CNVT 1830
Case Study

GRE Tunnel
10.105.0.0/30
OSPF 10 Area 0

200.0.0.1/30

.2 G0/0/1 .2 G0/0/0
R4 175.3.52.0/30 G0/0/1 .1 ISP .1
G0/0/0 .254 S0/1/1 .1 S0/1/0

140.69.212.0/30 NAT / PAT 64.27.3.0/30

S4 G0/0/1 S0/1/1 .2 .2 S0/1/0
.2 10.200.0.0/30 .1 R1 HSRP R2
R3 .254 G0/0/1 G0/0/0 G0/0/0
OSPF 10 Area 0 G0/0/0 OSPF 10 Area 0

.1
Remote Office
10.101.0.0/24

OSPF 10 Area 0

G1/0/1 LACP G1/0/1
.1 Fa0/1 Fa0/1
WWW
10.102.0.0/24

VLAN 10 S1 S2 VLAN 10

VLAN 20 OSPF 10 Area 0 VLAN 20

VLAN 30 PagP ON VLAN 30
S3

VLAN 10 VLAN 20 VLAN 30

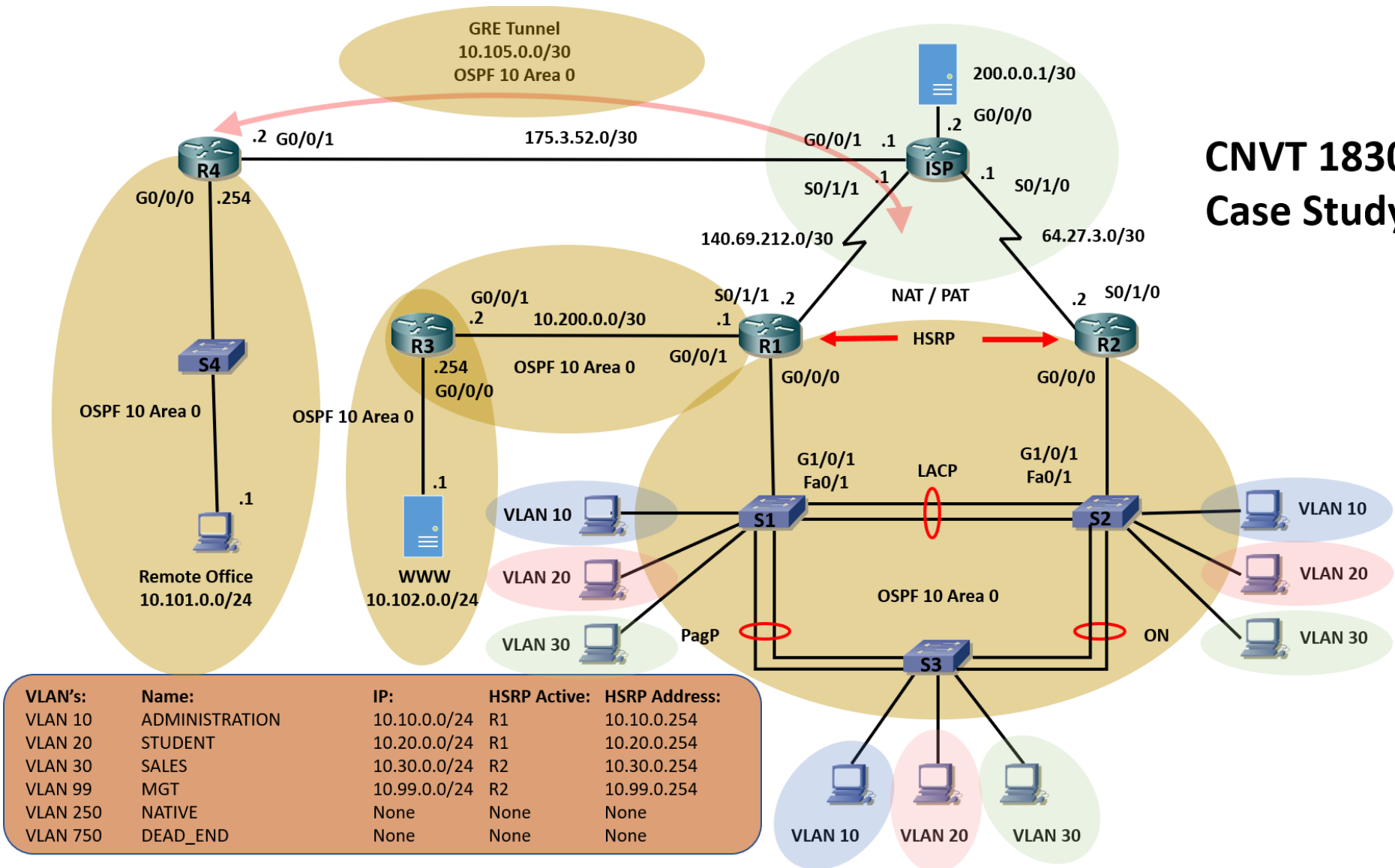| VLAN's:	Name:	IP:	HSRP Active:	HSRP Address:
VLAN 10	ADMINISTRATION	10.10.0.0/24	R1	10.10.0.254
VLAN 20	STUDENT	10.20.0.0/24	R1	10.20.0.254
VLAN 30	SALES	10.30.0.0/24	R2	10.30.0.254
VLAN 99	MGT	10.99.0.0/24	R2	10.99.0.254
VLAN 250	NATIVE	None	None	None
VLAN 750	DEAD_END	None	None	None

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 S1 – S2:
S1   Ports G1/0/2-3 ,Fa0/2-3
S1   Ports G1/0/2-3, Fa0/2-3
LACP

Ether-Channel S1 – S3:
S1   Ports G1/0/4-5, Fa0/4-5
S3   Ports G1/0/2-3, fa0/2-3
PagP

Ether-Channel S2 – S3:
S2   Ports G1/0/4-5, Fa0/4-5
S3   Ports G1/0/4-5, Fa0/4-5
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 and become part of the OSPF 10 Area 0 network
2. All traffic leaving the network will exit via the HSRP virtual interfaces.
3. 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 backup.
4. R2 will be the Active Router for HSRP as well as the OSPF Designated Router for VLAN's 30 and 99, R2 will be the backup.
5. Ether-Channel will be configured according to the chart above.
6. All access ports should be set to protect Spanning-Tree and unused ports should be disabled and placed into VLAN 750.
7. All other security measures applicable, should be applied to all access ports.
8. Access Control Lists should be placed on all routers to protect against outside attacks as well as limit remote access to SSH and/or CDP.
9. All traffic should use NAT/PAT to external addresses assigned by your company from IANA of 175.44.2.0/248.
10. Use the 175.44.2.1 address as the static NAT address of the 10.102.0.1 web server including PAT.
11. Reserve three (3) addresses for future expansion.
12. All access addresses except for the web server should be via DHCP with a domain of jmowry.com, a lease of three days, and DNS of 8.8.8.8 and 8.8.4.4
13. Each group will present a PowerPoint presentation of their solution as well as a printed copy of the configs and any relevant material. This is NOT a printout of the PowerPoint slides! The printout must list the group member names, typed using Word or PDF formats. Single sided and using a 12pt font.