

Temas Avanzados

Capa 2

LOVE PURPLE
LIVE GOLD





Opciones

- Seguridad
 - Seguridad de primer brinco para ipv6
- Multicast
 - Seguridad
 - Bonjour
 - IPv6
- Data Center
 - LISP
 - OTV
- SDN

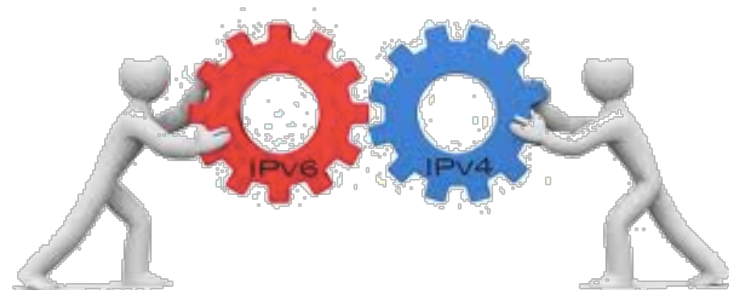


IPv6 SECURITY



IPv6 Security

- Run IPv6 on your routers!
- Same as IPv4 security
 - Border firewall
 - Local host firewalls (more to come)
- Lock down gear/servers/resources with ACLs
 - Known subnets





IPv6 Security (Continued)

- Addressing
 - WIN machines on AD
 - Tunneling protocols off
 - Privacy addressing off
 - DMCA
 - Tie user to NETREG-ed MAC address
- Tunneling not supported
 - Campus Firewall
 - Foo Router (a.k.a. black hole)





Host Firewalls

- Windows 7/Server 2008
 - Unified
 - Must specify both IPv4 and IPv6 addresses
 - Inadvertent exclusion of IPv4/IPv6
- Linux
 - Two separate controlling utilities(iptables and ip6tables)
 - Must configure both for dual-stack network
- Mac / BSD
 - IPFILTER (ipf)
 - IPFIREWALL (ipfw/ip6fw) – Mac OS 10.6 Snow Leopard and below
 - PacketFilter (pf) – Mac OS 10.7 Lion and above





First Hop Security

- Rogue router advertisements (RAs)
 - Bogus RAs – Self-created (story)
- Rogue DHCPv6 servers
- ACL protection

```
ipv6 access-list ipv6-secure
remark Block ipv6 DHCP server
deny udp any eq 547 any eq 546
remark Block router advertisements
deny icmp any any router-advertisement
permit ipv6 any any
```



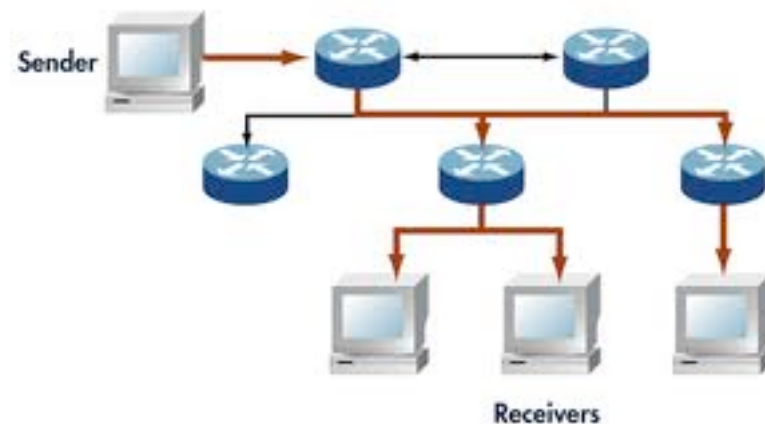


MULTICAST



Multicast Security

- Limitar quien puede conectarse
 - ACL
 - Permitir grupos locales
- Que fuentes son legítimas
 - Uso de grupos multicast adecuados
 - Control software





Bonjour



- Que es?
 - mDNS
- Para que me sirve?
 - Transmisison de imagenes, informacion, impression

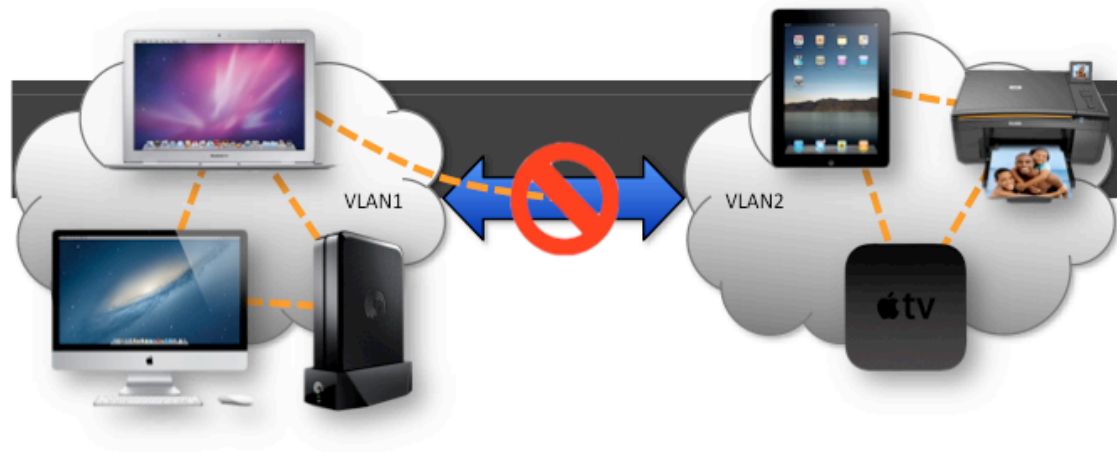




Problemas Bonjour

Bonjour Cannot Span Subnets or VLANs

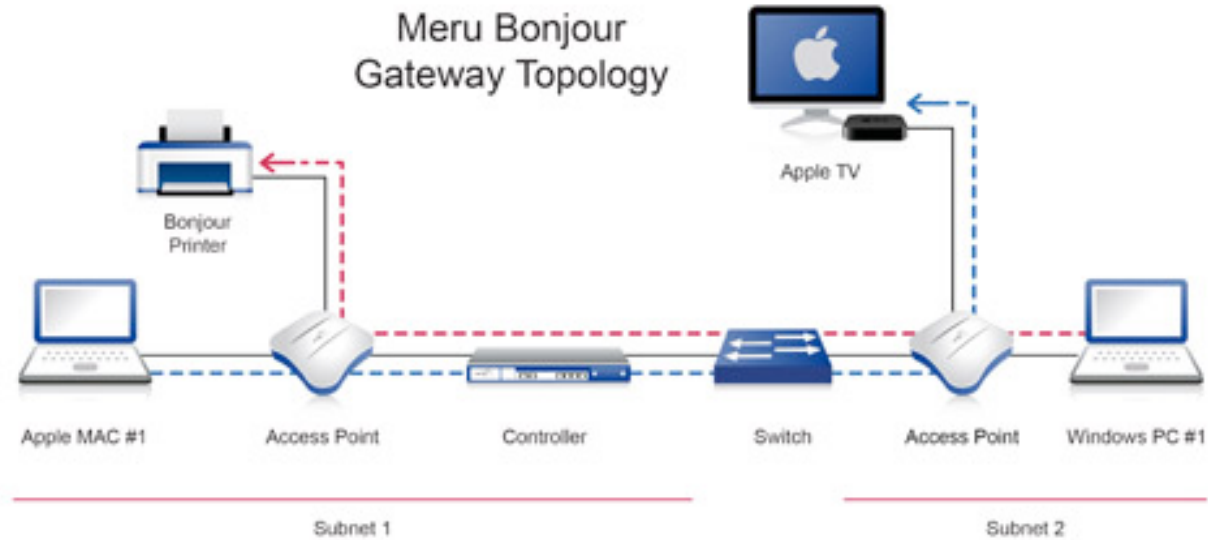
But users are demanding 'at home' functionality in the enterprise





Bonjour

- Soluciones propias de vendedores
- IETF trabajando en solucion
 - Bonjour Headers





Multicast and IPv6

- Used by unicast IPv6
- The New Broadcast
- Critical for IPv6 operations
 - ICMPv6 (e.g. NDP)
- MLD (Multicast Listener Discovery)
 - Equivalent to IGMP in IPv4 world



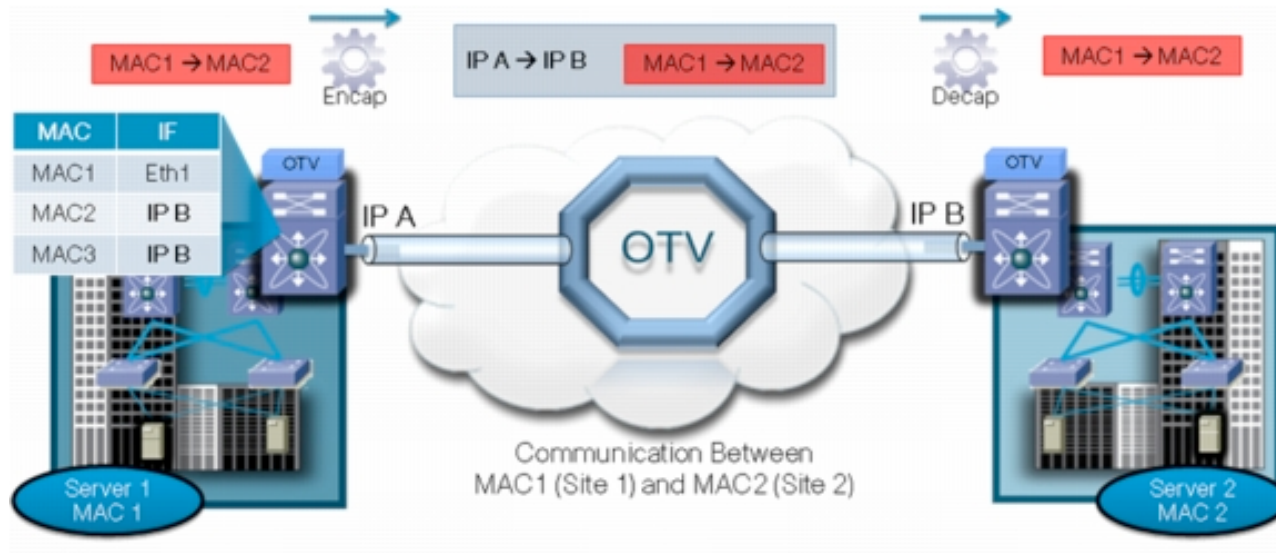


DATA CENTER



Data Center - OTV

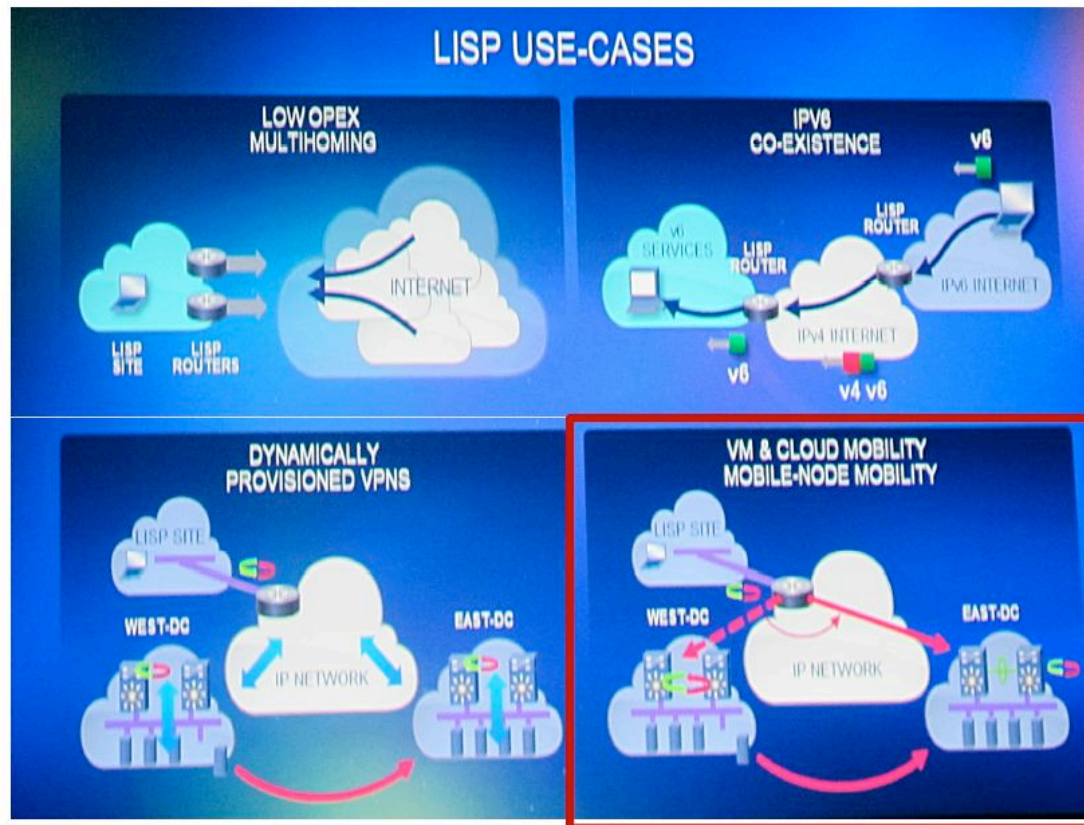
- Conexión a larga distancia
 - Broadcast controlado
 - Apariencia de una sola red





Data Center - LISP

- www.Lisp4.net



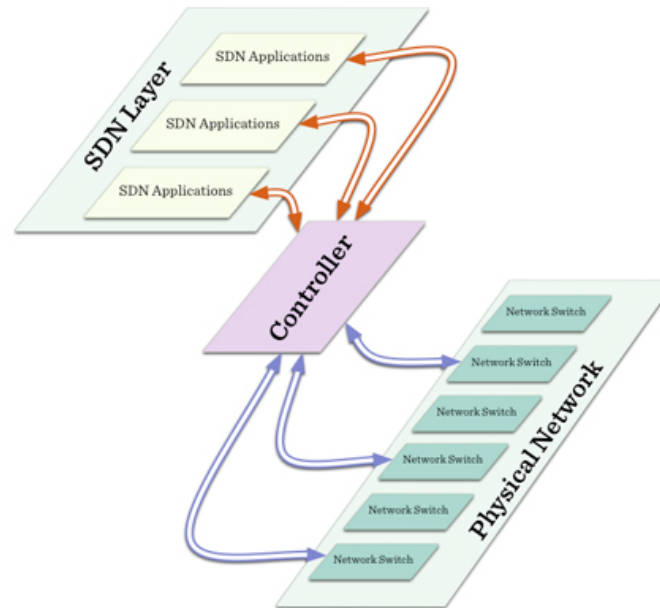


SDN



SDN

- Separacion de plano de control y data
- Crear concepto de “tienda App para la Red”
- Crear funcionalidades avanzados en la capa 2





¡Gracias!



Jeffry Handal
jhandal@lsu.edu