comma	nd Line Interface
Physical Config Fort node Fa0/1 on	IOS Comma	nd Line Interface
Physical Config Fort Mode Fa0/1 on Fa0/2 on Port Vlar Fa0/1 1-10	IOS Comma Encapsulation 802.1q 802.1q ns allowed on trunk	nd Line Interface
Physical Config Fort room Fa0/1 on Fa0/2 on Port Vlar Fa0/1 1-10 Fa0/2 1-10 Port Vlar Fa0/1 1,10	IOS Comma Encapsulation 802.1q 802.1q ns allowed on trunk 005 005 ns allowed and active in 0,20,30,40	nd Line Interface
Physical Config Fa0/1 on Fa0/2 on Port Vlar Fa0/1 1-10 Fa0/2 1-10 Fa0/2 1-10 Fa0/2 1-10 Port Vlar Fa0/1 1,10 Fa0/2 1,10 Port Vlar Fa0/1 1,10 Fa0/2 1,10 S2# S2#show flash:	IOS Comma Encapsulation 802.1q 802.1q as allowed on trunk 005 005 as allowed and active in 0,20,30,40 0,20,30,40 0,20,30,40 0,20,30,40	nd Line Interface
Physical Config Fa0/1 on Fa0/2 on Port Vlar Fa0/1 1-10 Fa0/2 1-10 Fa0/2 1-10 Fa0/2 1-10 Port Vlar Fa0/1 1,10 Fa0/2 1,10 Port Vlar Fa0/1 1,10 Fa0/2 1,10 S2# S2#show flash:	IOS Comma Encapsulation 802.1q 802.1q ns allowed on trunk 005 005 ns allowed and active in 0,20,30,40 0,20,30,40 ns in spanning tree forwa 0,20,30,40 0,20,30,40 ash:/ 4414921 <no dat<="" td=""><td>nd Line Interface</td></no>	nd Line Interface

5. Example of real message exchange in training environment – web access. When there are devices on different VLANs they must communicate through L3 device (L3 traditional routing scenario, Router on a stick or introducing SVI interfaces on L3 capable switch). Now it is important feel all protocols that support exchange of messages through our network – HTTP, DNS, TCP, IP, 802.2 LLC, 802.3 Ethernet, ARP, routing protocols if needed, VTP, STP, CDP (on cisco network but all managed network use something), SNMP for management ... and many many others. That all lies beneath network exchange of our communication (ICQ, e-mail, facebook, youtube, skype, VoIP ...).

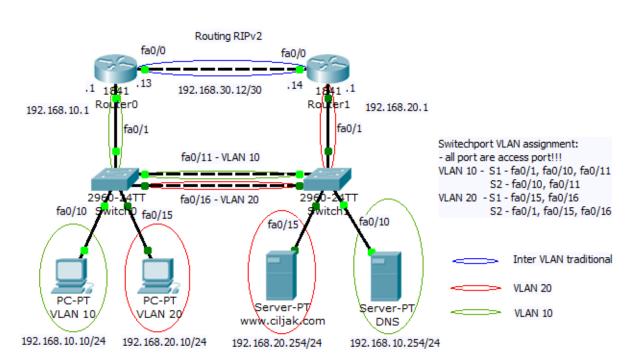


11. Examination of traditonal

inter VLAN routing with dedicated routers

Our training lab will focus on "academic" traditional inter VLAN communication. This routed connection uses two separate dedicated routers that are connected through two point fast ethernet speed connection (link). Our goal will be to understand how will data packet travel from one VLAN (red) to second VLAN (Green) using blue routed segment.

Network topology looks like this



Academic solution inter VLAN routing for eductional purposes

Please - feel free to try preconfigured scenarios 0, 1, 2 and 3 to send packet between endpoints in topology. What pathway is shortest and where is delivery worse? To use it, toogle in Simulation.

Preconfigured scenario can be obtained from here (PKT 5.2 or above).

This scenario is bundled with 4 Scenarios that can be selected from scenario drop box in bottom part of Cisco Packet tracer

(picture). For best PDU tracking go to simulation mode where you can look for events created during PDU traversing from source to its destination.

itional_purpose.pkt	
	i) ?
	New Cluster Move Object Set Tiled Background Viewport
Scenario 3 Description: 🔯	Event List
AN 20 to VLAN 20	Vis. Time (sec) Last Device At Device Type Ir
=	💿 0.000 www.ciljak.com ICMP
	*
VLAN assignment: access port!!!	Q
1 - fa0/1, fa0/10, fa0/11 2 - fa0/10, fa0/11	simple PDU ICMP ping
1 - fa0/15, fa0/16 2 - fa0/1, fa0/15, fa0/16	between selected devices
 Inter VLAN traditional 	· · · · ·
> VLAN 20	Reset Simulation Constant Delay Captured to: * 0.000 s
≻ VLAN 10	Play Controls 4)
	Back Auto Capture / Play Capture / Forward
gy.	automatic play selected
scenario selection box	Event List Filters PDU events sophisticated
	Visible Events: ICMP analyse
1)	Edit Filters Show All
······································	Select only important PDU type- look at all options available
apture / Forward	Event List Simulation
j) Scenario 3 - Fire L	ast Status Source Destination Type Color Time (sec) Periodic
	Progress www.ciljak.com VLAN 20 ICMP 0.000 N
Scenario 2	from to 2)
Togg Scenario 3	III. F

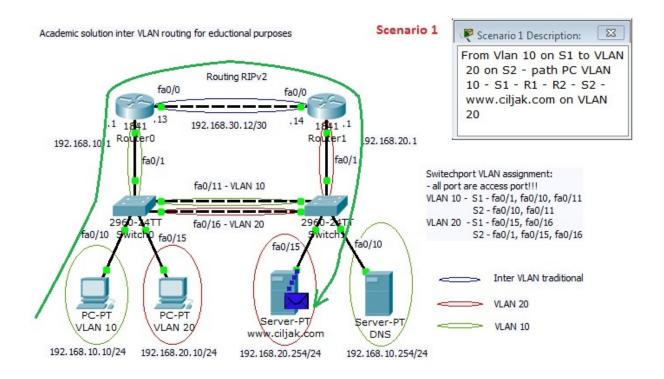
Scenario selection box is marked as nr. 1. Right pane consist of fire button that can optionally start PDU delivery from source to destination. Type mean PDU protocol and selectable color is color of PDU. Optionally can be altered PDU filter (default in this scenario will intercept only ICMP – ping PDU – ARP, RIP, STP, CDP … PDUs are hidden).

Now is all prepared for PDU delivery examination — open our scenario in PKT 5.2 or above and select scenario:

1) Scenario 0 — intra VLAN — from host 192.168.10.10 to DNS server 192.168.10.254 on same VLAN

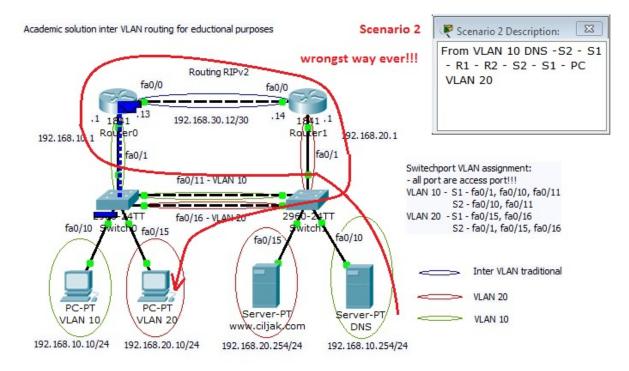
🗅 🗁 🖬 🗁 🗖 🚺	3 B @ @ / / / / m \$						1)?
Logical [Ri	oot]		N	ew Cluster	Move Object	Set Tiled Background	Viewport
Acad	lemic solution inter VLAN routing for eductional purposes Scenario 0	R Scenario 0 Description:	Event List				*
	fa0,0 fa0,0 1 161,1 192,168.30,12/20 14 161,1	VLAN 10 to VLAN 10 - no router needed	Vis. Tir 0.0 0.0	100 106		10 ICMP	
2	92.168.10.1 Router0 Router1 192.168.20.1 fs0/1 fs0/1 fs0/1 Swited fs0/1 VLAN 10 VLAN 10 VLAN 2 29/50-VCTT fs0/15 - VLAN 20 29/60-20TT VLAN 2	hport VLAN assignment: It are access port!!! 0 - S1 - Fa/J1, fa0/10, fa0/11 S2 - fa0/10, fa0/11 0 - S1 - fa0/15, fa0/16 S2 - fa0/16, fa0/15, fa0/16	0.0		witch0 Swit witch1 DNS		× <
/	PC-PT VLAN 10 2. 166. 10. 10/24 2. 168. 20. 10/24 2. 168. 20. 10/24 2. 168. 20. 10/24 192. 168. 20. 254/24 192. 168. 20. 254/	Inter VLAN traditional VLAN 20 VLAN 10	Play Cont	rols	Constant Delay	Captured to: , 0.009 s	
Please	e - feel free to try preconfigured scenarios 0, 1, 2 and 3 to send packet between endpoints in 1 pathway is shortest and where is delivery worse? To use it, toogle in Simulation.	opology. 4 scenarios for examination	Event List Visible Ev		luto Capture / Pla	Capture / Forward	
Time: 01:30:34.060 Por	mer Cycle Devices PLAY CONTROLS: Back Auto Capture / Play	Capture / Forward	Status Sol ogress VLA		nation Type ICMP	Event List S Color Time (sec)	Feriodic Num N 0
3 - 2 -	(Select a Device to Drag and Drop to the Workspace)	Toggle PDU List Window			ш		

2) Scenario 1 - inter VLAN - from host 192.168.10.10 to www.ciljak.com server with 192.168.20.254 on different VLAN

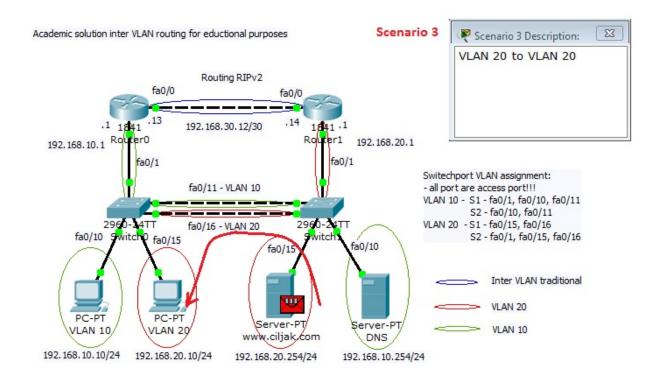


Please - feel free to try preconfigured scenarios 0, 1, 2 and 3 to send packet between endpoints in topology. What pathway is shortest and where is delivery worse? To use it, toogle in Simulation.

3) Scenario 2 - inter VLAN - from DNS server 192.168.10.254 to host 192.168.20.10 on different VLAN



Please - feel free to try preconfigured scenarios 0, 1, 2 and 3 to send packet between endpoints in topology. What pathway is shortest and where is delivery worse? To use it, toogle in Simulation. server www.ciljak.com 192.168.20.254 to host 192.168.20.10 on same VLAN



Please - feel free to try preconfigured scenarios 0, 1, 2 and 3 to send packet between endpoints in topology. What pathway is shortest and where is delivery worse? To use it, toogle in Simulation.

Conclusion: Different path for inter VLAN routed PDU is one of many great weakness. Price of dedicated server and time for cabling that can lead to network failures is another great weakness. Better solution is introduction of L3 capable switch or cheaper but not so strong (sharing trunk that mean potentially bottleneck in network) is well know router on a stick solution.

You are strongly encouraged exchange access link between two switches with one trunk link with ether channel.

10. Rootbridge election process in STP enabled environment

In redundant L2 topology STP ensures loop free path for frames traveling among endpoints blocking redundant paths that cause a loop.

STP — spanning tree protocol uses STA (spanning tree algorithm). STA designates a single switch as root bridge and uses it as reference for all calculations. Switch with lowest bridge ID (BID) becomes root bridge. After root bridge is determined — STA calculates shortest path to root bridge. Each switch use STA determine which ports block. Until STA on all switches is calculated — all traffic on broadcast domain is blocked. Port costs and path to rood bridge are considered when determining which path to leave unblocked.

This article will focus on root bridge election in STP enabled network.

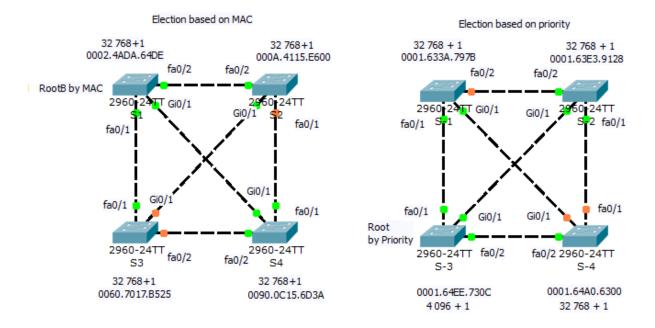
When root bride are elected this mechanism will be used:

1) lover priority - configured by spaning-tree vlan nr,nr, ... priority nr (1 to 65 536 with increment 4096, default 32 768) is better

2) if priorities are equal (default 32 768) then lower MAC address is preferred by STA.

Our lab will use these 2 mechanism for root bridge election:

Root bridge election and port roles in spanning tree (ieee or 802.1D)



For configuration root bridge priority in 802.1D(W) on STP capable switches can be used CLI command:

sw(config)#spanning-tree vlan number priority Priority_number

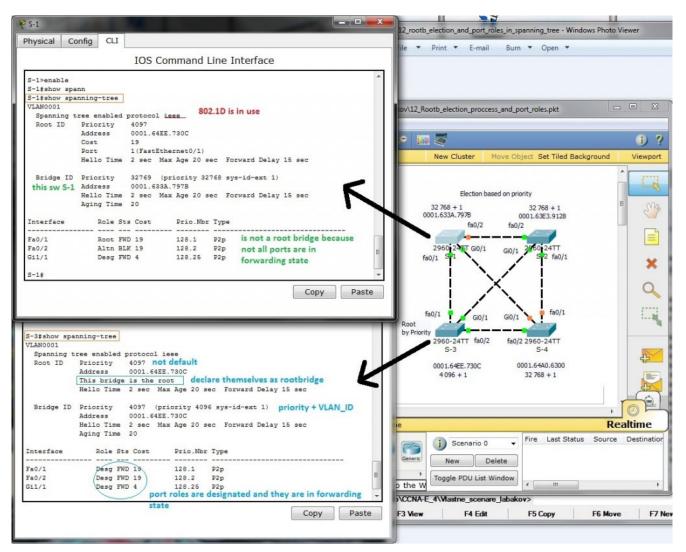
example spanning-tree vlan 1,99,150 priority 4096

or

sw(config)# spanning-tree vlan nr root primary

sw(config)# spanning-tree vlan nr root secondary

One of the most important thing is determine which switch is elected as root bridge using CLI commands. You can use show spanning-tree entered at privileged exec prompt as show next picture



What important thing show to us output from commands executed on two different switches?

Root bridge mark themselves as root bridge (this bridge is ...)

2) All root bridge ports are in designated role and are in forwarding state

3) 802.1D implementation of STP is in use (not rapid-PVST) because ieee is in output

4) Priority 4096 was important for root bridge selection (if equal then lover MAC break the tie and S-1 going to be root bridge

Our preconfigured training topology can be obtained from here (PKT 5.2 or above required).

Prerequisites for our simulations

What we will need for our next simulation articles is Cisco Packet tracer. Most preferred way is obtain it from official site

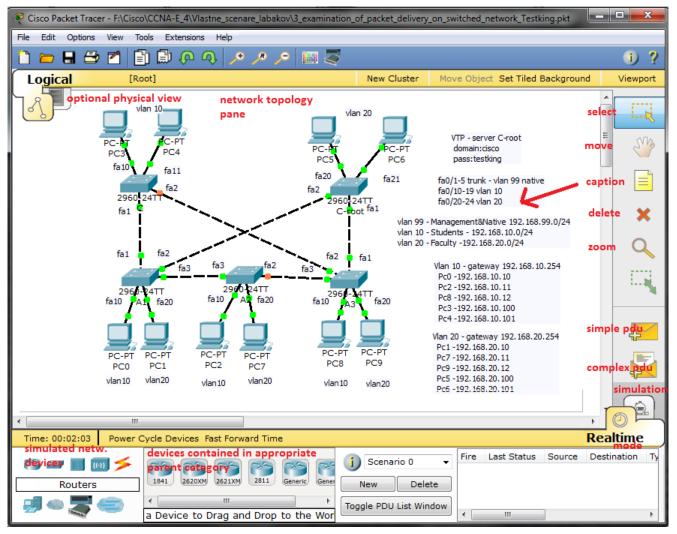
but you need:

To Download Packet Tracer:

- Log in to Academy Connection (you must be a registered Networking Academy student, alumni, instructor, or administrator)
- After logging into Academy Connection, select the Packet Tracer graphic to download.

Or you can use another method for obtaining it, at your mind must be that it will be version 5.2 or above.

Closer look at GUI of our simulation application:



Next published articles focus on SOHO environment simulations or case study of some network configurations (single area ospf, wrong default route, AD route preference, STP, rapid STP ...).

But there were presented only final topology with device configurations, closer description is for you. Please take my lab series only as a announcement of problems for solving and as a optional learning opportunity not as a substitution of labs spreaded with academy. All content is providet as is without any warranty to obtain you CCNA or CCNA Voice certification. There are many skills that must be gained.

9. Small office configuration scenario with VLAN and internet access nr. 3

New network scenario consist of one branch router with default routing to ISP. WAN internet access use PPP serial link with old PAP authentication. Office hosts are separated in 3 VLAN. Vlan 1 remain default, VLAN 2 is staff and for guests is reserved guest VLAN 3. Administrator use Admin Laptop for direct console CLI access. Switched network remain very simple, there is only one switch extended with old hub Hub0 (clients C and D share same subnet but also same collision domain).

 Serial link with PPPencapsulation and PAP authentication:
 On Office router: username ISP password 0 cisco

interface Serial0/0/0
ip address 209.165.200.225 255.255.255.252
encapsulation ppp
ppp authentication pap
ppp pap sent-username Office password 0

cisco

On ISP router:

username Office password 0 cisco

interface Serial0/0/0
ip address 209.165.200.226 255.255.255.252
encapsulation ppp
ppp authentication pap
ppp pap sent-username ISP password 0 cisco
clock rate 64000

•loop back interface on ISP router for testing remote

```
connectivity
     interface Loopback0
     ip address 198.160.131.1 255.255.255.0

    static route in ISP pointing to Office inside global

 (public) address
     ip route 209.165.201.0 255.255.255.224 Serial0/0/0

    default routing to ISP

     ip route 0.0.0.0 0.0.0.0 Serial0/0/0

    static NAT and NAT with interface serial 0/0/0 overload

 PAT for local hosts internet connectivity
     ip nat inside source list NAT interface Serial0/0/0
 overload
        ip nat inside source static 10.0.4.254
 209.165.201.1
     ip access-list standard NAT
     permit 10.0.0.0 0.0.255.255

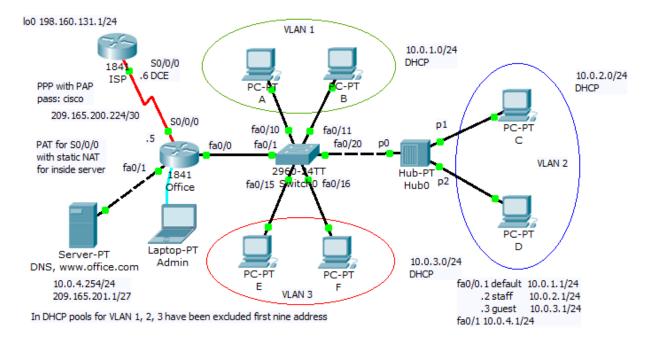
    DHCP address assignment for all VLAN clients

     ip dhcp excluded-address 10.0.1.1 10.0.1.9
     ip dhcp excluded-address 10.0.2.1 10.0.2.9
     ip dhcp excluded-address 10.0.3.1 10.0.3.9
     1
     ip dhcp pool VLAN1
     network 10.0.1.0 255.255.255.0
     default-router 10.0.1.1
     dns-server 10.0.4.254
     ip dhcp pool VLAN2
     network 10.0.2.0 255.255.255.0
     default-router 10.0.2.1
     dns-server 10.0.4.254
     ip dhcp pool VLAN3
     network 10.0.3.0 255.255.255.0
     default-router 10.0.3.1
     dns-server 10.0.4.254
```

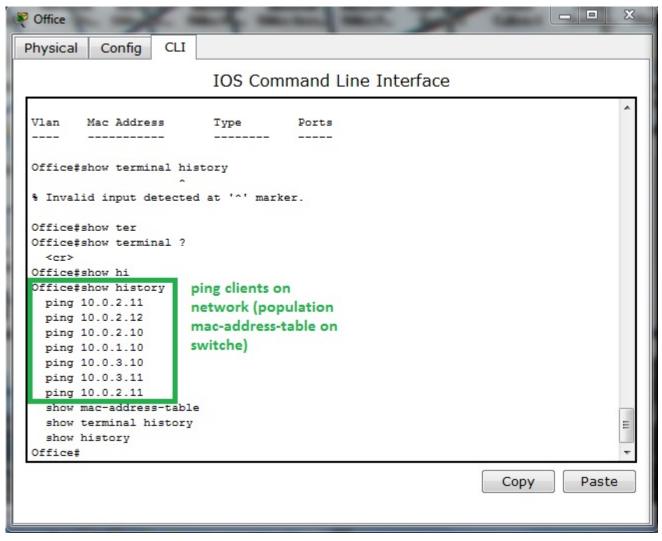
```
• inter VLAN routing with router-on-a-stick
     interface FastEthernet0/0
     no ip address
     duplex auto
     speed auto
     interface FastEthernet0/0.1
     encapsulation dot10 1 native
     ip address 10.0.1.1 255.255.255.0
     ip nat inside
     1
    interface FastEthernet0/0.2
    encapsulation dot10 2
    ip address 10.0.2.1 255.255.255.0
    ip nat inside
    L.
    interface FastEthernet0/0.3
    encapsulation dot10 3
    ip address 10.0.3.1 255.255.255.0
    ip nat inside
```

Preconfigured scenario you can download from here (PKT 5.2 and above). Network topology show next picture

Samll business office with vlan and internet access 3



Interesting part of this scenario is shared network segment using hub for extension switched LAN. Our interests is in switching table of Switch0. We can ask: how will be macaddress-table finally populated? At first we must ping devices on network that will populate switching (mac.addresstable).Example of ping from Office router to all network device:



Our SwitchO mac-address-table look like this

🏹 Switch0	Statement of the local division of the local		
Physical Config CLI			
	IOS Comm	and Line Int	terface
Switch#ping 10.0.2.11 Type escape sequence to Sending 5, 100-byte ICMP Success rate is 0 percen Switch#show mac Switch#show mac-address- Mac Address Ta Vlan Mac Address	Echos to 10.0 t (0/5) table ble		is 2 seconds:
1 0040.0bd5.7809 1 00d0.ba84.dc01 2 0010.111b.2670 2 0060.3ee0.e044 2 00d0.ba84.dc01 3 0030.a34e.94b5 3 0090.0c50.6657 3 00d0.ba84.dc01 Switch# fa0/1 trunk link to router on stick	DYNAMIC DYNAMIC DYNAMIC DYNAMIC DYNAMIC DYNAMIC DYNAMIC	Fa0/20 Fa0/1 Fa0/16 Fa0/15 Fa0/1	PC connected on same switch - shared network segment switch or hub (refer duplex or commands output)

Two or more PC assigned to one switch port in address table (switching table) is example of shared network segment connected on port fa0/20. But we can not examine from this that this is next switch or hub (you must use CDP show cdp neighbors or show interface fa0/20 that is in full or half duplex mode).

Switch port assignment to appropriate VLAN examine show vlan brief command issued on switch0

hysical	Config CLI			
		IOS Com	nmand Lir	ne Interface
1	0000.0284.0001	DINAMIC	rau/1	
2	0010.111b.2670	DYNAMIC	Fa0/20	
2	0060.3ee0.e044	DYNAMIC	Fa0/20	
2	00d0.ba84.dc01		Fa0/1	
3	0030.a34e.94b5		Fa0/16	VI AN port assignment
3	0090.0c50.6657	DIMINIC	Fa0/15	VLAN port assignment
3		DYNAMIC	Fa0/1	
Switch#	show vlan br			
VLAN Na	me		Status	Ports
1 de	fault		active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Gig1/1, Gig1/2
2 st	att		active	Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24
3 gu	lest		active	Fa0/15, Fa0/16, Fa0/17, Fa0/18
				Fa0/19
1002 fd	di-default		active	
1003 to	ken-ring-default		active	
1004 fd	dinet-default		active	E
1005 tr	net-default		active	
Switch#			anne provinsie 22	-
				Copy Paste

Switch port fa0/1 is excluded from list because is trunk port connecting switch and Office router in router-on-a-stick inter vlan. For port fa0/1 state examination we can use show interface fa0/1 switch port CLI command

👰 Switch0	
Physical Config CLI	
IOS Command Line Interface	
Switch*show interface fa0/1 switchport Name: Fa0/1 Switchport: Enabled Administrative Mode: trunk Operational Mode: trunk Administrative Mode: trunk Administrative Trunking Encapsulation: dotlq Operational Trunking Encapsulation: dotlq Operational Trunking Encapsulation: dotlq Operational Trunking Encapsulation: dotlq Negotiation of Trunking: On Access Mode VLAN: 1 (default) Trunking Native Mode VLAN: 1 (default) Voice VLAN: none Administrative private-vlan host-association: none Administrative private-vlan host-association: none Administrative private-vlan trunk normal VLAN: none Administrative private-vlan trunk normal VLANs: none Operational private-vlan: none Trunking VLANs Enabled: ALL Pruning VLANs Enabled: 2-1001 Capture Mode Disabled Capture VLANs Allowed: ALL Protected: false Appliance trust: none Switch#	

Native (default) VLAN is 1 that is default switch out of box configuration and trunk encapsulation is dot1q.

Same command issued on access port fa0/20 result in output:

Switch0		x
Physical Config CLI		
IOS Command Line Interface		
<pre>Switch#show interface fa0/20 switchport Name: Fa0/20 Switchport: Enabled Administrative Mode: dynamic auto Operational Mode: static access Administrative Trunking Encapsulation: dot1q Operational Trunking Encapsulation: native Negotiation of Trunking: On Access Mode VLAN: 2 (staff) Trunking Native Mode VLAN: 1 (default) Voice VLAN: none Administrative private-vlan host-association: none Administrative private-vlan mapping: none Administrative private-vlan trunk native VLAN: none Administrative private-vlan trunk native VLAN: none Administrative private-vlan trunk normal VLANs: none Administrative private-vlan trunk private VLANs: none Operational private-vlan: none Trunking VLANs Enabled: ALL Pruning VLANs Enabled: 2-1001 Capture Mode Disabled Capture VLANs Allowed: ALL Protected: false Appliance trust: none</pre>		- III -
Switch#	Copy Paste	e

Port is bounded with VLAN 2 as you can see on topology diagram and from show vlan brief CLI command output.

Please remember that there is also one show command for trunk ports examination — it is show interface trunk

Physical					
		IOS Comm	and Line Ir	nterface	
Administ	ative private	-vlan mapping: no	one		
Administ	ative private	-vlan trunk nativ	ve VLAN: none		
	-	-vlan trunk encap		-	
	-	-vlan trunk norma			
	-	-vlan trunk priva	ate VLANs: no	ne	
-	al private-vl				
-	VLANs Enabled /LANs Enabled:				
-	fode Disabled	2-1001			
-	LANs Allowed:	AT.T.			
Protected		ADD			
	trust: none				
	now interface	trunk			
Port	Mode	Encapsulation	Status	Native vlan	
Fa0/1	on	802.1q	trunking	1	
Port	Vlans allo	wed on trunk			
Fa0/1	1-1005				
Port	Vlans allo	wed and active in	n management	domain	
Fa0/1	1,2,3				
Port	Vlans in s	panning tree forw	varding state	and not pruned	
	1,2,3				
Fa0/1					
Fa0/1 Switch#				_	
					Pas