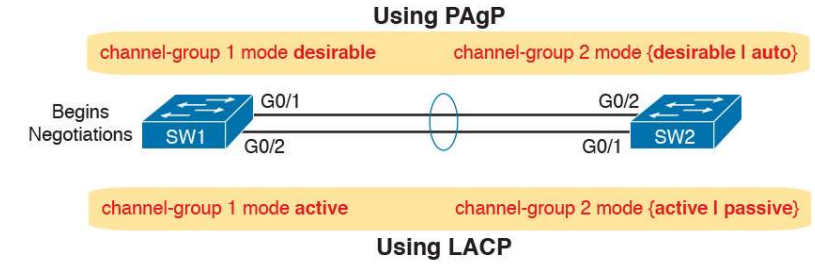
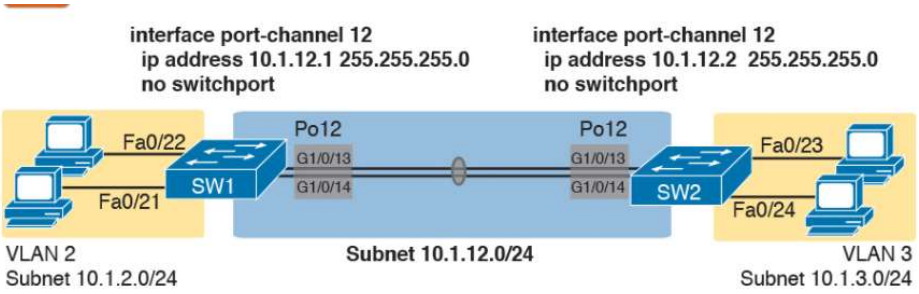
ICND2.STUDY GUIDE

Friday, November 3, 2017 12:14 PM

SHOW SPANNING-TREE VLAN 1
SHOW interface g0/1 switchport
router ospf command and interface






```
interface GigabitEthernet1/0/13
 no switchport
 no ip address
 channel-group 12 mode on
!
interface GigabitEthernet1/0/14
 no switchport
 no ip address
 channel-group 12 mode on
!
interface Port-channel12
 no switchport
 ip address 10.1.12.1 255.255.255.0
```

Criteria	Open SDN	ACI	APIC Enterprise
Changes how the device control plane works versus traditional networking	Yes	Yes	No
Creates centralized point from which humans and automation control the network	Yes	Yes	Yes
Degree to which the architecture centralizes the control plane	Mostly	Partially	N/A[1]
SBIs used	OpenFlow	OpFlex	CLI, SNMP
Controllers mentioned in this chapter	OpenDaylight, Cisco OSC	APIC	APIC-EM
Organization that is the primary definer/owner	ONF	Cisco	Cisco

Distractors: Never Cause an OSPF Failure

Reasons	Required by OSPFv2?
Identical OSPFv2 routing process IDs (**router ospf x**)	no
Both use **network** or both use **ip ospf** to enable OSPFv2 on interfaces	no
Neither router can make its interface passive to OSPFv2	no*
Identical K-value settings	no*

* Cannot be configured for OSPFv2

Po ts

Setting	Will a Mismatch Prevent VTP from Working?
VTP Domain Name	Yes
VTP Password	Yes (if Set on Either/Both)
VTP Pruning (on|off)	No
VTP Version (1|2)	No

R1 Migration: Step 3: Add CHAP

```
hostname R1
username R2 password Barney
!
interface s0/0/0
  encapsulation ppp
  no ip address
  ppp multilink
  ppp multilink group 3
  ppp authentication chap
!
interface s0/0/1
  encapsulation ppp
  no ip address
  ppp multilink
  ppp multilink group 3
  ppp authentication chap
```

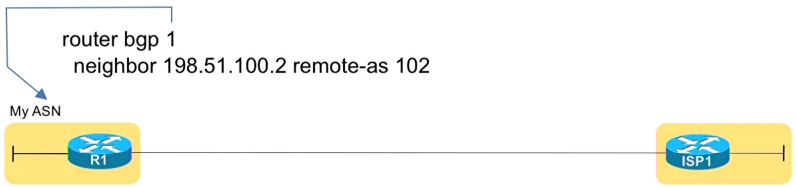
```
hostname R1

!
interface multilink 3
  encapsulation ppp
  ip address 172.25.123.1 255.255.255.252
  ppp multilink
  ppp multilink group 3
```

Comparison Points: GRE and DMVPN

Attribute	GRE	DMVPN
Dynamically Learns Some Info About Endpoints?	No	Yes
Does Remote Router Pre-configure an IP Address of the Central Router?	Yes	Yes
Does Central Router Pre-configure an IP Address of Each Remote Router?	Yes	No
Central Router Acts as NHRP Server?	No	Yes
Uses Point-to-point GRE Tunnels	Yes	No
Uses Multipoint GRE Tunnels	No	Yes

eBGP BGP Peer (Neighbor)



HSRP Neighbor Requirements

Parameter	Values on Neighbors Must…
Interface IP Addresses	…Be Different Addresses; Must Not Be VIP
Interface IP Subnet	…Be in Same Subnet
VIP Address	…Be Exact Same Value on All Routers
HSRP Group Number	…Be Same Number on All Routers
HSRP Version	…Match

Interface and VIP IP Addresses

- Interface
- Different
- Same Subnet

```
int g0/1                          int g0/1
 ip address 172.16.2.3 ...         ip address 172.16.2.2 ...
 standby 1 ip 172.16.2.1           standby 1 ip 172.16.2.1
```

- Virtual IP (VIP)
- Same Address
- Same Subnet as Interface Address

livelessons

Answer Analysis: Generic Terms (A, E)

Which terms refer to Cisco products that can run in a public cloud environment, but are under the complete control of the enterprise IT staff?

A) ✖ NFV
B) ✓ ASAv
C) DHCPv
D) IOSv
E) VNF
F) ✓ CSR

Network Functions Virtualization:
- principle of
- separating network functions from the hardware they run on
- by using virtual hardware abstraction

Virtual Network Function:
- Implementation of an Network Function (which is virtual)
- on hardware and software

Paraphrased from ETSI Group Specification NFV 003 (www.etsi.org)

livelessons

MC Question #2: Answers A, C

After experiencing some issues with SNMP, an engineer wants to use Wireshark on PC3 to capture all SNMP messages sent and received by the NMS on server S1. Which answers best describe the SNMP messages gathered by the SPAN session?

(Choose 1 Answer)

A) All Except SNMP Get Responses ← Received by NMS
B) All Except SNMP Get Requests
C) All Except Unsolicited SNMP messages (Trap or Inform)
D) All SNMP Messages

livelessons

RADIUS Vs. TACACS+

Feature	RADIUS	TACACS+
Layer 4 Protocol	UDP	TCP
Ports Used	1645, 1812	49
Encrypts Entire Packet?	No	Yes
Encrypts Password Only?	Yes	No
Defined By…	RFC 2865	Cisco
Command Authorization	No	Yes

A) Uses well-known UDP ports 1645 and/or 1812
B) When sending packets for authentication, it encrypts the entire packet
C) Defined by an IETF RFC

livelessons

HSRP priority higher is better

Route Source	Administrative Distance
Directly Connected	0
Static	1
EIGRP	90
EIGRP Summary route	5
OSPF	110
RIP	120

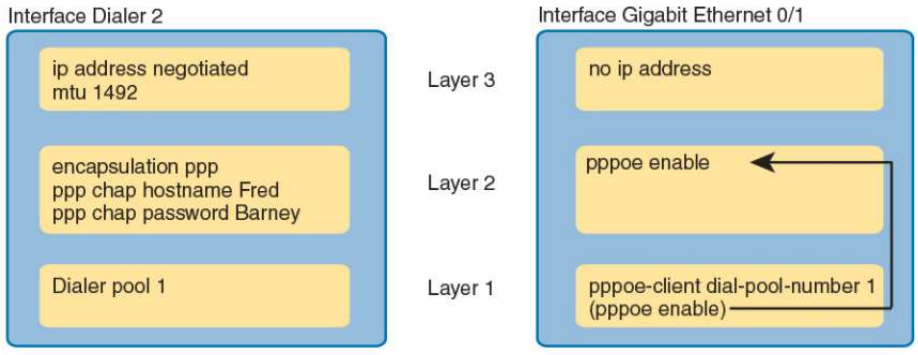


Figure 15-28 *PPPoE Client Configuration on Router R1 (Duplicate of Figure 15-25)*

Below is the range of standard and extended access list:

Access list type	Range
Standard	1-99, 1300-1999
Extended	100-199, 2000-2699

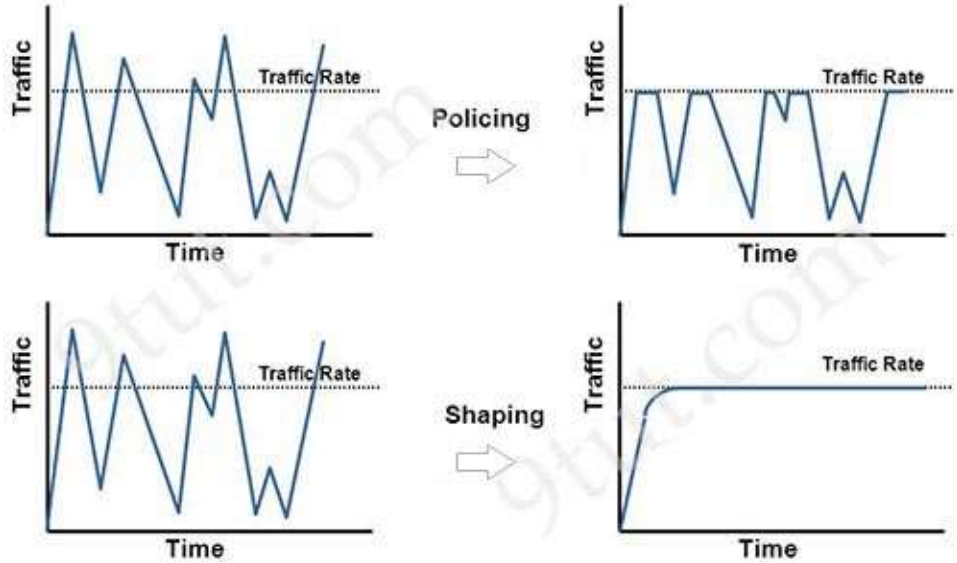
In most cases we only need to remember 1-99 is dedicated for standard access lists while 100 to 199 is dedicated for extended access lists.

0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

The highest level is level 0 (emergencies). The lowest level is level 7. By default, the router will send informational messages (level 6). That means it will send all the syslog messages from level 0 to 6.

snmp

Command Keyword	Keyword in Messages	Checks Message Integrity?	Performs Authentication?	Encrypts Messages?
noauth	noAuthNoPriv	Yes	No	No
auth	authNoPriv	Yes	Yes	No
priv	priv	Yes	Yes	Yes



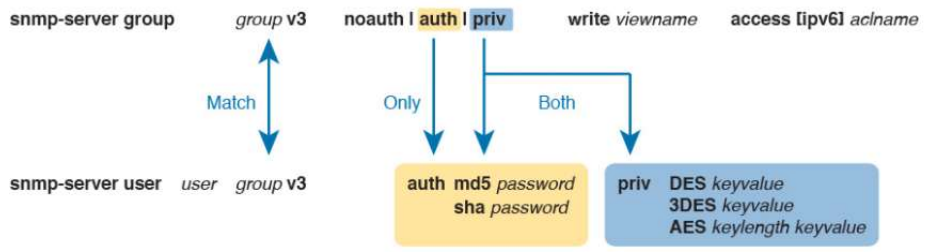
STP Port Role	STP Port State
Root port	Forwarding
Designated port	Forwarding
Nondesignated port	Blocking
Disabled	-
In transition	Listening Learning

RSTP Port Role	RSTP Port State
Root port	Forwarding
Designated port	Forwarding
Alternative or backup port	Discarding
Disabled	Discarding
In transition	Learning

A BPDU is superior than another if it has:

1. A lower Root Bridge ID
2. A lower path cost to the Root
3. A lower Sending Bridge ID
4. A lower Sending Port ID

Link speed	Cost
10Mbps	100
100Mbps	19
1 Gbps	4



Follow these guidelines when configuring port security:

+ **Port security can only be configured on static access ports, trunk ports, or 802.1Q tunnel ports**. -> A is not correct.

+ A secure port cannot be a dynamic access port.

+ A secure port cannot be a destination port for Switched Port Analyzer (SPAN).

+ A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group. -> D is not correct

+ **You cannot configure static secure or sticky secure MAC addresses on a voice VLAN**. -> B is not correct.

+ When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to at least two.

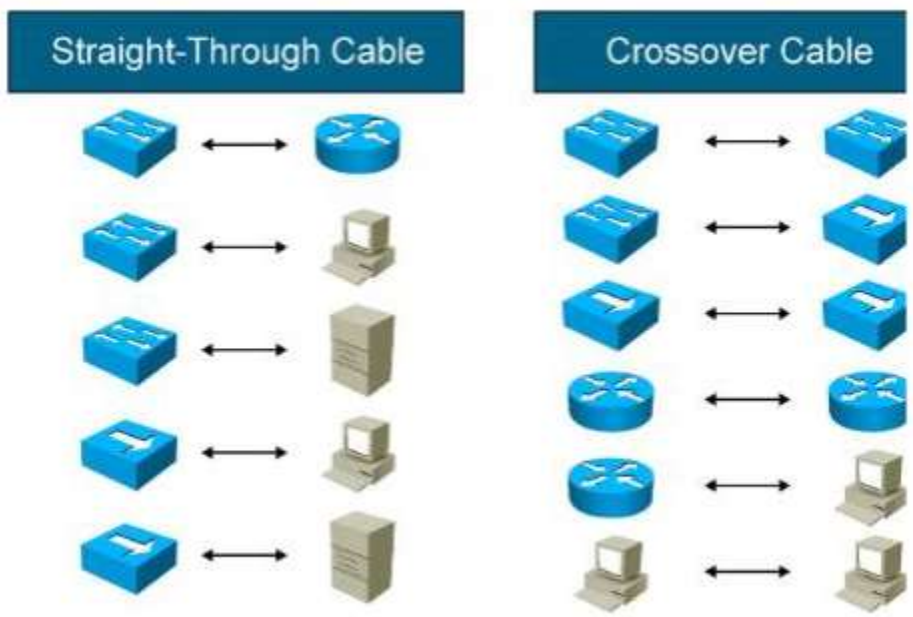
+ If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

+ When a voice VLAN is configured on a secure port that is also configured as a sticky secure port, all addresses seen on the voice VLAN are learned as dynamic secure addresses, and all addresses seen on the access VLAN (to which the port belongs) are learned as sticky secure addresses.

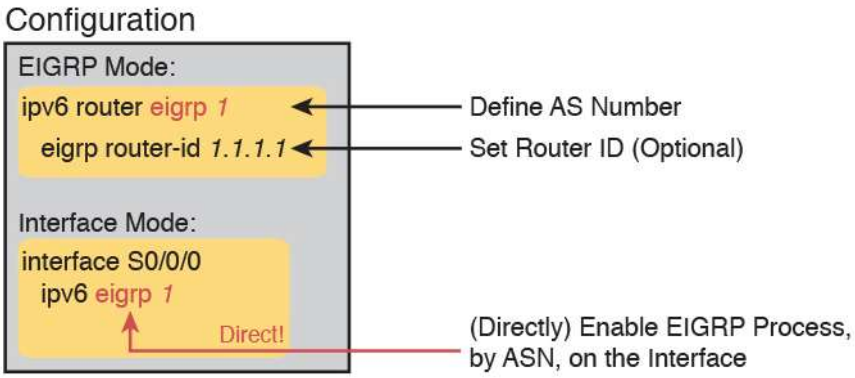
+ The switch does not support port security aging of sticky secure MAC addresses.

+ The protect and restrict options cannot be simultaneously enabled on an interface.

From <http://www.9tut.net/new-updated-questions/new-icnd2v3-questions-part-2>



45-55 questions
90 mins
EIGRPv6



OSPFv3

```
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 mac-address 0200.0000.0002
 ipv6 address 2001:db8:1:23::2/64
 ipv6 ospf 2 area 23
!
interface serial 0/0/1
 ipv6 address 2001:db8:1:12::2/64
 ipv6 ospf 2 area 23
!
ipv6 router ospf 2
 router-id 2.2.2.2
```