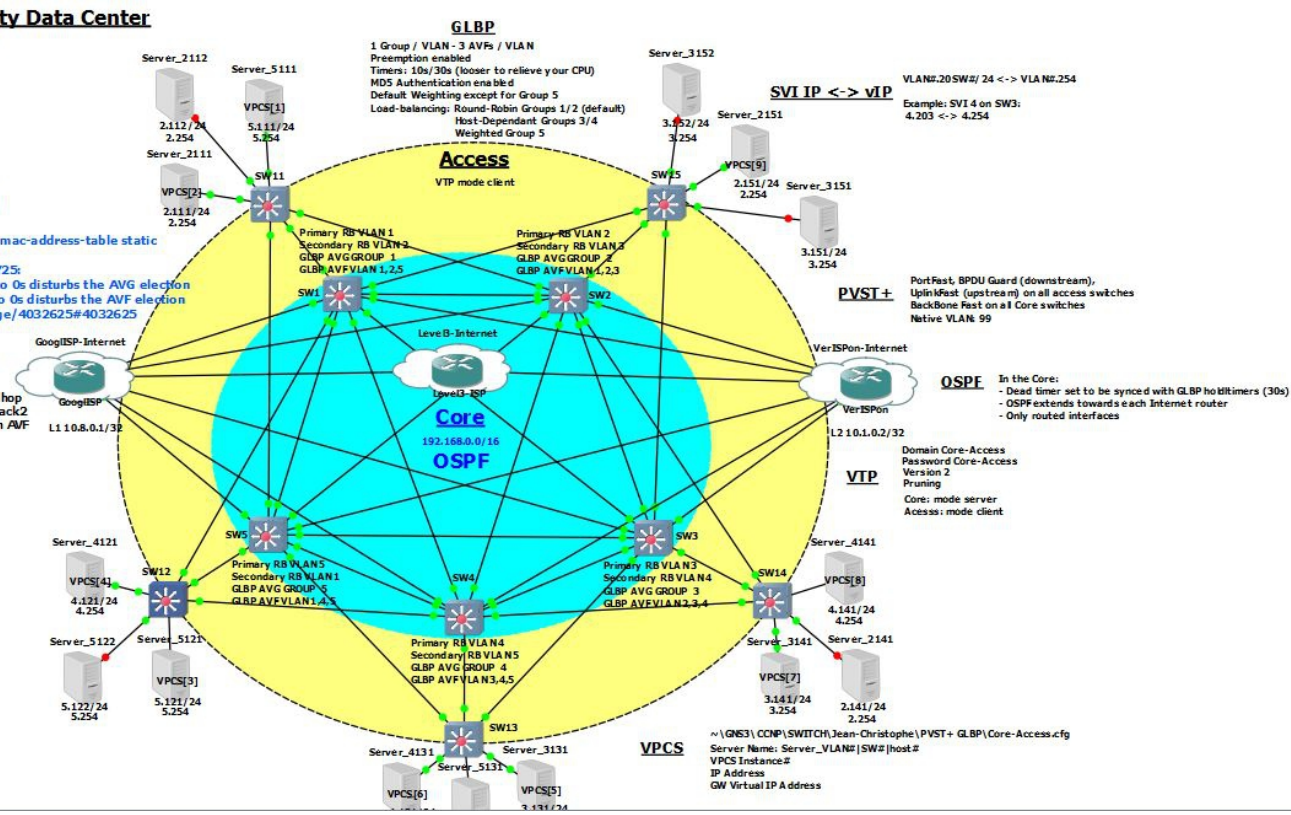
Innovative High-Availability Data Center

GLBP - OSPF

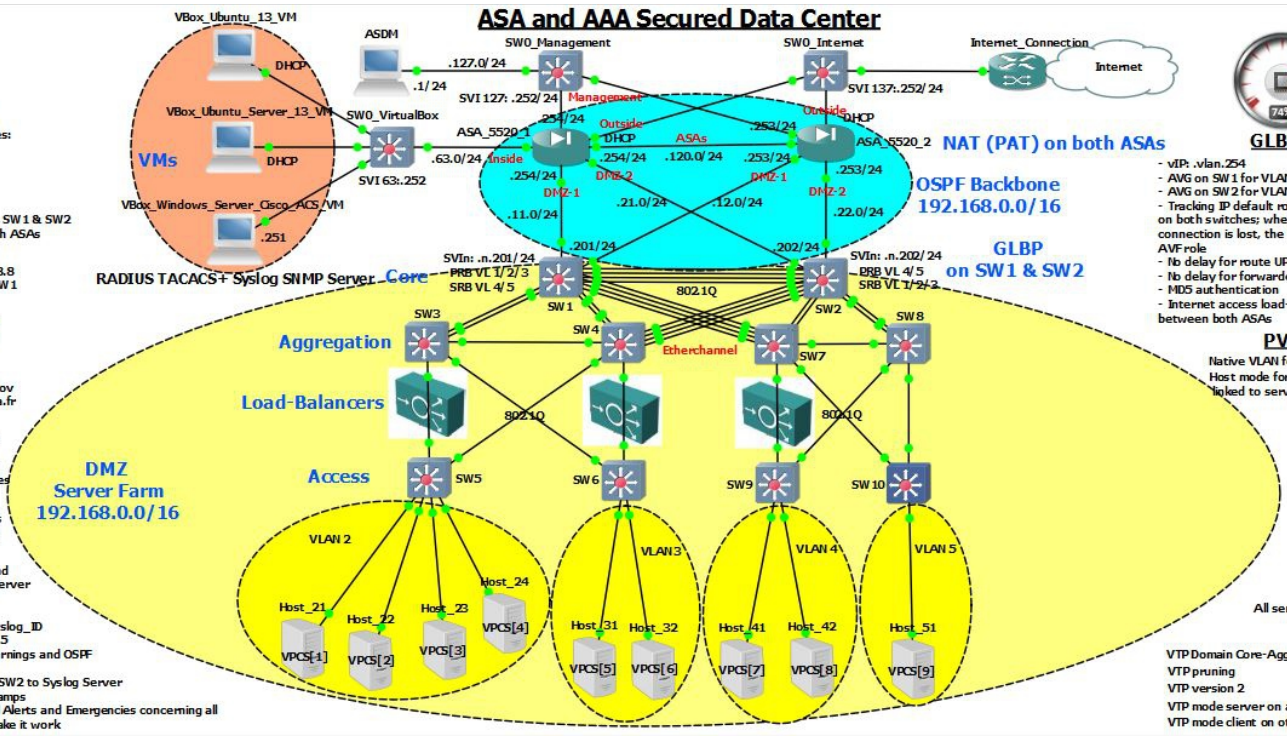


On production networks, GLBP should be implemented on the distribution switches with a L2 link/bundle between them, alongside IP route tracking and the L3 domain should at least include the Core-Distribution links.

To workaround general GLBP Issue: #clear mac-address-table static
Clear the MAC Table regularly !!!
There are 2 bugs with IOS 12.4(15)T5 on 3725:
- setting the minimum AVG preempt delay to 0s disturbs the AVG election
- setting the minimum AVF preempt delay to 0s disturbs the AVF election
cf. https://supportforums.cisco.com/message/4032625#4032625

For each Switch/Router acting as AVF:
- traffic to Internet is load-balanced betweeen both links
- loses its AVF role as soon as it is more than 1 hop away from Internet Routers Loopback1/Loopback2
- other AVF takes over with a 0 s delay when an AVF gives up its role as AVF

ASA and AAA Secured Data Center



Security

Security level of interfaces:
- management: 100
- inside: 100
- ASAs 50
- DMZ-1 and DMZ-2: 50
- outside: 0

SSH access on both ASAs, SW1 & SW2
Identity Certificate on both ASAs

DNS

Primary Server on 8.8.8.8
Secondary Server on SW1

DHCP

DHCP Server on SW1 & SW2
DHCP Relay on ASA-5520-1

NTP

On both ASAs, SW1 & SW2:
Preferred server: time.nist.gov
canon.inria.fr

AAA

- Cisco ACS TACACS+ server (VirtualBox VM) authenticates all ASAs users
- 802.1x on all access switches

NAT

Static Auto-NAT for the VMs and all VLANs on both ASAs

SNMP

All Traps from both ASAs and SW1 & SW2 sent to SNMP Server

Logging

- Modified severity level of Syslog_ID messages: 711004 from 4 to 5
- Logging Filters to ASDM: Warnings and OSPF notifications
- Logging Errors from SW1 & SW2 to Syslog Server (Cisco_ACS_VM) with timestamps
- Alert Admin by e-mail for all Alerts and Emergencies concerning all event Classes - Unable to make it work

GLBP

- vIP: .vlan.254
- AVG on SW1 for VLANs 2/3
- AVG on SW2 for VLANs 4/5
- Tracking IP default route to Internet on both switches: when Internet connection is lost, the switch loses its AVF role
- No delay for route UP/DOWN detection
- No delay for forwarder preemption
- MD5 authentication
- Internet access load-balanced between both ASAs

PVST+

Native VLAN for all Switchs: 99
Host mode for all Access ports linked to servers

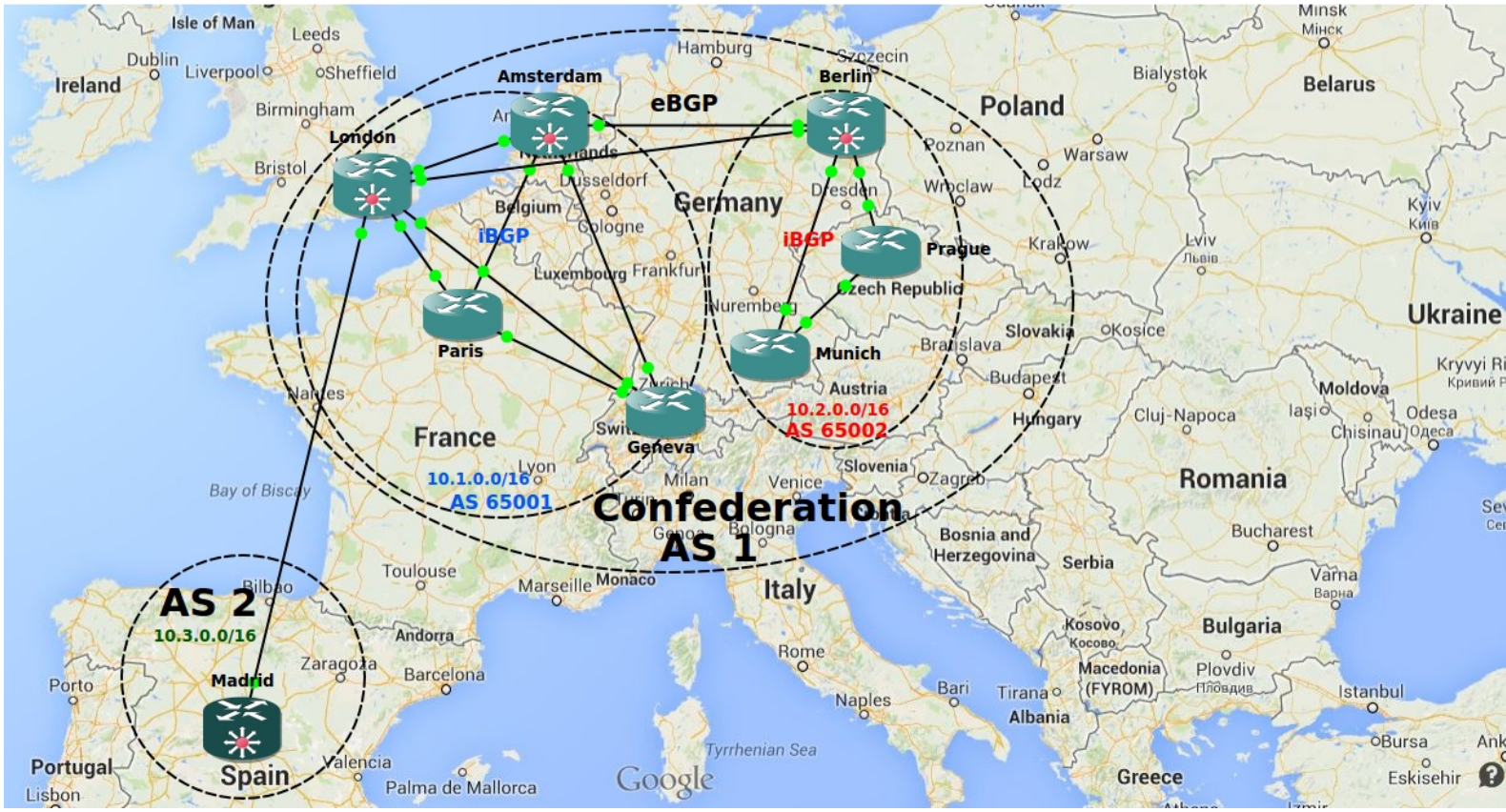
VPCS

Servers.cfg
All servers: DHCPv4/v6

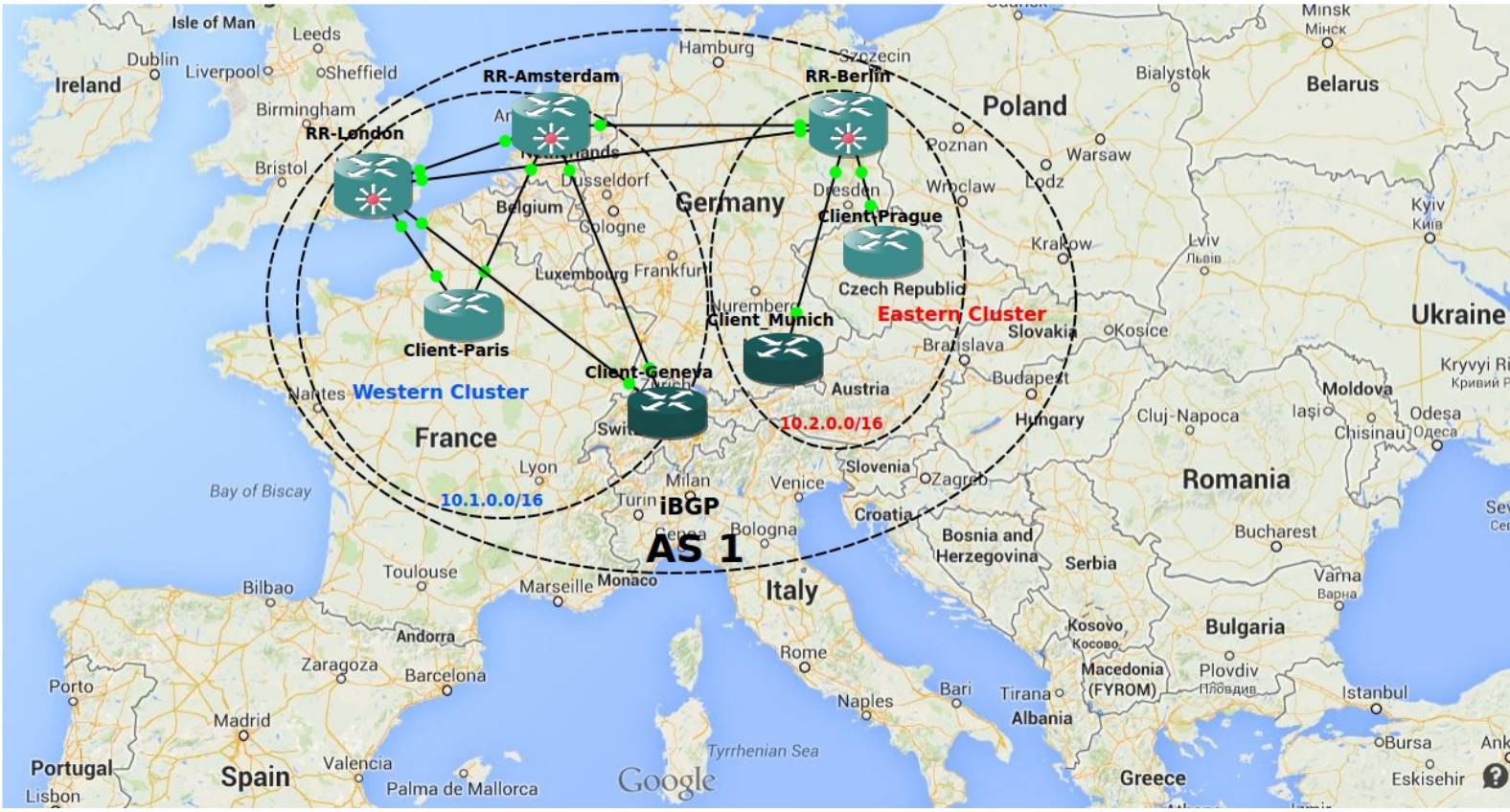
VTP

VTP Domain Core-Aggregation-Access
VTP pruning
VTP version 2
VTP mode server on all core switches
VTP mode client on other switches

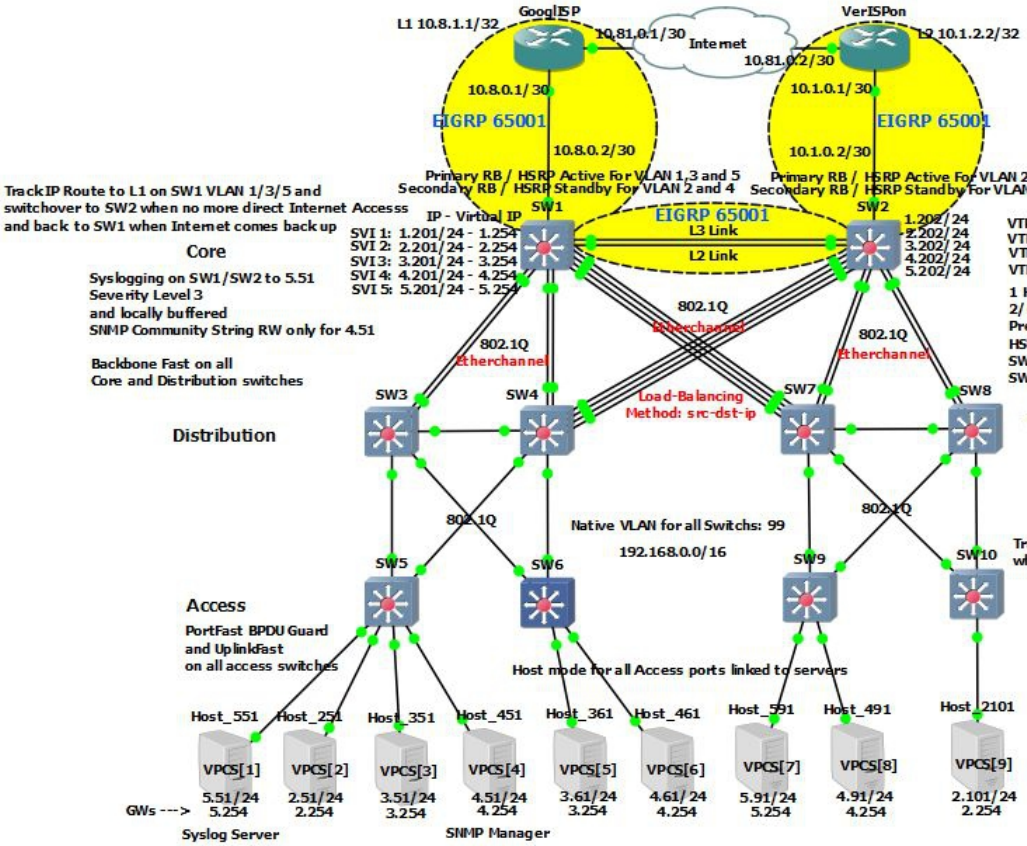
BGP Confederation



BGP Route Reflectors



Highly Available Campus Network
HSRP - EtherChannel



Track IP Route to L1 on SW1 VLAN 1/3/5 and switchover to SW2 when no more direct Internet Accesss and back to SW1 when Internet comes back up

Core

Syslogging on SW1/SW2 to 5.51
Severity Level 3
and locally buffered
SNMP Community String RW only for 4.51

Backbone Fast on all
Core and Distribution switches

EIGRP Hold timer set to be synced with HSRP Hold timer (6s)
PVST+ forward-delay and max-age timers set so the convergence time is synced with HSRP and EIGRP hold timers

Track IP Route to L2 on SW2 VLAN 2/4 and switchover to SW1 when no more direct Internet Access and back to SW2 when Internet comes back up

VTP Domain Core-Distribution-Access
VTP mode server
VTP version 2
VTP pruning

To workaround GNS3 HSRP Issue:
#clear mac-address-table static

1 HSRP Group / VLAN
2/6 sec for HSRP timers
Preemption enabled with 6s min delay on Primary RBs
HSRP MD5 Authentication enabled
SW1-SW2 L3 Link for IGP alternate path
SW1-SW2 L2 Trunk for HSRP synchronization (out of EIGRP AS)

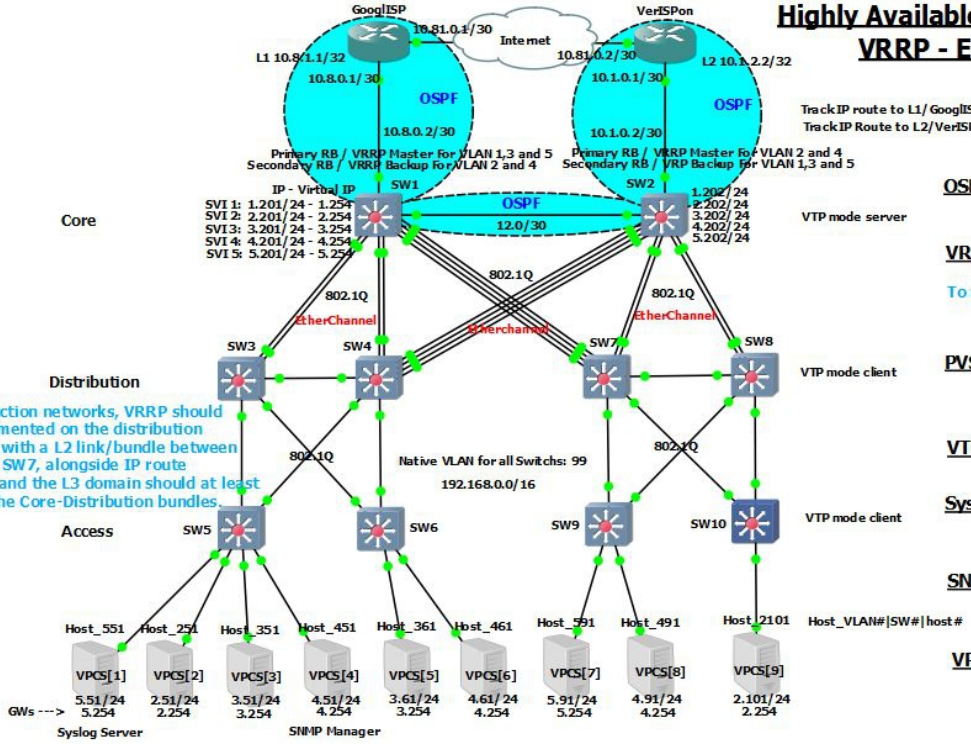
On production networks, HSRP should be implemented on the distribution switches with a L2 link/bundle between SW4 and SW7, alongside IP route tracking and the L3 domain should at least include the Core-Distribution bundles.

Track the RTT server 2.51 and send an SNMP trap to SNMP Manager when RTT is above 500 ms threshold or if one server is not responding

Host_VLAN#|SW#|host#
All Access ports: portfast

VPCS Config:
~\GNS3\CCNP\SWITCH\Jean-Christophe\PVST+ EtherChannel HSRP\Core-Distribution-Access.cfg

Highly Available Campus Network
VRRP - EtherChannel



Core

Distribution

On production networks, VRRP should be implemented on the distribution switches with a L2 link/bundle between SW4 and SW7, alongside IP route tracking and the L3 domain should at least include the Core-Distribution bundles.

Access

Tracking Objects

Track IP route to L1/GoogIISP on SW1 VLAN 1/3/5 and switchover to SW2 when no more direct Internet Accesss
Track IP Route to L2/VerISPon on SW2 VLAN 2/4 and switchover to SW1 when no more direct Internet Access

OSPF OSPF Dead timer set to be synced with VRRP Master Down Interval (6s)

VRRP
1 VRRP Group / VLAN
Advertisement timer 2s
Preemption enabled with 6s min delay on Primary RBs
MD5 Authentication enabled

To workaround VRRP Issue: #clear mac-address-table static

PVST+
BackboneFast on all Core and Distribution Switches
Forward-delay and max-age timers set so the convergence time is synced with OSPF and VRRP timers
PortFast BPDU Guard and UplinkFast on all access switches
Host mode for all Access ports linked to servers

VTP
Domain Core-Distribution-Access
Version 2
Pruning

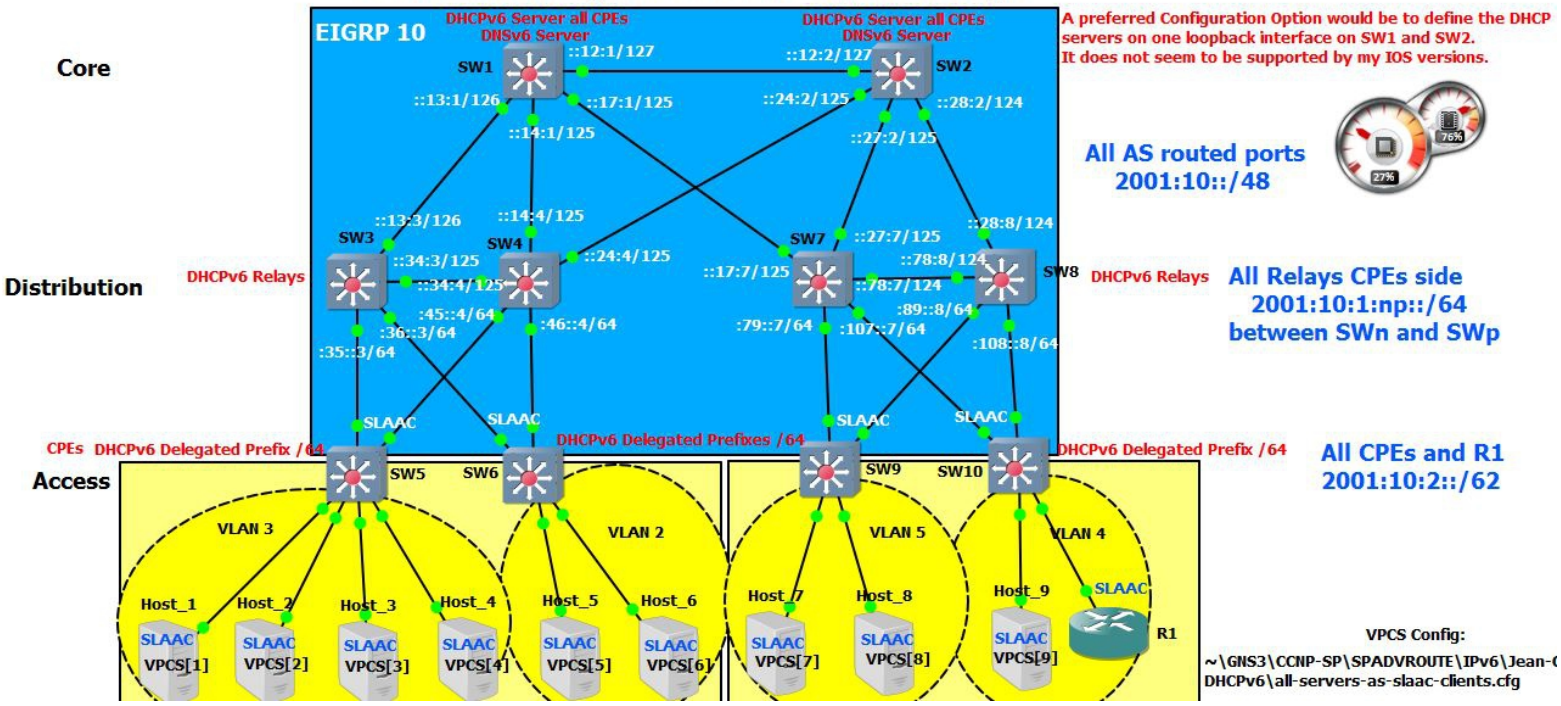
SysLog On SW1 & SW2
Syslogging to 5.51
Severity Level 3
and locally buffered

SNMP On SW1 & SW2
Send traps to 2.51
Version 3 with Security Level authPriv
with one username
Enable VRRP Traps

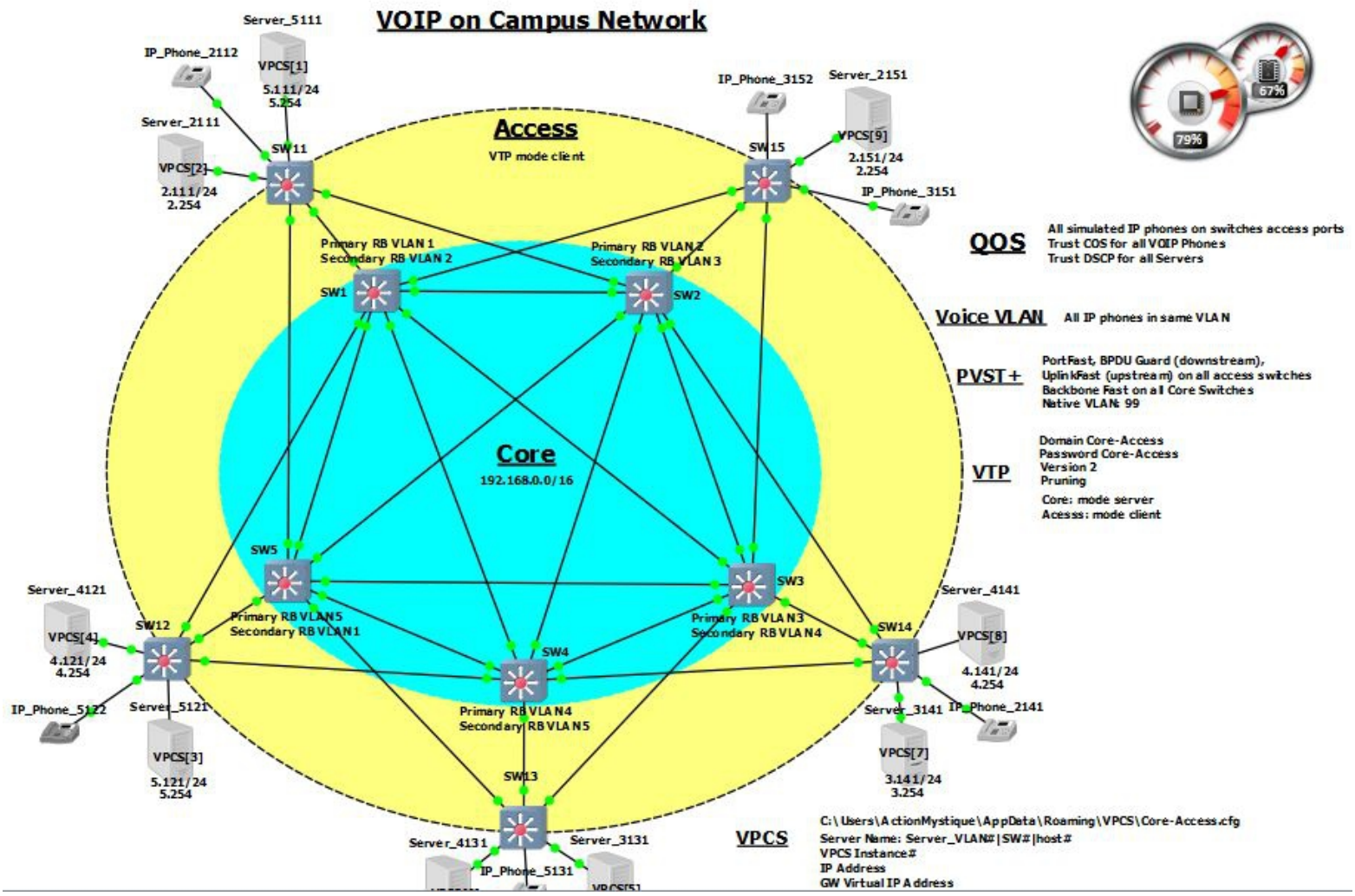
Host_VLAN#|SW#|host#

VPCS ~\GNS3\CCNP\SWITCH\Jean-Christophe\PVST+ EtherChannel VRRP\Core-Distribution-Access.cfg

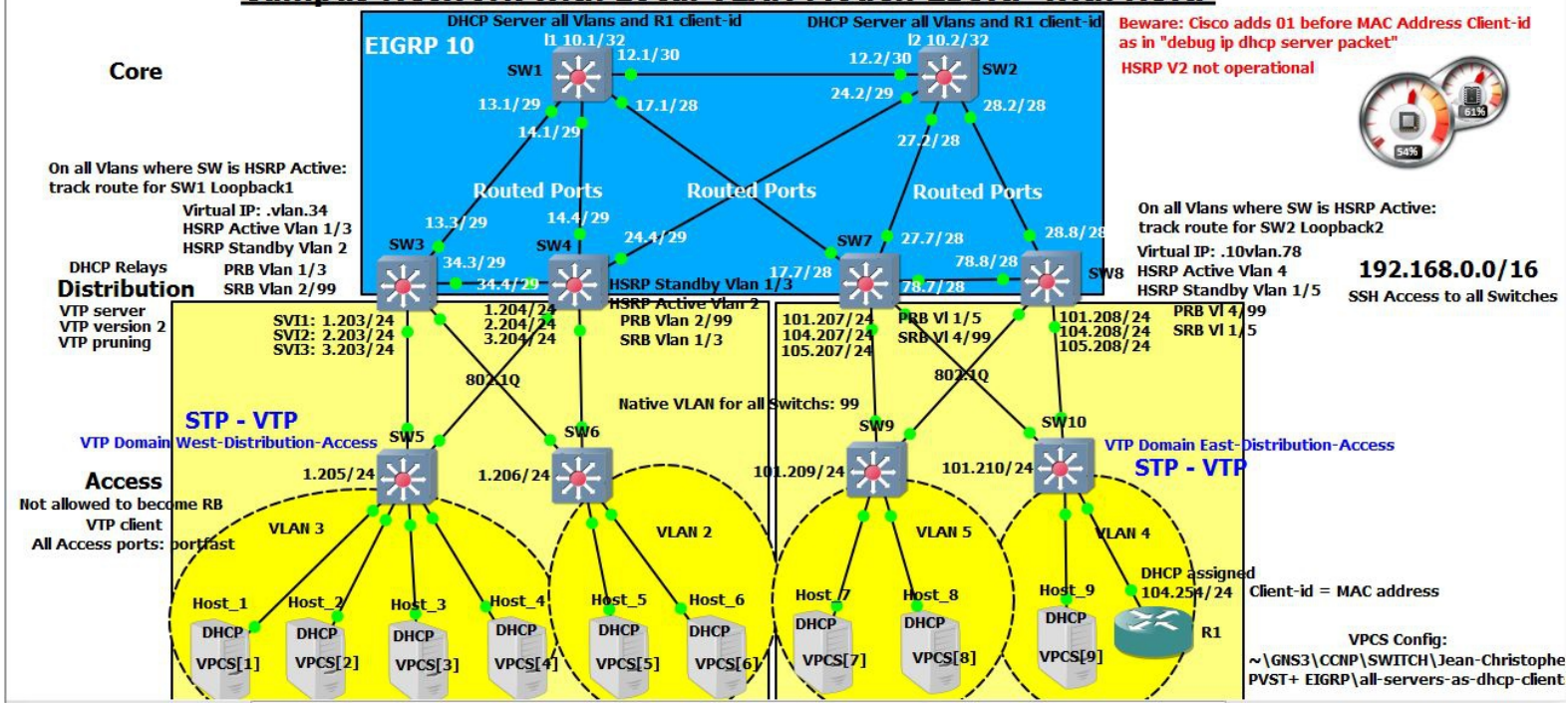
DHCPv6 Delegated Prefixes with Relays



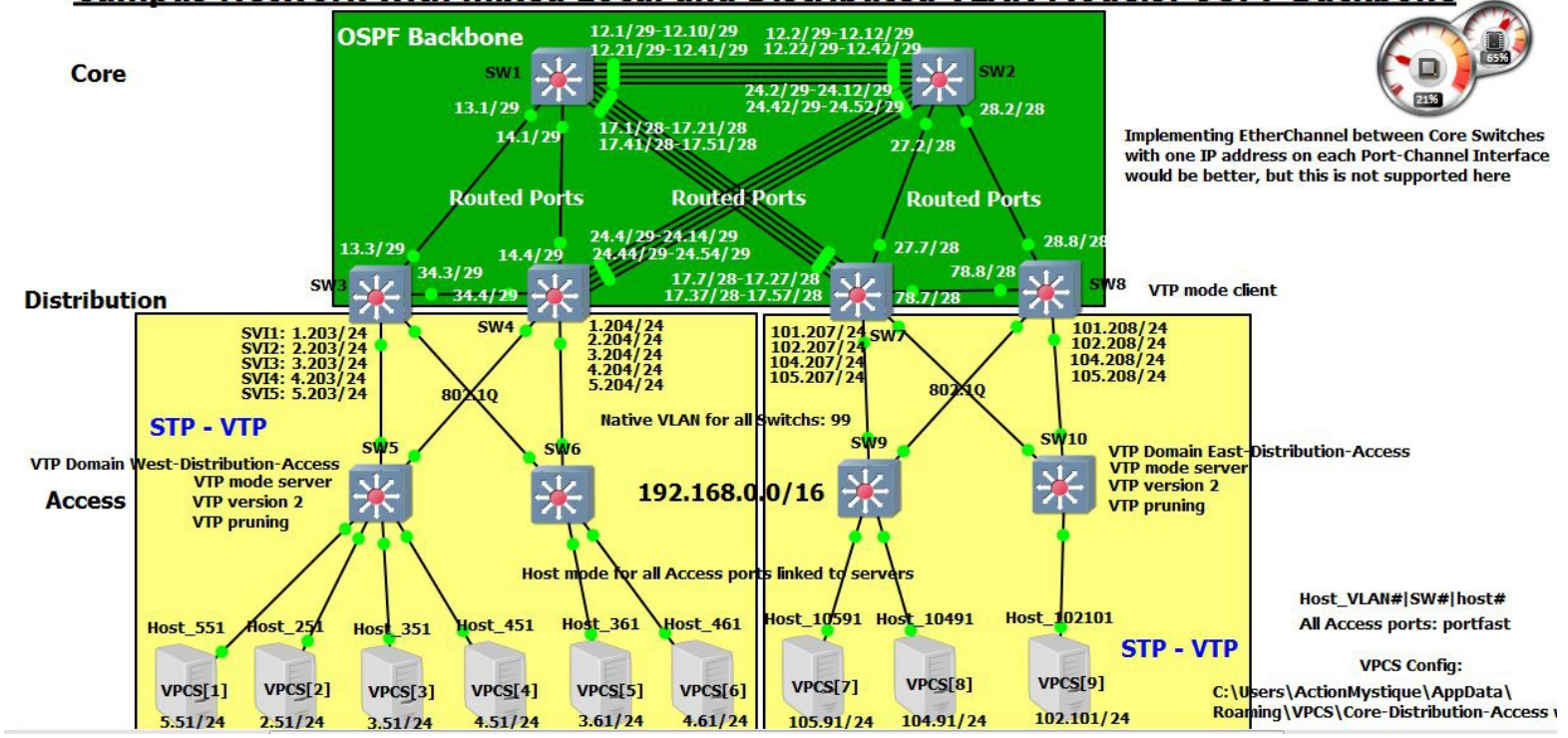
VOIP on Campus Network



Campus Network with Local VLAN Model: EIGRP with HSRP

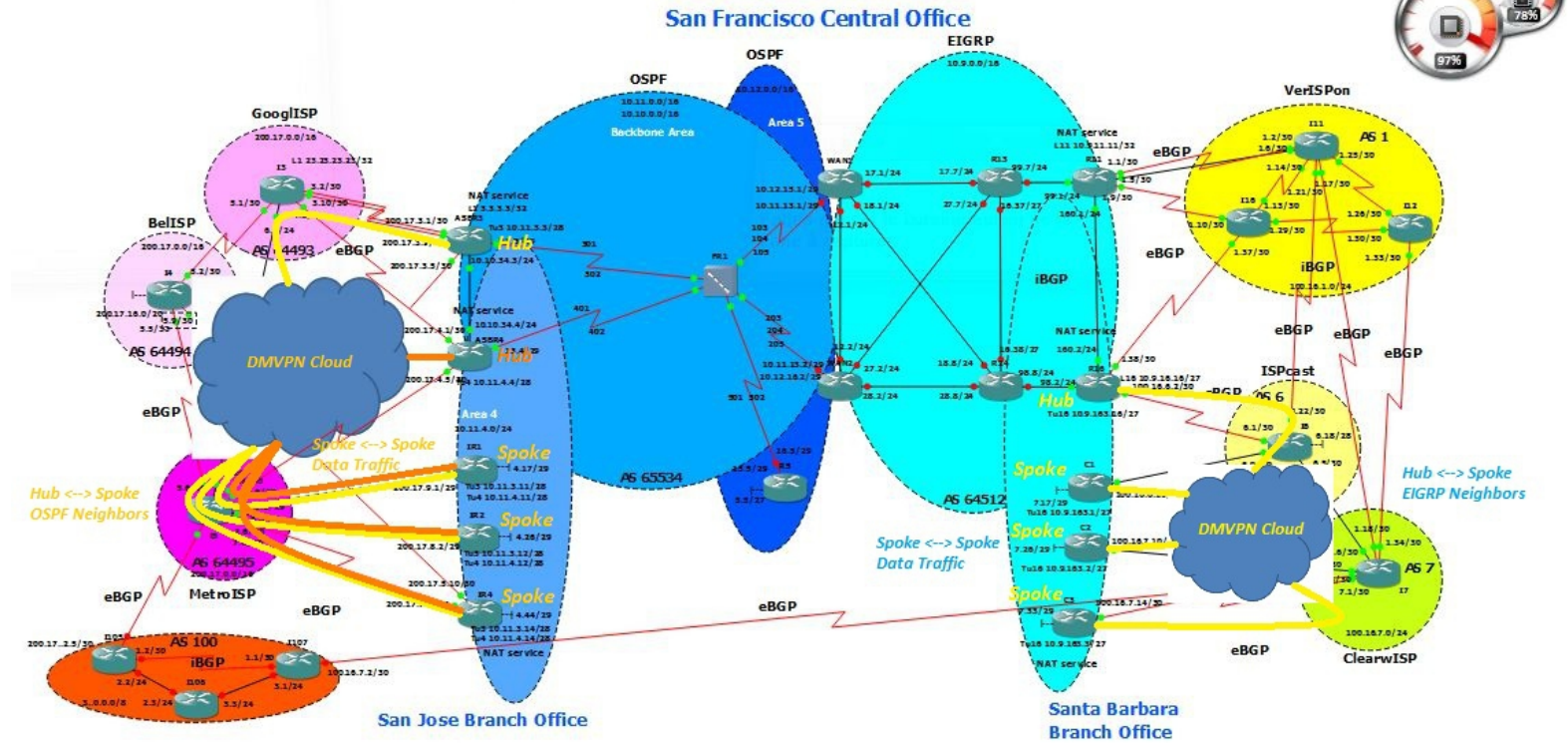


Campus Network with mixed Local and Distributed VLAN Models: OSPF Backbone



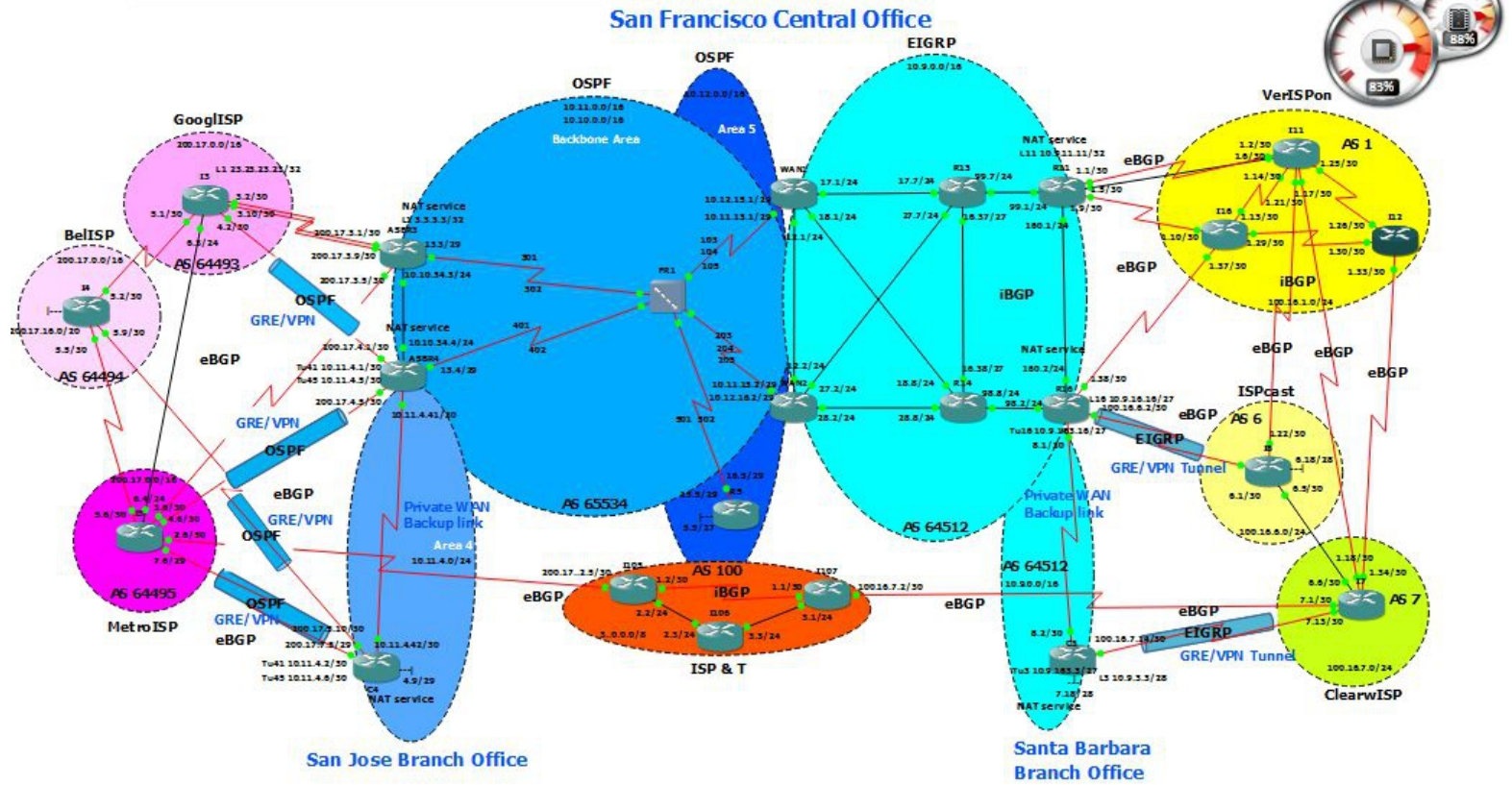
Securing communications between Dual Muti-homed Core Enterprise network and Remote Branch Offices

Redundant DMVPN Tunnels (phase II): mGRE over IPsec with NHRP **BGP with EIGRP and OSPF**



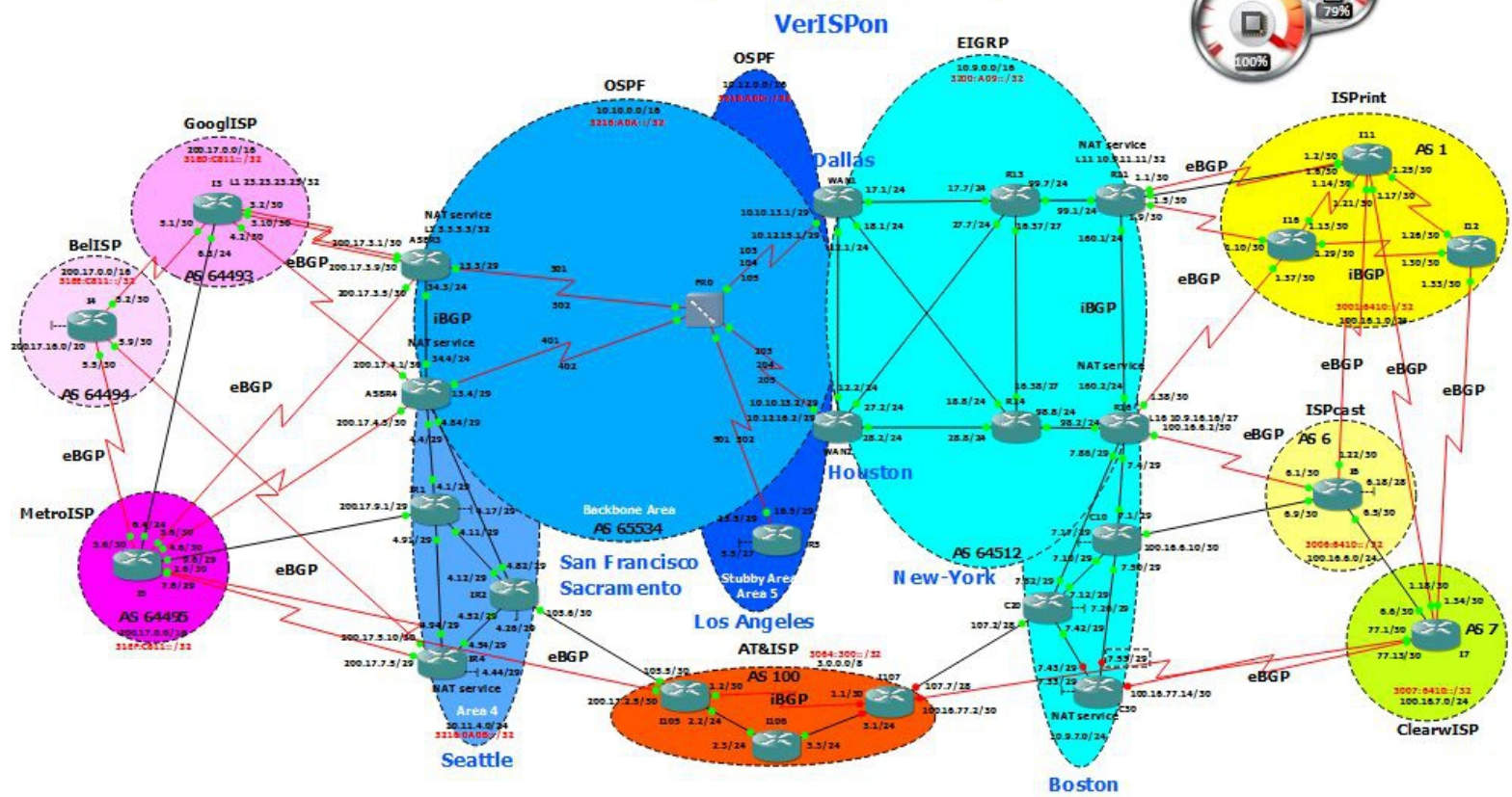
Securing communications between Dual Muti-homed Core Enterprise network and Remote Branch Offices

Double VPN Tunnels : GRE over IPsec **BGP with EIGRP and OSPF**

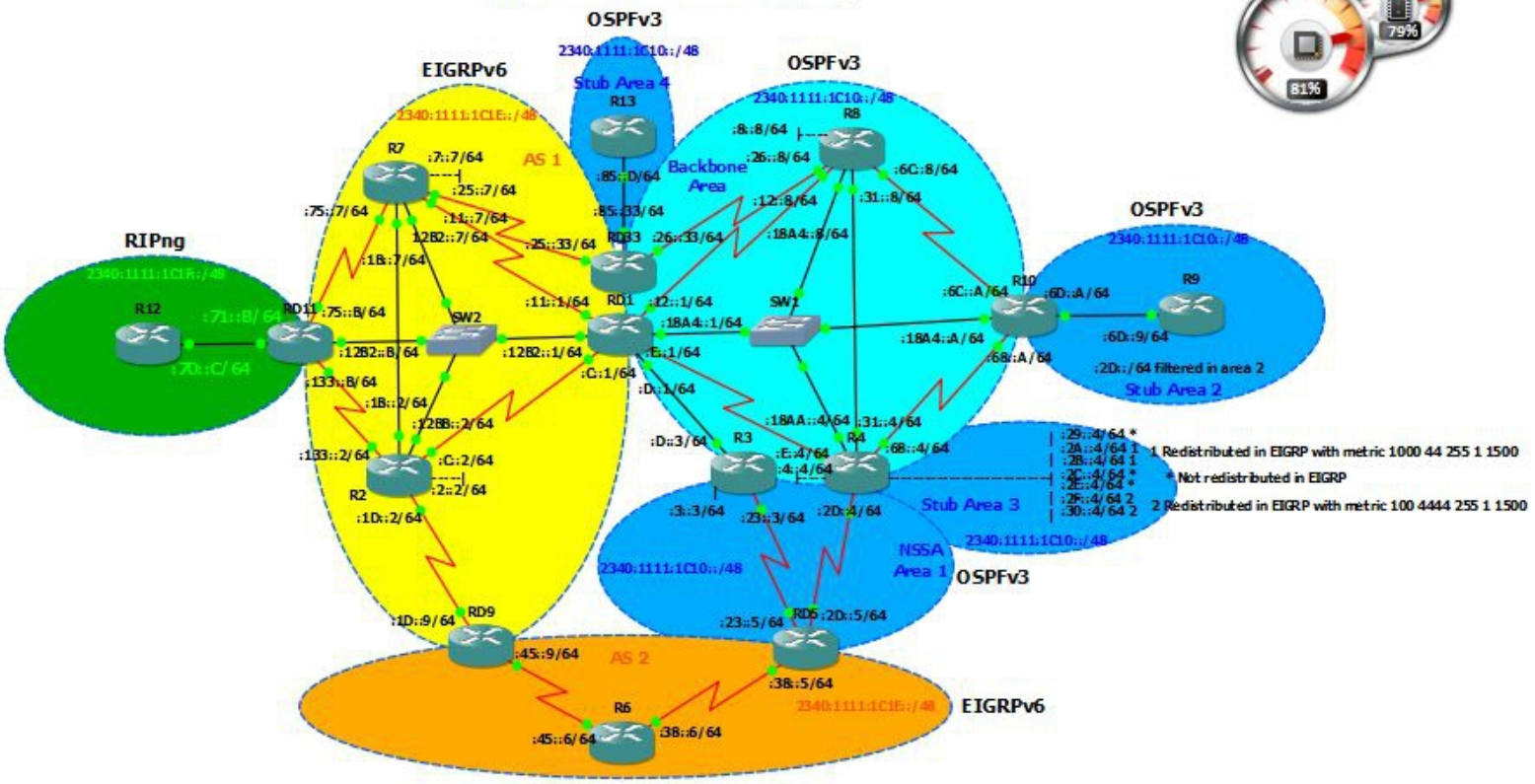


Interconnected ISP Networks

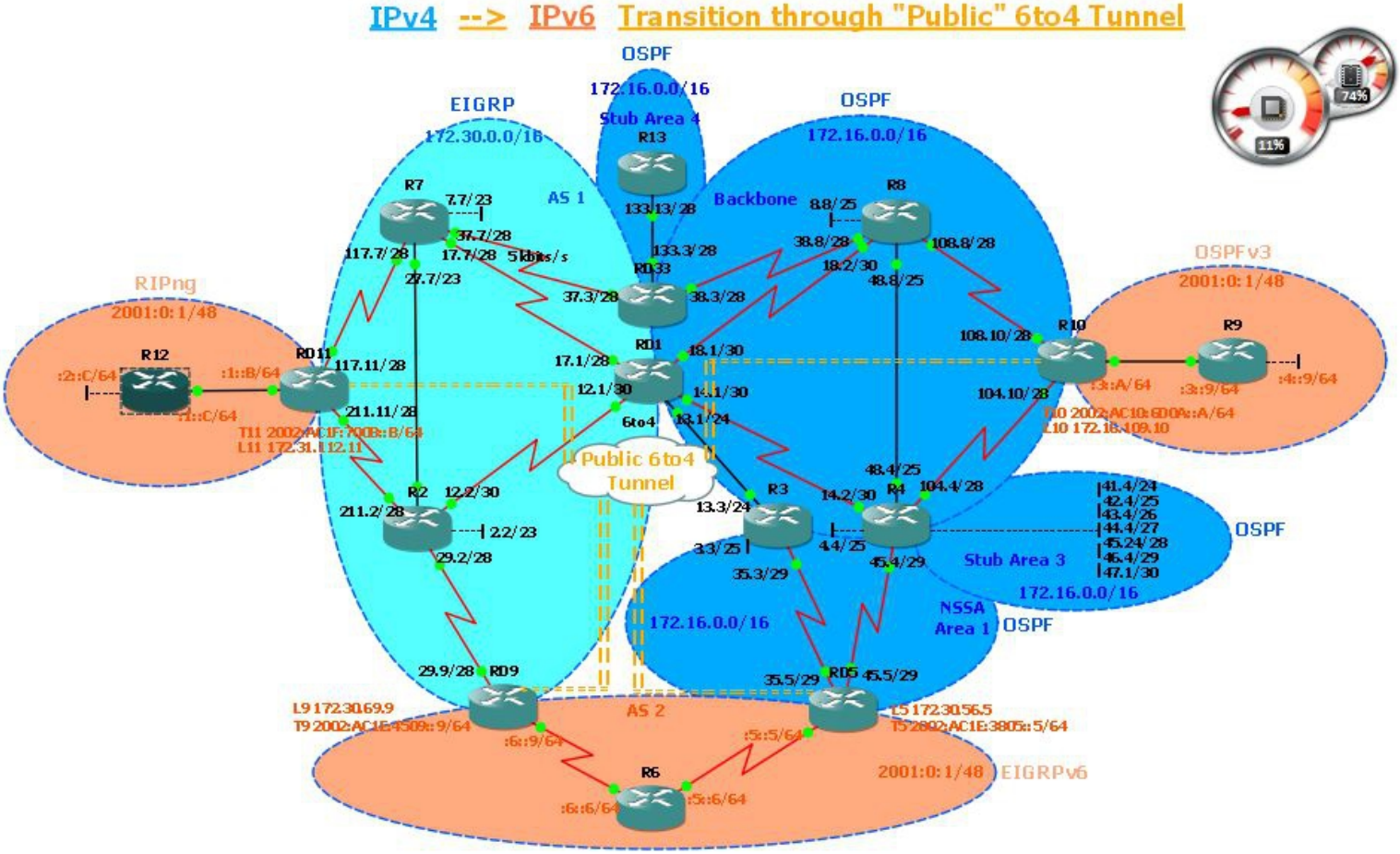
BGP - EIGRP - OSPF over IPv4 and IPv6



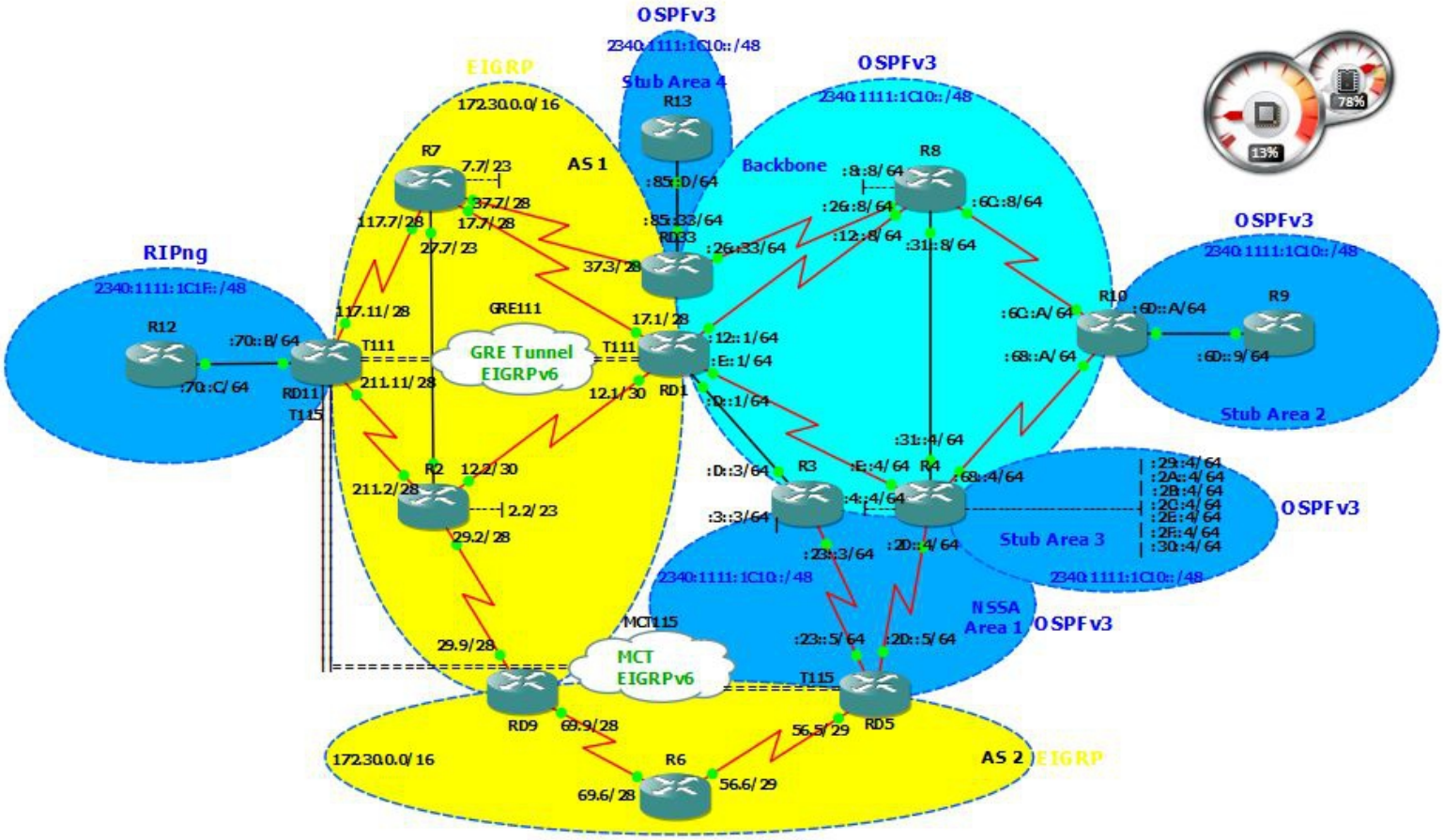
IPv6 Routing Protocols : EIGRPv6, OSPFv3 and RIPng Redistribution and Filtering



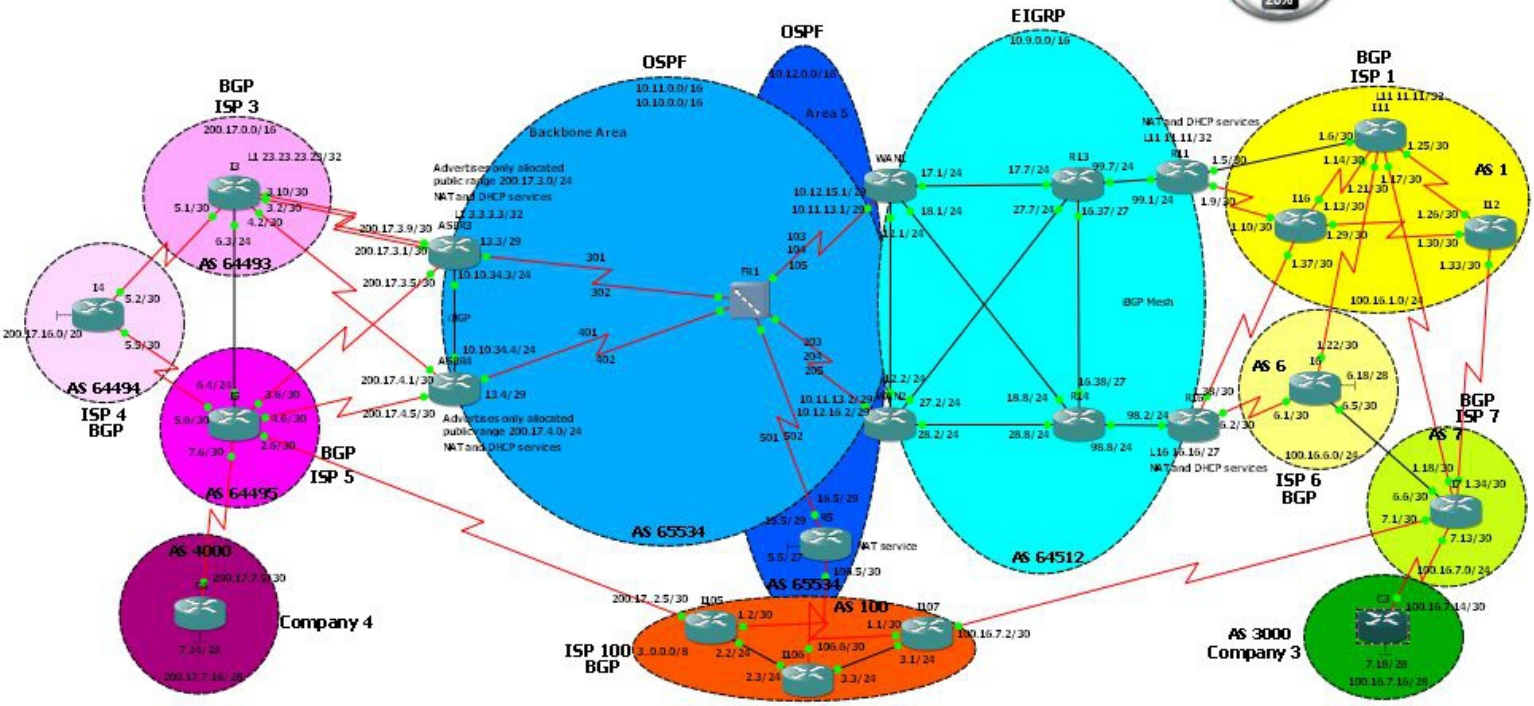
IPv4 --> IPv6 Transition through "Public" 6to4 Tunnel



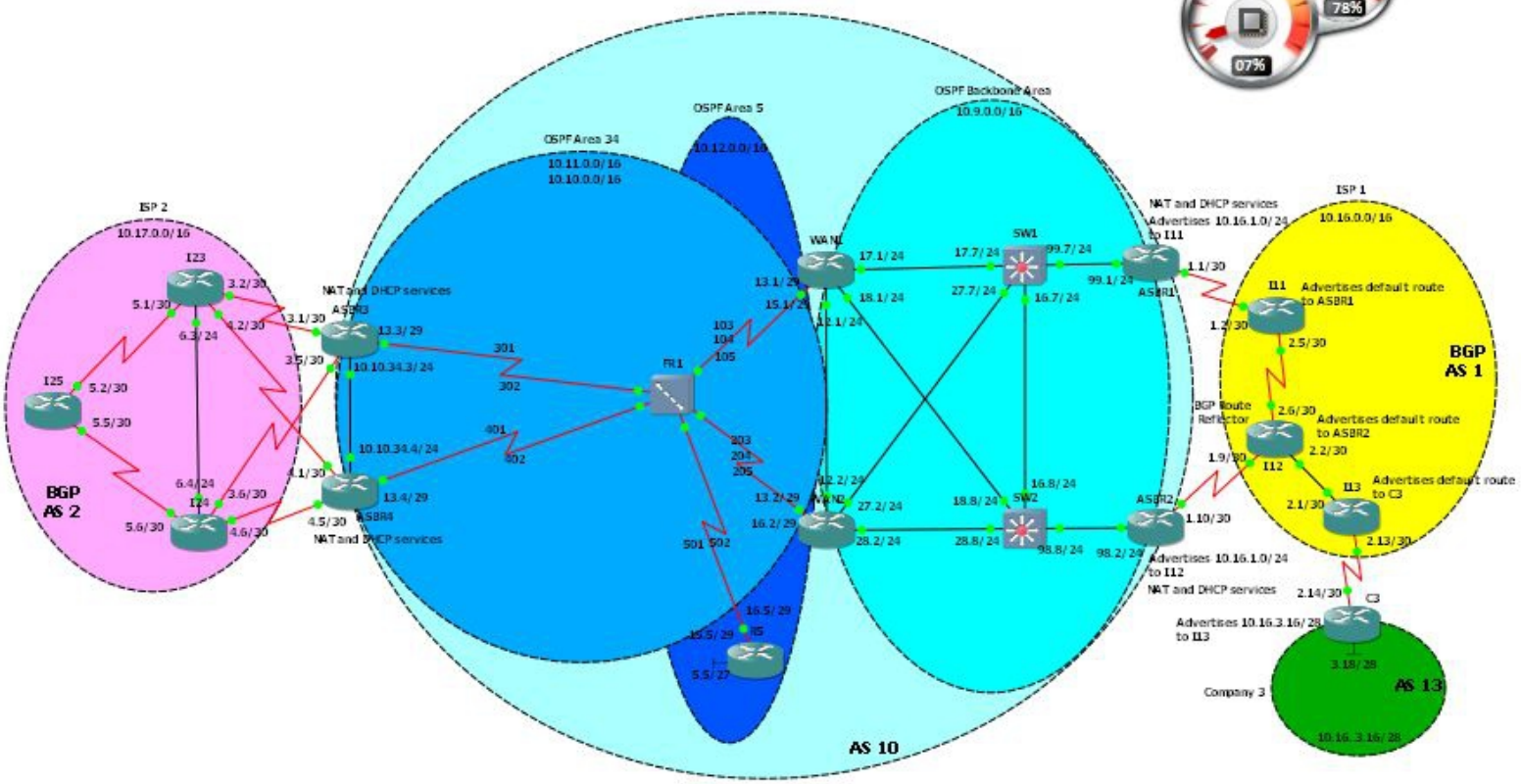
IPv4 --> IPv6 Transition through Static Tunnels



Multiple AS BGP - EIGRP - OSPF

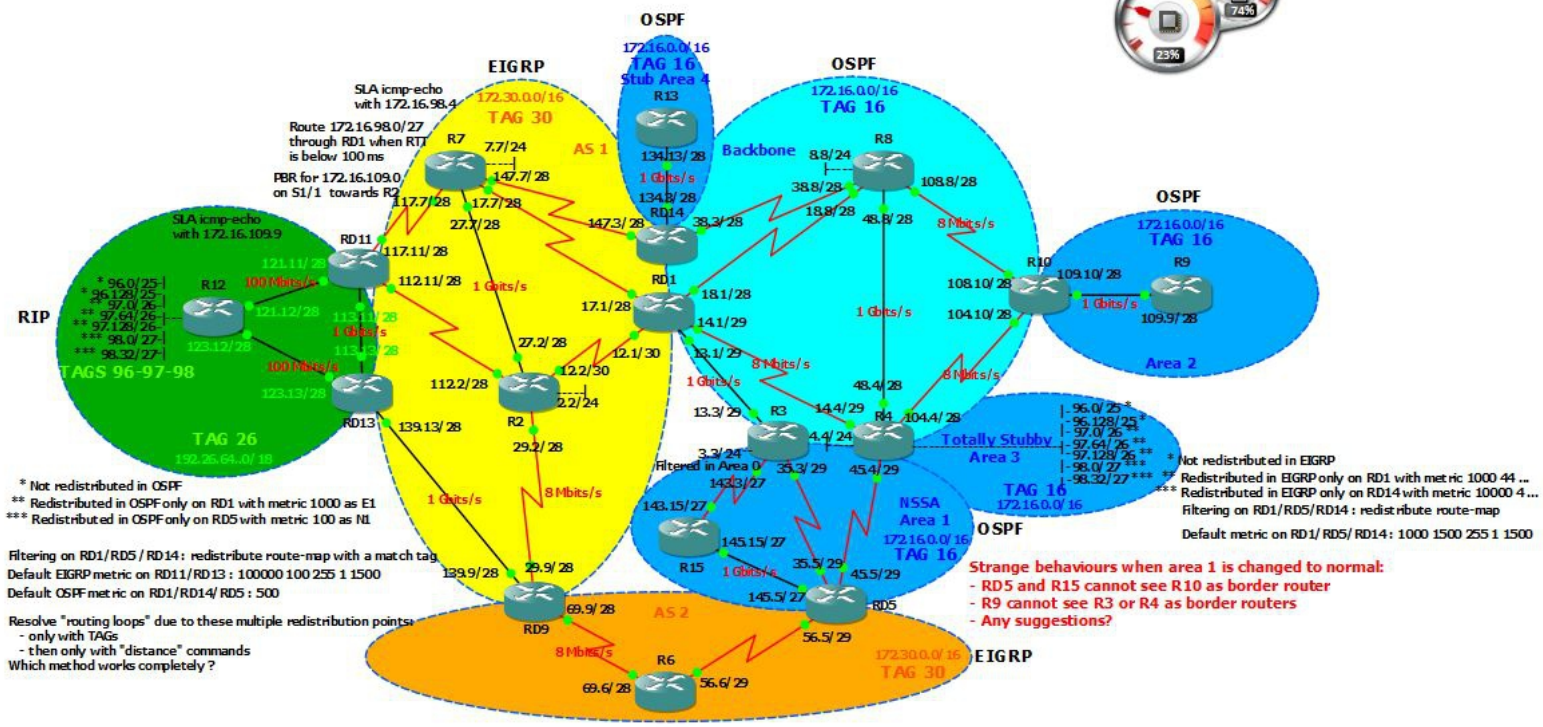


BGP with multiple OSPF Areas



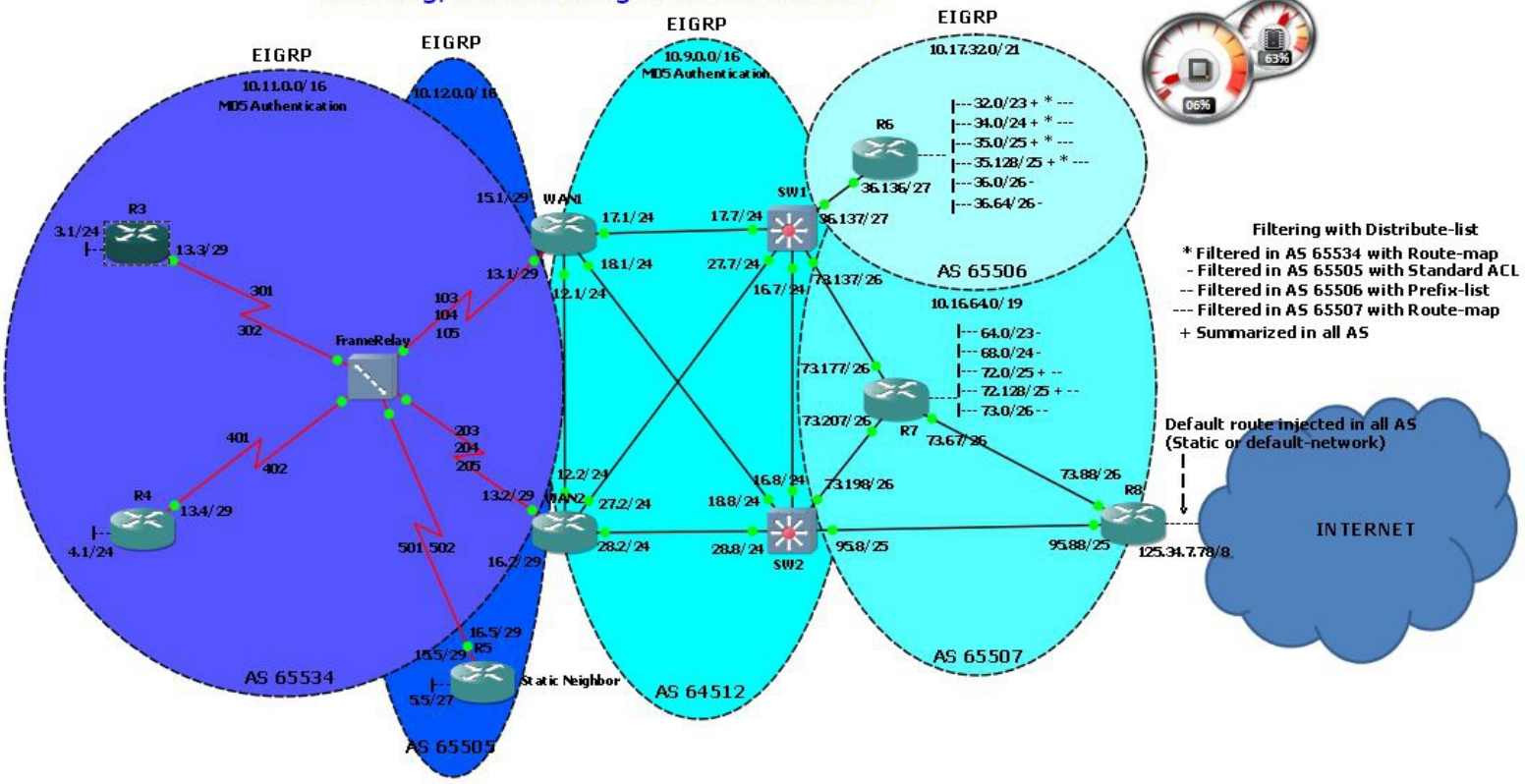
IPv4 Routing Protocols : EIGRP, OSPF and RIP

Redistribution, Filtering, PBR and SLA

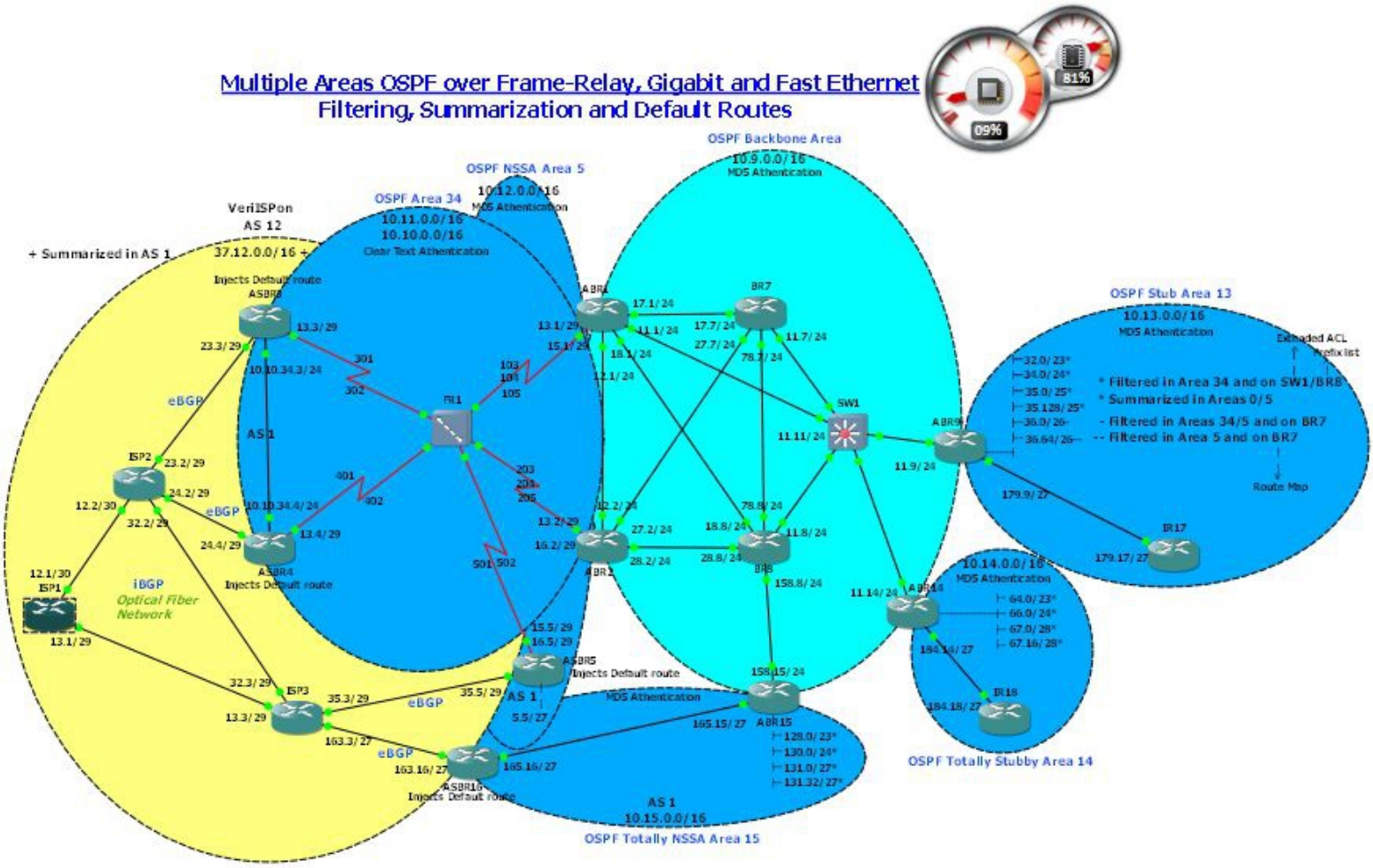
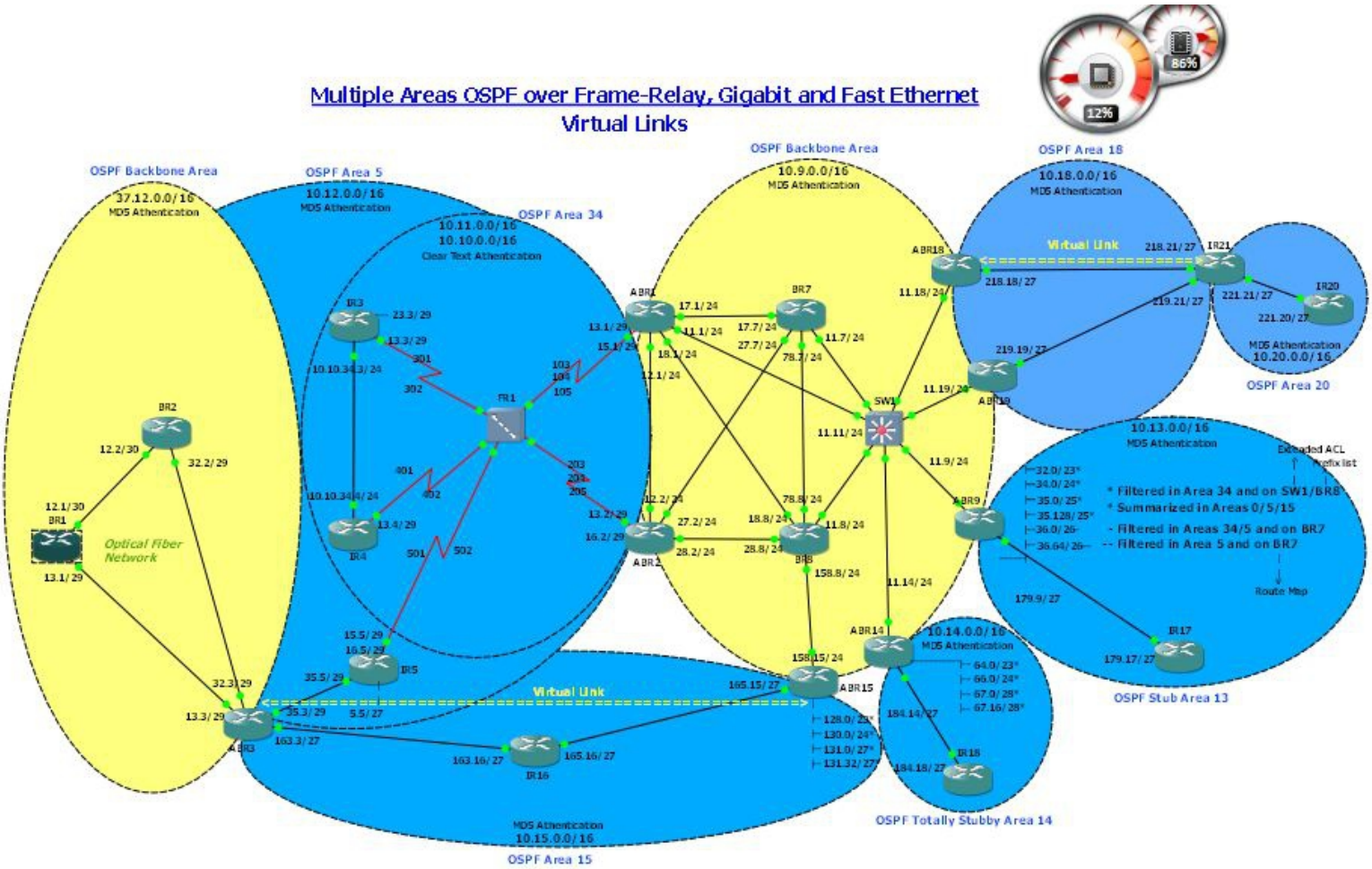


Multiple AS EIGRP over Frame-Relay, Gigabit Ethernet and Fast Ethernet

Filtering, Summarizing and Default route



Multiple Areas OSPF over Frame-Relay, Gigabit and Fast Ethernet
Filtering, Summarization and Default Routes



Multiple Areas OSPF over Frame-Relay, Gigabit and Fast Ethernet
Virtual Links