

Putting 2 & 2 Together

By Stephen Dugan, CCSI
scdugan@101labs.com

Introduction

Welcome to the presentation
and
Thank you for coming!

- Who is the speaker?
- What is the focus of the presentation?

Agenda

Introduction

Extras?

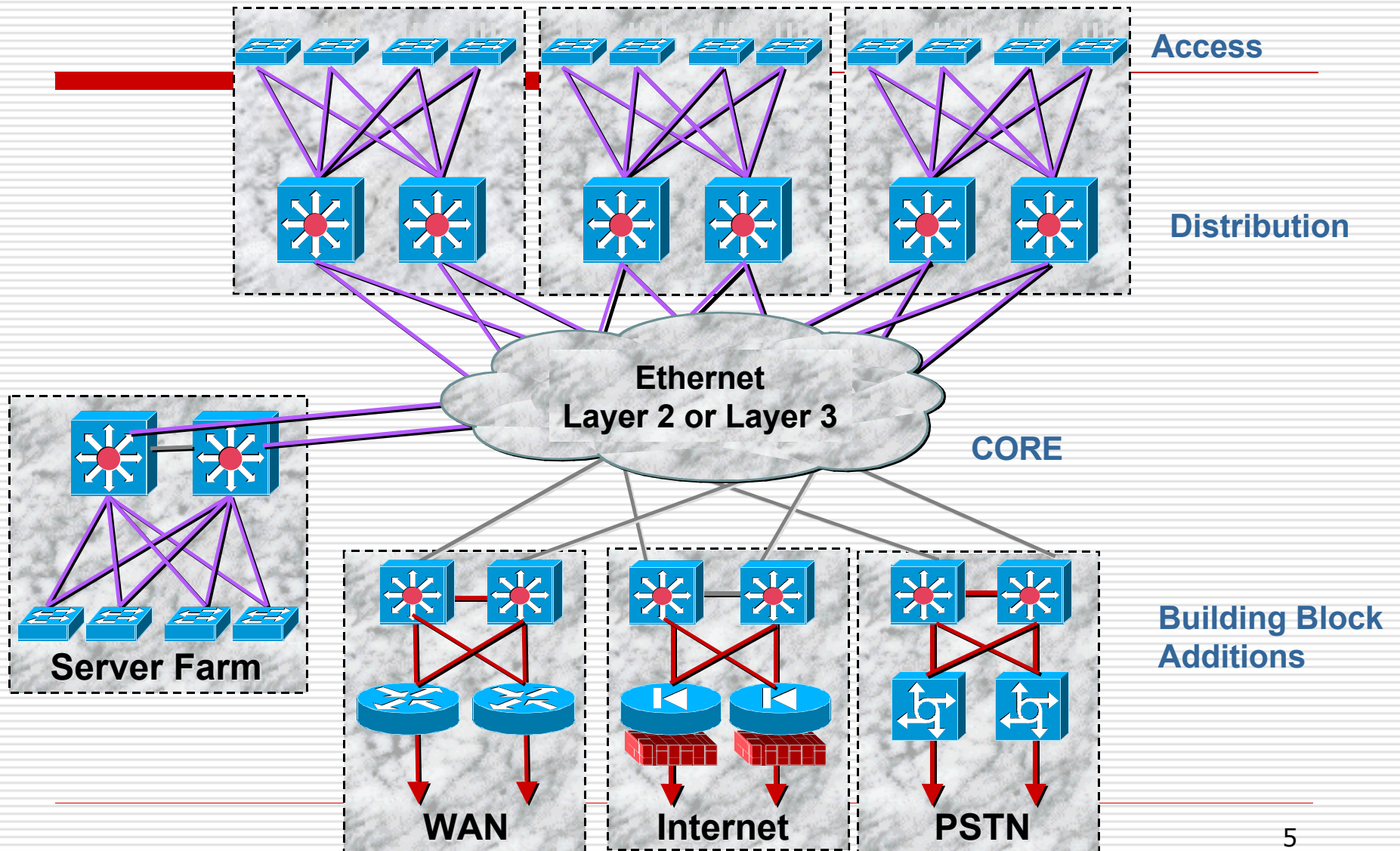
Section 1 –
Current Design
Best Practices

Section 2 –
Emerging
Design
Practices

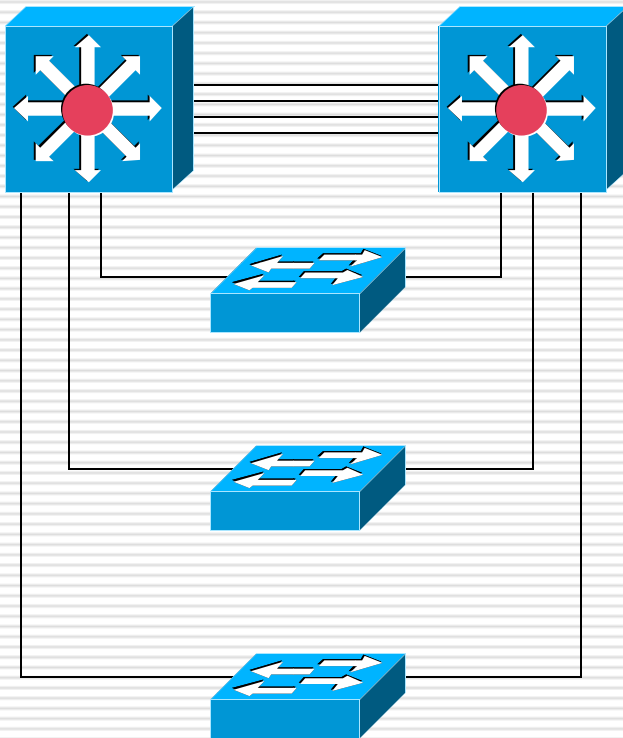
Section 1

Current Design Model

Building Block of Network Design



Section 1 – Current Design Model



Features:

Link redundancy

Load-Sharing

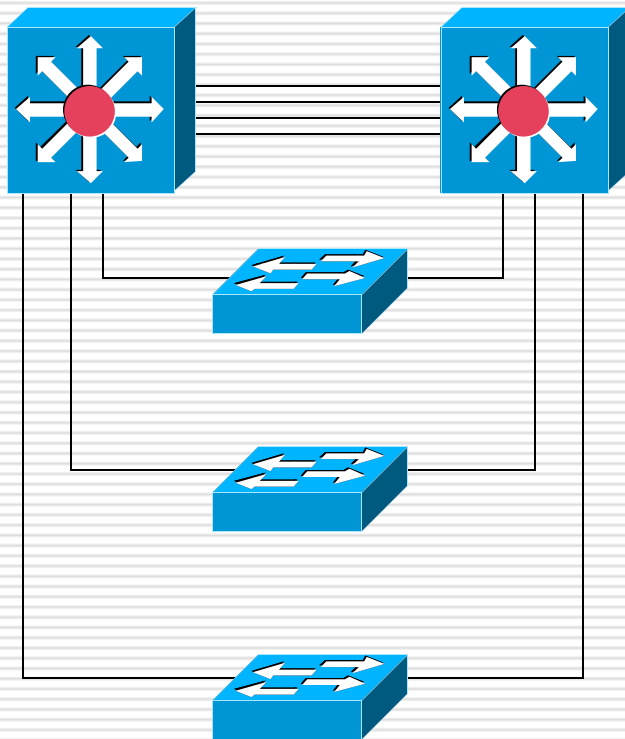
Fast Convergence

Manageable

Scalable

Security could be stronger....

Section 1 – Current Design Model



L2 Functions that provide security:

Root Guard

PortFast

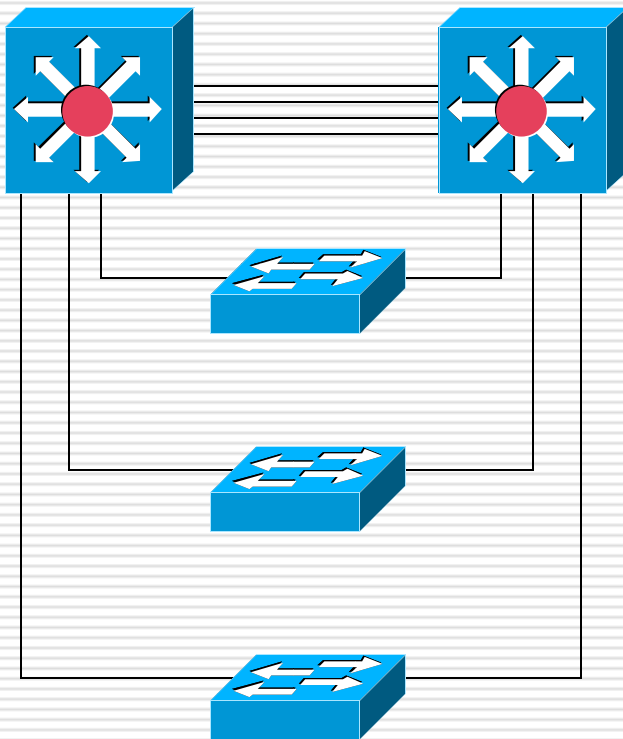
BPDU Guard

Port Security

Management VLAN

Private VLANs

Section 1 – Current Design Model



L3 Functions that provide security:

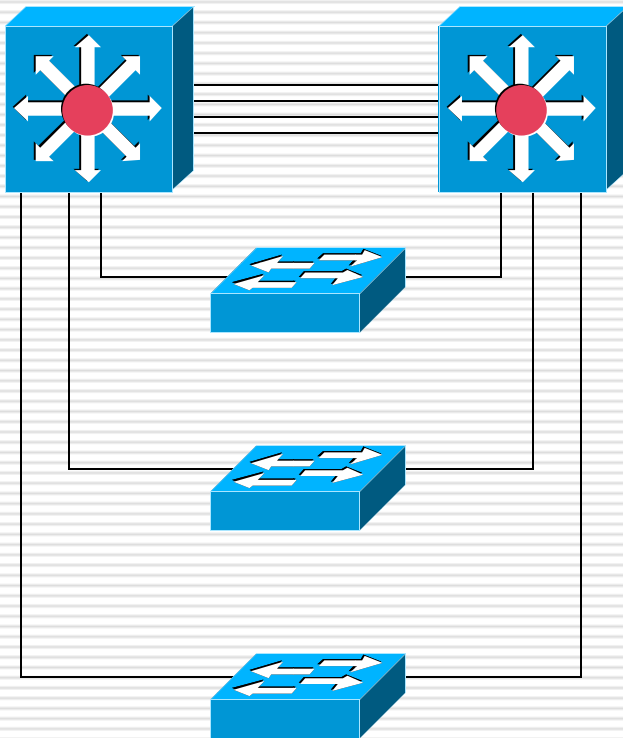
ACLs at Distribution Layer:

Ingress - Egress from Core

Route Filtering

Network Based IDS (if used?!?)

Section 1 – Current Design Model



Hard issues to Address with this design:

HSRP insecurities

STP weaknesses

ARP Spoofing

Common mis-configurations

Section 2

Emerging Changes to Design Model

Section 2 – Emerging Changes

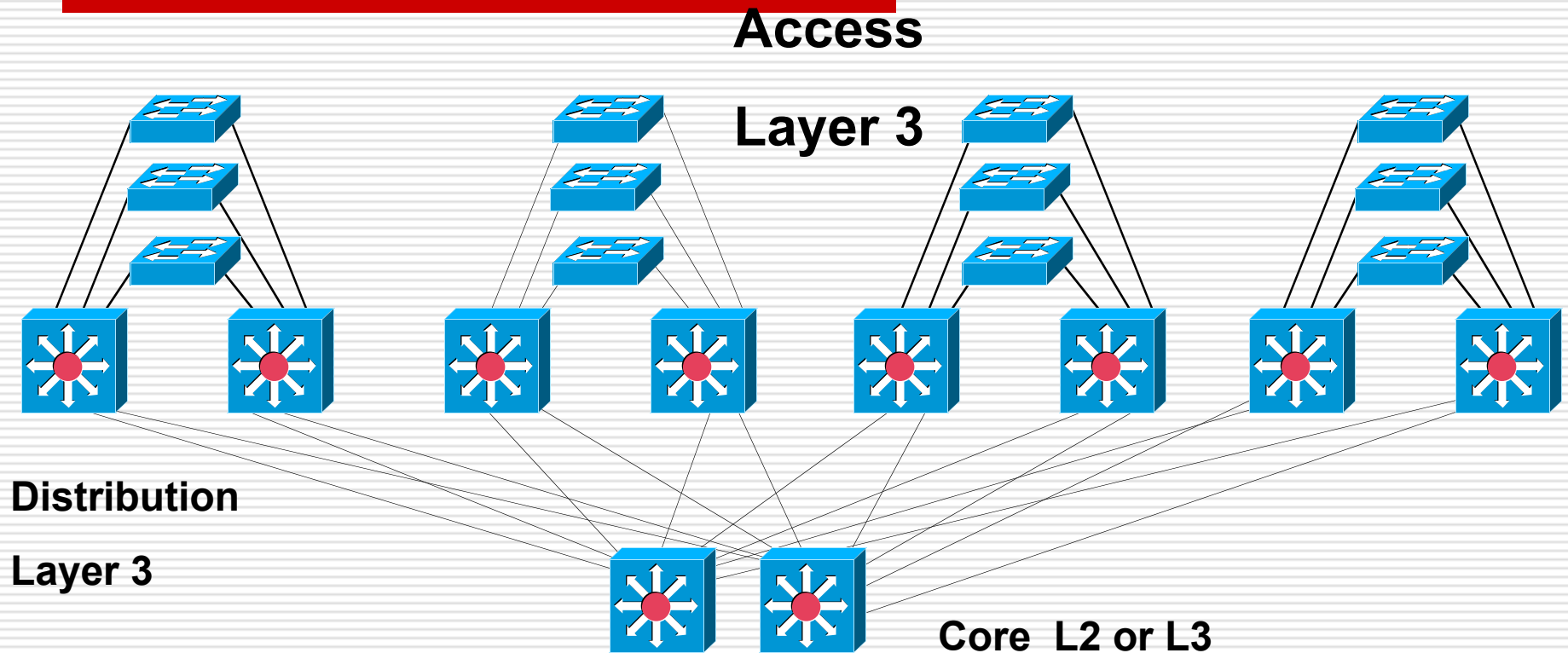
Main Changes is focusing around bringing the Layer 3 Routing functionality close to the end stations.

OR

R2D

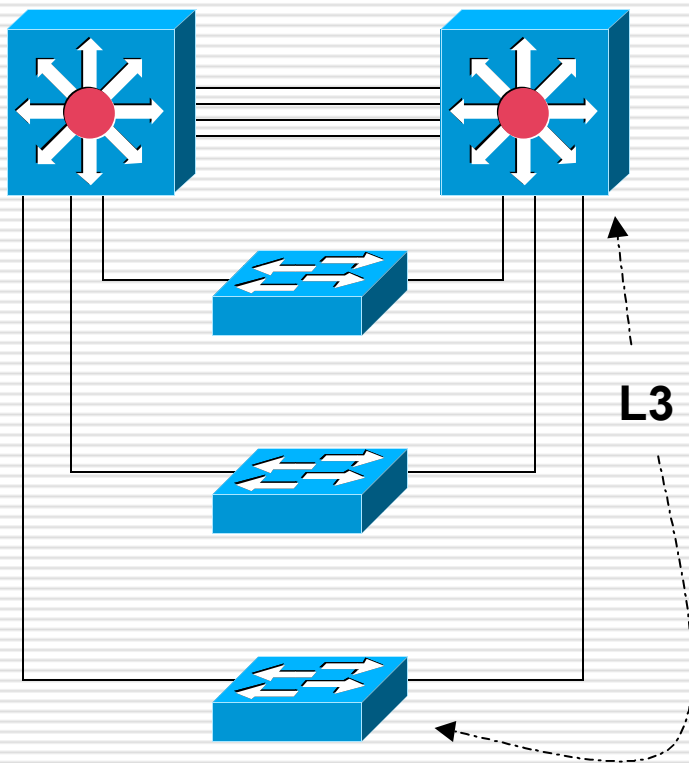
Routing to Desktop

Section 2 – Emerging Changes



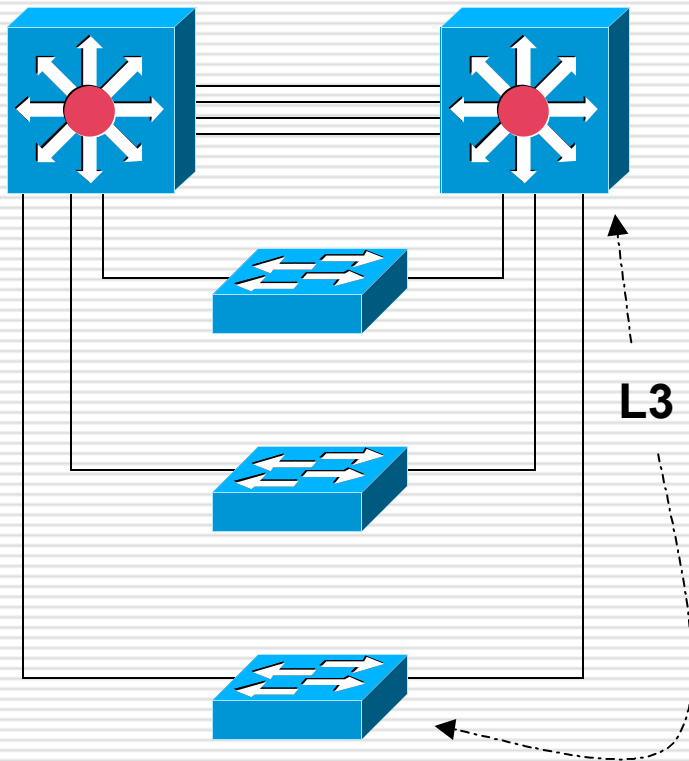
From the Physical Layout it looks the same (Good news no Rewire!)

Section 2 – Emerging Changes



**With L3 Capabilities within the
Access-Layer Box:
HSRP isn't needed
STP is irrelevant
Routing to Distribution Layer
Concept of "Private-VLANs" can
be implemented easily**

Section 2 – Emerging Changes



Security Problems Solved:

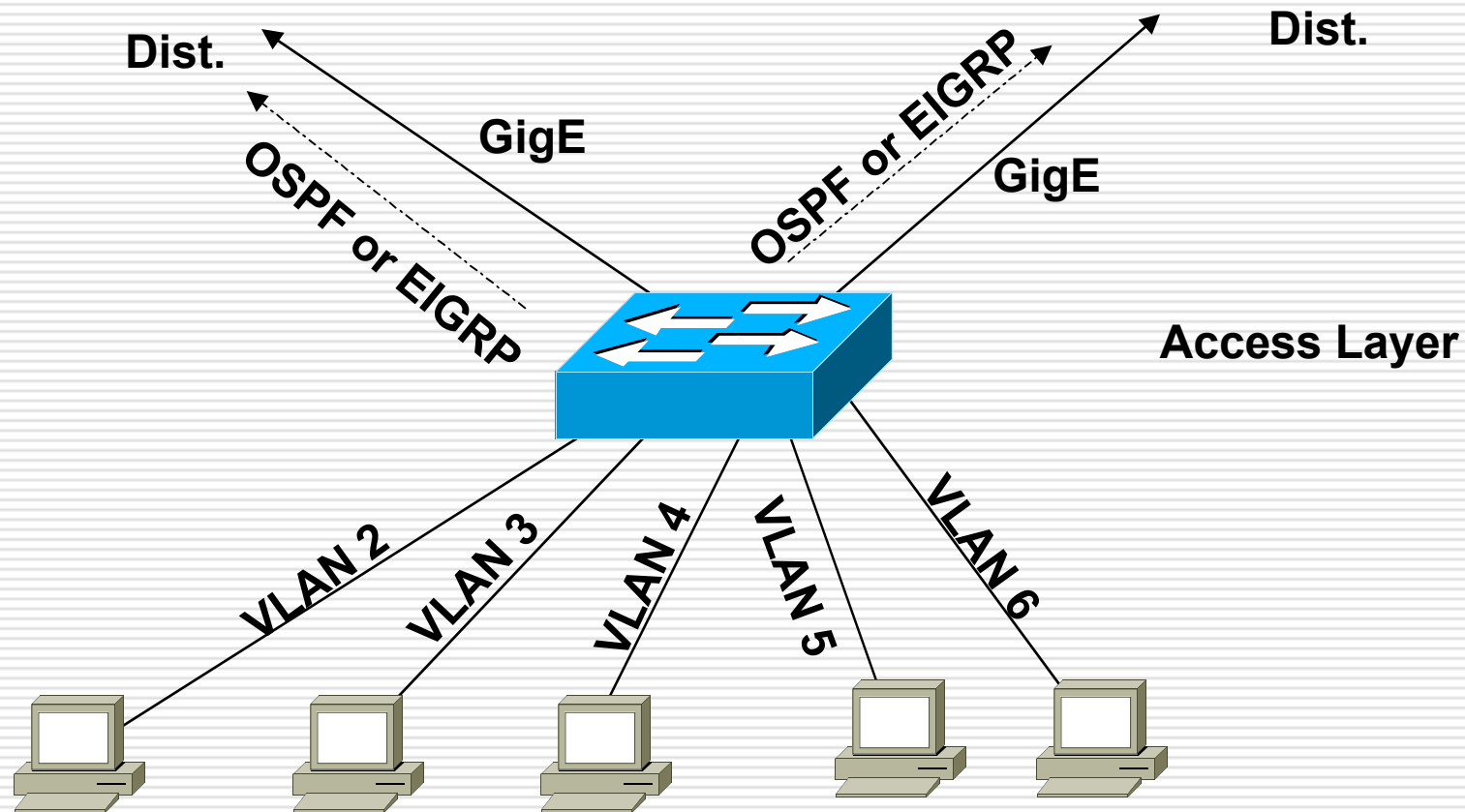
ARP Spoofing

ROOT Take over

HSRP MiTM Attack (or DOS)

Better QOS handling (NBAR)

Section 2 – Emerging Changes



Links

- General Cisco Security
 - <http://www.cisco.com/warp/public/707/21.html#http>
 - <http://www.cisco.com/public/cons/isp/documents/IOSEssentialsPDF.zip>
 - http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm
- Design
 - http://www.cisco.com/warp/public/cc/so/neso/Inso/cpsogcnd_wp.htm

Thank you for coming!!

Special thanks to
Jeff Moss, Keith Myers and the
rest of the Black Hat Crew.