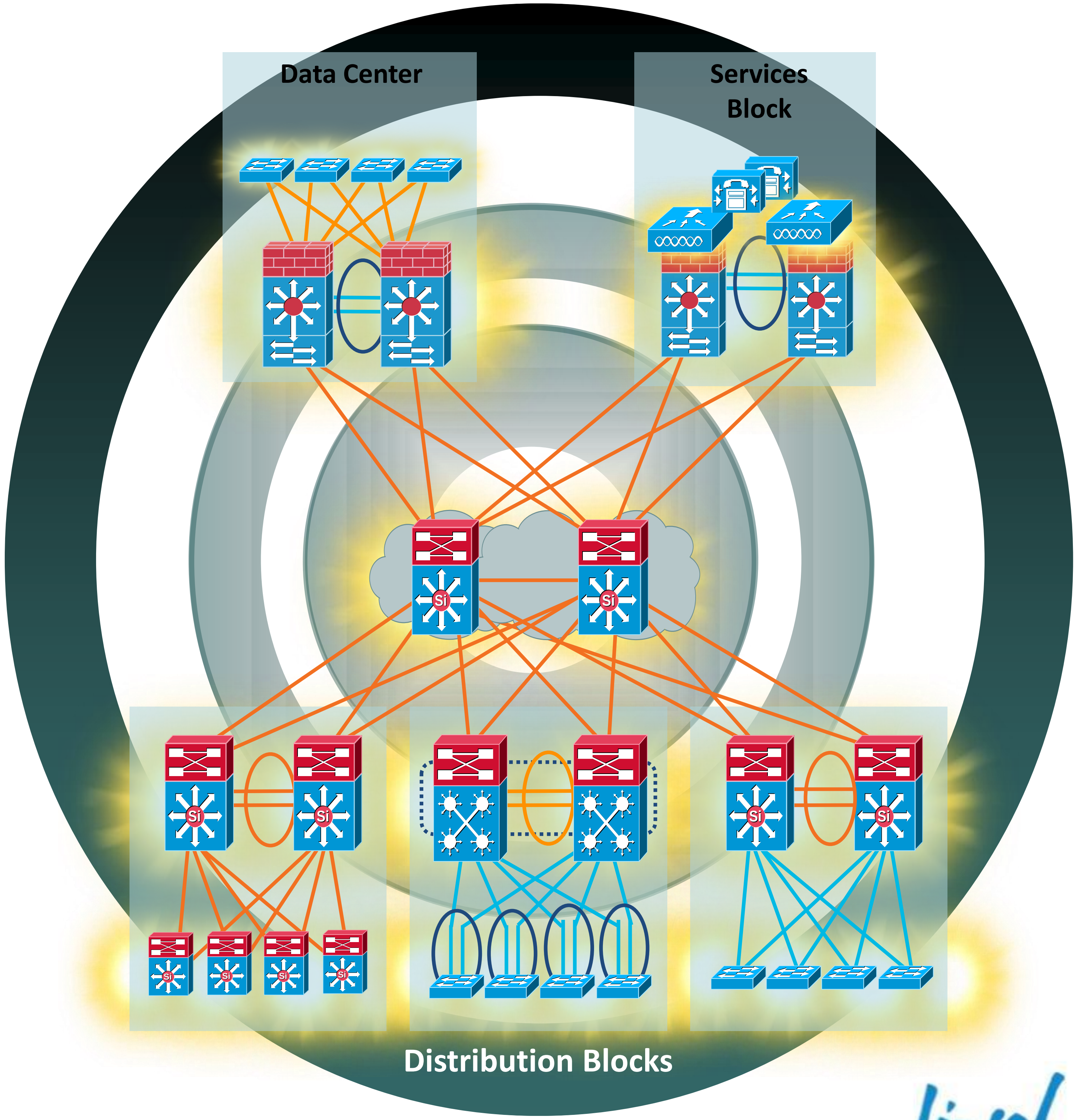
Multilayer Campus Architectures and Design

BUILT FOR
THE HUMAN
NETWORK

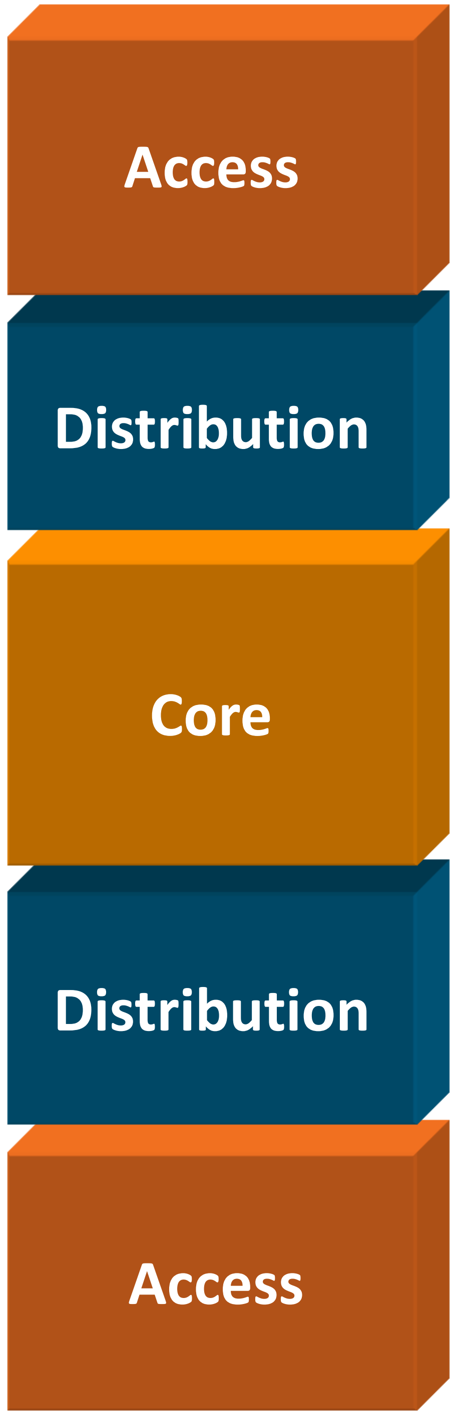
Agenda

- Multilayer Campus Design Principles
- Security Considerations
- Summary

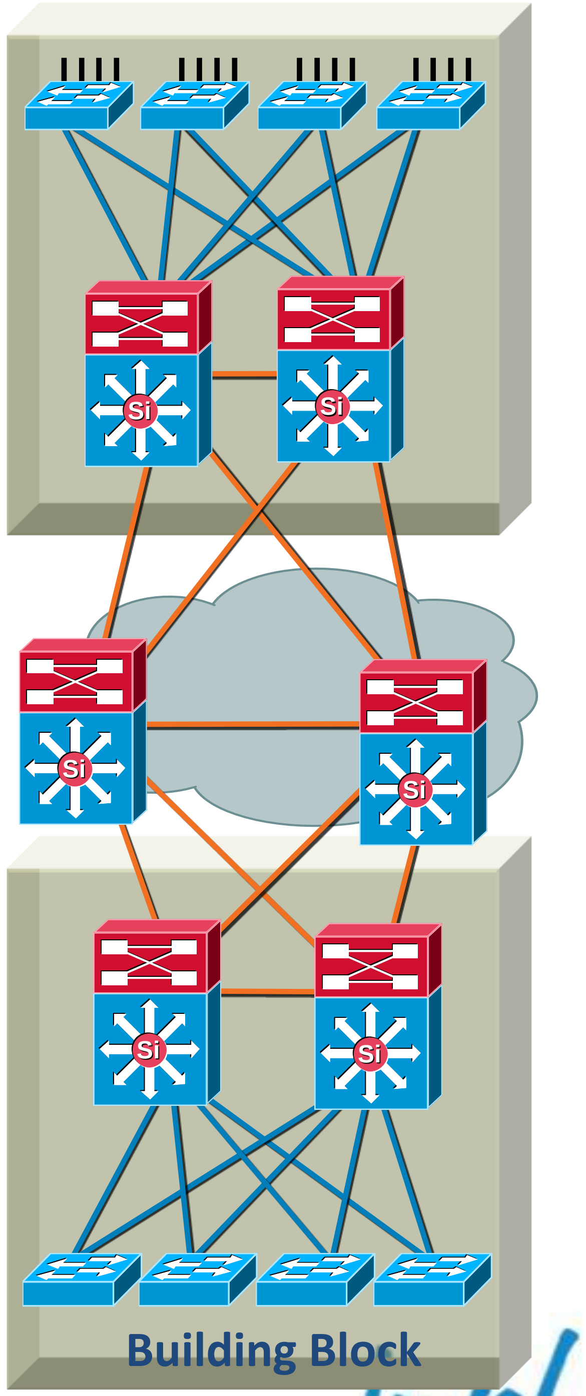


Hierarchical Network Design

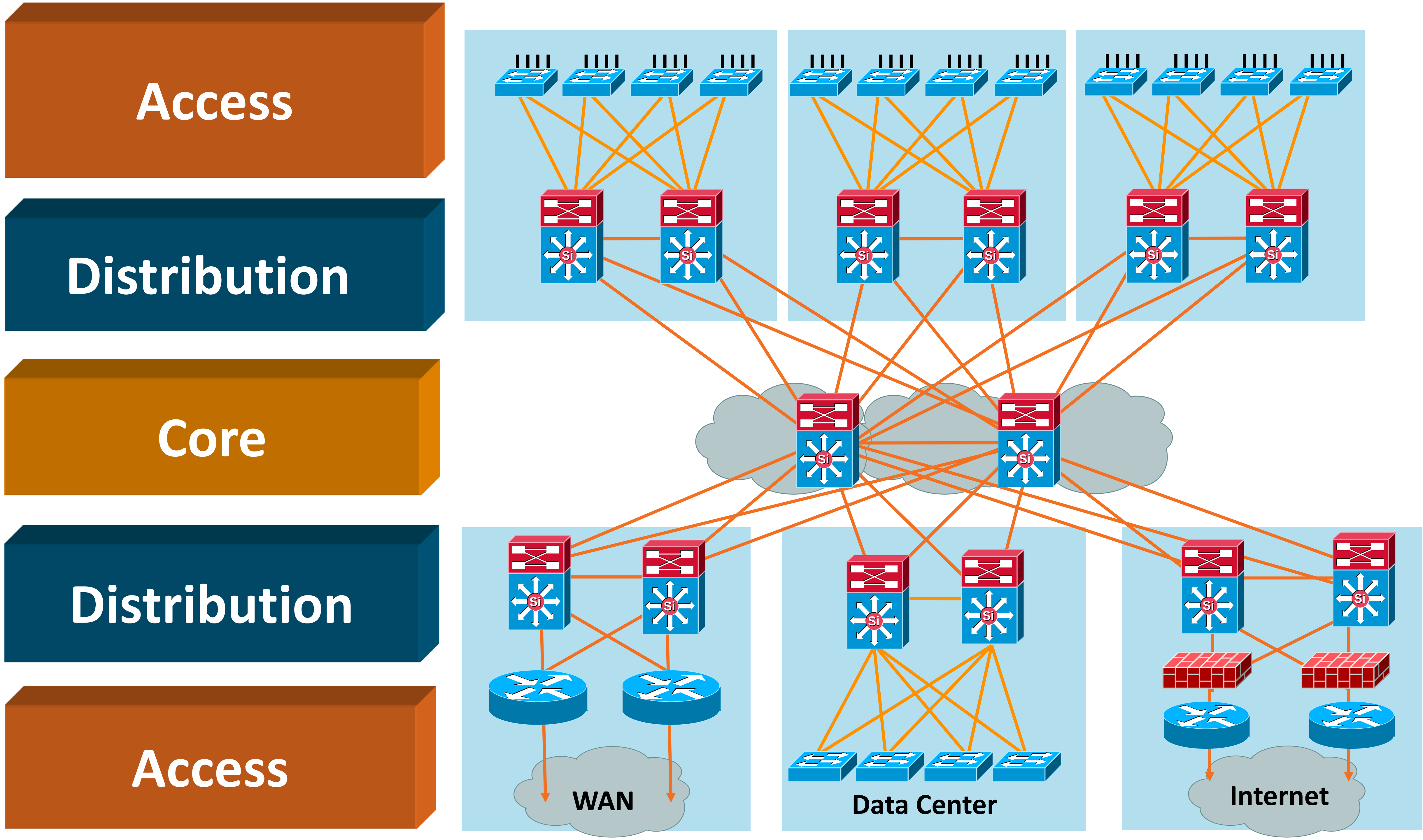
Without a Rock Solid Foundation the Rest Doesn't Matter



- Offers hierarchy—each layer has specific role
- Modular topology—building blocks
- Easy to grow, understand, and troubleshoot
- Creates small fault domains— clear demarcations and isolation
- Promotes load balancing and redundancy
- Promotes deterministic traffic patterns
- Incorporates balance of both Layer 2 and Layer 3 technology, leveraging the strength of both
- Utilizes Layer 3 routing for load balancing, fast convergence, scalability, and control



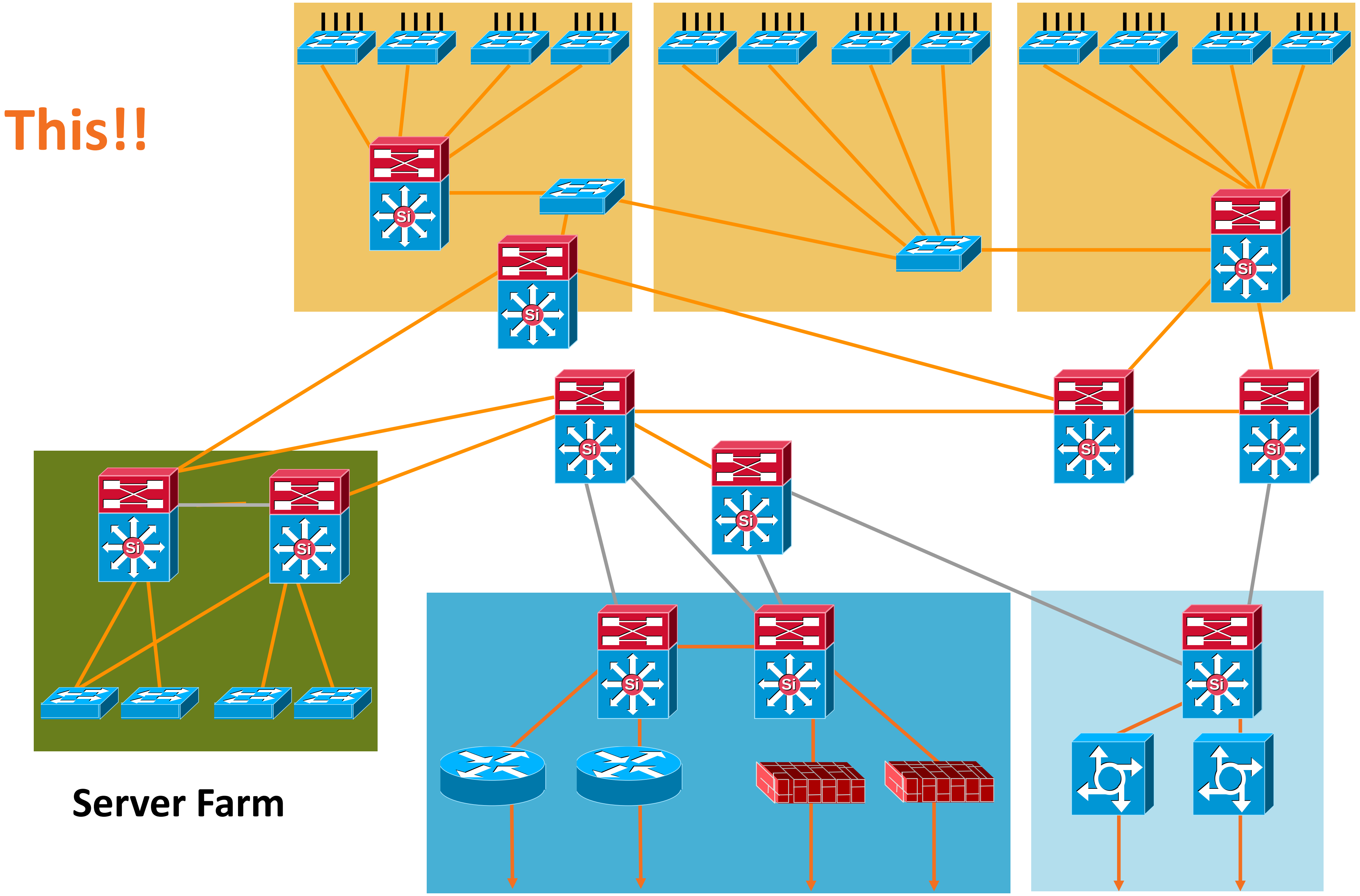
High-Availability Campus Design Structure, Modularity, and Hierarchy



Hierarchical Campus Network

Structure, Modularity and Hierarchy

Not This!!



Server Farm

WAN

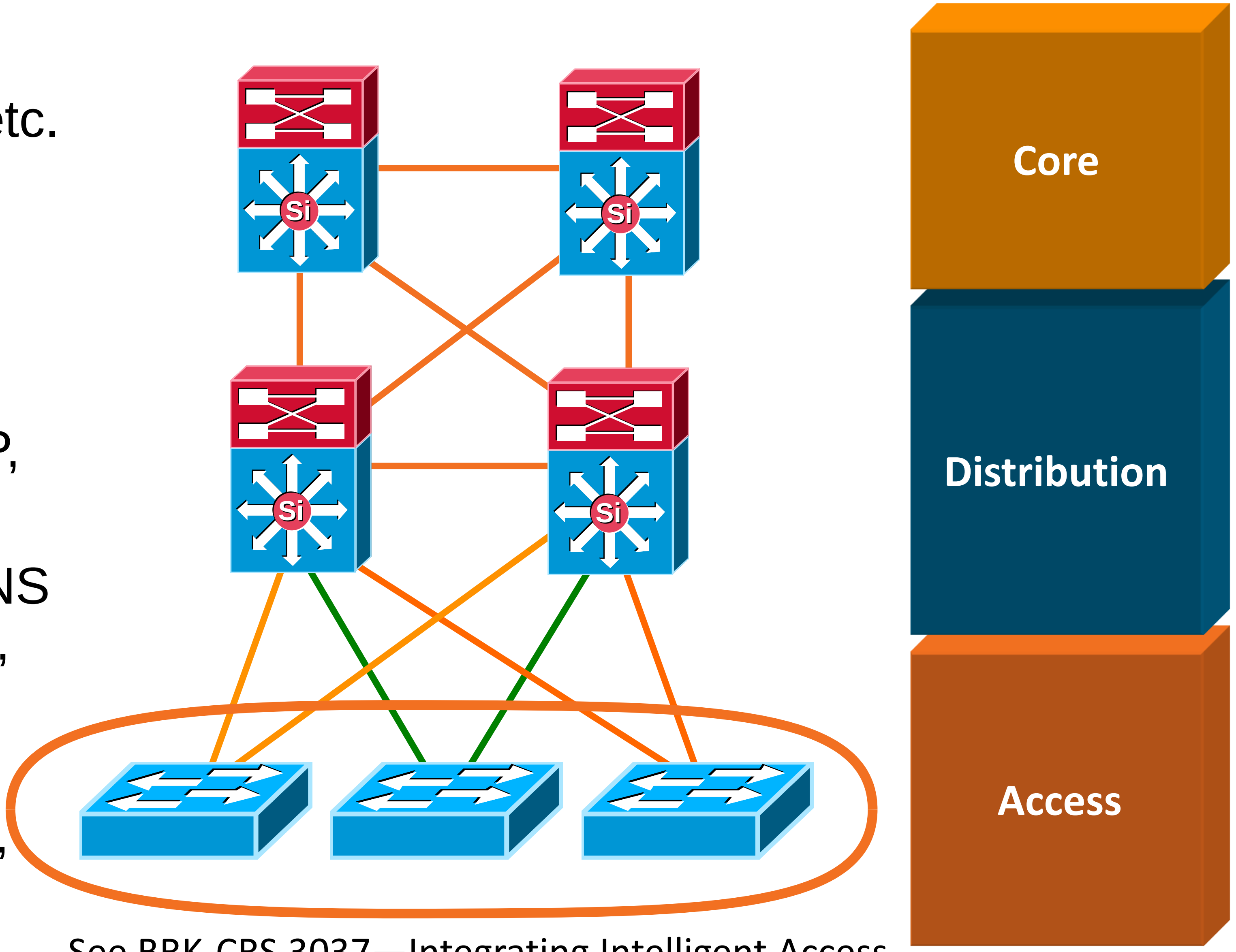
Internet

PSTN

Access Layer

Feature Rich Environment

- It's not just about connectivity
- Layer 2/Layer 3 feature rich environment; convergence, HA, security, QoS, IP multicast, etc.
- Intelligent network services: QoS, trust boundary, broadcast suppression, IGMP snooping
- Intelligent network services: PVST+, Rapid PVST+, EIGRP, OSPF, DTP, PAgP/LACP, UDLD, FlexLink, etc.
- Cisco Catalyst® integrated security features IBNS (802.1x), (CISF): port security, DHCP snooping, DAI, IPSG, etc.
- Automatic phone discovery, conditional trust boundary, power over Ethernet, auxiliary VLAN, etc.
- Spanning tree toolkit: PortFast, UplinkFast, BackboneFast, LoopGuard, BPDU Guard, BPDU Filter, RootGuard, etc.

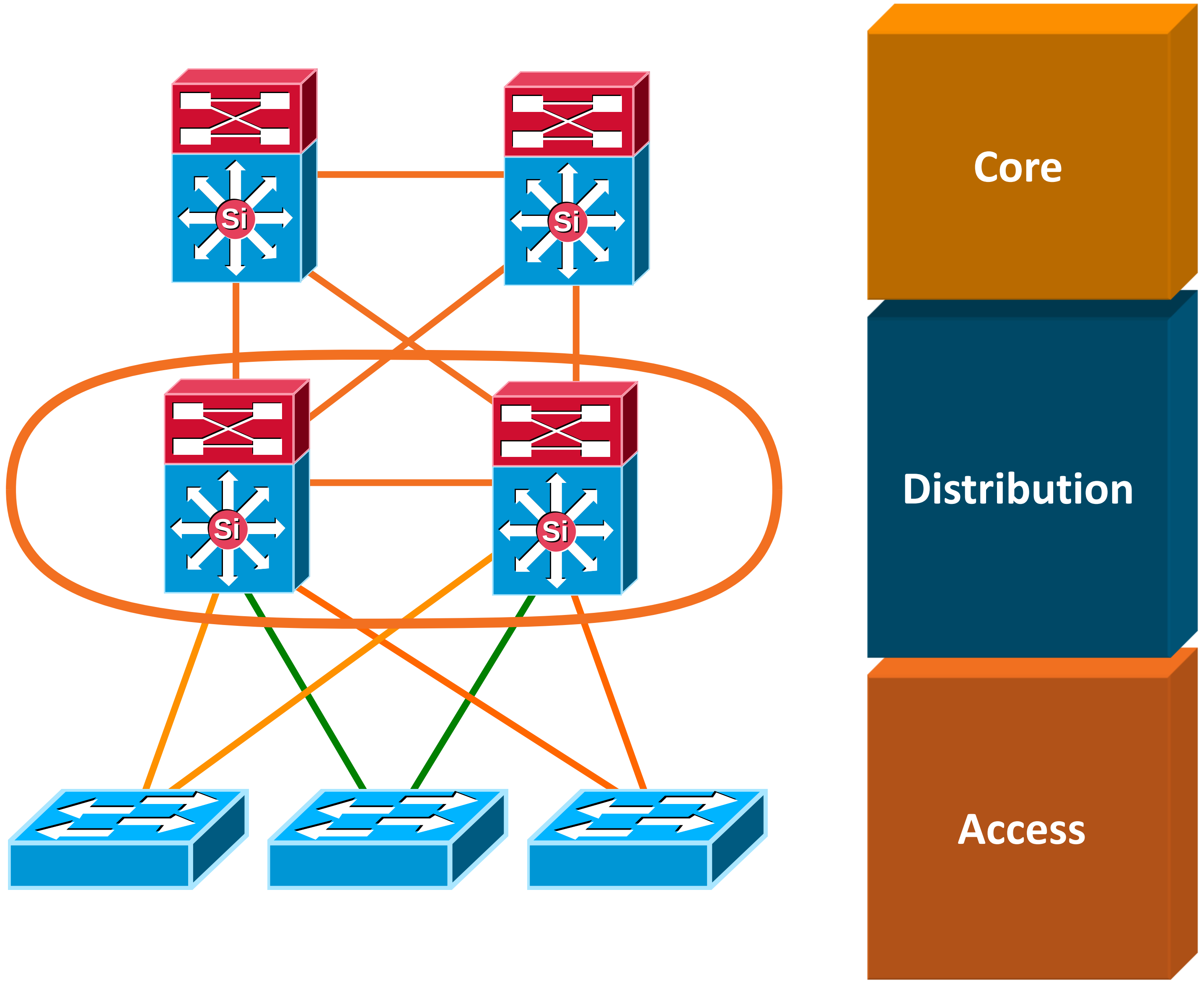


See BRK-CRS 3037—Integrating Intelligent Access

Distribution Layer

Policy, Convergence, QoS, and High Availability

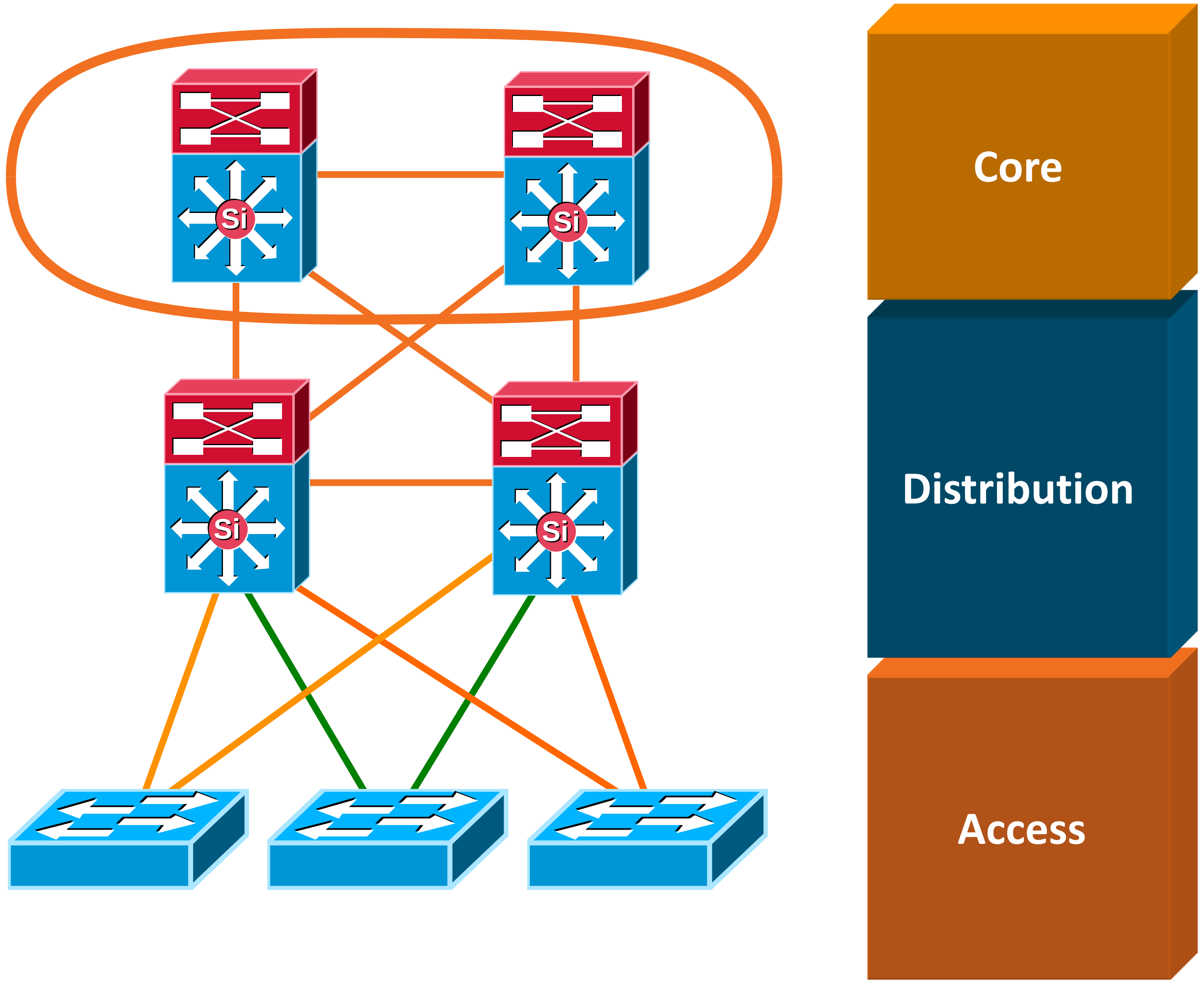
- Availability, load balancing, QoS and provisioning are the important considerations at this layer
- Aggregates wiring closets (access layer) and uplinks to core
- Protects core from high density peering and problems in access layer
- Route summarization, fast convergence,
  redundant path load sharing



Core Layer

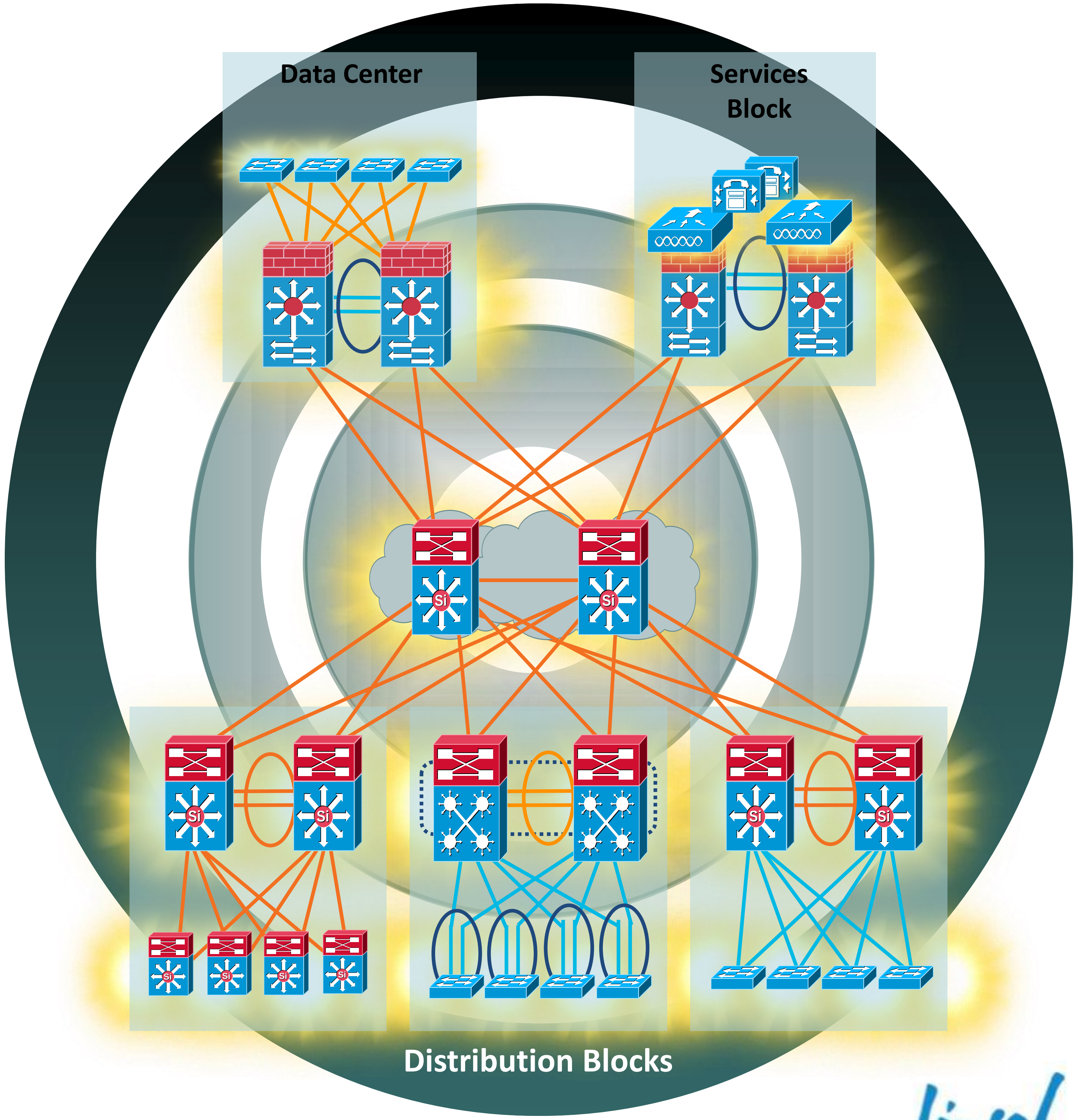
Scalability, High Availability, and Fast Convergence

- Backbone for the network—connects network building blocks
- Performance and stability vs. complexity— less is more in the core
- Aggregation point for distribution layer
- Separate core layer helps in scalability during future growth
- Keep the design technology-independent



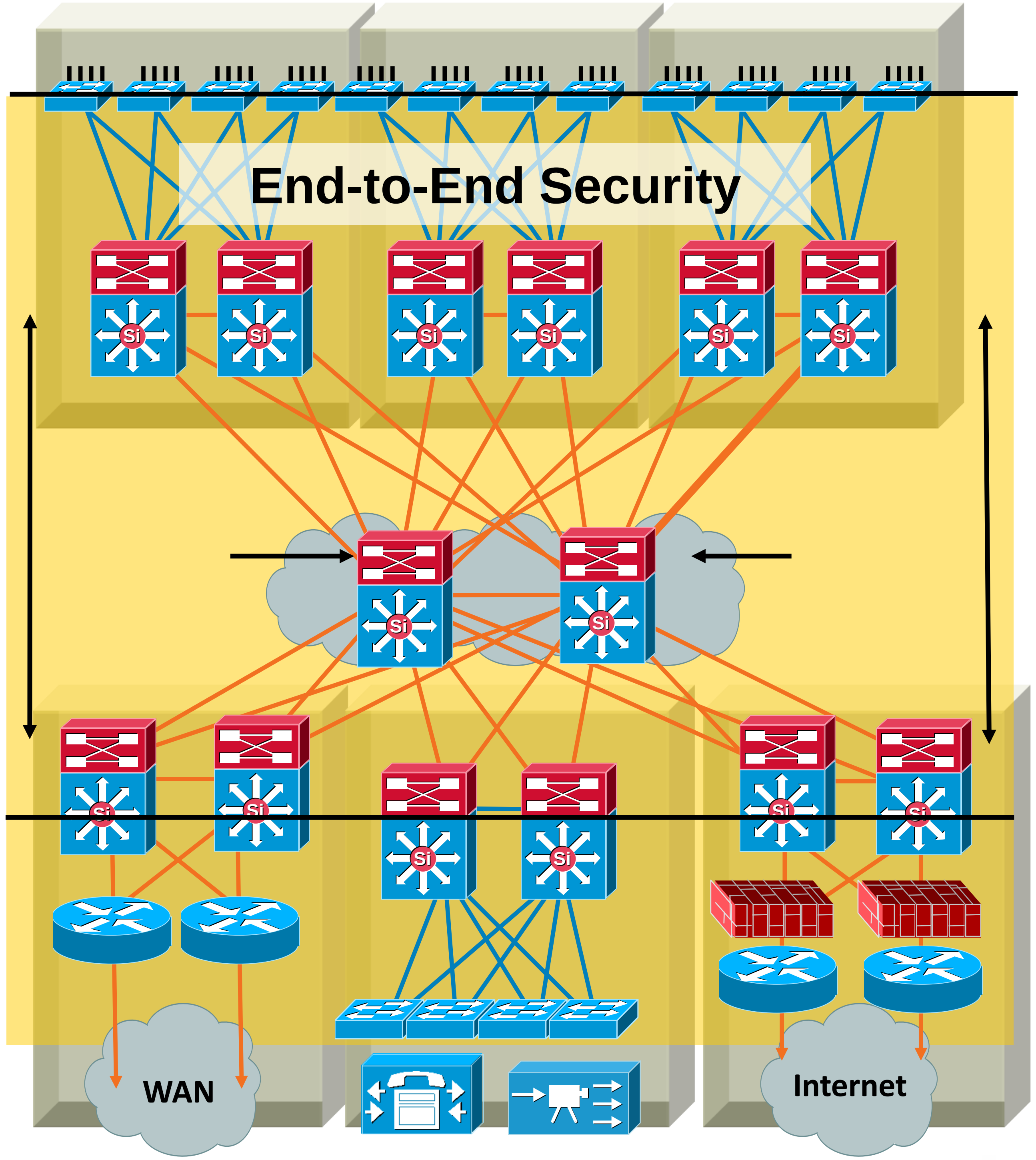
Agenda

- Multilayer Campus Design Principles
- Security Considerations
- Summary



Best Practices—Campus Security

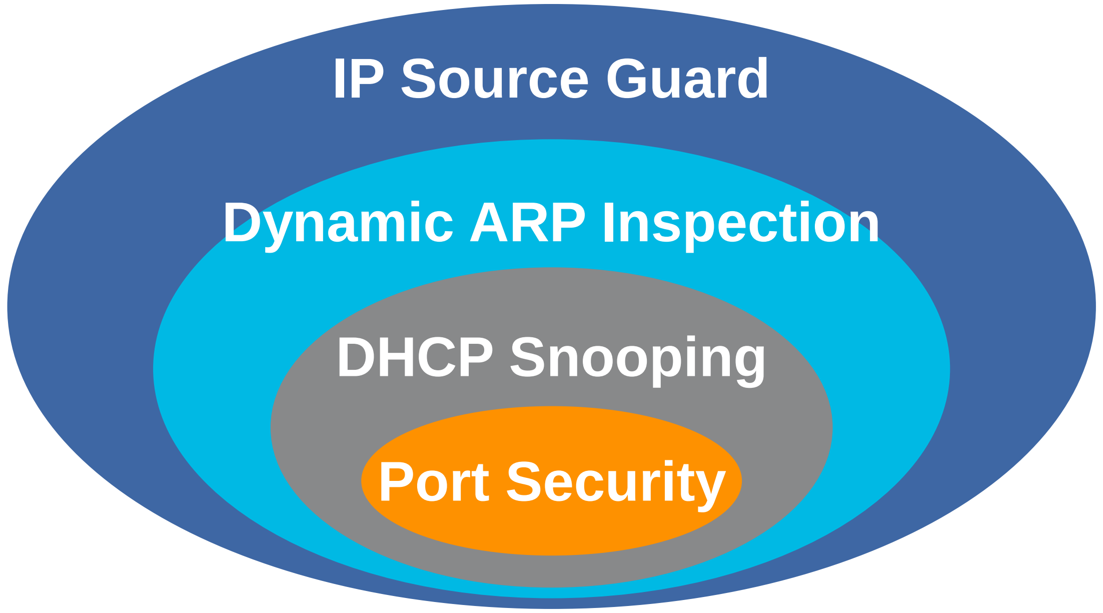
- **Couple of items that we will highlight!**
  - Catalyst integrated security feature set!
  - Dynamic port security, DHCP snooping, Dynamic ARP inspection, IP source guard
- Other best practices we won't cover…yet
  - Use SSH to access devices instead of Telnet
  - Enable AAA and roles-based access control (RADIUS/TACACS+) for the CLI on all devices
  - Enable SYSLOG to a server. Collect and archive logs
  - When using SNMP use SNMPv3
  - Disable unused services:
  - No service tcp-small-servers
    No service udp-small-servers
  - Use FTP or SFTP (SSH FTP) to move images and configurations around—avoid TFTP when possible
  - Install VTY access-lists to limit which addresses can access management and CLI services
  - Enable control plane protocol authentication where it is available (EIGRP, OSPF, BGP, HSRP, VTP, etc.)
  - Apply basic protections offered by implementing RFC2827 filtering on external edge inbound interfaces



For More Details, See BRKSEC-2002 Session, Understanding and Preventing Layer 2 Attacks

Catalyst Integrated Security Features

Summary Cisco IOS

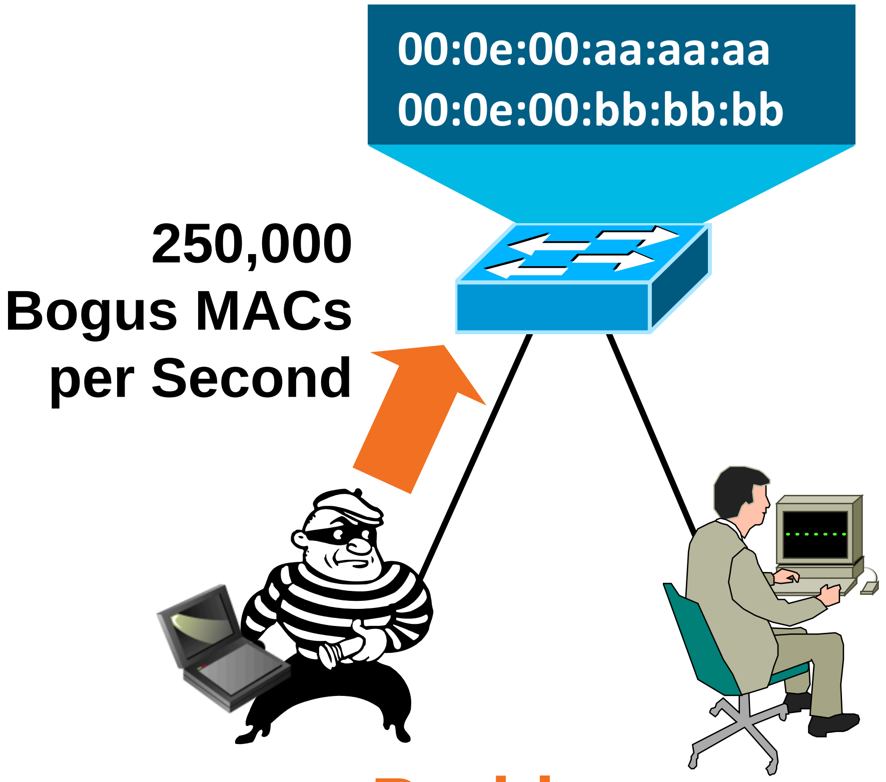


- Port security prevents MAC flooding attacks
- DHCP snooping prevents client attack on the switch and server
- Dynamic ARP Inspection adds security to ARP using DHCP snooping table
- IP source guard adds security to IP source address using DHCP snooping table

```
ip dhcp snooping
ip dhcp snooping vlan 2-10
ip arp inspection vlan 2-10
!
interface fa3/1
switchport port-security
switchport port-security max 3
switchport port-security violation
restrict
switchport port-security aging time 2
switchport port-security aging type
inactivity
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100
ip verify source vlandhcp-snooping
!
Interface gigabit1/1
ip dhcp snooping trust
ip arp inspection trust
```

Securing Layer 2 from Surveillance Attacks

Cutting Off MAC-Based Attacks



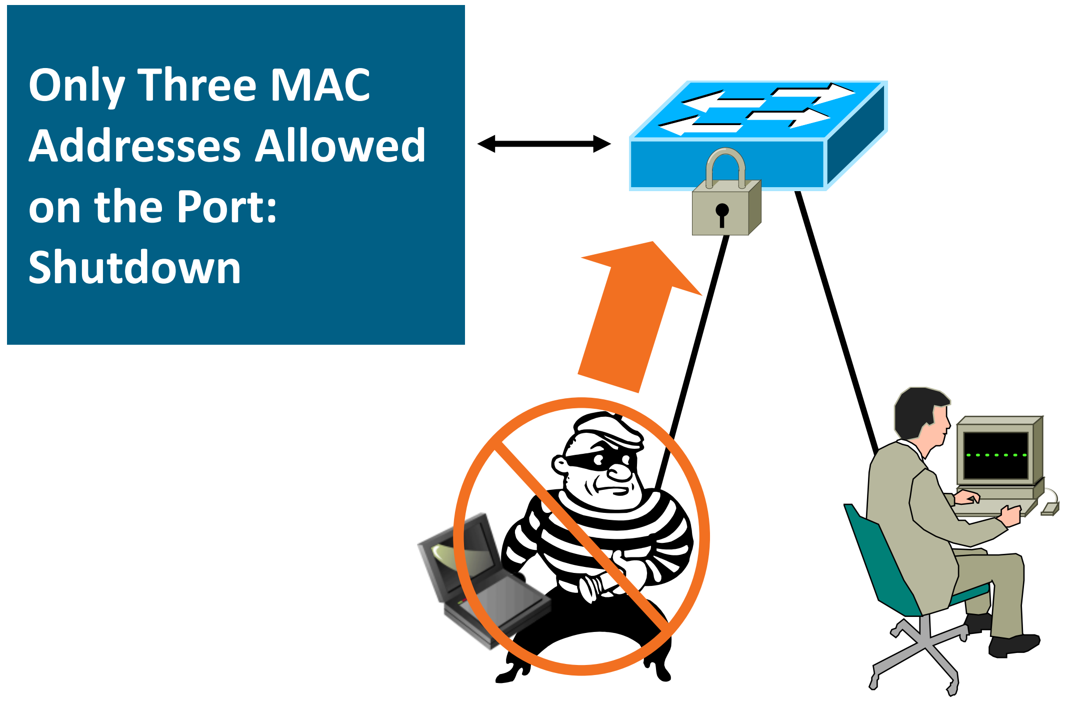
00:0e:00:aa:aa:aa
00:0e:00:bb:bb:bb

250,000 Bogus MACs per Second

Problem:

Script Kiddie Hacking Tools Enable Attackers Flood Switch CAM Tables with Bogus Macs; Turning the VLAN into a Hub and Eliminating Privacy

Switch CAM Table Limit Is Finite Number of Mac Addresses



Only Three MAC Addresses Allowed on the Port: Shutdown

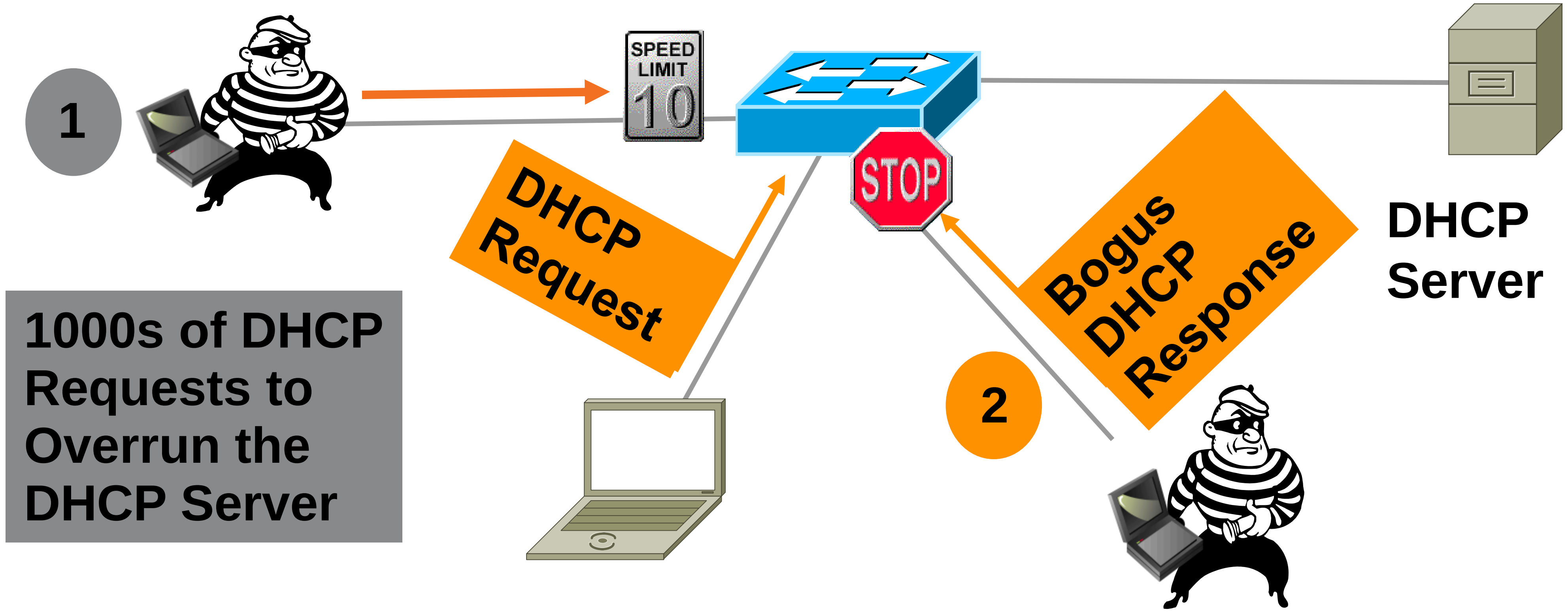
Solution:

Port Security Limits MAC Flooding Attack and Locks Down Port and Sends an SNMP Trap

```
switchport port-security
switchport port-security maximum 10
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

DHCP Snooping

Protection Against Rogue/Malicious DHCP Server

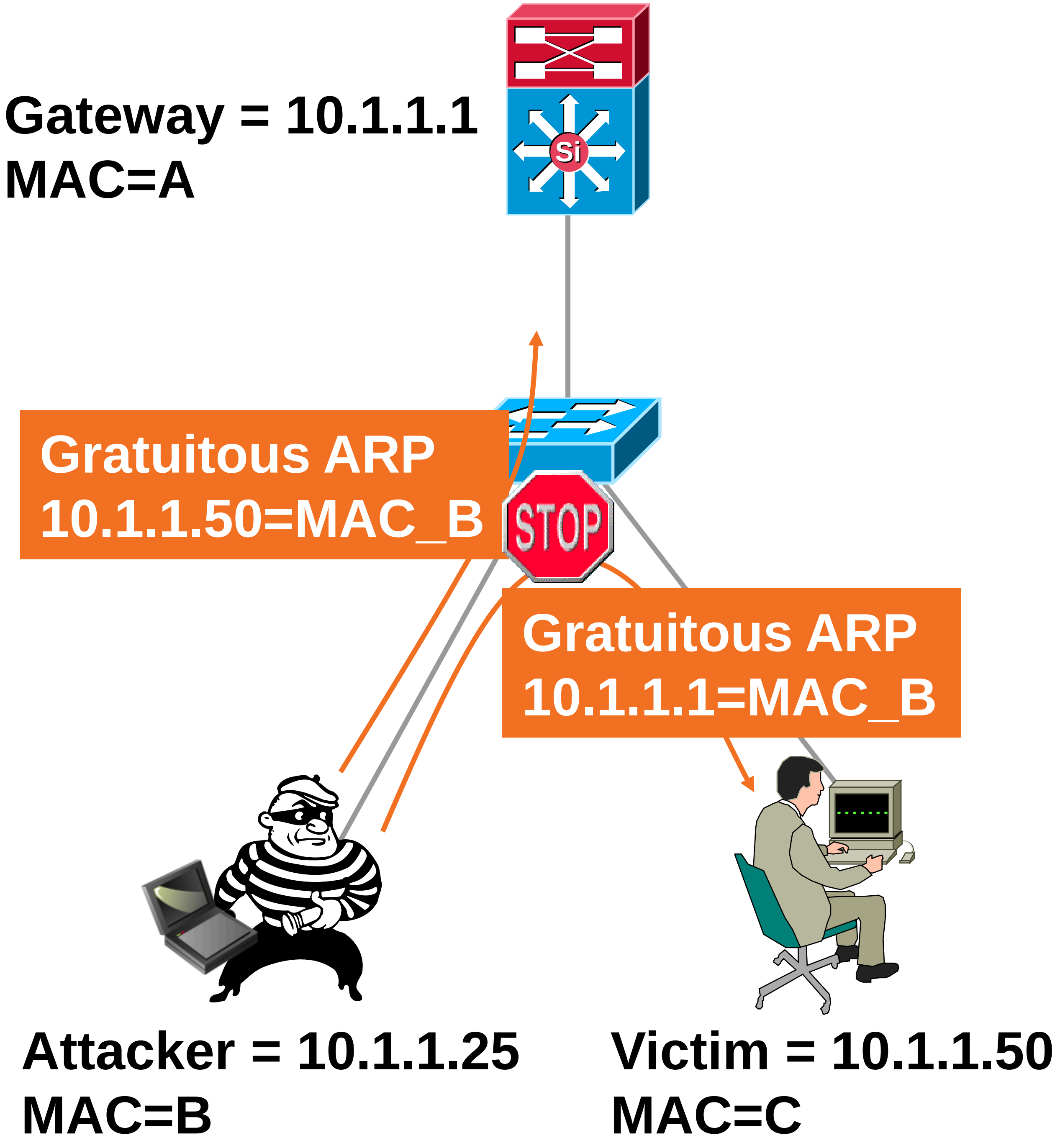


- DHCP requests (discover) and responses (offer) tracked
- Rate-limit requests on trusted interfaces; limits DoS attacks on DHCP server
- Deny responses (offers) on non trusted interfaces; stop malicious or errant DHCP server

Securing Layer 2 from Surveillance Attacks

Protection Against ARP Poisoning

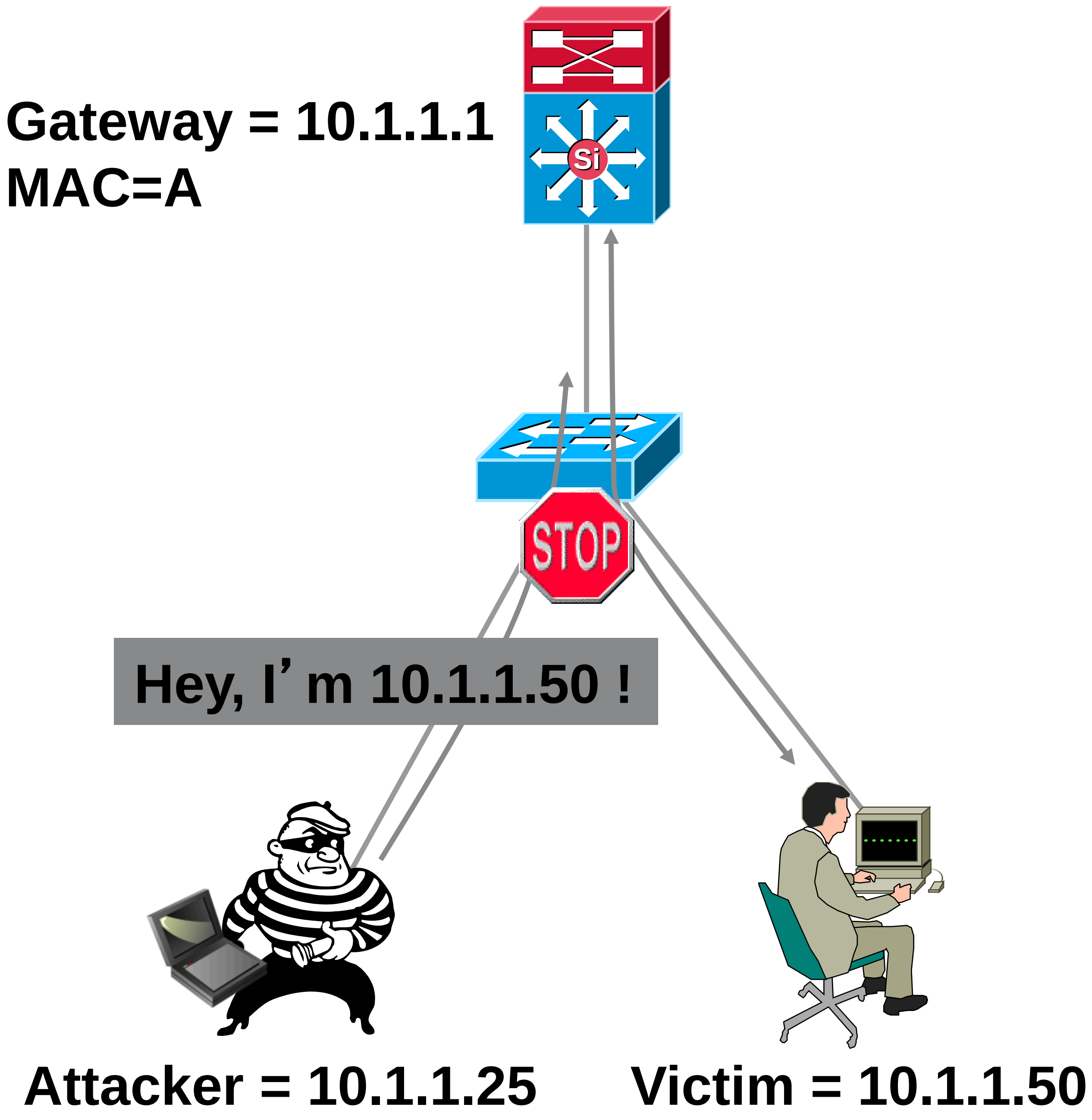
- Dynamic ARP inspection protects against ARP poisoning (ettercap, dsnif, arpspoof)
- Uses the DHCP snooping binding table
- Tracks MAC to IP from DHCP transactions
- Rate-limits ARP requests from client ports; stop port scanning
- Drop **bogus** gratuitous ARPs; stop ARP poisoning/MIM attacks



IP Source Guard

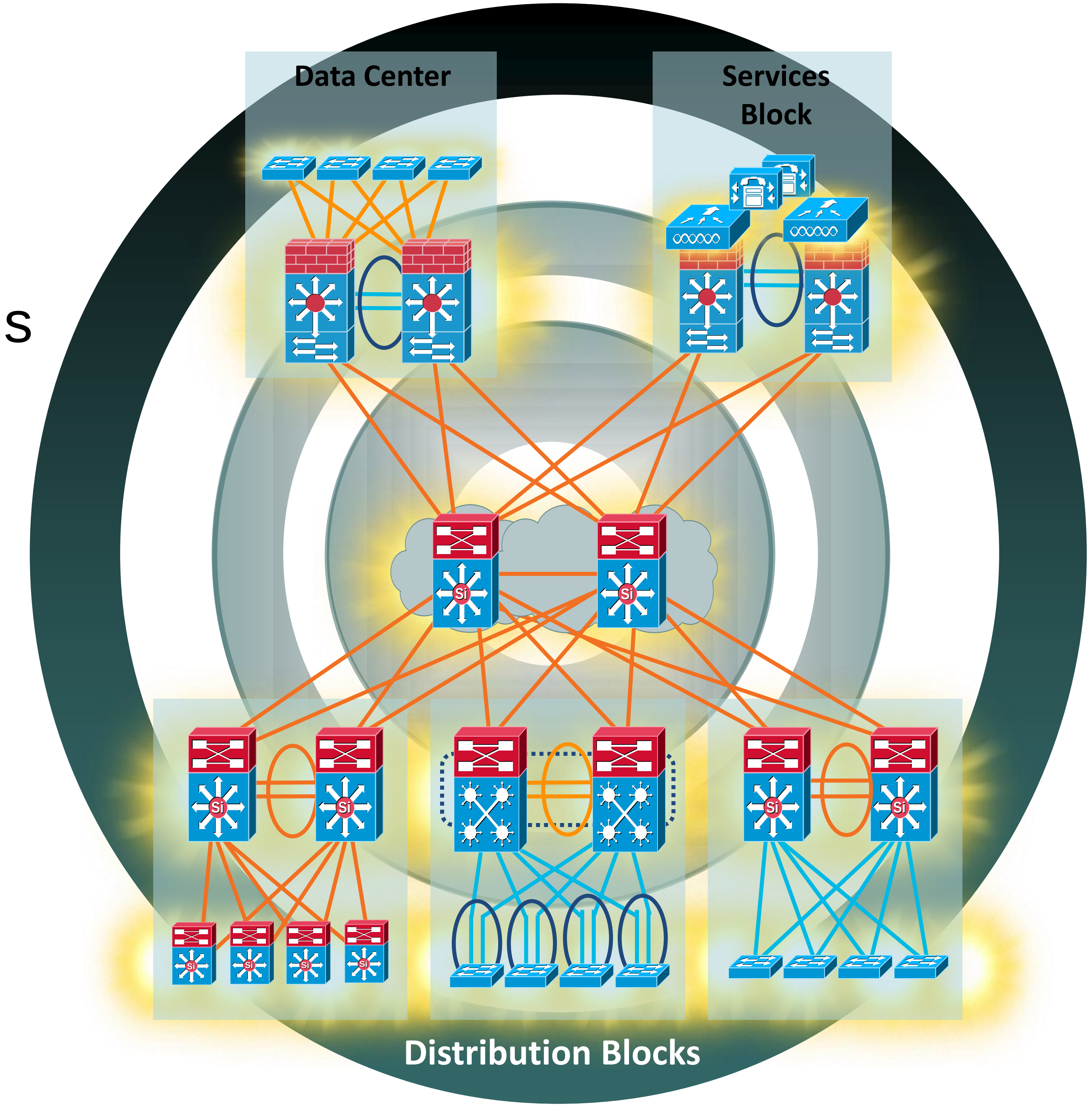
Protection Against Spoofed IP Addresses

- IP source guard protects against spoofed IP addresses
- Uses the DHCP snooping binding table
- Tracks IP address to port associations
- Dynamically programs port ACL to drop traffic not originating from IP address assigned via DHCP



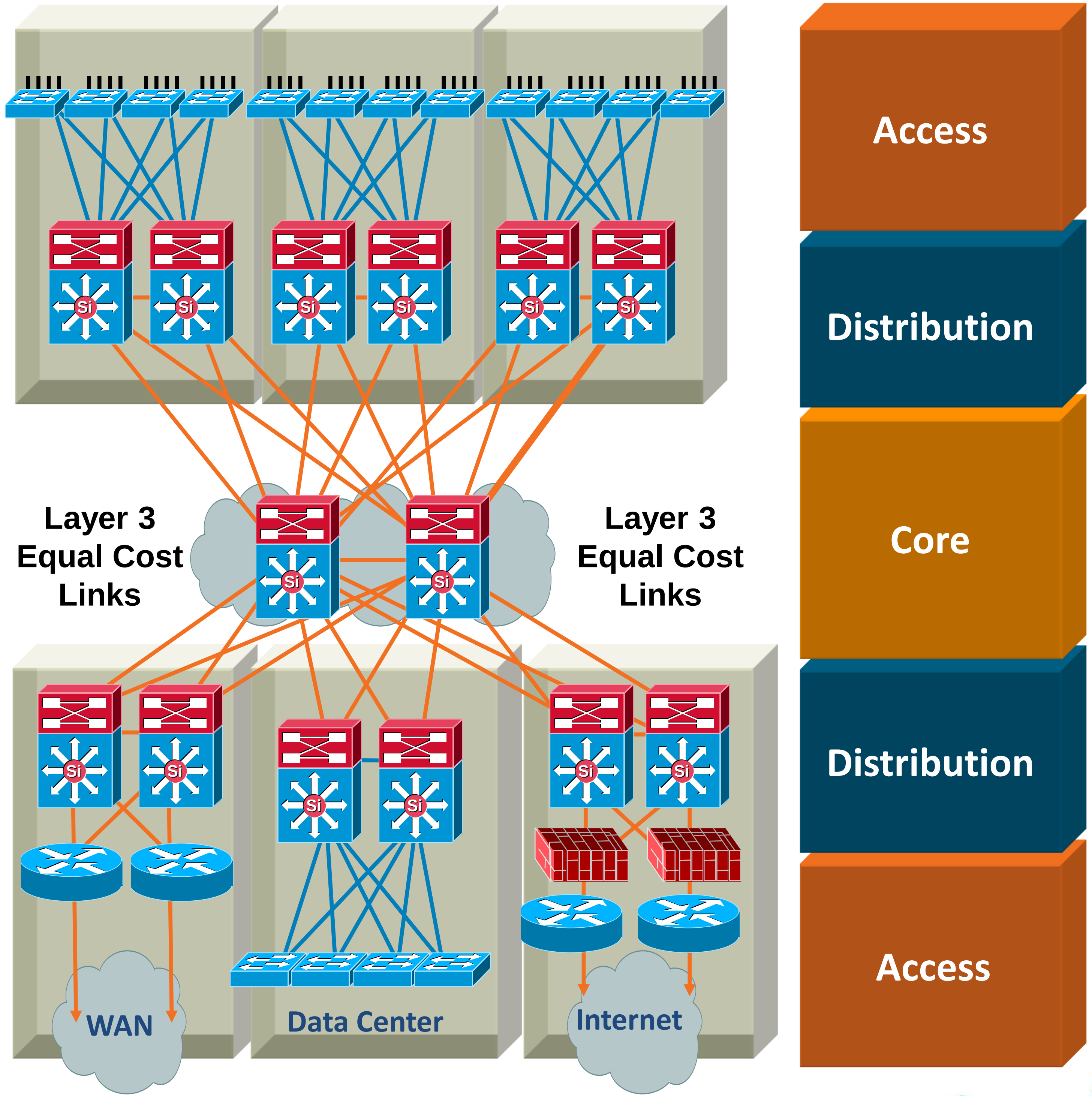
Agenda

- Multilayer Campus Design Principles
- Security Considerations
- Summary



Summary

- Hierarchy—each layer has specific role
- Modular topology—building blocks
- Easy to grow, understand, and troubleshoot
- Creates small fault domains— clear demarcations and isolation
- Promotes load balancing and redundancy
- Promotes deterministic traffic patterns
- Incorporates balance of both Layer 2 and Layer 3 technology, leveraging the strength of both
- Utilizes Layer 3 routing for load balancing, fast convergence, scalability, and control



Summary

Performance and Stability:

- Improved Performance: Support for deterministic traffic engineering designs
- Minimize Downtime: by providing redundancy and alternative-path routing
- Faster Convergence: Use Equal Cost Links & paths to enable traffic load-share and convergence
- Minimize Network Events: Enable Deterministic Convergence through design

Adapting to New Models - Change Management

- Ease Change: Building-block approach and well-defined boundaries
- Maximize Services Capability: QoS, Security, Policy, are implemented at appropriate layers & roles
- Enable Mission-specific Design: Modular structure: use platform, protocols and new solutions in well-defined modules as needed

BUILT FOR
THE HUMAN
NETWORK