Cisco Value Proposition for the Server Decision Maker

Marcus Phipps

Version 0.6

Applications Drive Server and Network Requirements

Server Requirements

- Processing power – scale-out or scale-up
- Speed of server provisioning
- Integrated server security
- Virtual machines and physically stateless servers
- Greater I/O
- Low latency

Network Requirements

Network Requirements

- Scalability of ports, MAC addresses, throughput and services
- High Availability
- Integrated network security
- Speed of service provisioning
- Blade server integration
- Low latency

Server Challenges Driving Change in Compute Infrastructure

Server Challenges

- Proliferation of disparate platforms, operating systems
- "Stovepiped" infrastructure
- Low server utilization
- Power/ cooling inefficiency
- Security and patches
- Reduces planned and unplanned downtime
- Standards-based affordable high performance

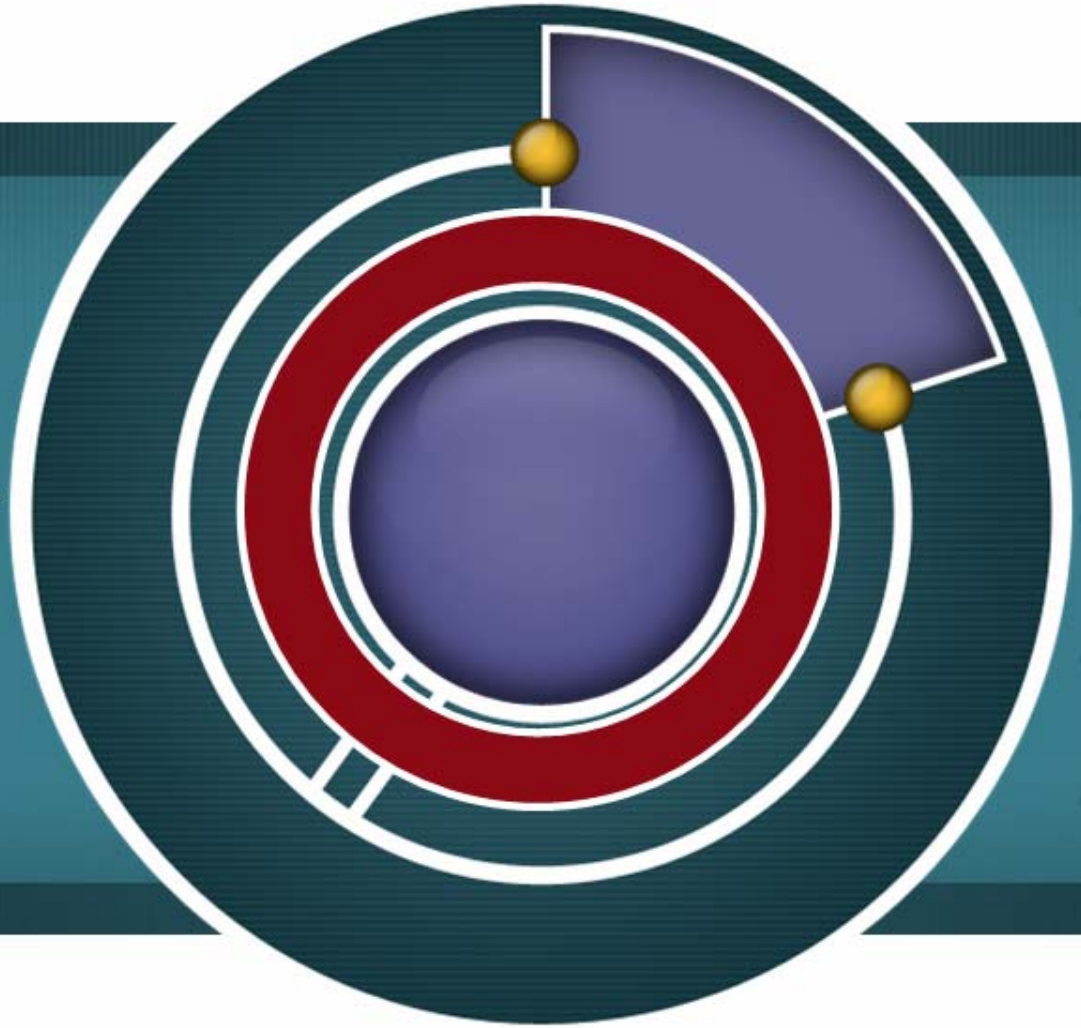
Server Trends

- Standardization
- Server consolidation
- Virtual Machines
- Blade servers and rack optimized x86 servers
- Day-zero security
- Clustering and High Performance Computing
- Dynamic bare-metal server provisioning

Bringing Network Value to the Server

Server Trends

- Standardization & consolidation
- Virtual Machines
- Blade servers/ x86 server scale-out
- Day zero Security
- Clustering and high performance computing

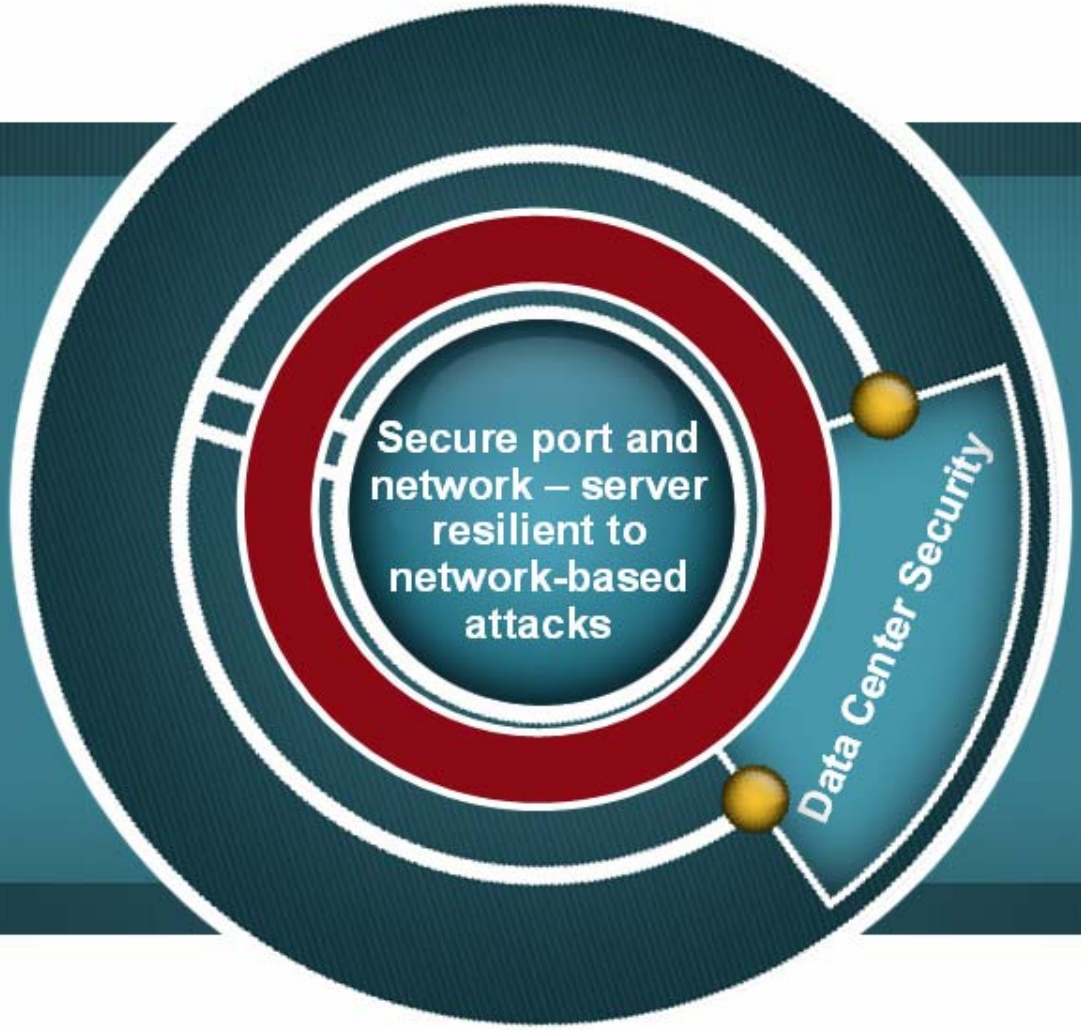


Network Requirements

- Virtual machine support
- Network-based security
- High availability and business resilience
- Visibility and automated provisioning
- Consolidated and virtualized I/O

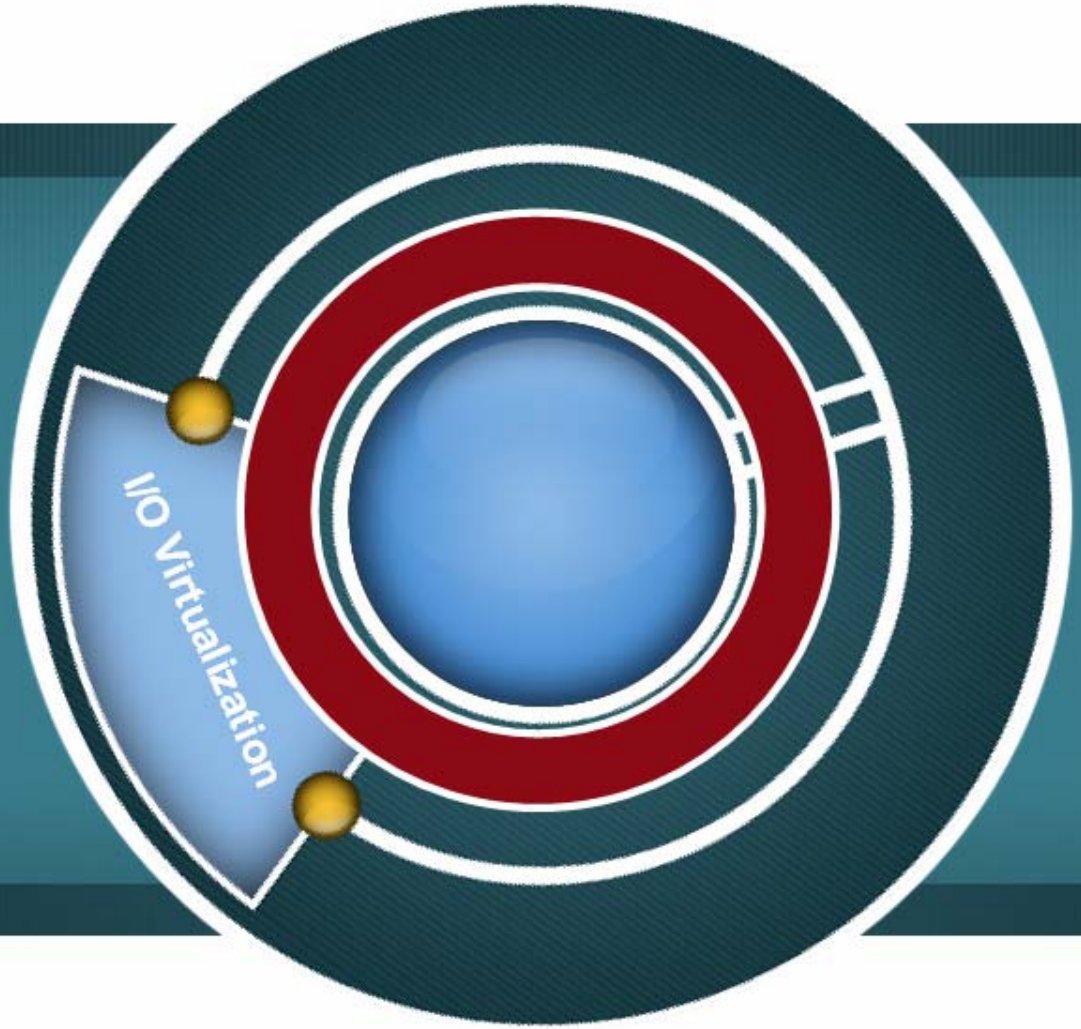
Bringing Network Value to the Server

Bringing Network Value to the Server

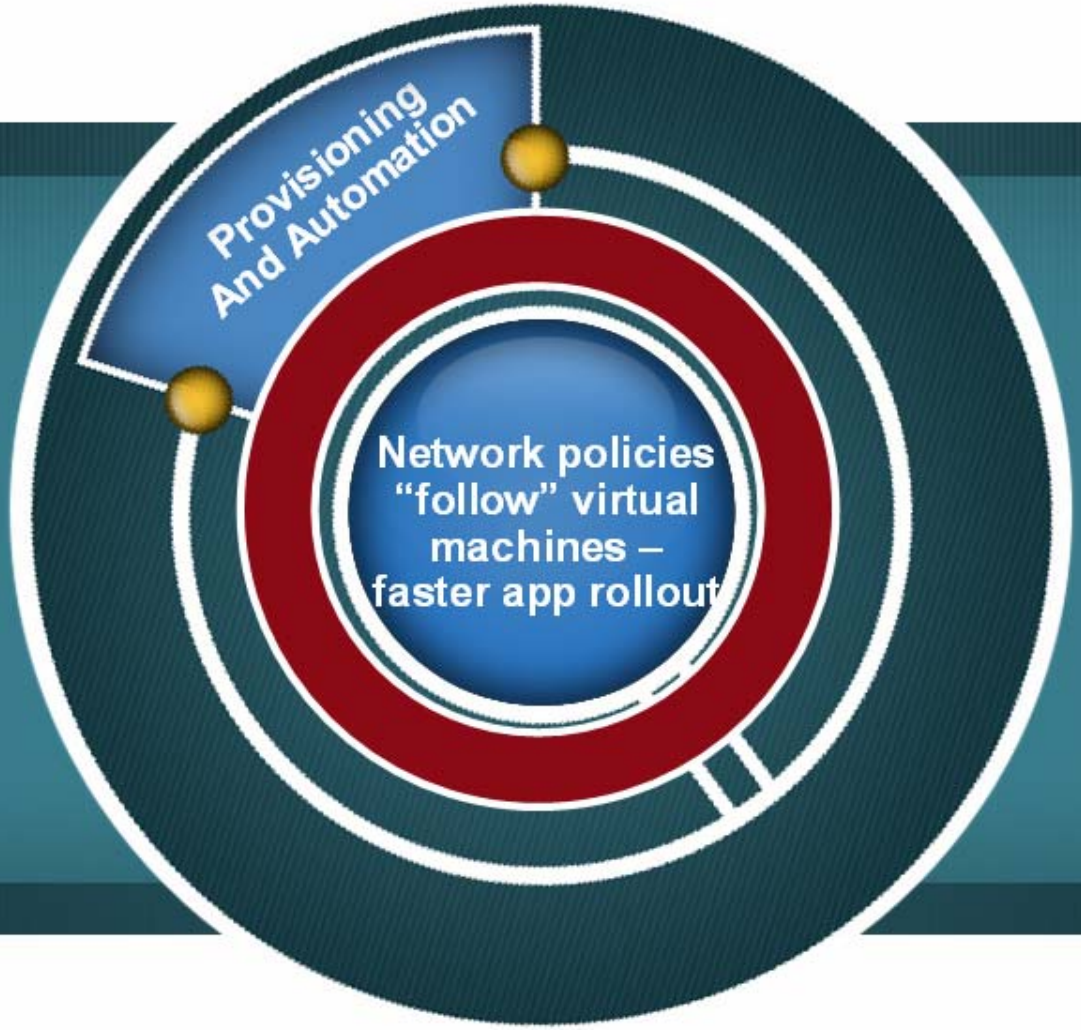


Bringing Network Value to the Server

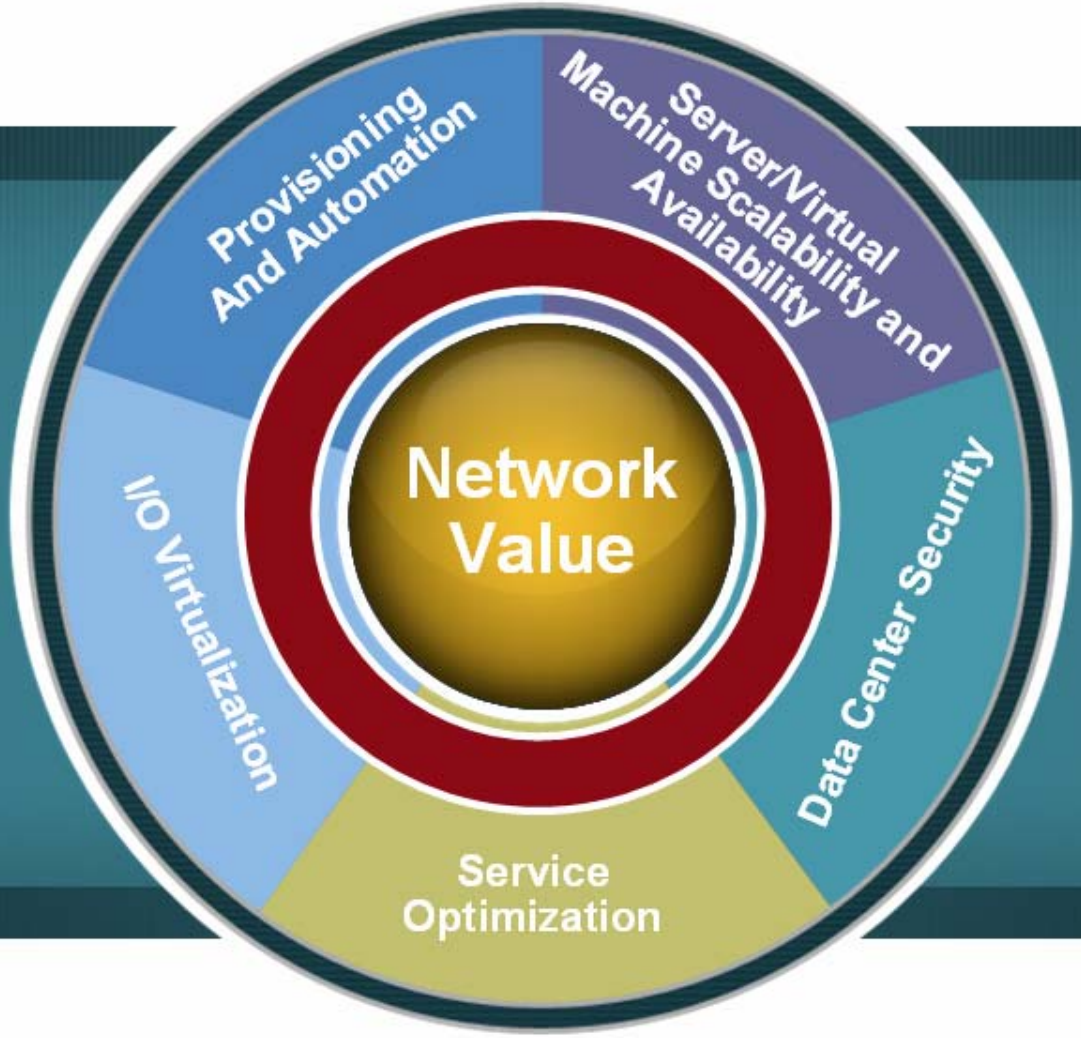
Bringing Network Value to the Server



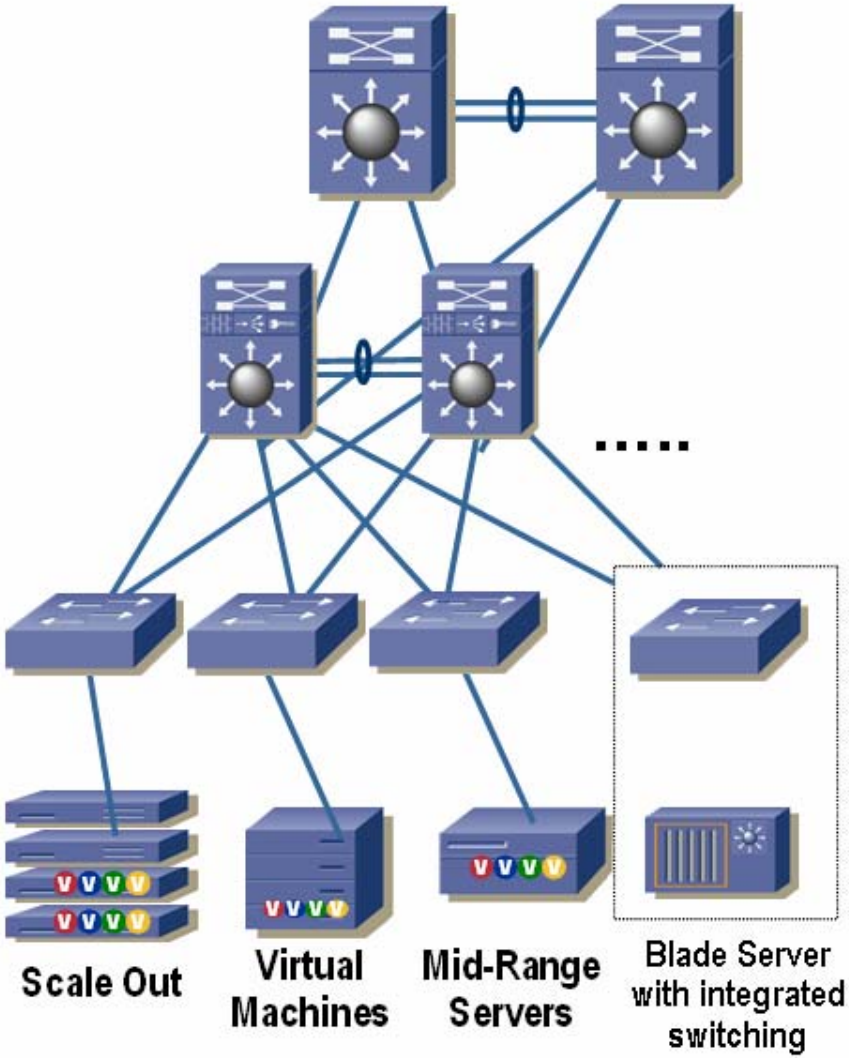
Bringing Network Value to the Server



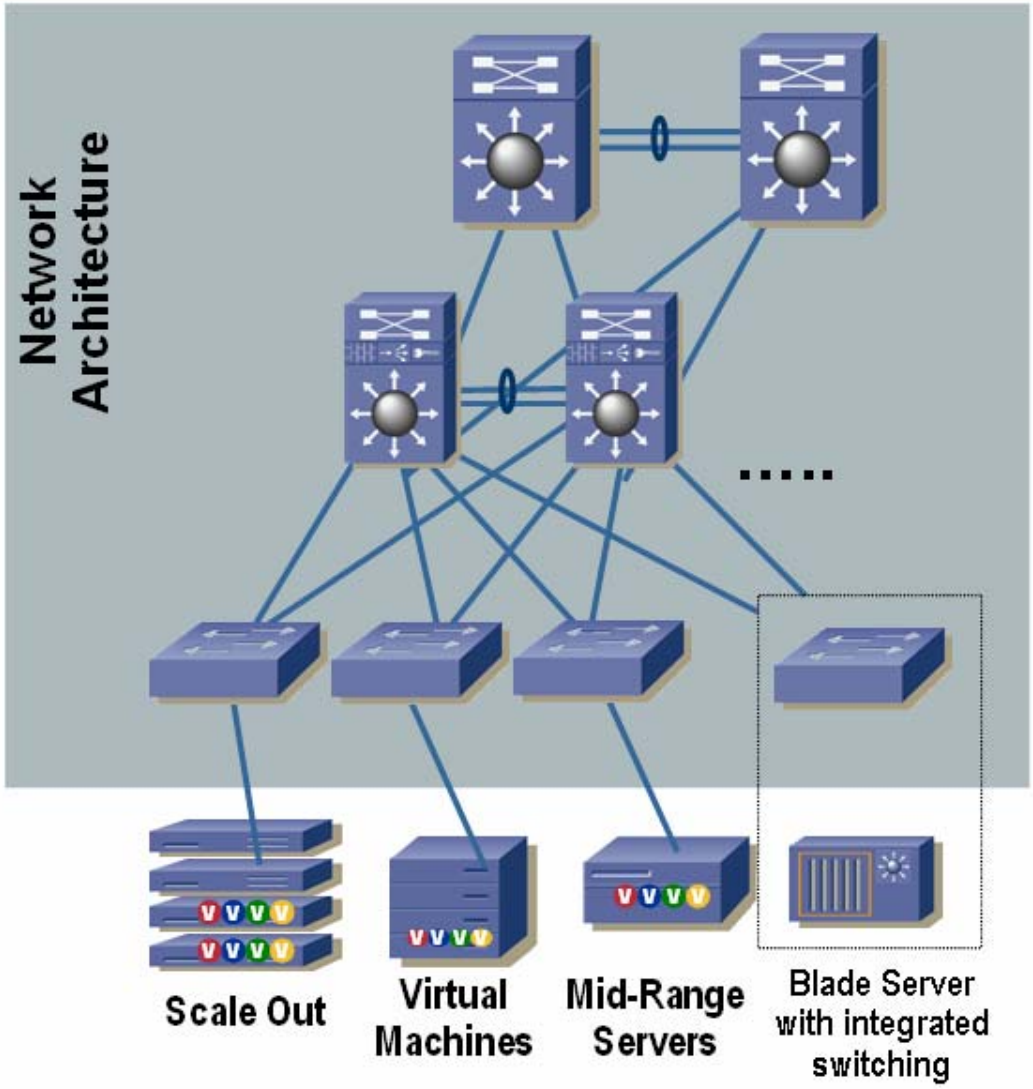
Bringing Network Value to the Server



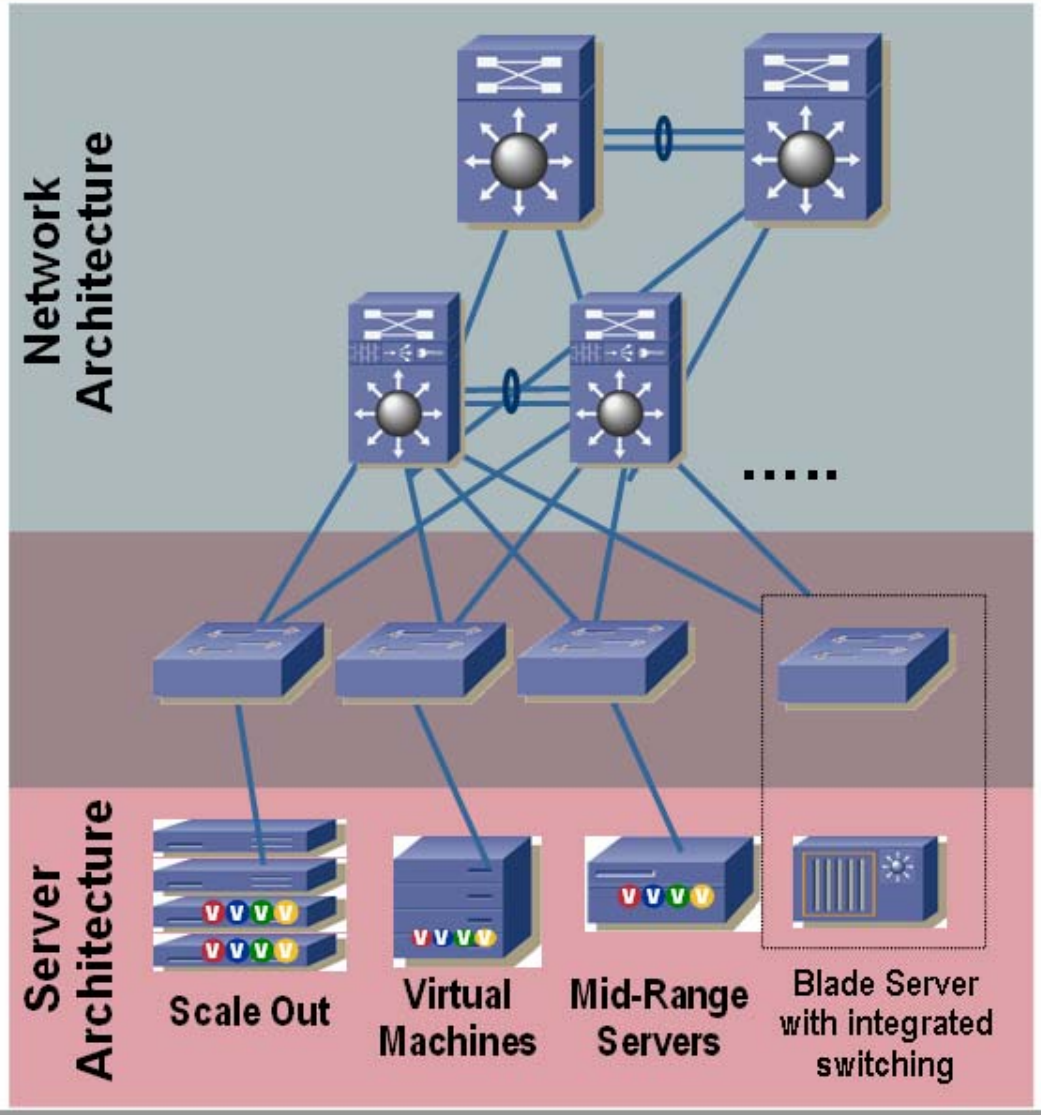
Cisco Server Farm Architecture



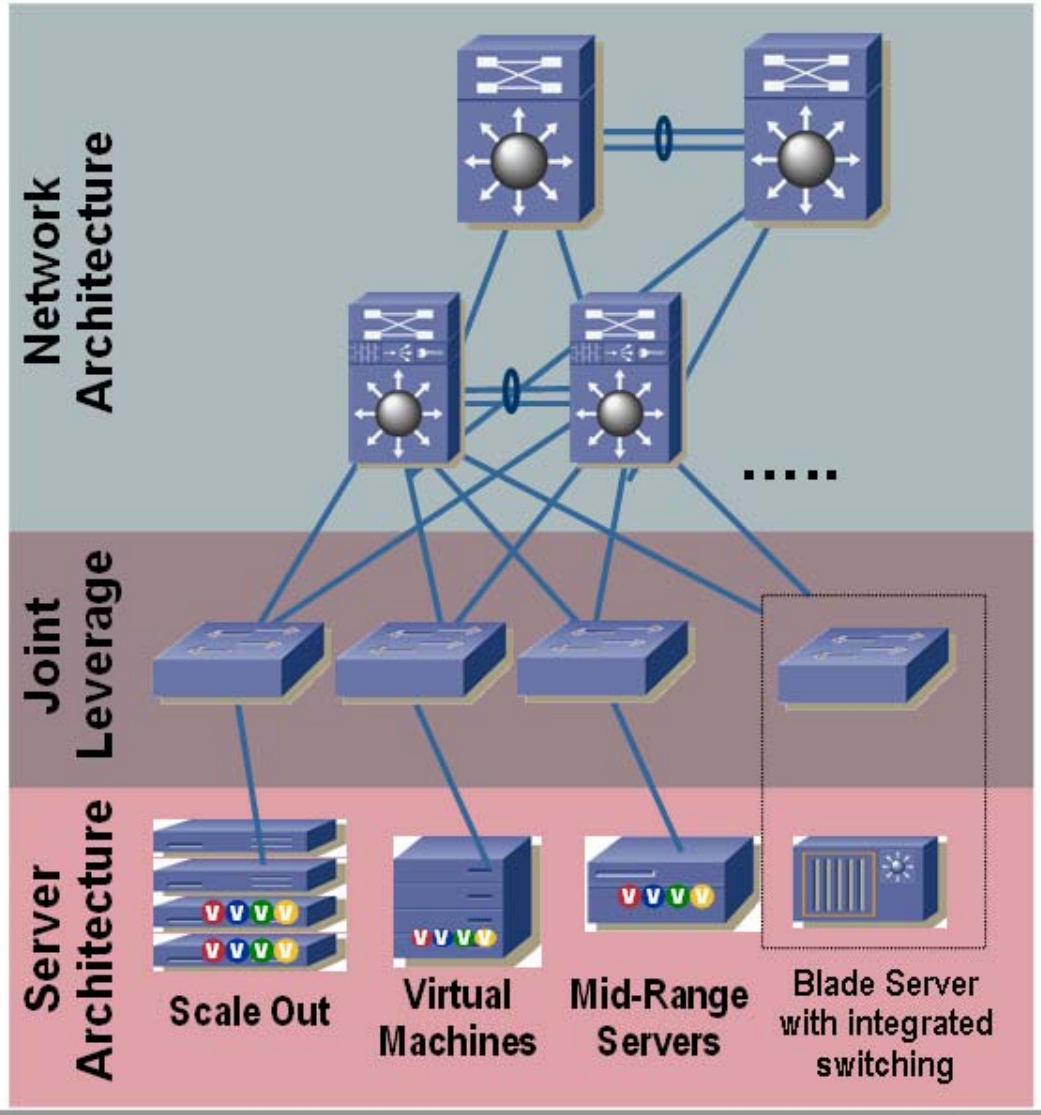
Cisco Server Farm Architecture



Cisco Server Farm Architecture



Cisco Server Farm Architecture

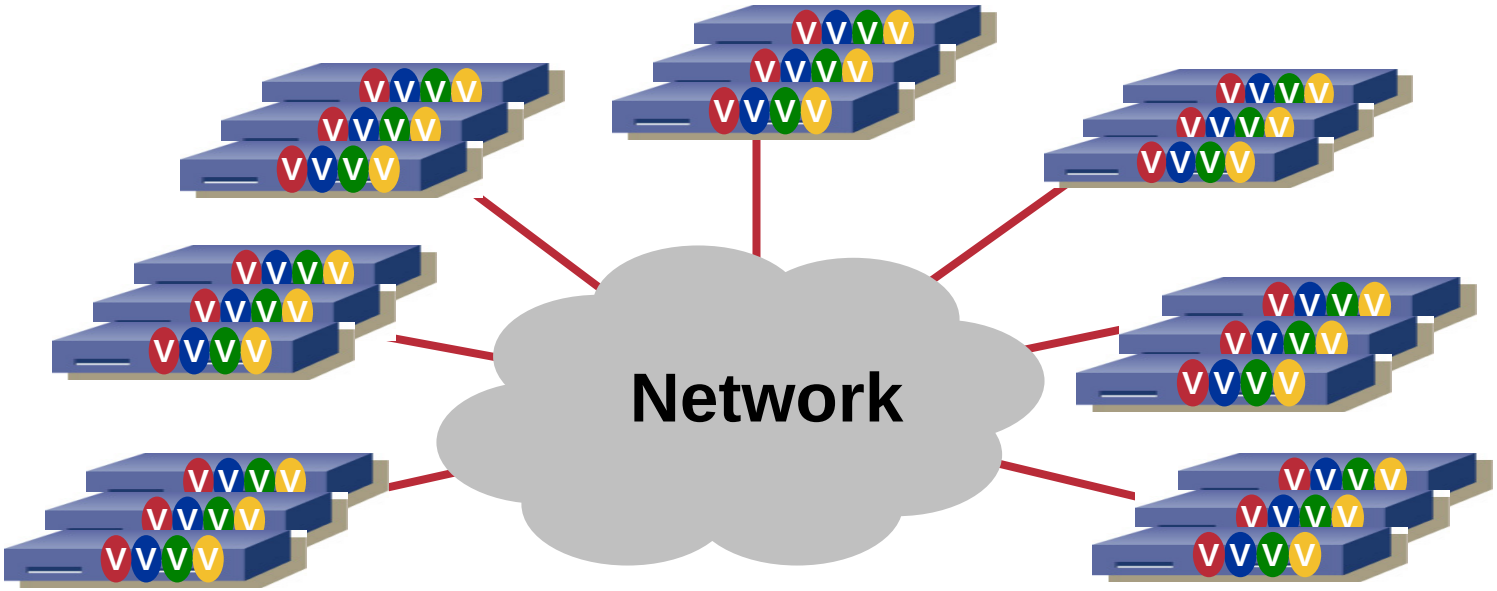


- **Server choice influences network access mechanism**
- **Flexible architecture required to deliver**
  - Scalability to grow as needed
  - Comprehensive resilience
  - Segmented workgroups
- **Ensures optimal support for scale-out, scale-up and virtual machine support**

The Impact of Virtual Machines on Networking

Before	After
Physically separate infrastructure	Logical and virtualized infrastructure
Identity of the physical servers (network address) used to provide differentiated application services within the network	Multiple VMs can be identified by separate MAC addresses. Software virtual switch enables communication between VMs and the network
Network services and policies are fully contained within the network (single management domain)	Hypervisor virtual switch creates a dual management domain as network services and policies exist both within the server and the network
Lower I/O requirements	High I/O requirements
Lower security risk impact – port based mapping and access control	High security risk impact – per virtual server control needed

Example: Virtual Machine and Scale-Out Deployments – Server Requirements…

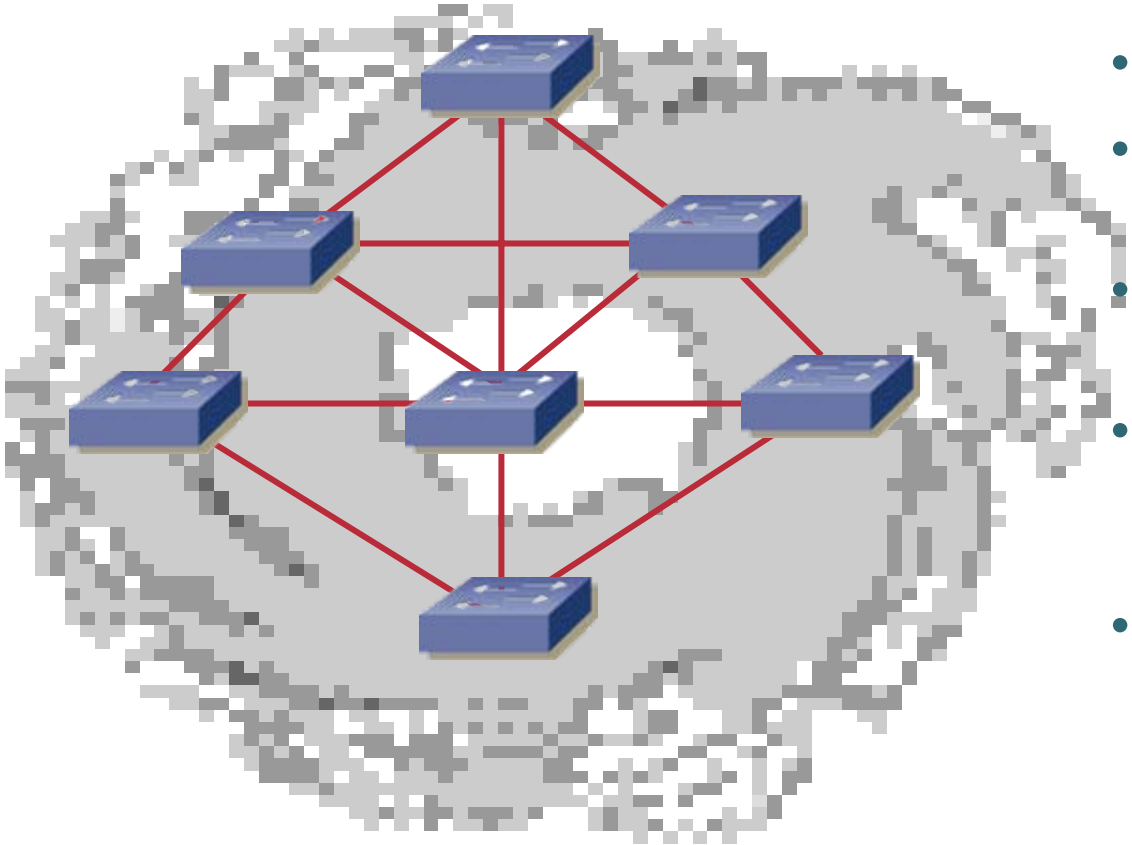


- **Design Requirements**

  500 Servers with each server having 8 Virtual Machines assigned with a flat address space

  Connectivity on a single VLAN – provides rapid VM bring-up and network connectivity (ie, no request needed to network team for support)

…And the Effect on the Network

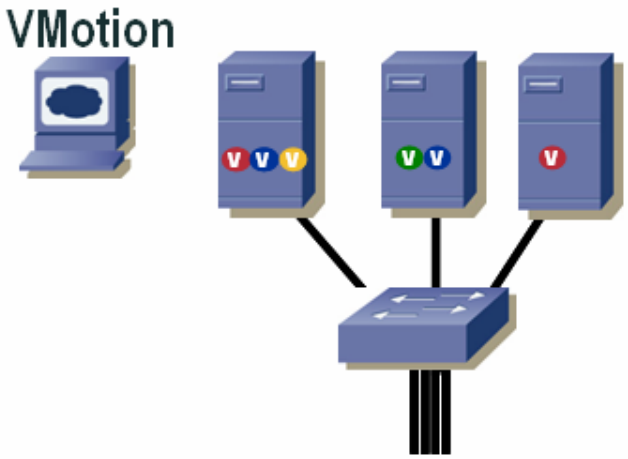


- Massive Layer 2 domain
- Uncontrolled multicasts and broadcasts
- Broadcast storms can affect server performance
- Spanning Tree complexities can adversely affect availability
- Network wide open to security attacks and address spoofing

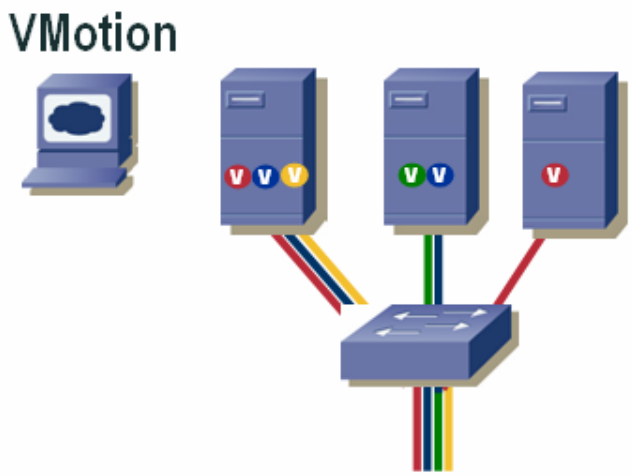
Result: A poorly designed network which will affect server performance

The Impact of Mobility on Networking

- **Flat Layer 2 Topology**
  - It works, but…
  - … grouping too many physical servers on the same VLAN creates scalability, availability and security issues
  - Not a recommended practice, but still very common today

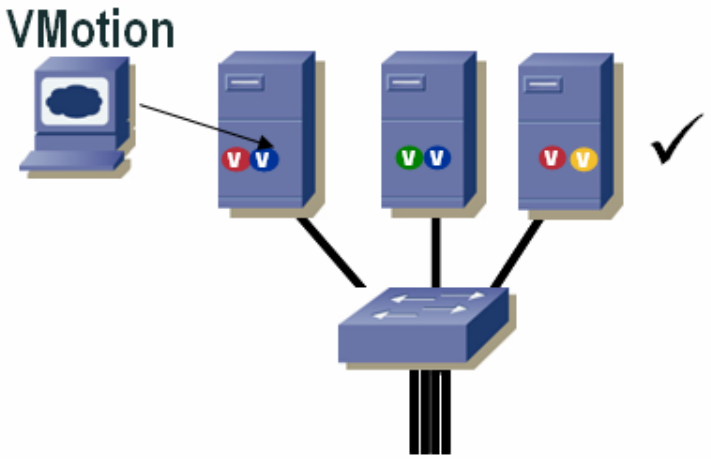


- **Segmentation Using VLANs**
  - VLAN Tagging implemented by software virtual switch
  - Requires Ethernet NICs that support VLAN tagging
  - It works better, but…
  - …VMs need to be migrated within same VLAN

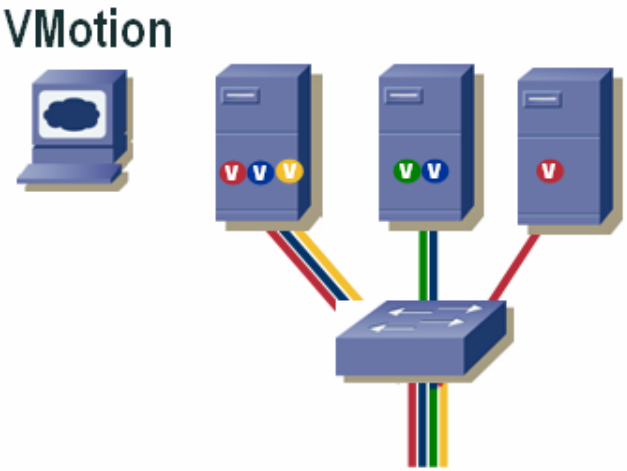


The Impact of Mobility on Networking

- **Flat Layer 2 Topology**
  - It works, but…
  - … grouping too many physical servers on the same VLAN creates scalability, availability and security issues
  - Not a recommended practice, but still very common today



- **Segmentation Using VLANs**
  - VLAN Tagging implemented by software virtual switch
  - Requires Ethernet NICs that support VLAN tagging
  - It works better, but…
  - …VMs need to be migrated within same VLAN



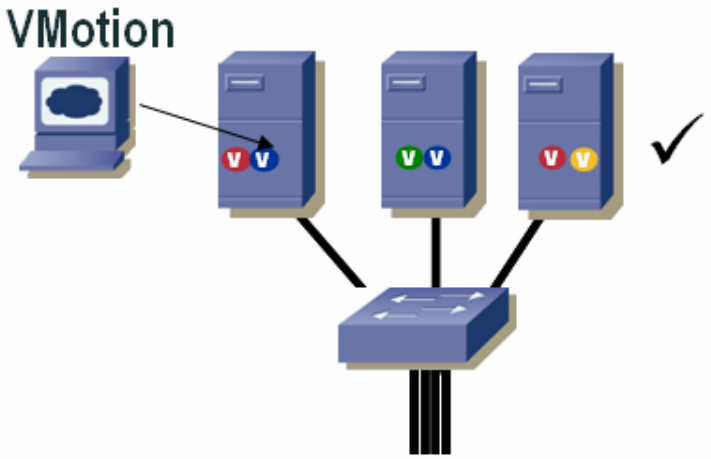
The Impact of Mobility on Networking

- **Flat Layer 2 Topology**

  It works, but…

  … grouping too many physical servers on the same VLAN creates scalability, availability and security issues

  Not a recommended practice, but still very common today



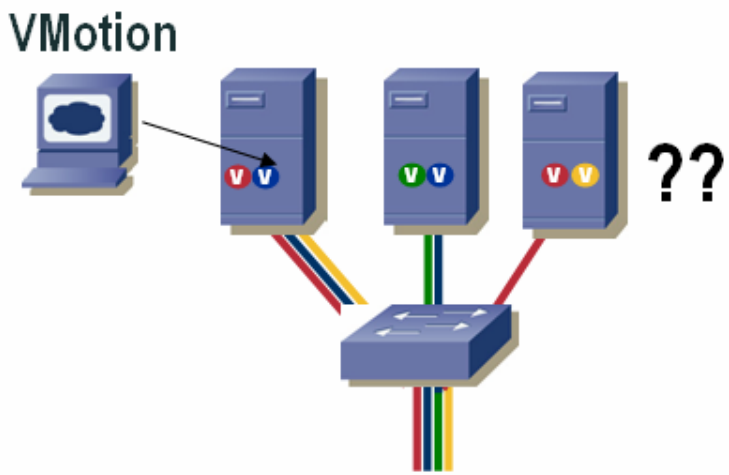
- **Segmentation Using VLANs**

  VLAN Tagging implemented by software virtual switch

  Requires Ethernet NICs that support VLAN tagging

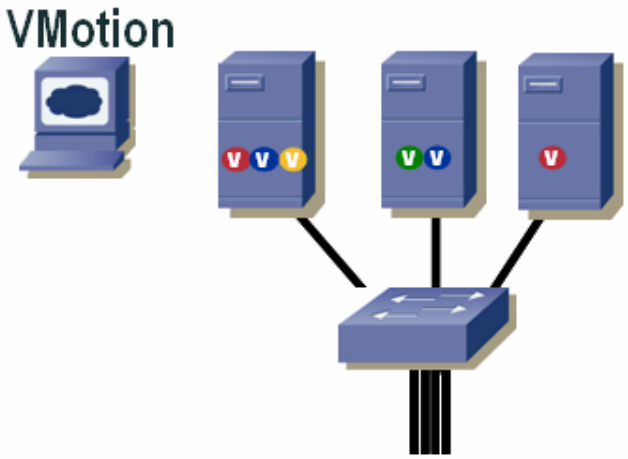
  It works better, but…

  …VMs need to be migrated within same VLAN

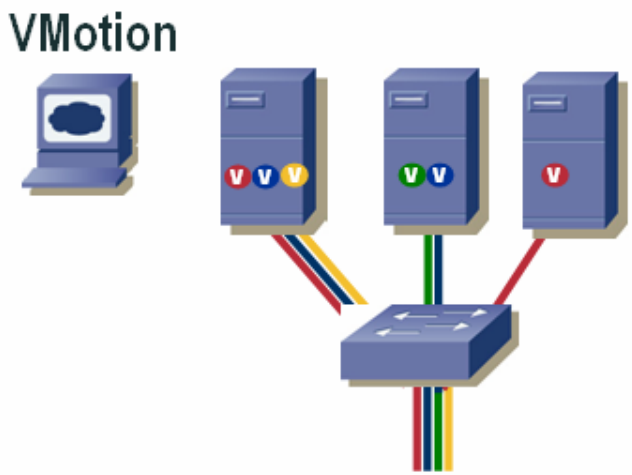


The Impact of Mobility on Networking

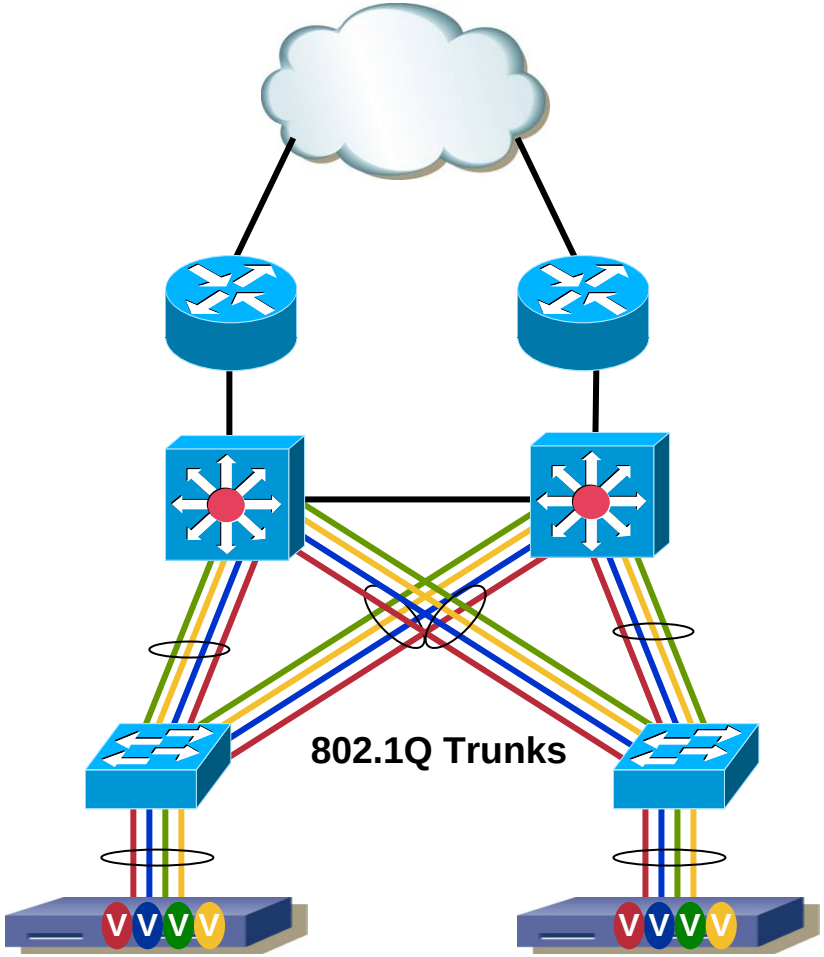
- **Flat Layer 2 Topology**
  - It works, but…
  - … grouping too many physical servers on the same VLAN creates scalability, availability and security issues
  - Not a recommended practice, but still very common today



- **Segmentation Using VLANs**
  - VLAN Tagging implemented by software virtual switch
  - Requires Ethernet NICs that support VLAN tagging
  - It works better, but…
  - …VMs need to be migrated within same VLAN



Virtual LANs and 802.1Q Trunking – Logical Separation between Virtual Machines



- **What VLANs do:**

  Provides traffic isolation at Layer 2 into different broadcast domains.

  IEEE 802.1Q trunks allows multiple VLANs onto a common Ethernet link

- **Benefit:**

  Mapping of virtual machines to VLANs provides traffic and application segmentation for policy management and control.

  Smaller Layer 2 domains increase availability by simplifying Spanning Tree and

EtherChannel for Link Aggregation

- **Problem**

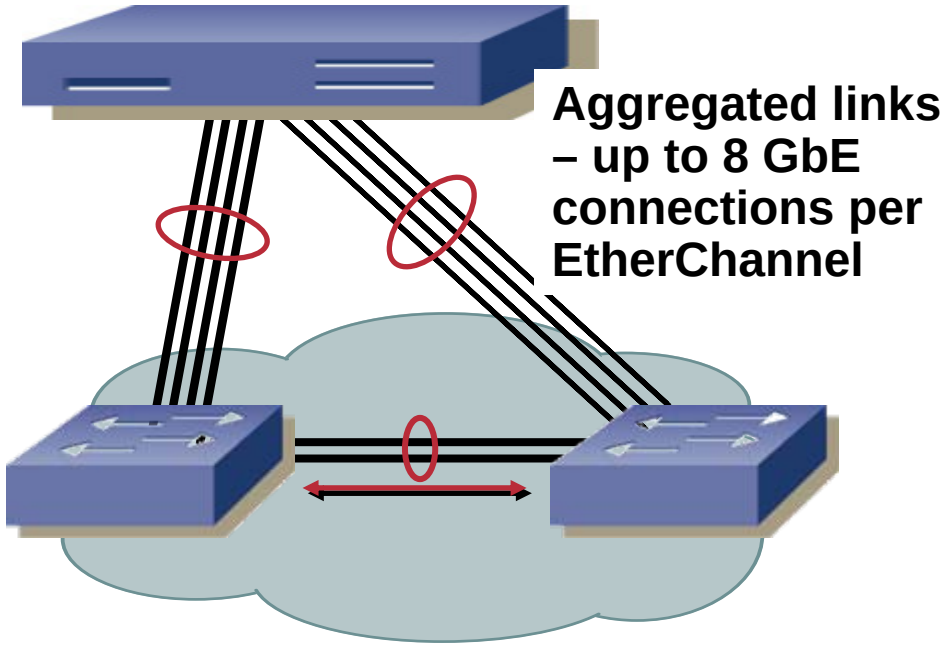
  Incremental bandwidth needed between server or virtual machines and the network

  1GbE or 10GbE?

- **Solution**

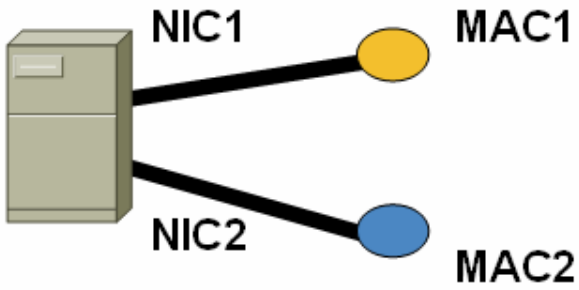
  EtherChannel provides a point-to-point logical aggregation of up to eight 100 Mbps, 1 Gbps or 10Gbps ports.

  Cisco supports IEEE 802.3ad Link Aggregation Control Protocol (LACP) for channel detection



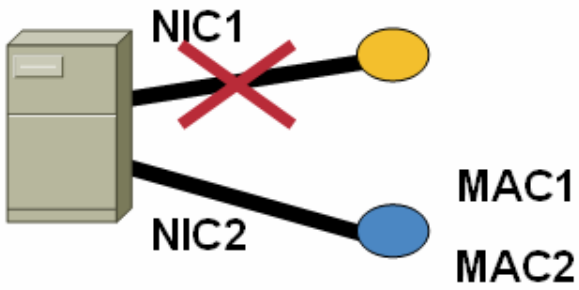
NIC Failover Design Implications

- Servers are often dual connected for high availability - NIC drivers allow to bundle multiple NIC cards as if they were a single interface
- If one NIC loses connectivity the redundant NIC becomes active and inherits the same MAC address as the primary one
- The server is always reachable at the same IP address



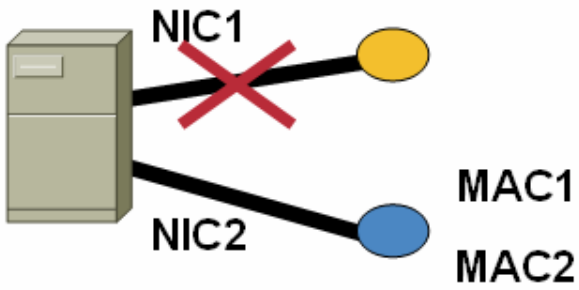
NIC Failover Design Implications

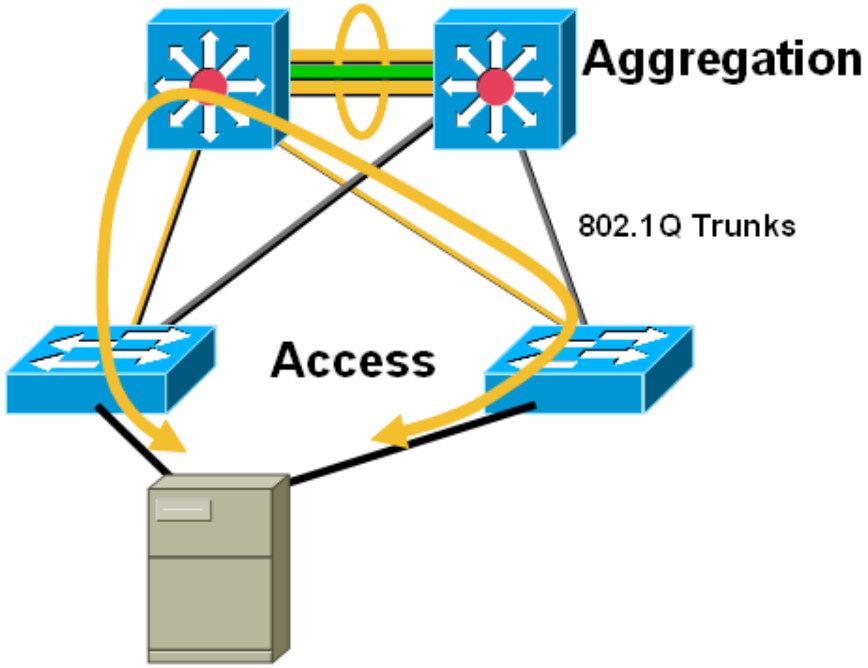
- Servers are often dual connected for high availability - NIC drivers allow to bundle multiple NIC cards as if they were a single interface
- If one NIC loses connectivity the redundant NIC becomes active and inherits the same MAC address as the primary one
- The server is always reachable at the same IP address



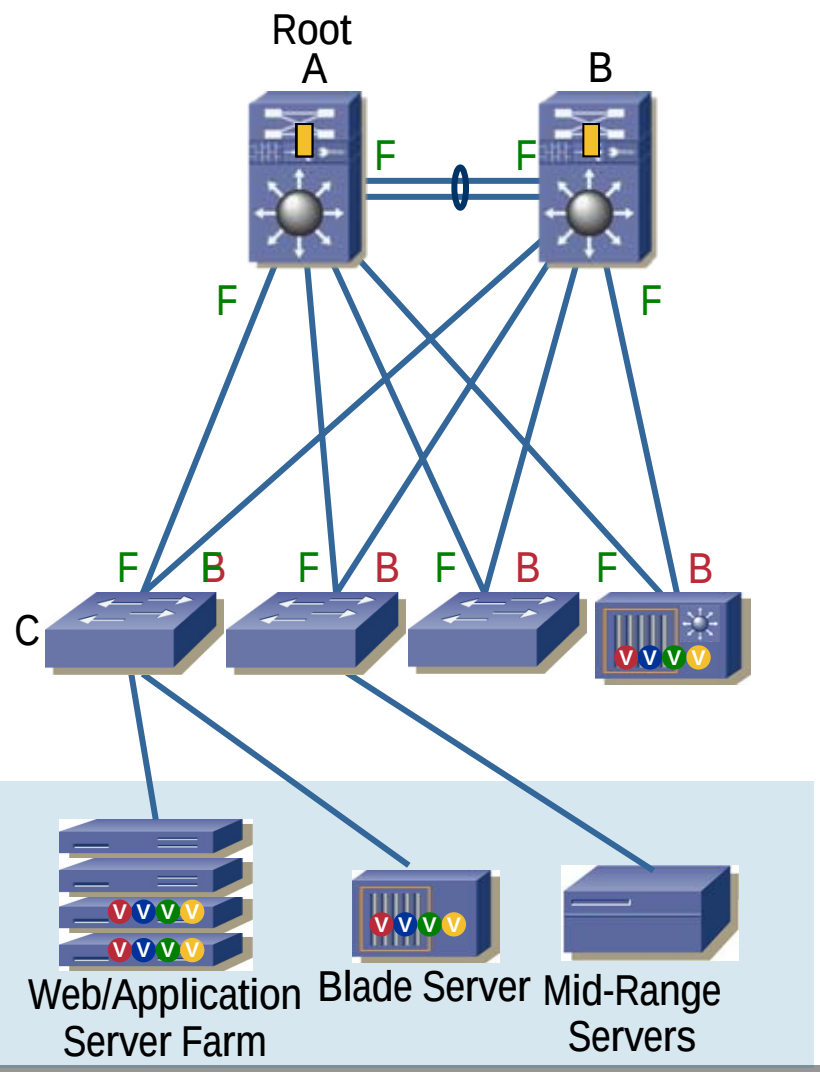
NIC Failover Design Implications

- Servers are often dual connected for high availability - NIC drivers allow to bundle multiple NIC cards as if they were a single interface
- If one NIC loses connectivity the redundant NIC becomes active and inherits the same MAC address as the primary one
- The server is always reachable at the same IP address
- This means that both NIC need to belong to the same broadcast domain, VLAN and subnet
- The access switches need to provide layer 2 adjacency between the NIC cards of servers with NIC teaming configured . A layer 2 path must exist between such servers





Why Care About Spanning Tree?



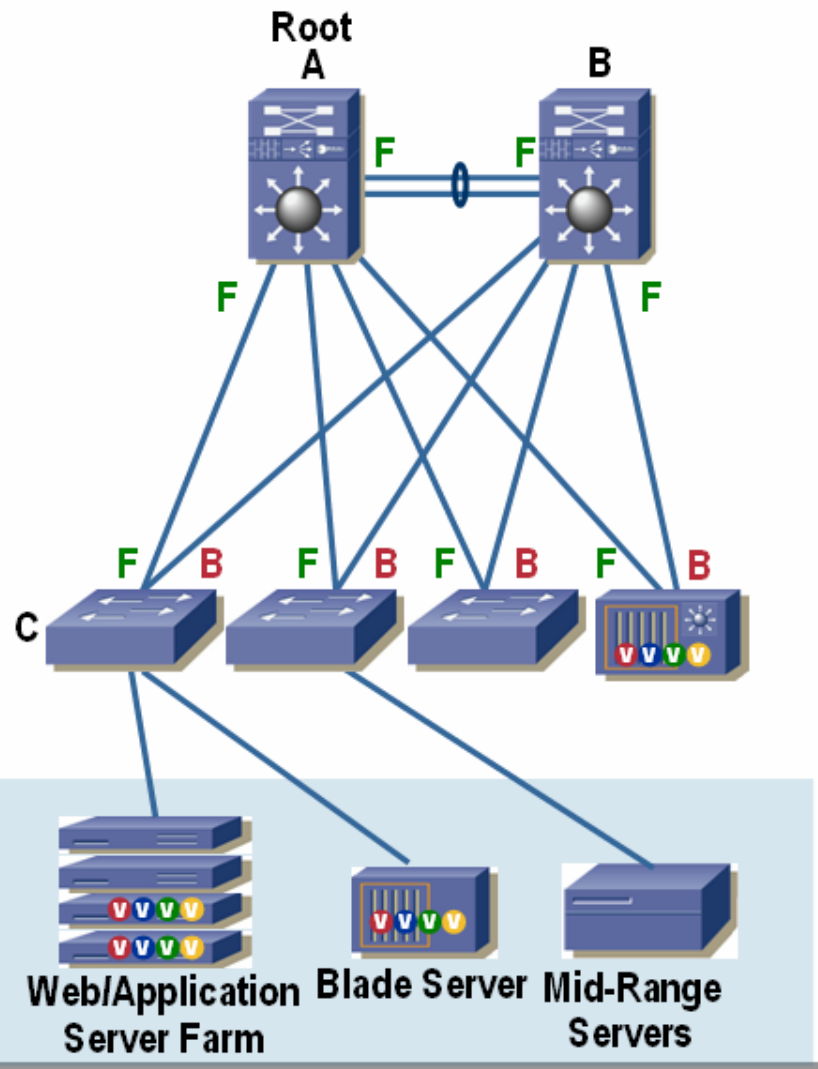
- Server and VM design can severely affect network and server availability
- What happens if a link fails (IEEE 802.1s/w)?
- Benefits of Cisco Spanning Tree implementations

Cisco has the most Spanning Tree development, design and deployment experience in the industry (since 1993)

Measured failover for blade servers and edge switches at 1-2 seconds (VERIFY!)

Hardware-based MAC learning provides rapid re-learning after recovery

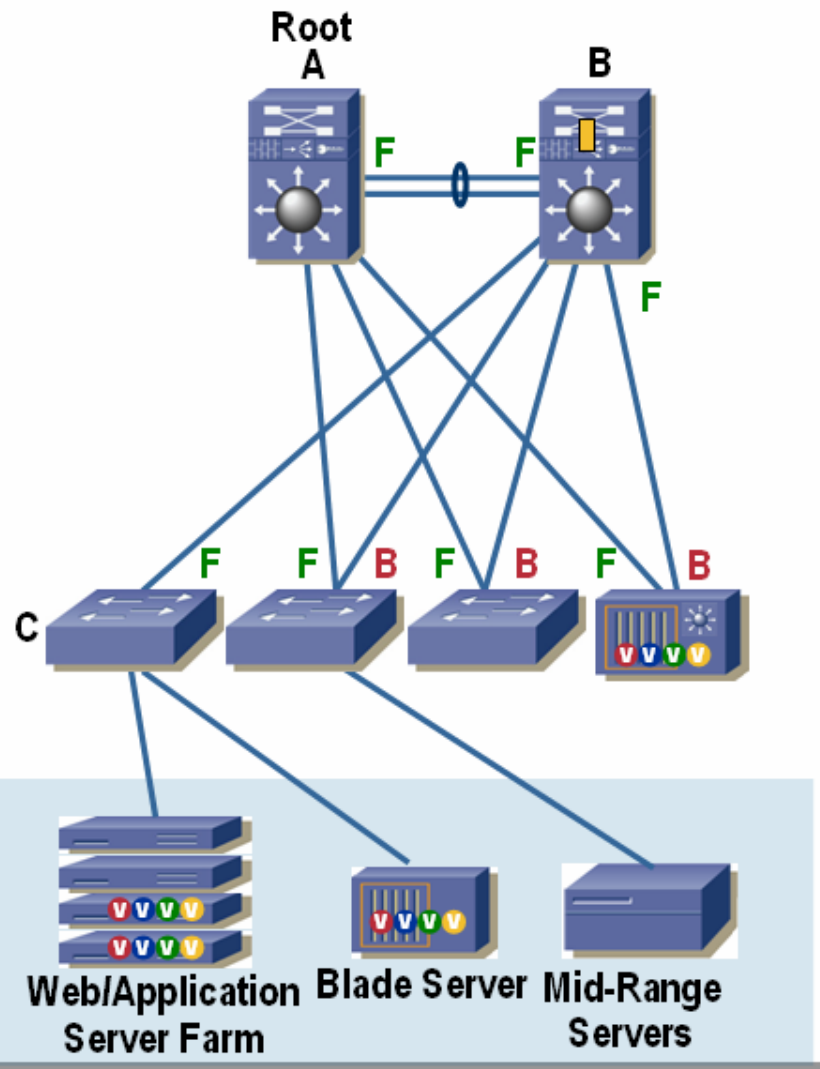
Why Care About Spanning Tree?



Server and VM design can severely affect network and server availability

- Size of Layer 2 network will affect how fast the network converges in the event of a failure
- Number of MAC addresses in a VLAN can slow the rate of switch learning
- Feature consistency between blade servers and network switches can cause longer service outages

Why Care About Spanning Tree?



Server and VM design can severely affect network and server availability

What happens if a link fails (IEEE 802.1s/w)?

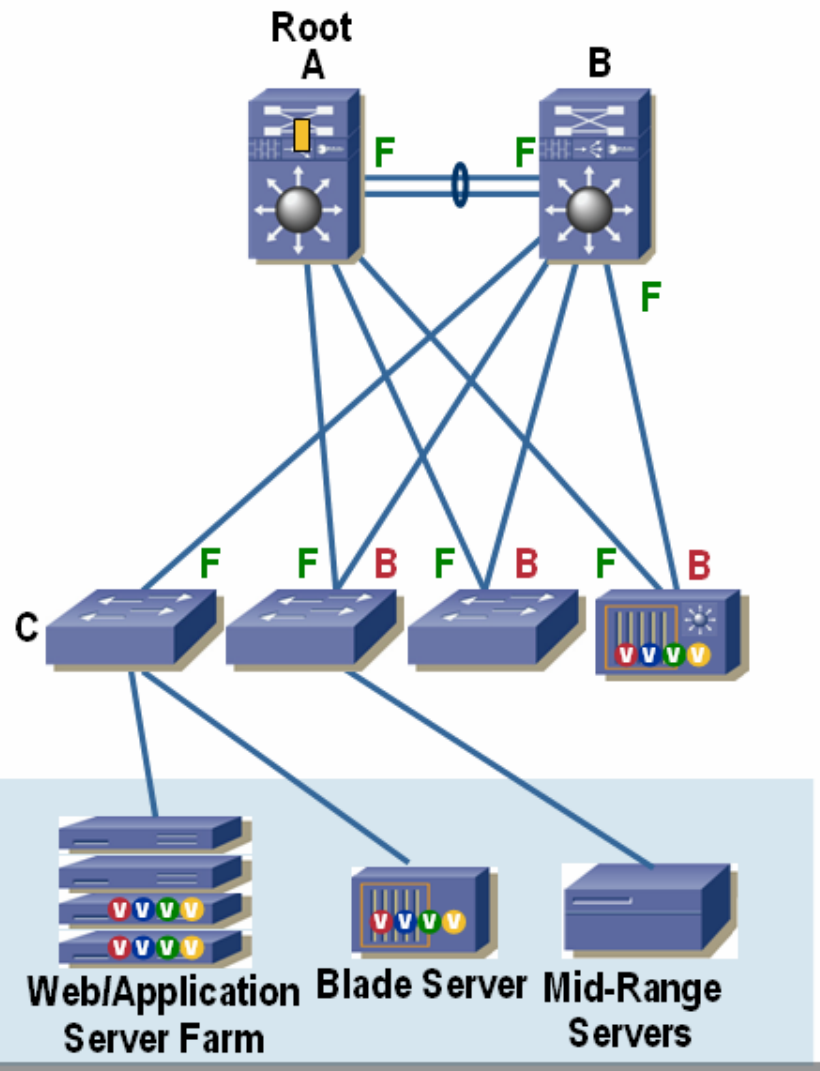
1. Link A-C fails
2. New path must be found and verified to be loop-free – Switch B and C exchange STP information
3. Switch B tells Switch A to flush all MAC addresses in all common VLANs EXCEPT those learnt from Switch B
4. Switch A sends a Topology Change message to all adjacent switches (except B) telling them to forget all MAC addresses EXCEPT those learnt via Switch A

Network stabilizes – traffic forwarded between B-C.

Servers and VMs on Switch C in that VLAN unreachable while STP converges

Time to "repair" – 1-50 seconds depending on implementation

Why Care About Spanning Tree?



- Server and VM design can severely affect network and server availability
- What happens if a link fails (IEEE 802.1s/w)?
- Benefits of Cisco Spanning Tree implementations

Cisco has the most Spanning Tree development, design and deployment experience in the industry (since 1993)

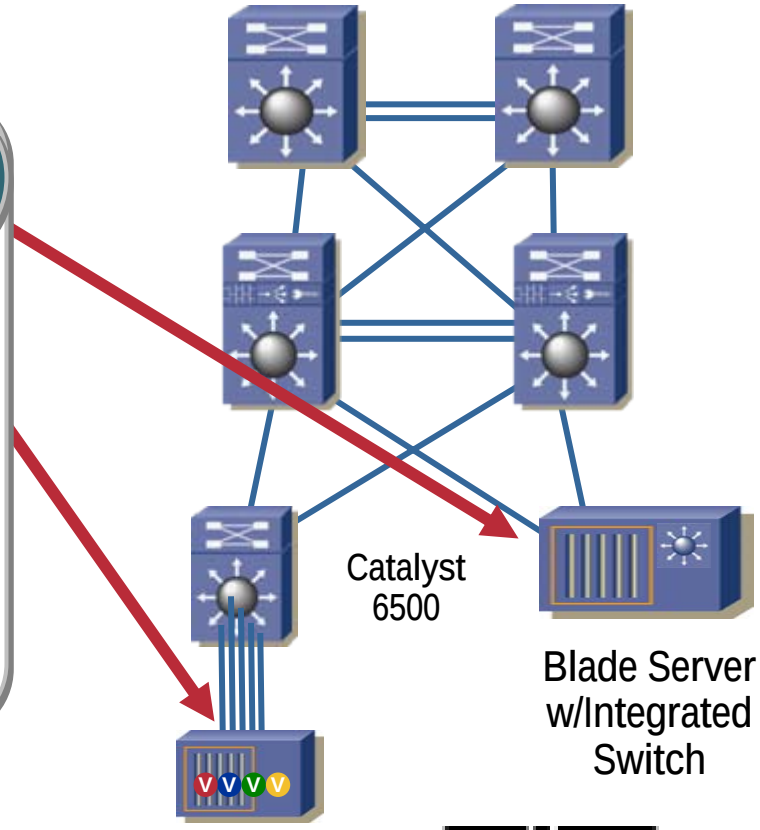
Measured failover for blade servers and edge switches at 1-2 seconds (VERIFY!)

Hardware-based MAC learning provides rapid re-learning after recovery

Cisco Server Farm Solution
Blade Server Topological Considerations

Requirement: integrate blade servers into a scalable server farm

- Cisco integrated Ethernet switch modules provide a consistent feature set with server farm network
- "Trunk groups" feature eliminates the need for Spanning Tree in the blade center
- Support for IBM, HP & Dell Blade Servers

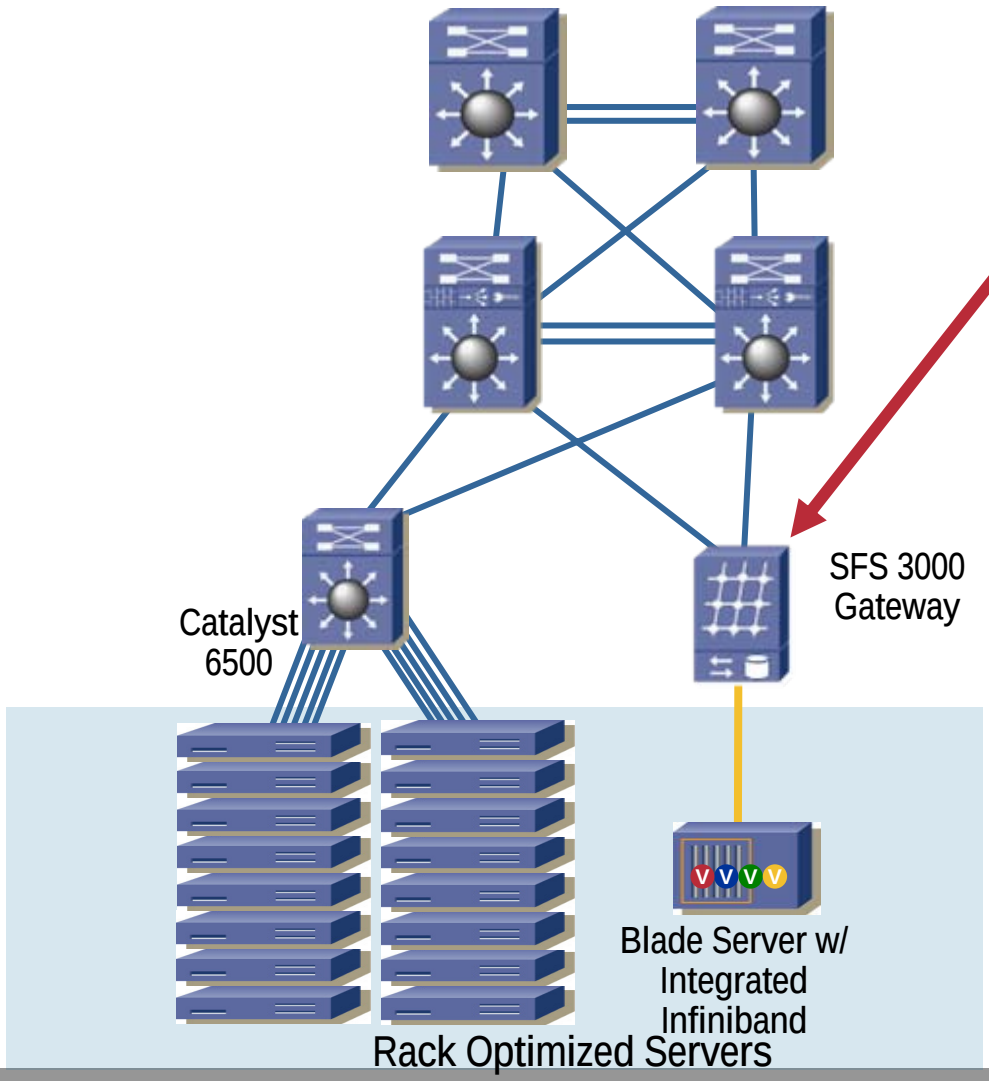


IBM

hp invent

DELL
www.dell.com

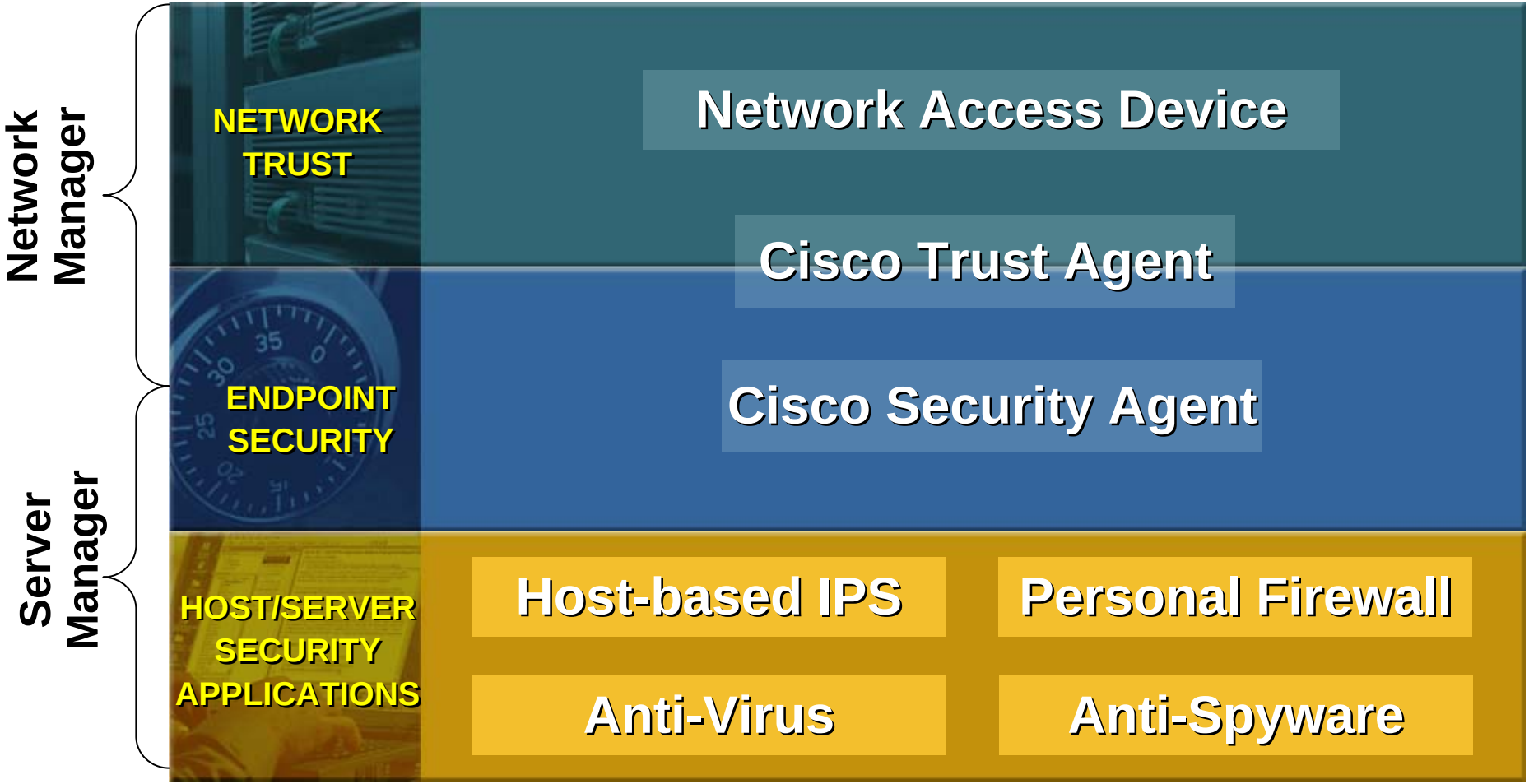
Cisco Server Farm Solution
Blade Center Topological Considerations



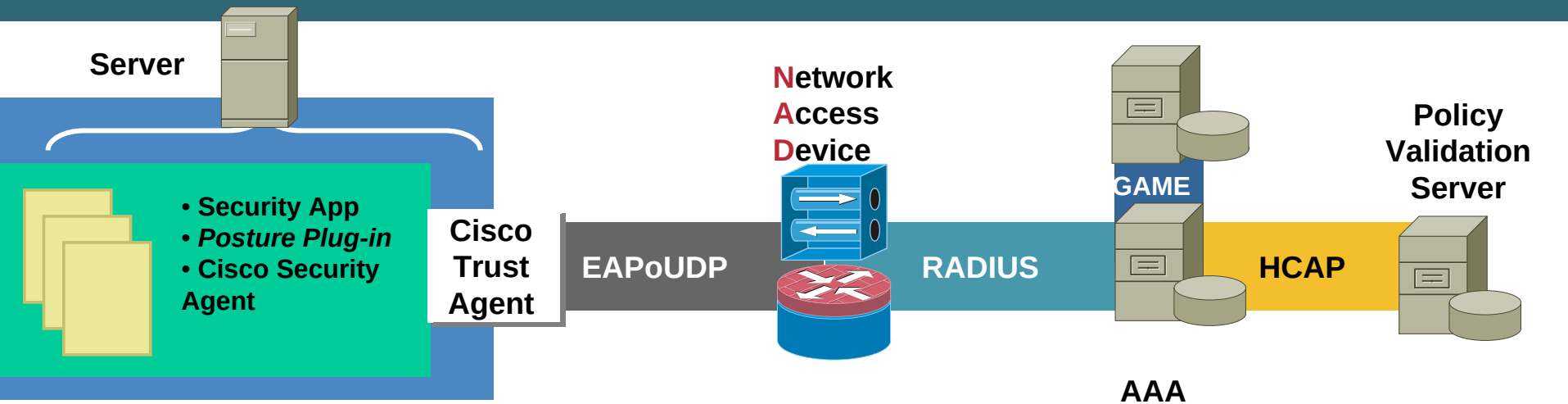
Requirement: Consolidate I/O for very large blade server deployments

- Integrated Cisco Infiniband switching enable virtualized access to LAN and SAN over a single connection
- Gateway switches provide access to native Ethernet and Fibre Channel
- Cisco Infiniband switches for IBM & Dell Blade Servers

Aligning Security Policy in the Data Center: Network Admission Control



Network Admission Control Solution Components



Subject

- Day Zero protection via application/worm behavior analysis
- Offers ID and posture state
- Assist in remediation

Policy Enforcement Point

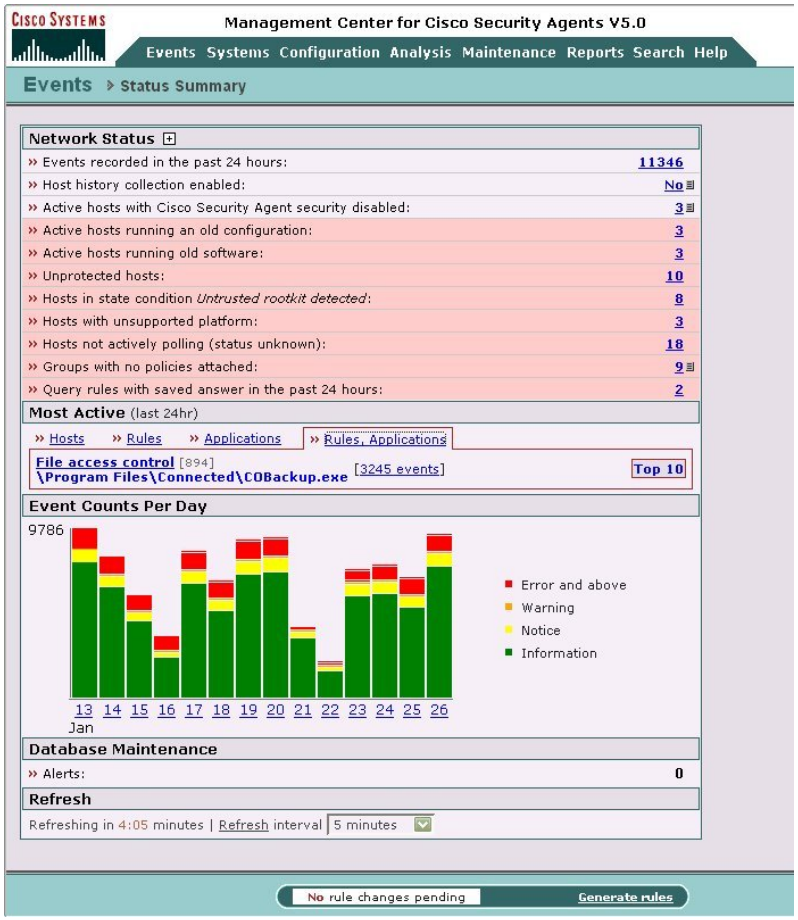
- Visibility and assessment trigger
- Authorization control

Policy Decision Point

- AAA function
- Remediation services
- Ties to many existing (and new) services/tools
- Audits 'Agentless' systems (non-responsive)

Cisco Security Agent for Endpoint Security

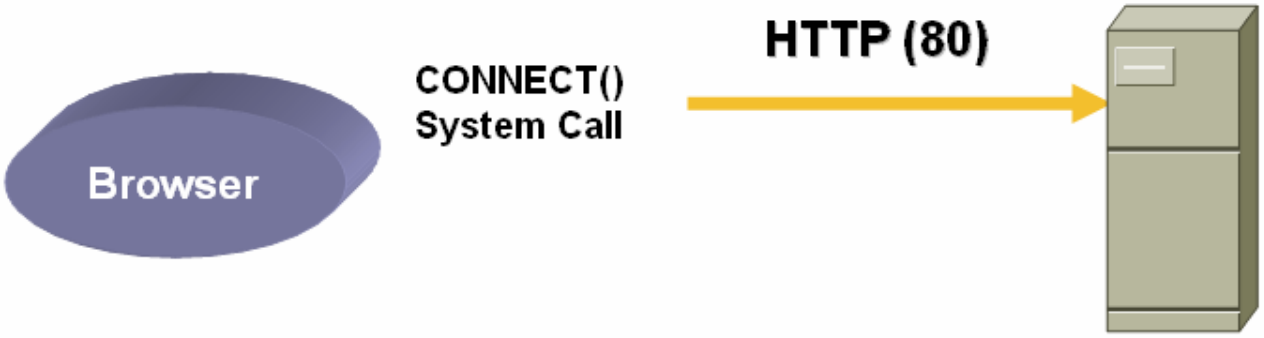
- **Comprehensive security for desktops and servers that collaborates and integrates with the network infrastructure**
- **The Cisco Security Agent intercepts application OS calls and invokes an allow/deny response**
- **Interceptors monitor calls for resource access:**
  - **File system**
  - **Network (inbound/outbound)**
  - **Registry**
  - **Execution (process creation, library access, executable invocation)**
- **"Zero Update" architecture – behavior based control means you don't need a new signature to stop the next attack**



Correlation

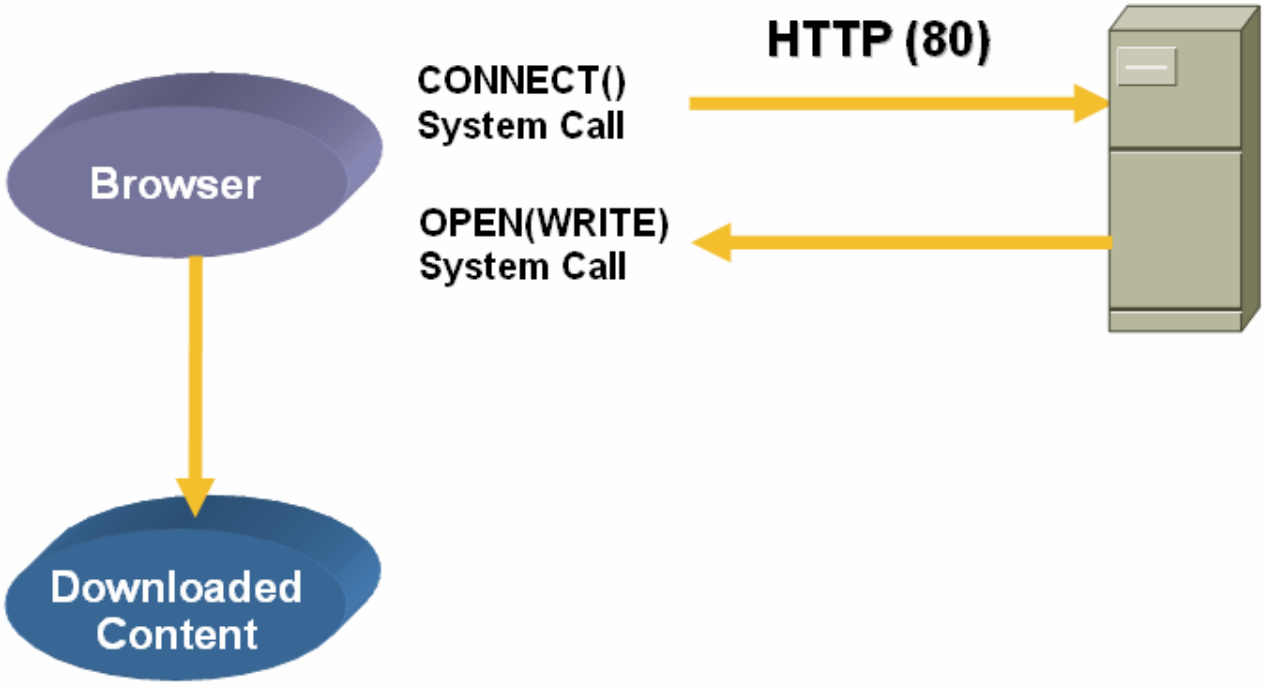
Malicious behavior is most accurately identified in context. Cisco Security Agent correlation does this automatically – no configuration required.

Correlation



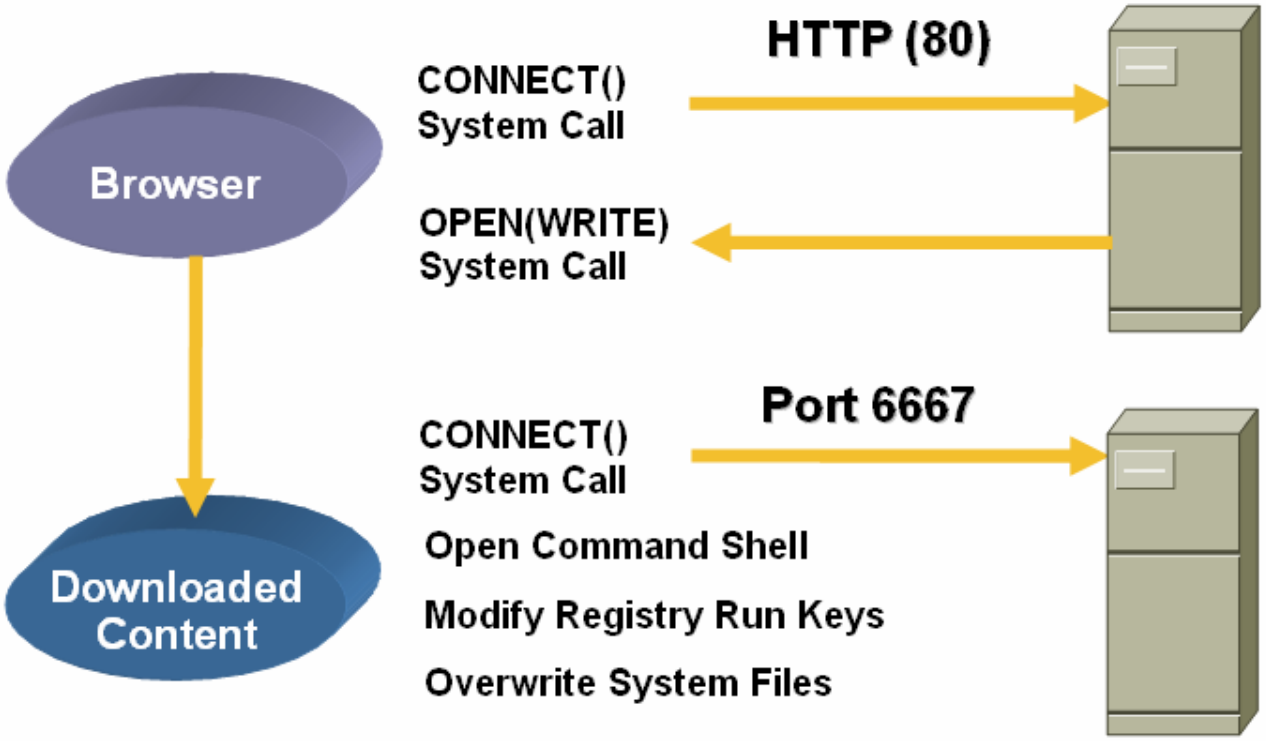
Malicious behavior is most accurately identified in context. Cisco Security Agent correlation does this automatically – no configuration required.

Correlation



Malicious behavior is most accurately identified in context. Cisco Security Agent correlation does this automatically – no configuration required.

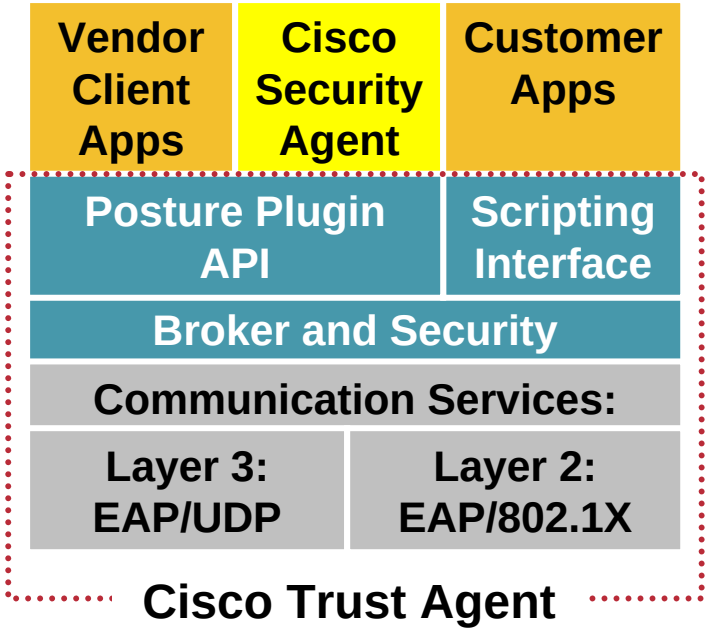
Correlation

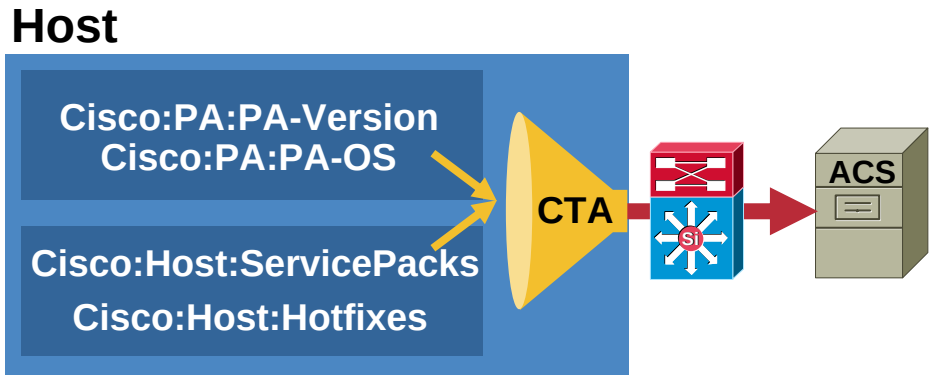


Malicious behavior is most accurately identified in context. Cisco Security Agent correlation does this automatically – no configuration required.

Cisco Trust Agent 2.0.1 (Posture Agent)

- Supported on Windows 2000, XP, 2003, and Red Hat Linux
- Supports two transport layers
  - EAPoUDP—layer three
  - EAPo802.1x—layer two (Windows only)
- Built-in posture plugins gather OS information including patch and hotfixes
- Support browser auto-launch
- Includes customer scripting interface
- Backward compatible with CTA 1.0 posture plugins from NAC program participants

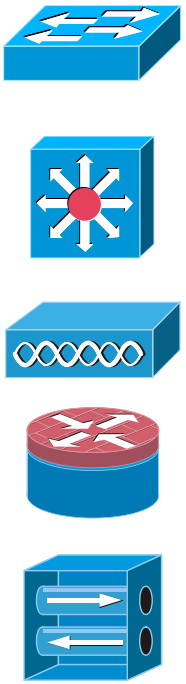




Network Access Device (Policy Enforcement Point)

- **Policy enforcement point for NAC framework; policies defined in ACS are enforced by NAD**
- **Includes NAC support for layer two, layer three, wireless, VPN**
- **Initiates EAP through client discovery**
- **Support for NAC assessment methods**
  - **NAC L3 IP (router, VPN)**
  - **NAC L2 IP (switch)**
  - **NAC L2 802.1x (switch, wireless)**

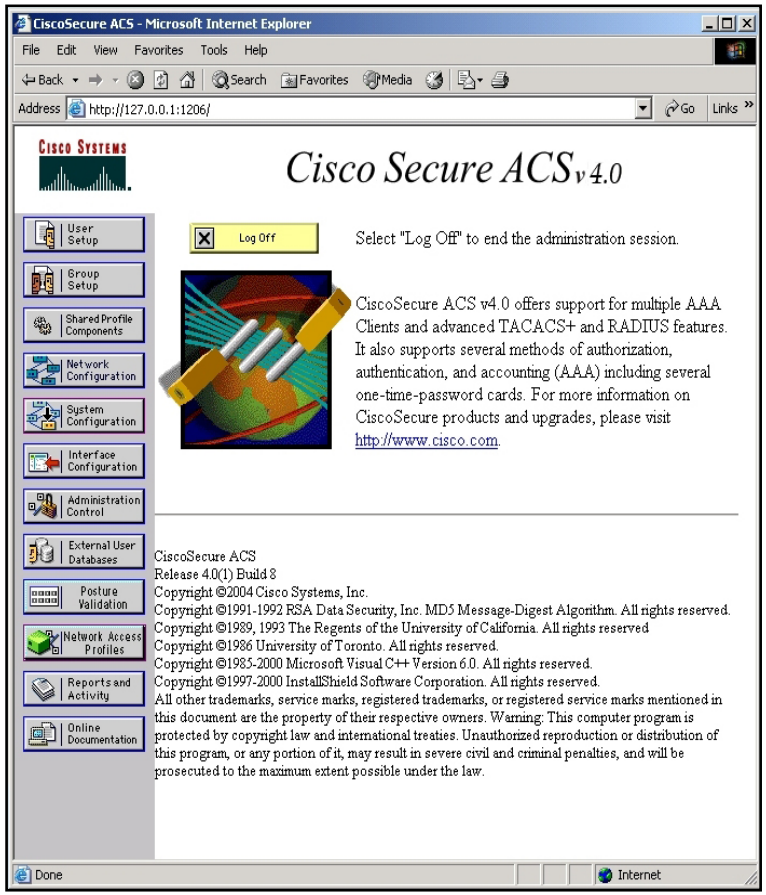
Network Access Device (NAD)



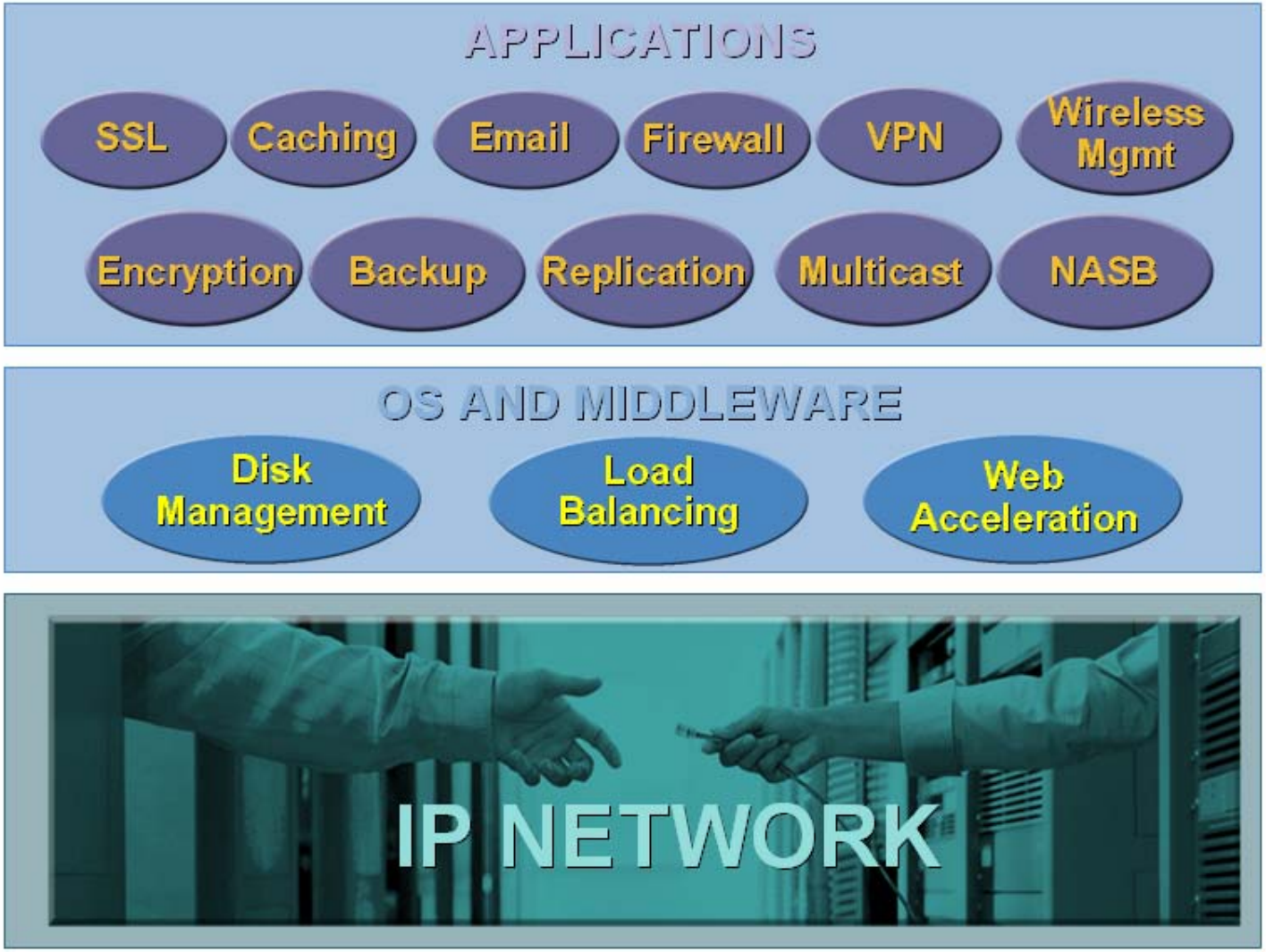
Policy Enforcement Point

Access Control Server (ACS) v4.0 (Policy Creation and Decision Point)

- NAC policy and enforcement decision are made here
- Integration point for external policy servers, remediation servers, audit servers, reporting servers
- EAP-FAST, HCAP, GAME protocol support for NAC
- Network access profiles
  - Services: groups, protocols, attributes
  - Authentication: protocols, directories
  - Compliance: posture and audit policies
  - Authorization: groups, RACs, ACLs
- Template configuration
- Configuration cloning



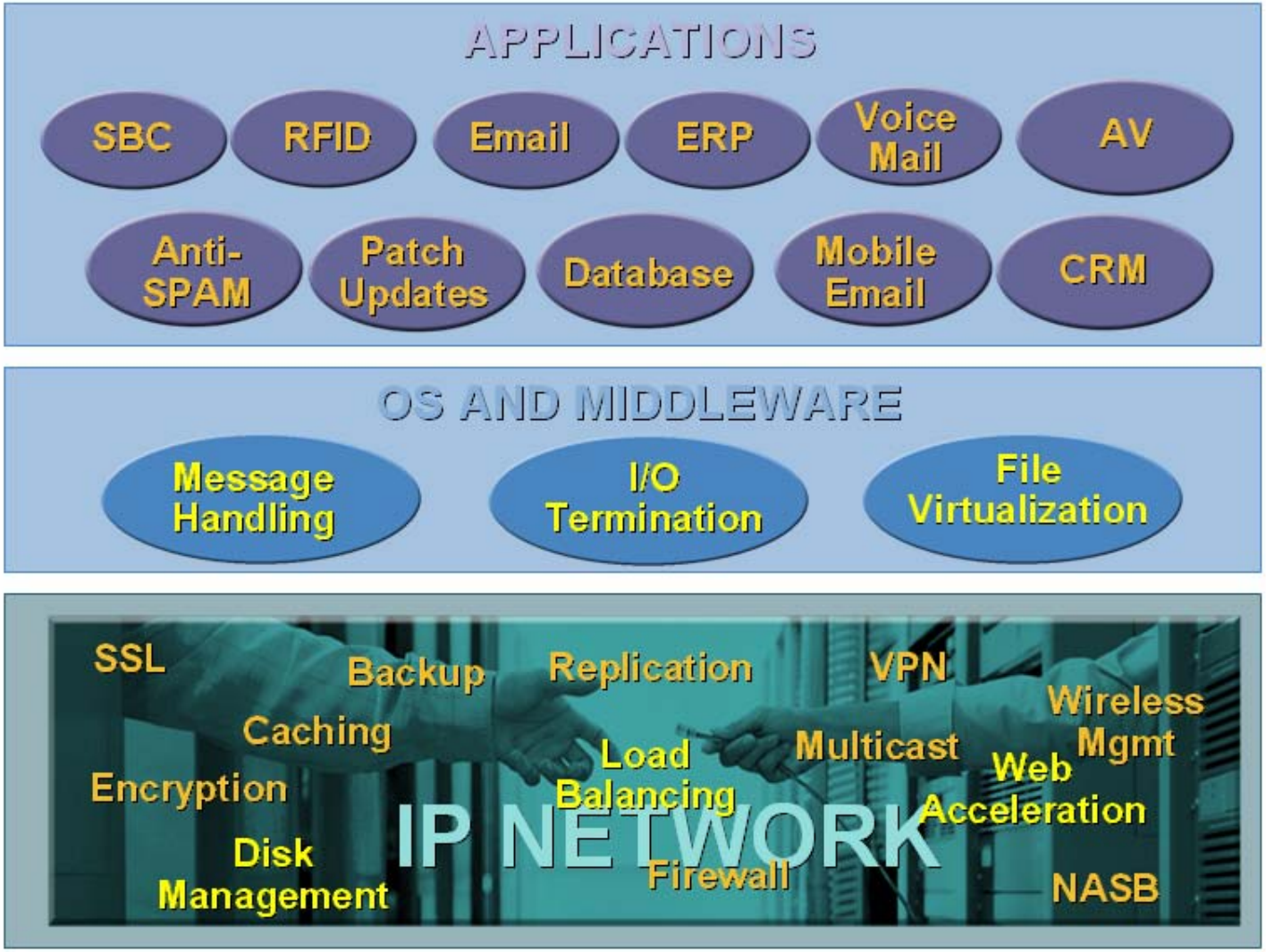
Service Optimization through Network Intelligence



Service Optimization through Network Intelligence

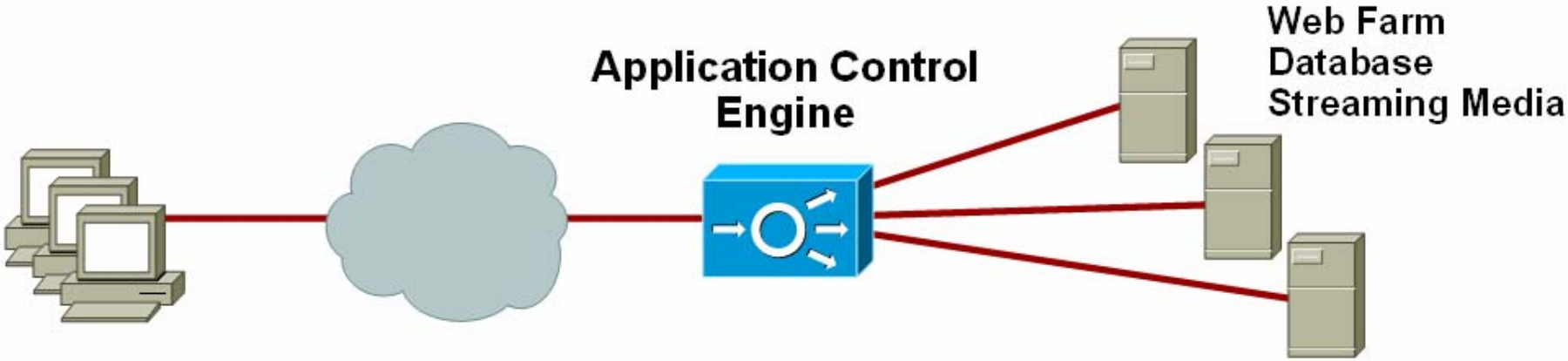
Returning compute power and cycles to applications and operating systems

Accelerating the Service by offloading some server capabilities



Optimizing Application Delivery

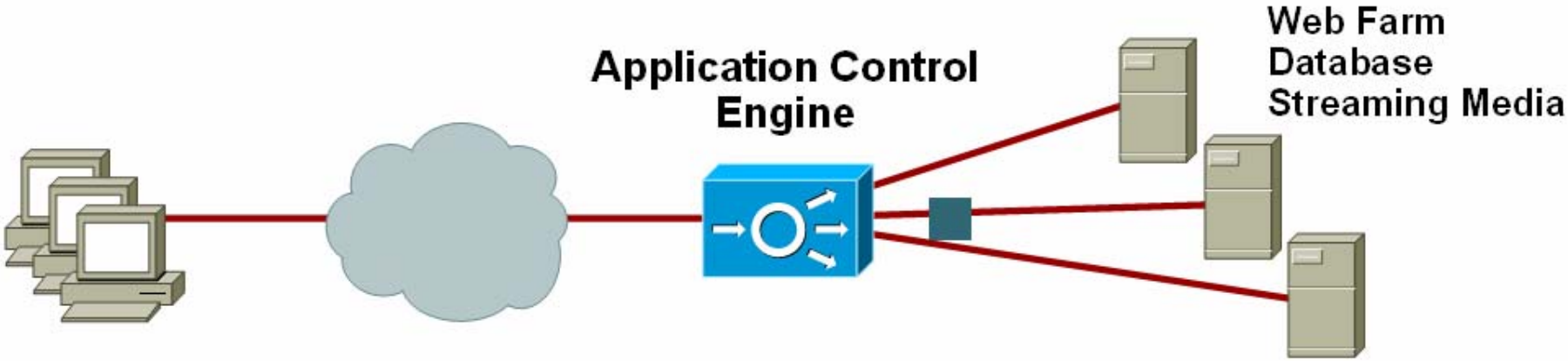
Application Control Engine for Server Load Balancing



- **Load balances between multiple servers for content distribution, web access or media download**
  - Provides faster client access to information
- **Monitors health and load on servers to dynamically distribute traffic**
  - Prevents server "hot-spots"
- **Layer 7 decision criteria and stickiness**
  - Enhances granularity, control and security through protocol-layer inspection
- **Virtualized contexts**
  - Consolidates multiple modules/appliances onto a single virtualized platform

Optimizing Application Delivery

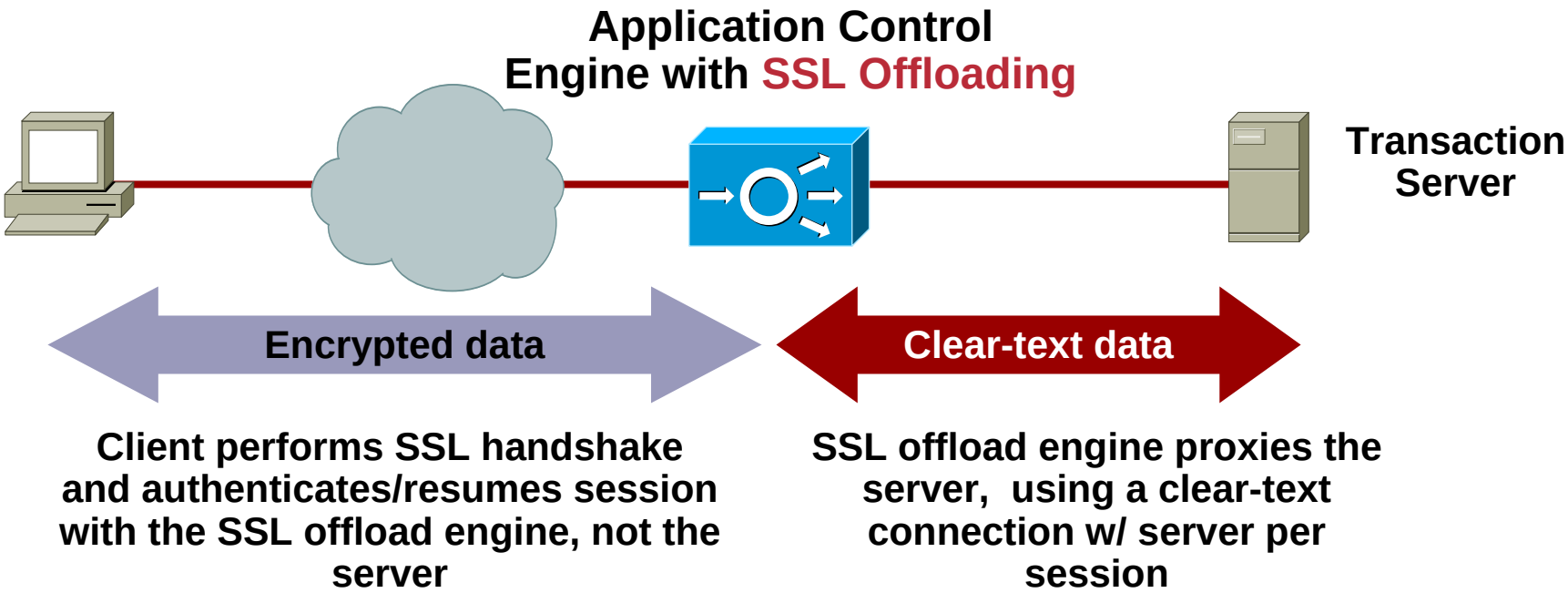
Application Control Engine for Server Load Balancing



- **Load balances between multiple servers for content distribution, web access or media download**
  - Provides faster client access to information
- **Monitors health and load on servers to dynamically distribute traffic**
  - Prevents server "hot-spots"
- **Layer 7 decision criteria and stickiness**
  - Enhances granularity, control and security through protocol-layer inspection
- **Virtualized contexts**
  - Consolidates multiple modules/appliances onto a single virtualized platform

Offload Unnecessary Server Processing

Application Control Engine for SSL and TCP Offload



Benefits of Network-based SSL offload:

- Offloads server of encryption/decryption of SSL secure sessions
- Proxies the server by managing the SSL certificate
- Performs full proxy functions, including dedicated client and server-side TCP buffers

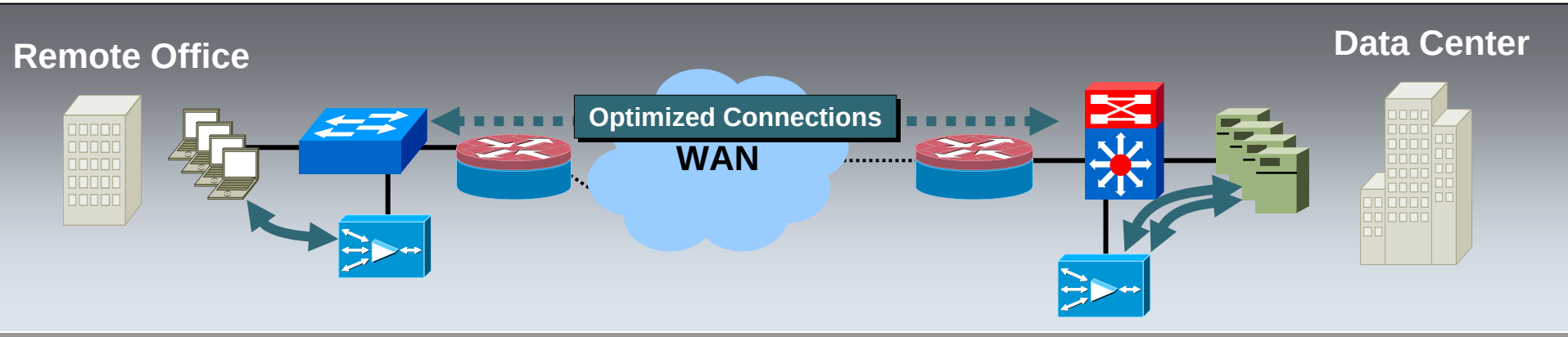
Optimizing Application Delivery to the Branch
Cisco Wide Area Application Services (WAAS)

Problem

- **Branch server consolidation introduces latency and congestion over WAN – branch users may opt not to use applications**

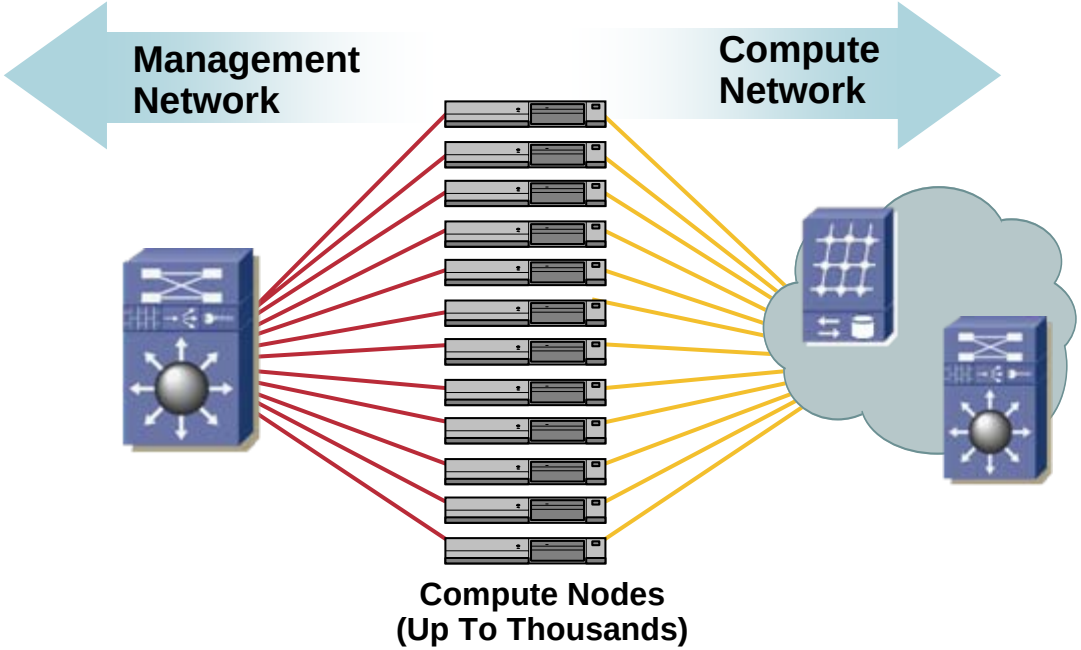
Solution

- **WAAS solution overcome application performance problems in WAN environments by:**
  - **Optimizing TCP connections to reduce round-trip time (RTT)**
  - **Caches data and information at the branch site**
  - **Virtualizes file access**



Clustering Compute Resources

Cisco High Performance Computing Solution



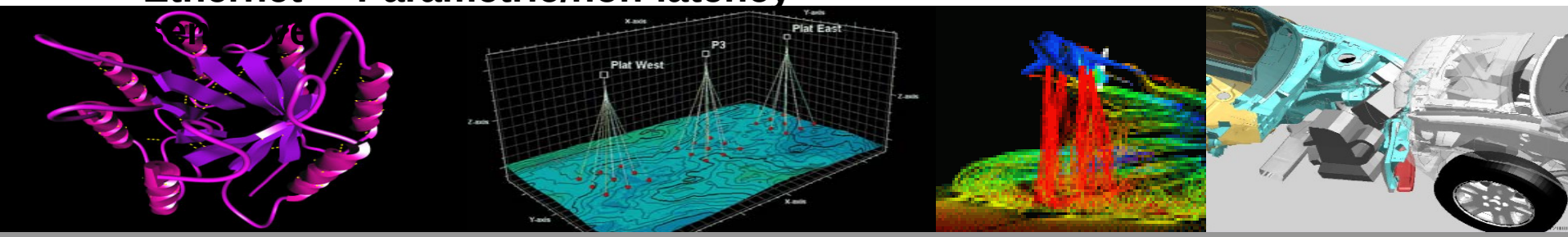
Infiniband – Parallel/MPI-based applications
Ethernet – Parametric/non-latency

Problem

- Increase application performance through clustered x86 servers

Solution

- Optimized interconnect – Ethernet or Infiniband – based on application requirements
- Leadership in Open Fabrics and Open MPI
- Qualified with server vendor and ISV solutions

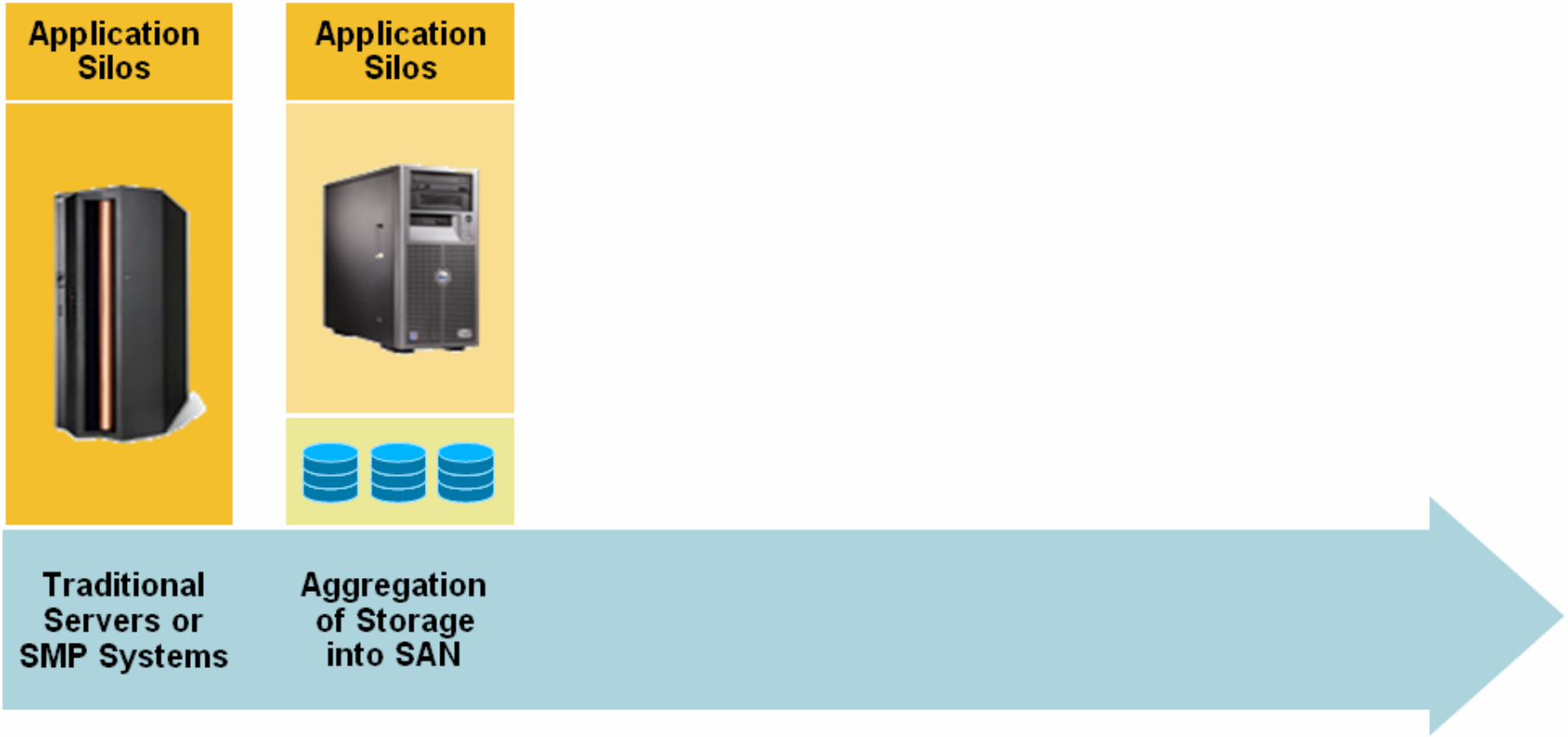


Server Disaggregation and I/O Virtualization

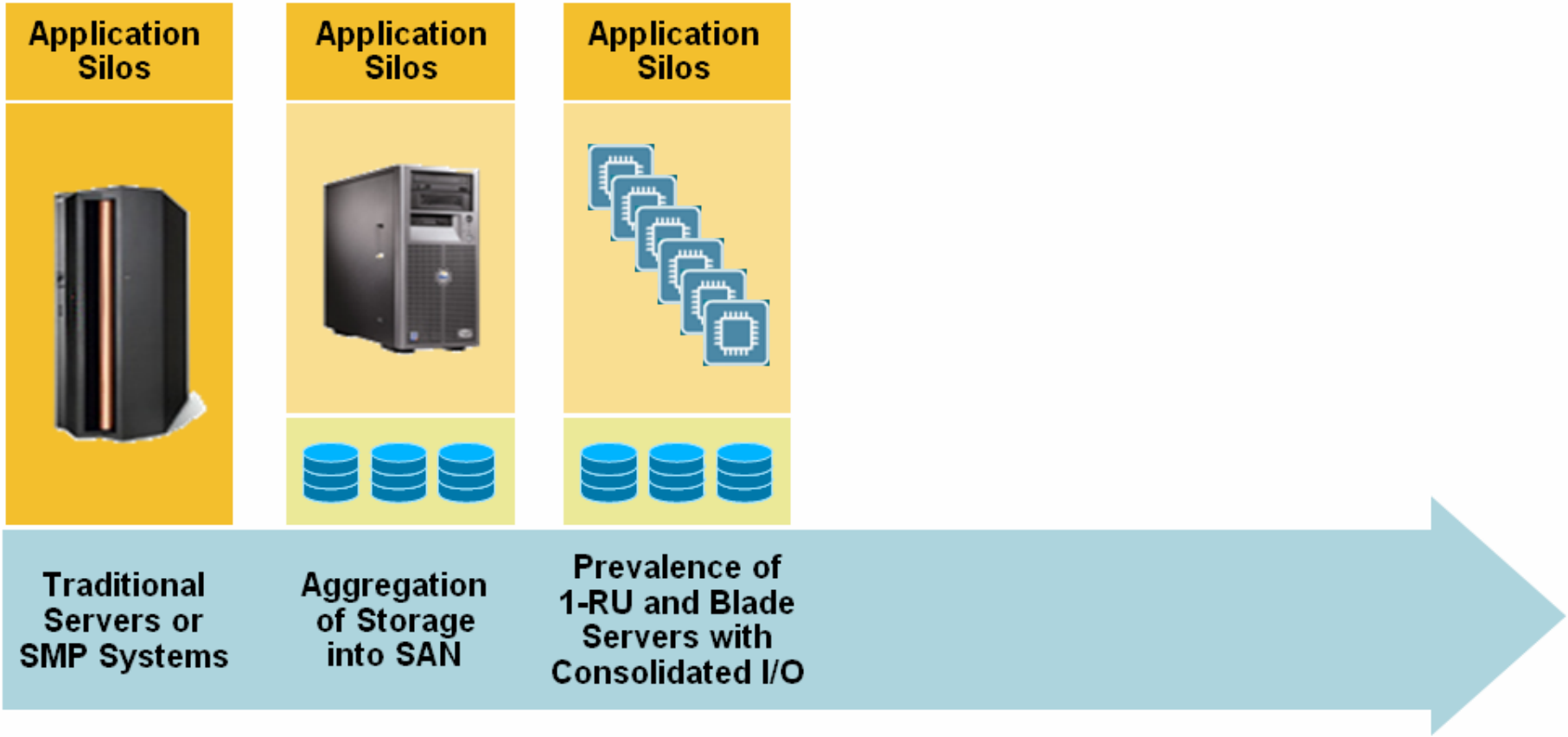
Application Silos

Traditional Servers or SMP Systems

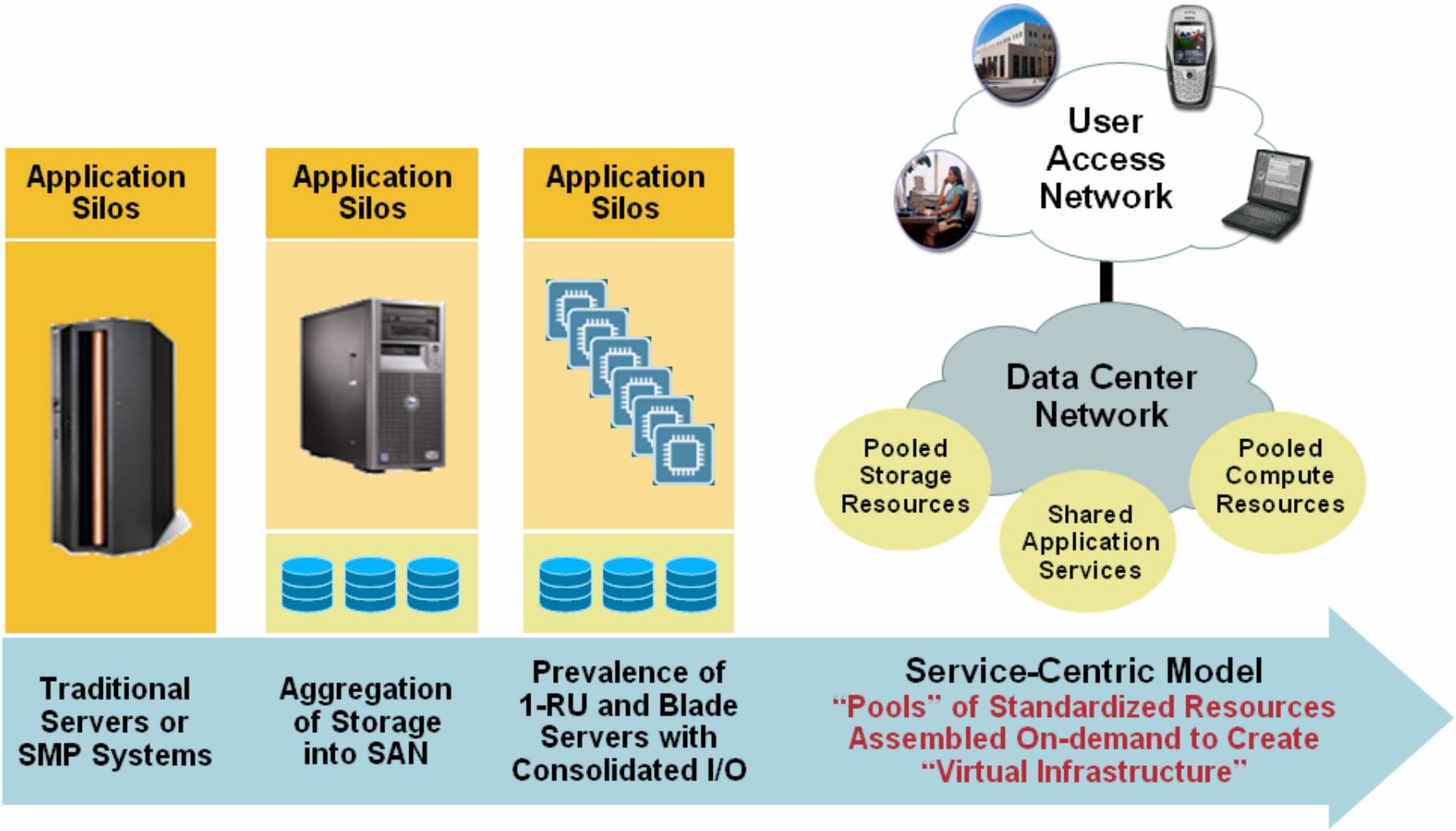
Server Disaggregation and I/O Virtualization



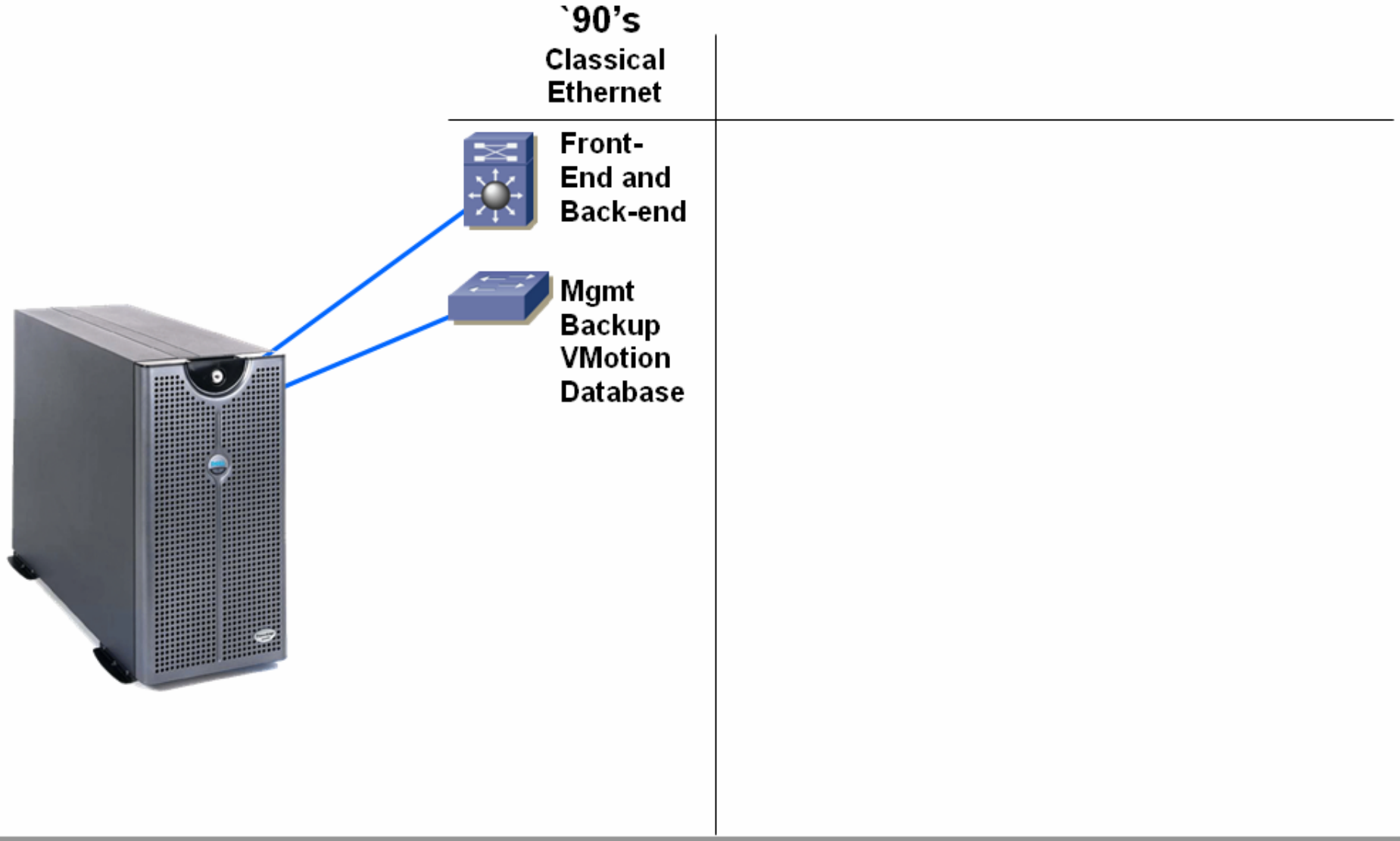
Server Disaggregation and I/O Virtualization



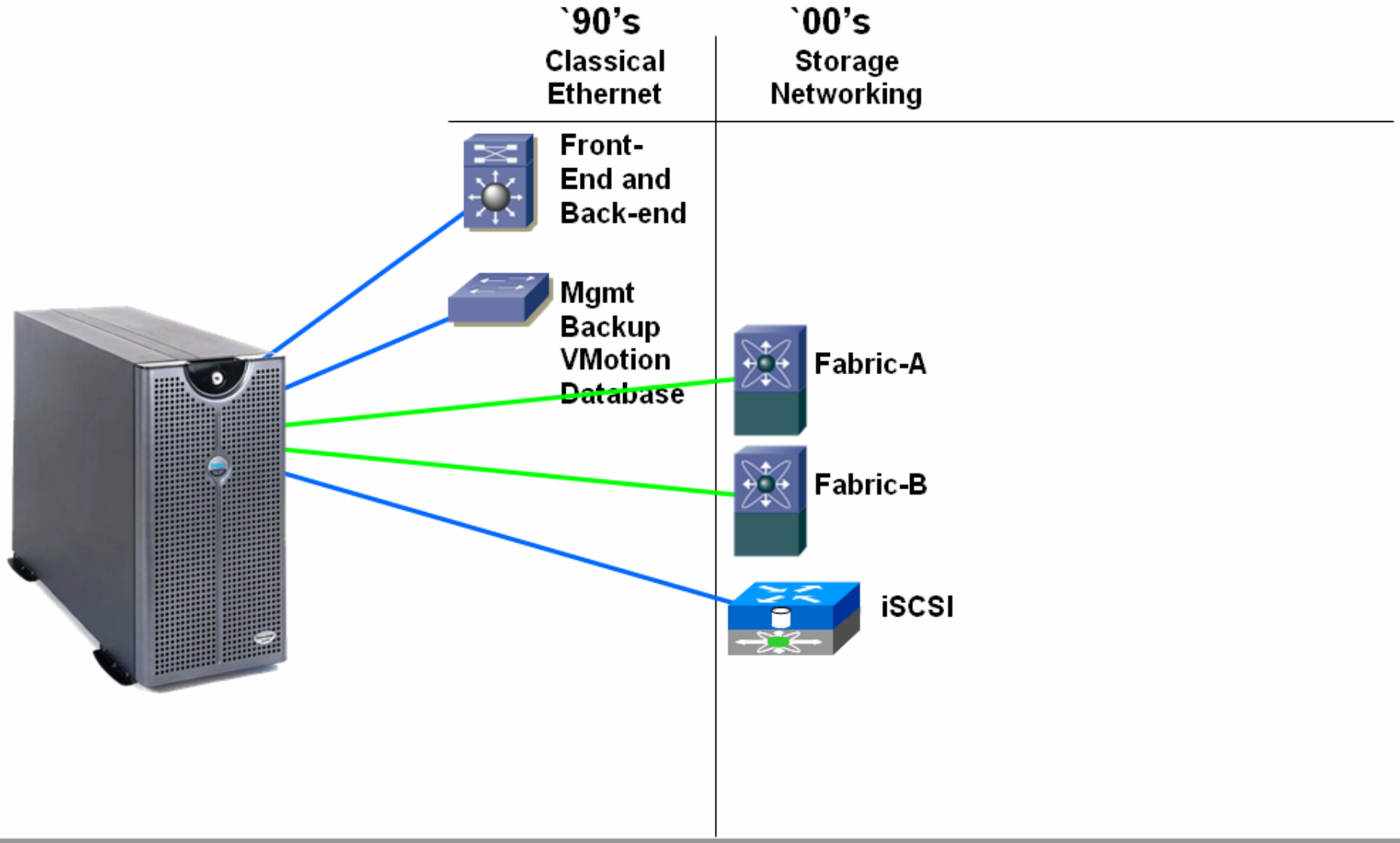
Server Disaggregation and I/O Virtualization



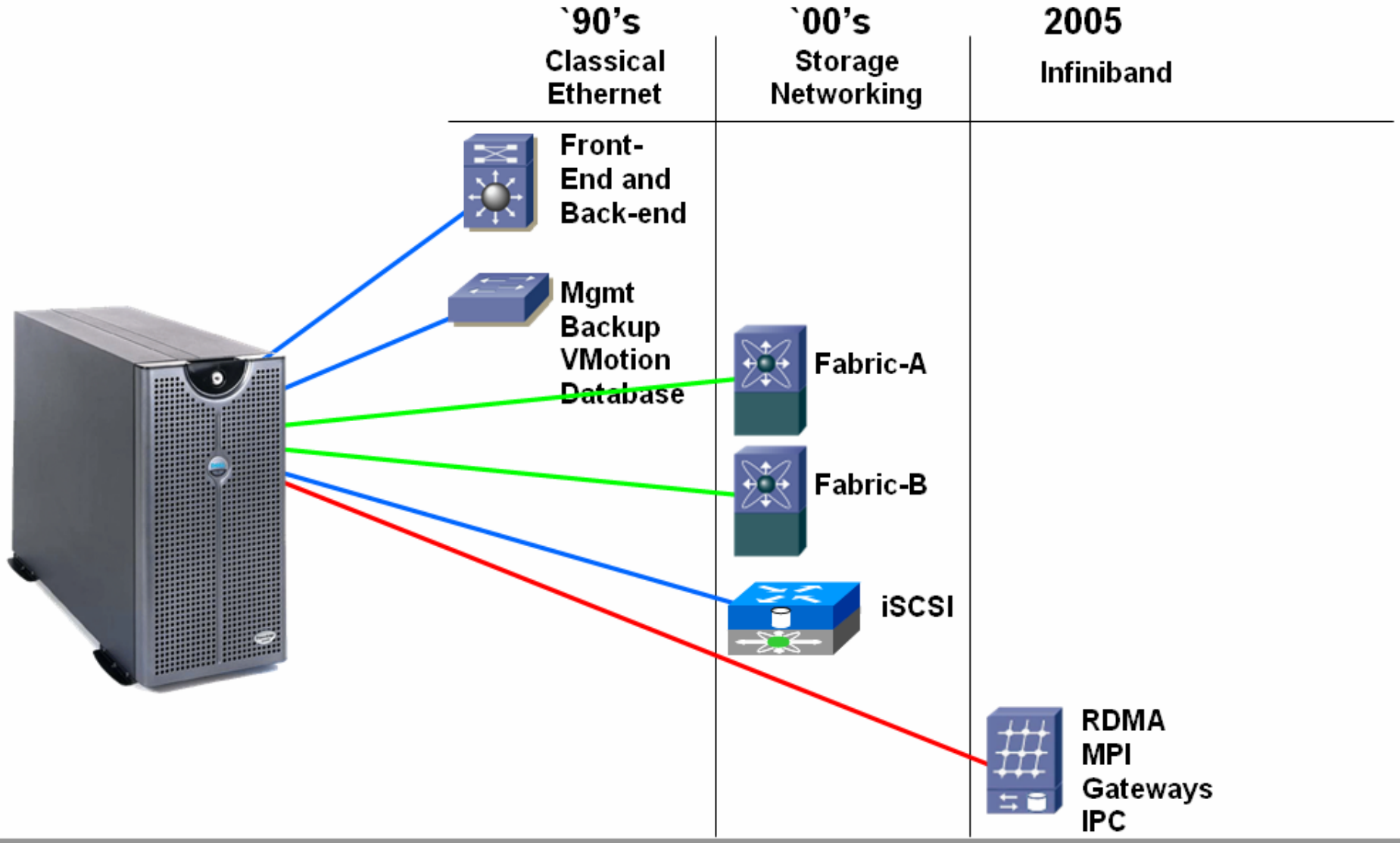
The Evolution of Server Communications



The Evolution of Server Communications

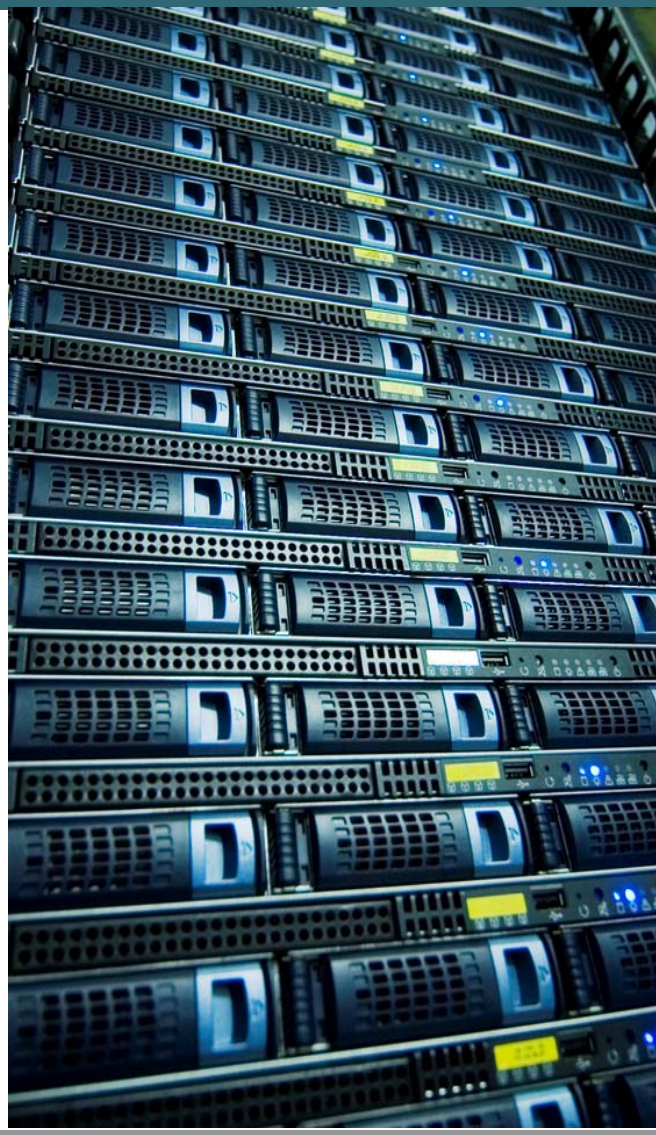


The Evolution of Server Communications



Unified Fabric for a Common I/O

- **What if we could combine connectivity on a single network?**
- **Benefits**
  - **Smaller servers**
  - **Diskless operation**
  - **Less power**
  - **Less Interfaces**
  - **Less cabling**
  - **Simpler Operations & management**



I/O Virtualization with iSCSI

- **What is iSCSI**

  iSCSI is a SCSI protocol that allows block-storage to operate over an IP network

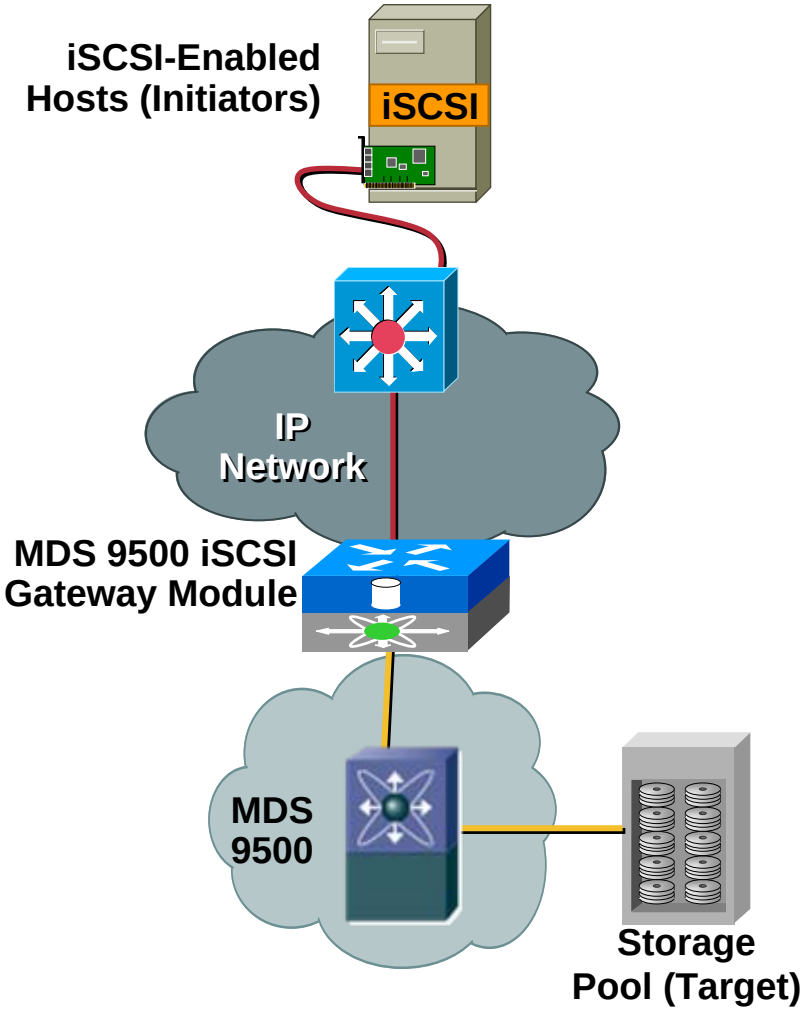
  Allows servers to run storage over the existing Ethernet front-end network while providing an interface to the FibreChannel network

- **Benefit**

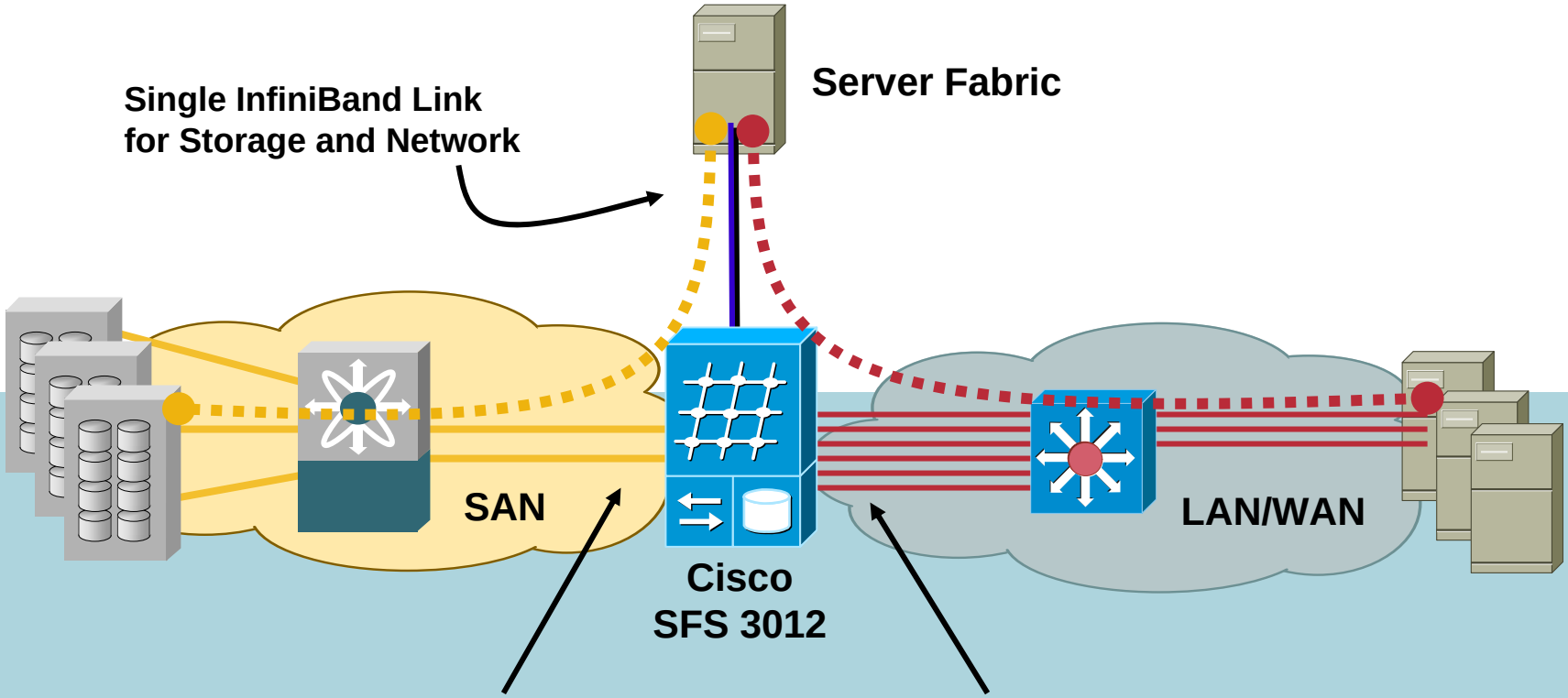
  Consolidates storage traffic over Ethernet network, allowing block level storage

  Still can leverage FibreChannel network through the MDS 9500 iSCSI Gateway module

  Leverage remote boot capabilities for diskless servers



Infiniband for I/O Virtualization



Fibre Channel to Infiniband Gateway for Storage Access Creates a 10-gbps Virtual Storage Pipe to Each Server

Ethernet to Infiniband Gateway for LAN Access Creates a Virtual IP Connection to Each Server

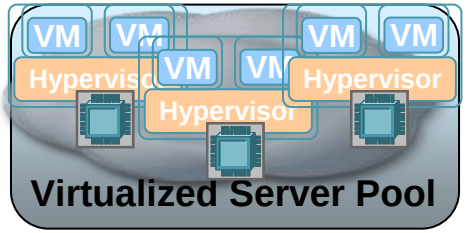
Resource Virtualization – Benefits and Challenges

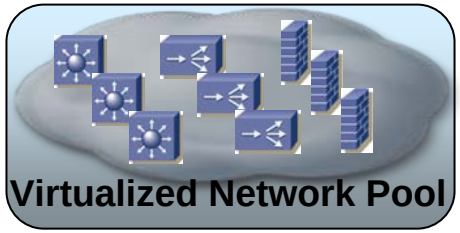
Benefits

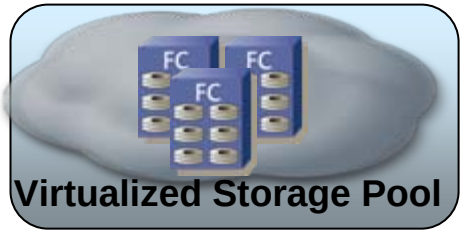
- Dynamic provisioning within technology pool
- Improved Utilization
- Lower power and cooling costs due to fewer devices
- Non-disruptive planned downtime
- Fast recovery within virtualized domains
- Capacity planned for average, not peak

Challenges

- Rapid provisioning resources across virtualization domains
- Manual mapping of application environments to virtualized infrastructure
- Slow end-to-end application recovery due to manual operations
- Coordination across organization silo's
- Alignment of intelligent network and services







Server Virtualization and Network Synergy

Server Consolidation without Compromise

Challenge

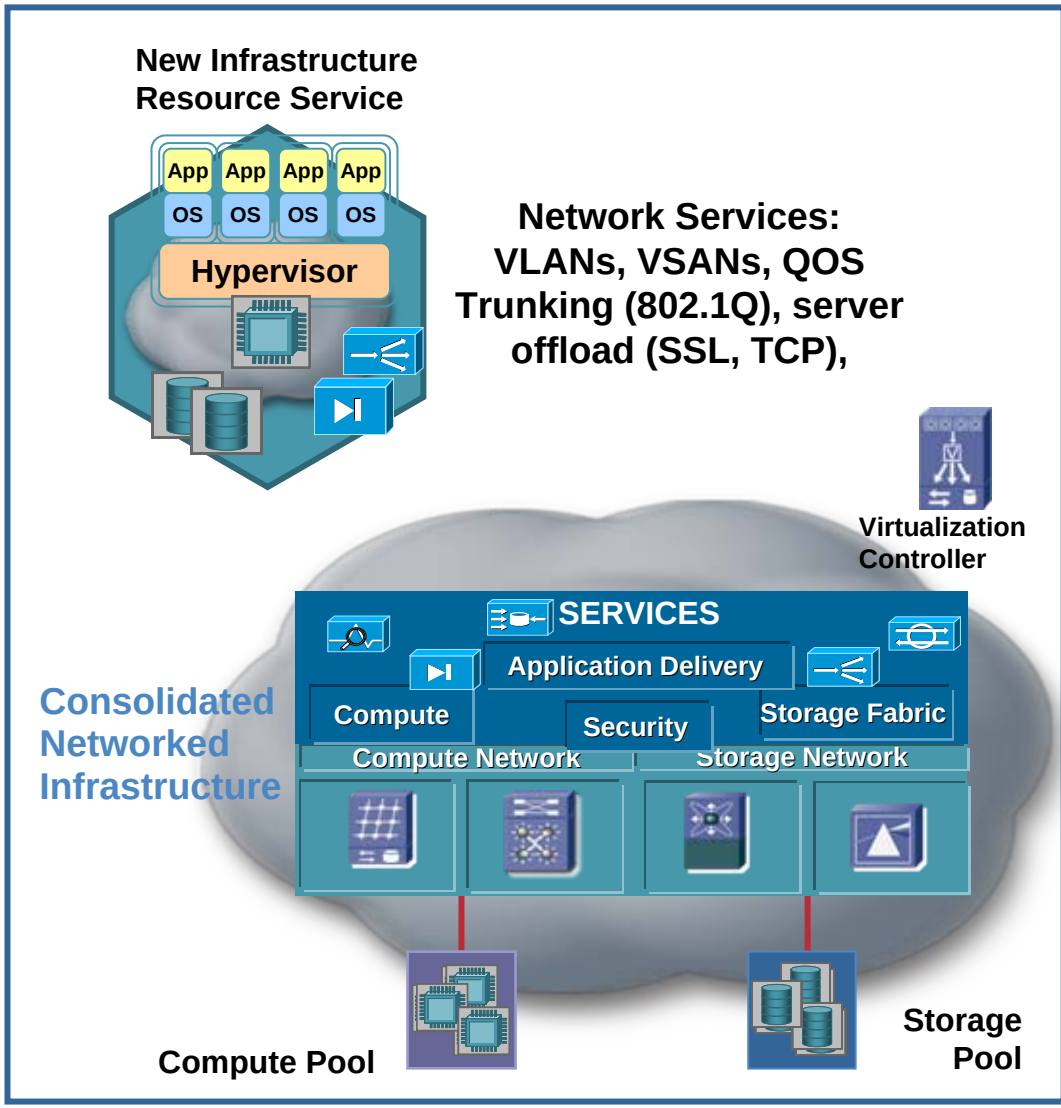
- Achieving server consolidation with security, availability and performance

Network Requirements

1. Provide per server or per VM front-end segmentation (VLANs, ACLs, 802.1Q etc)
2. Provide per server back end segmentation (VSANs)
3. Optimize server performance (I/O trunking and consolidation, SSL/TCP offload, multicast etc)
4. Apply services according to per VM policies (firewall, SLB, app optimization etc)

Benefits

- Meet application performance and availability service levels and meet compliance requirements



Server Virtualization and Network Synergy

High Availability without Compromise

Challenge

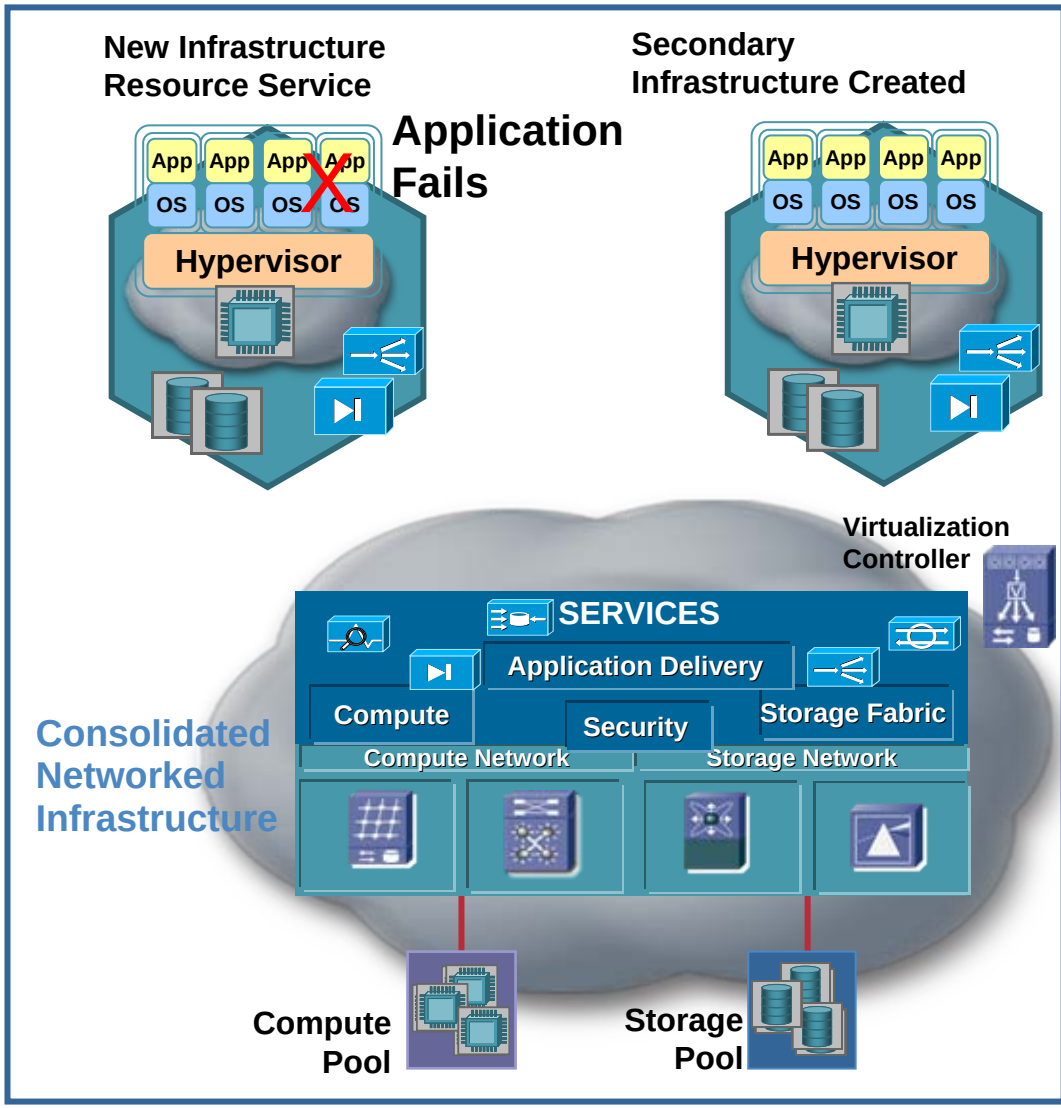
- Achieve recovery within minutes, without need for replicated hardware for each application

Network Requirements

1. Dynamically connect bare-iron server to required VLAN / VSAN
2. Enable loading of OS, image etc from appropriate LUN
3. Associate required network properties to newly loaded server or VM (IP addresses, security, network services etc)

Benefits

- Servers / VMs can be dynamically provisioned from generic pool
- Doesn't require propositioning of servers on same network segment



Server Virtualization and Network Synergy

Infrastructure Mobility without Compromise

Challenge

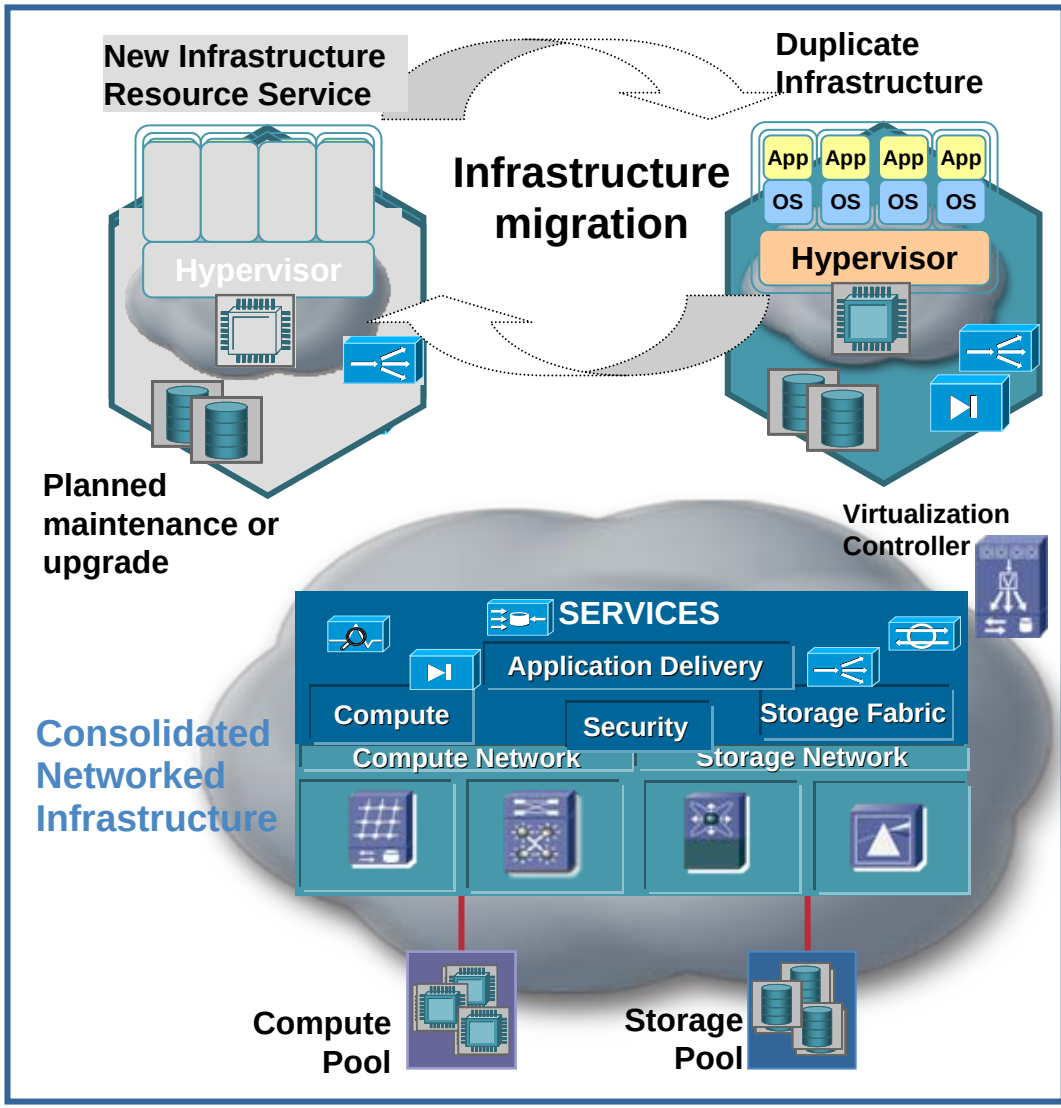
- Migrate applications without compromising application availability, security, performance

Network Requirements

1. Provision network and network services to support duplicated VM and application instance
2. Network enables replication of data to secondary DC or high performance access to primary
3. Network enables seamless client or system connectivity to secondary and then back to primary.

Benefits

- Ensures continuous access to application during planned downtime even in secondary data center



Why You Care about an Intelligent Network?

The network **touches all resources** (compute, storage, other peripherals) –

Scalability starts here

The network **connects all resources**, providing the lifeline for <u>information</u> –

Availability starts here

The network **services all resources,** helping to scale applications, compute power, virtualized storage and servers

Automation starts here

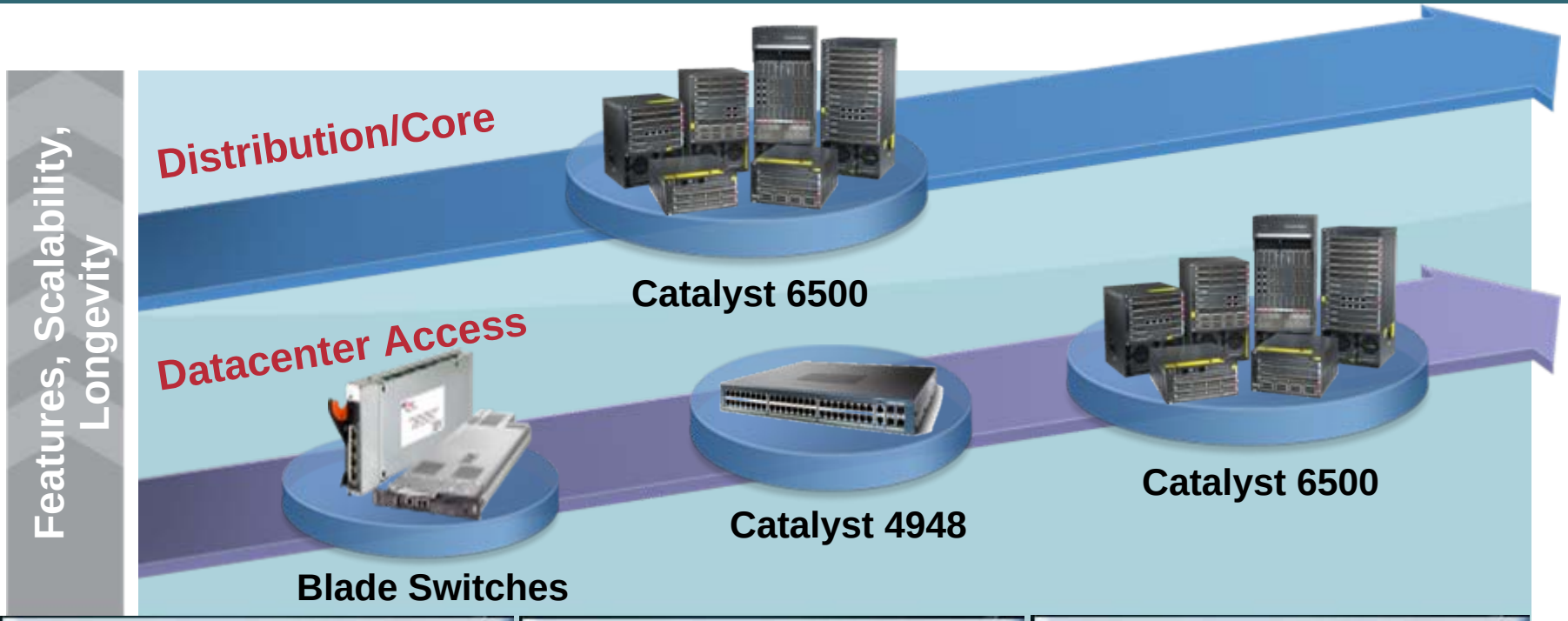
Summary

- **A robust server deployment requires an intelligent network to provide**
  - **Scalability**
  - **High Availability**
  - **Network-based security**
  - **Accelerated application performance**
  - **I/O consolidation and virtualization**
- **Cisco can help the server manager focus on the server, not the network**

Product Overview

Appendix

Catalyst Switching Portfolio for the Data Center



Catalyst 6500

- Industry's best investment protection
- Lowest TCO
- Highest Availability
- Integrated Services

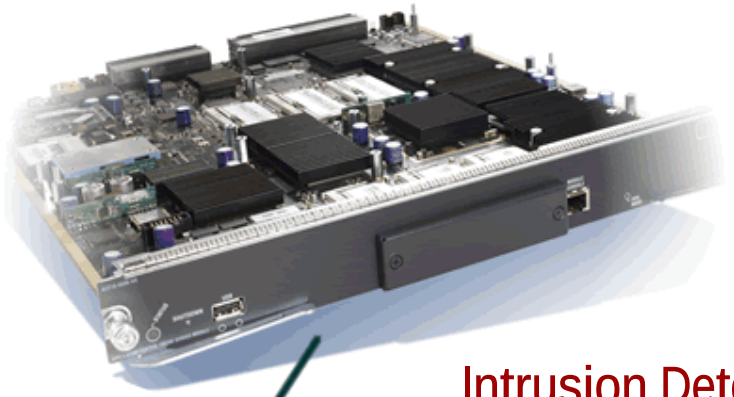
Catalyst 4948

- Wire-speed switching and services
- Optimizes rack modularity and cabling
- GbE and 10GbE ports

Blade Server Switches

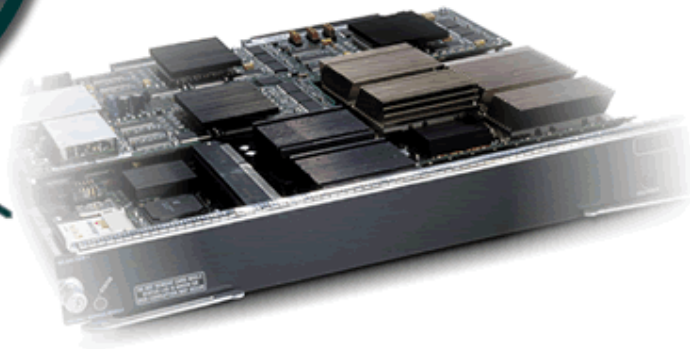
- Integrated L2+ Ethernet Switches for IBM and HP Blade Chassis
- Integrated Infiniband Switches for IBM and Dell Blade Chassis

Application Service Integration into the Server Farm



Application Control Engine (ACE): Server Load Balancing with SSL optimization for improved Server security…

Intrusion Detection and Prevention: Limits attacks from worms and other malicious traffic…



Firewall (FWSM): Protects the Data Center with a high performance (up to 5Gb/sec) stateful security firewall…

Virtualization Delivers Service Density

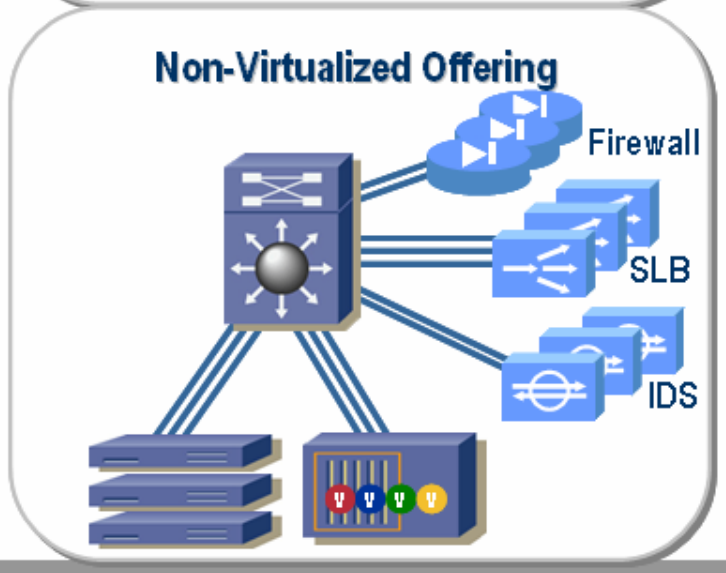
Business Requirements:

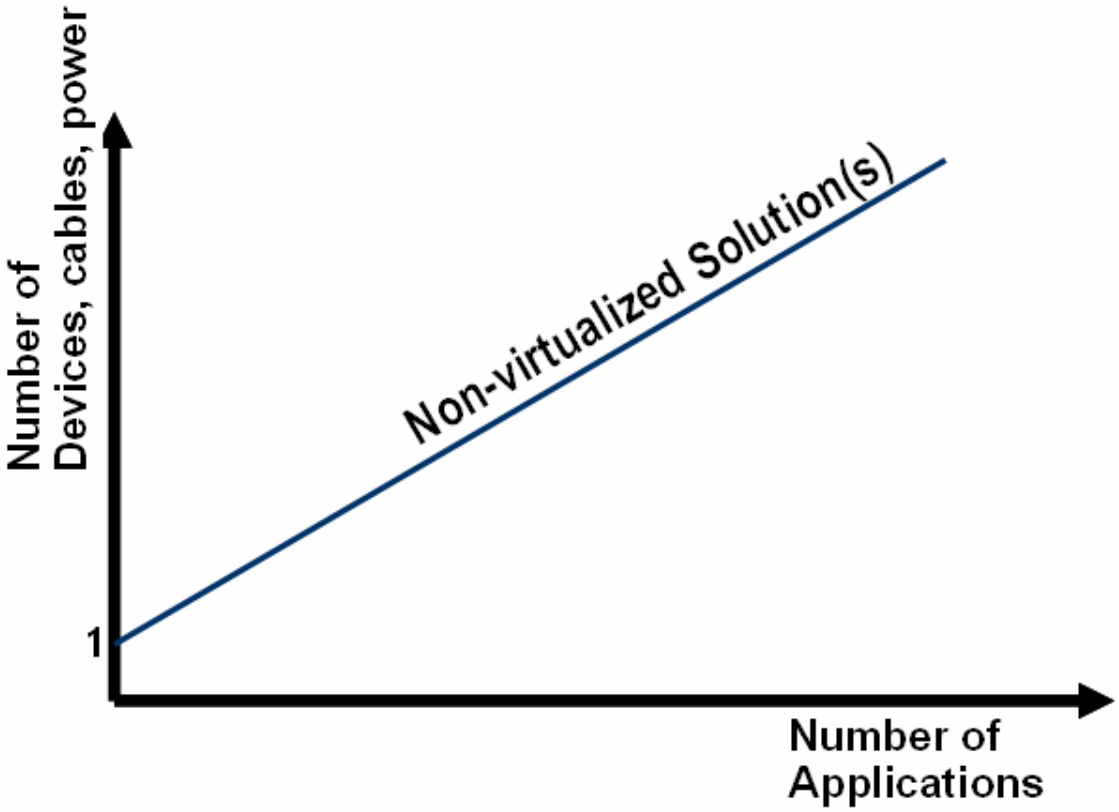
1. Business Segmentation
2. Application Specific Security
3. Discrete Service Levels
4. Service Velocity
5. High Availability
6. Predictable Performance

Virtualization Delivers Service Density

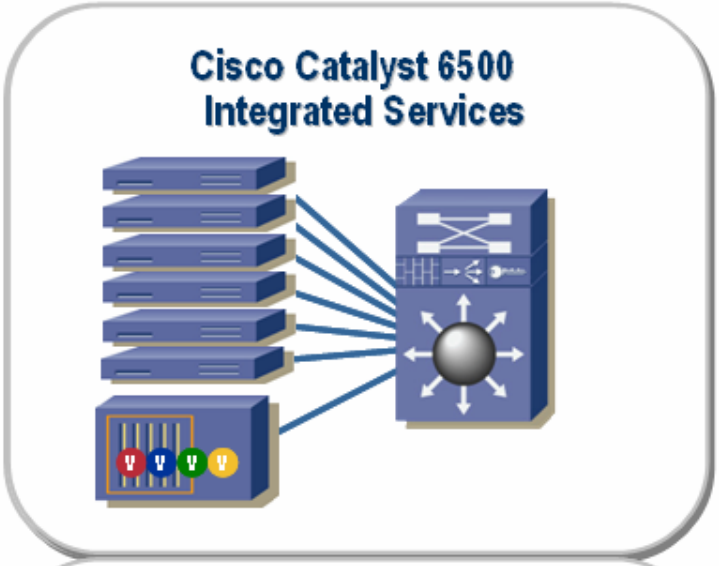
Business Requirements:

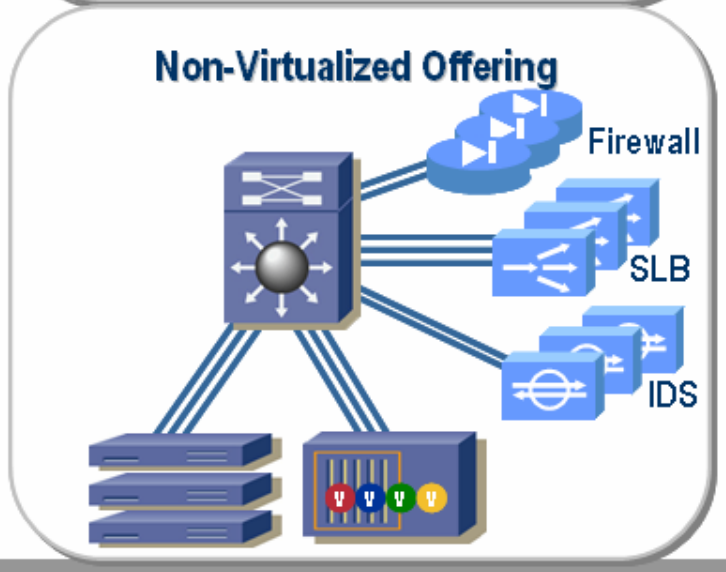
1. Business Segmentation
2. Application Specific Security
3. Discrete Service Levels
4. Service Velocity
5. High Availability
6. Predictable Performance





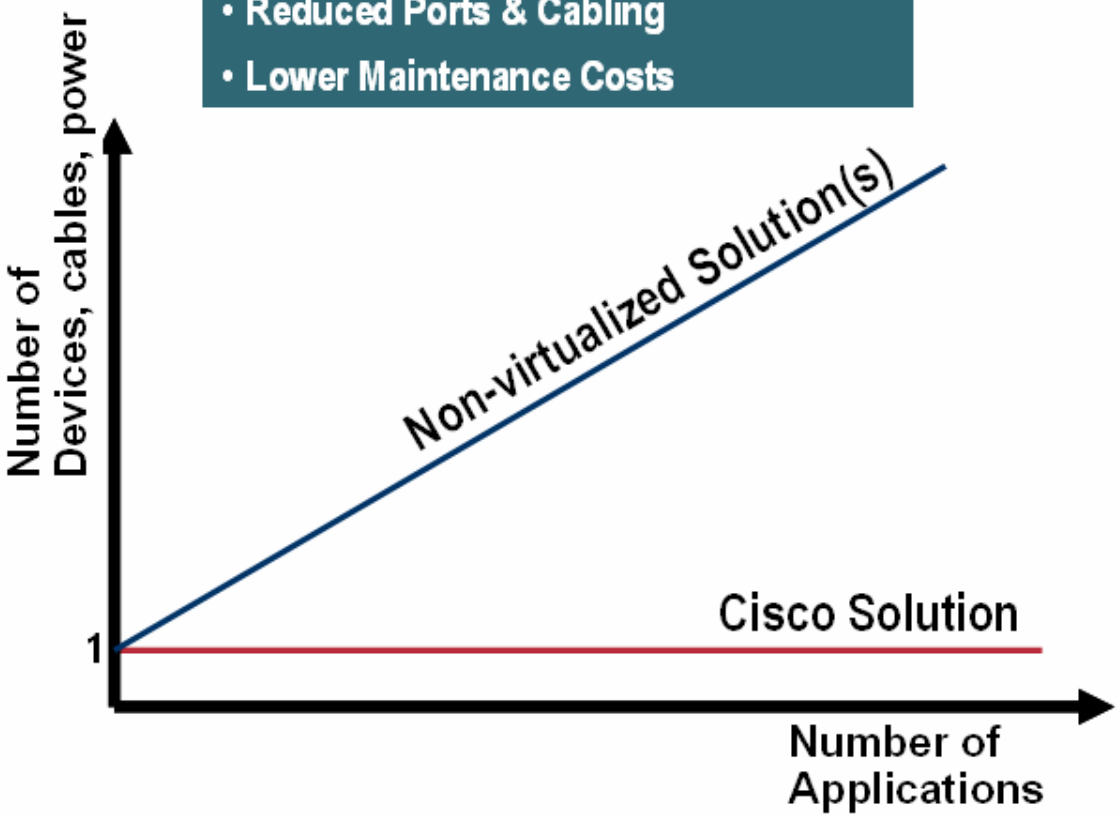
Virtualization Delivers Service Density





Cisco Solution Benefits:

- Simplified Operational management
- Less Power Consumption
- Less Rack Space
- Reduced Ports & Cabling
- Lower Maintenance Costs



Cisco Server Fabric Switching Products

Server Fabric Switch

InfiniBand

SFS 7000

(24) 4XIB

SFS 7008

(96) 4XIB

SFS 7012

(144) 4XIB

SFS 7024

(288) 4XIB

Multifabric

SFS 3001

(12) 4XIB + 1 Gw

SFS 3012

(24) 4XIB + 12 Gws

(2) 2G FC GW

(6) GE GW

Blade Server

IBM BladeCenter

- HCA (2) 1XIB PCI-X
- Embedded switch (14) 1XIB (Internal) + (1) 4XIB and (1) 12XIB (External)

Dell 1855

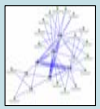
- HCA (2) 4XIB PCI-ex
- Passthru Module (10) 4XIB

HCA

- (2) 4XIB PCI-X
- (2) 4XIB PCI-ex

- Remote Boot
- Linux Host Driver
- Windows Host Driver

Subnet Mgt



- High Performance Subnet Manager Software

- Embedded Subnet Manager