CNVT 1830
Case Study

GRE Tunnel
10.105.0.0/30
Use Static Routing to
and from R4

ISP

200.0.0.1/30

R4
G0/0/1
.2

G0/0/1
.1   .2   G0/0/0

S0/0/1
.1   .1   S0/0/0

.254
G0/0/0

140.69.212.0/30
S0/0/0

NAT / PAT

64.27.3.0/30
S0/0/0

**Static Routing to R1
and R2 via GRE
Tunnel**

R3
G0/0/1
.2   **OSPF 10 Area 51**   G0/0/1
.1

.6

10.200.0.0 /30

.2   ← **HSRP** →   .2   **R2**

SW5

G0/0/0
.254

R1   G0/0/0

SW4

G0/0/0

SW1   G1/0/1   **LACP**   G1/0/1   **SW2**

VLAN 10

OSPF 10 Area 51

.1

.1

VLAN 10

VLAN 20

OSPF 10 Area 0

VLAN 20

10.101.0.0 /24

10.102.0.0 /24

VLAN 30

SW3

VLAN 30

PagP

ON

VLAN 10   VLAN 20   VLAN 30

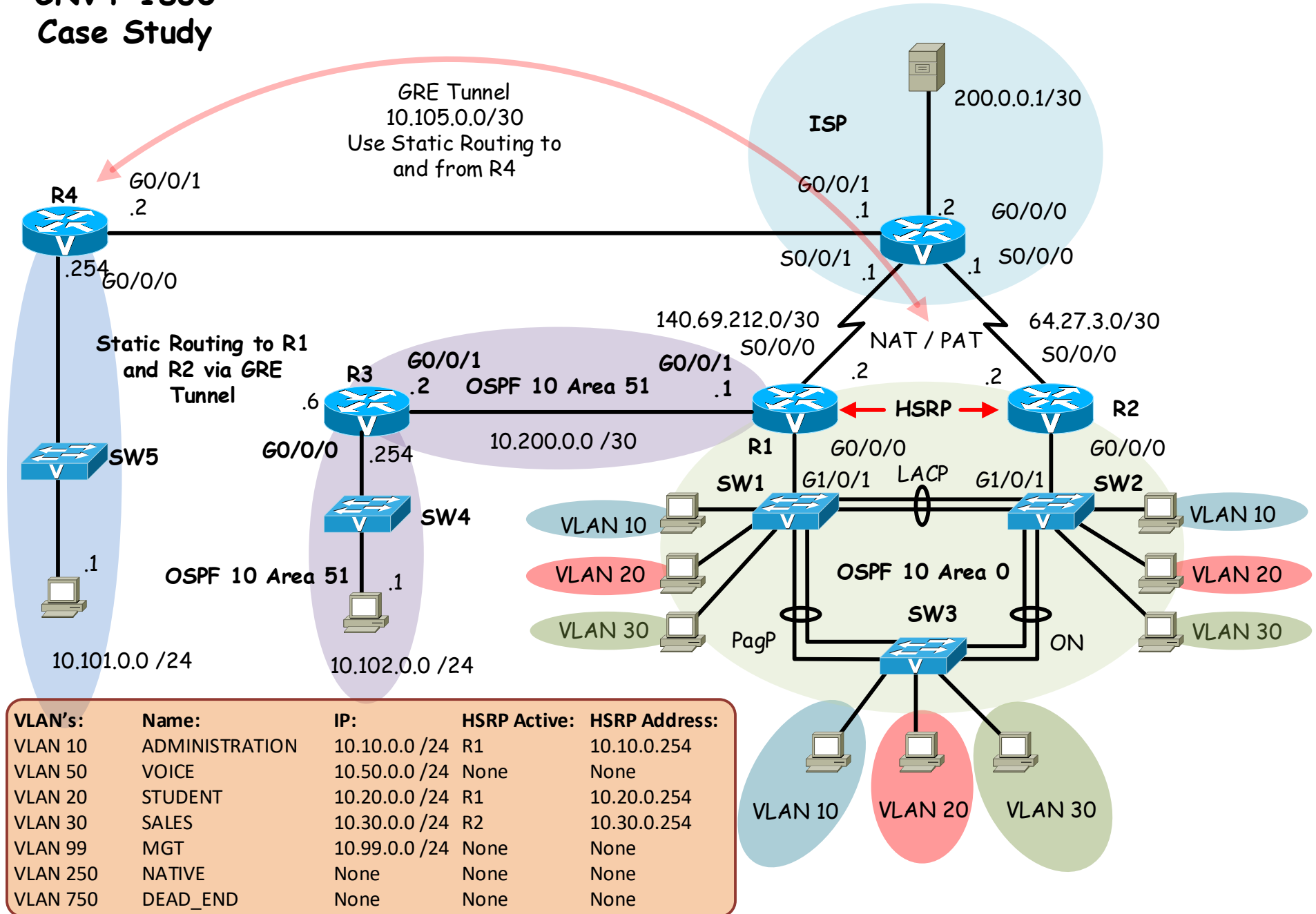| VLAN's:	Name:	IP:	HSRP Active:	HSRP Address:
VLAN 10	ADMINISTRATION	10.10.0.0 /24	R1	10.10.0.254
VLAN 50	VOICE	10.50.0.0 /24	None	None
VLAN 20	STUDENT	10.20.0.0 /24	R1	10.20.0.254
VLAN 30	SALES	10.30.0.0 /24	R2	10.30.0.254
VLAN 99	MGT	10.99.0.0 /24	None	None
VLAN 250	NATIVE	None	None	None
VLAN 750	DEAD_END	None	None	None

Notes:
R1 OSPF:
Designated Router for:
VLAN's 10, 20
Backup Designated Router for:
VLAN's 30, 99
R2 OSPF:
Designated Router for:
VLAN's 30, 99
Backup Designated Router for:
VLAN's 10, 20

Ether-Channel SW1 – SW2:
SW1 Ports G1/0/2-3
SW2 Ports G1/0/2-3
LACP
Ether-Channel SW1 – SW3:
SW1 Ports G1/0/4-5
SW3 Ports G1/0/2-3
PagP

Ether-Channel SW2 – SW3:
SW2 Ports G1/0/4-5
SW3 Ports G1/0/4-5
ON

1. All traffic from the 10.101.0.0/24 network will return to the central network by the GRE VPN tunnel of 10.105.0.0/30 network address space via static routing.
2. All traffic going to the 10.101.0.0/24 network will use static routing over the GRE VPN and be redistributed within the OSPF routers,
3. All traffic leaving the network will exit via the HSRP virtual interfaces.
4. R1 will be the Active Router for HSRP as well as the OSPF Designated Router for VLAN's 10 and 20, R2 will be the HSRP Backup.
5. R2 will be the Active Router for HSRP as well as the OSPF Designated Router for VLAN's 30 and 99, R1 will be the HSRP Backup.
6. Ether-Channel will be configured according to the chart above.
7. All Access ports should be set to protect Spanning-Tree and unused ports should be disabled and placed into VLAN 750.
8. All other security measures applicable, should be applied to all Access ports.
9. Access Control Lists should be places on all routers to protect against outside attacks as well as limit remote access to SSH and/or CDP

10. All traffic should use NAT/PAT to external addresses assigned by your company from the IANA IPv4 address space of 175.44.2.0/29

11. Use the 175.44.2.1 address as the static NAT address for the 10.102.0.1 Web server including PAT.

12. Reserve three (3) addresses for future expansion.

13. All access addresses except for the Web server should be via DHCP with a domain of jmowry.com, a lease of three (3) days, and DNS of 8.8.8.8 and 8.8.4.4.

14. Each group will present their solution via PowerPoint, as well as a printed copy of all configurations and any additional relevant material. The printout must list the group member names, what each member was responsible for, and be typed using Word or a PDF format in a 12pt font. **The printout is not a copy of the presentation slides!**