



Application Networking Services

Hicham Tout
Manager, Sales Business Development, MEA
Cisco Expo 2007

Agenda

- Where is the industry going?
- Why application services?
- What does cisco offer in the ANS Space?



Where the Industry is Going Today

Everything over IP

All Services Virtualized



Everything on Ethernet

All Devices Networked

What Does the above Mean?

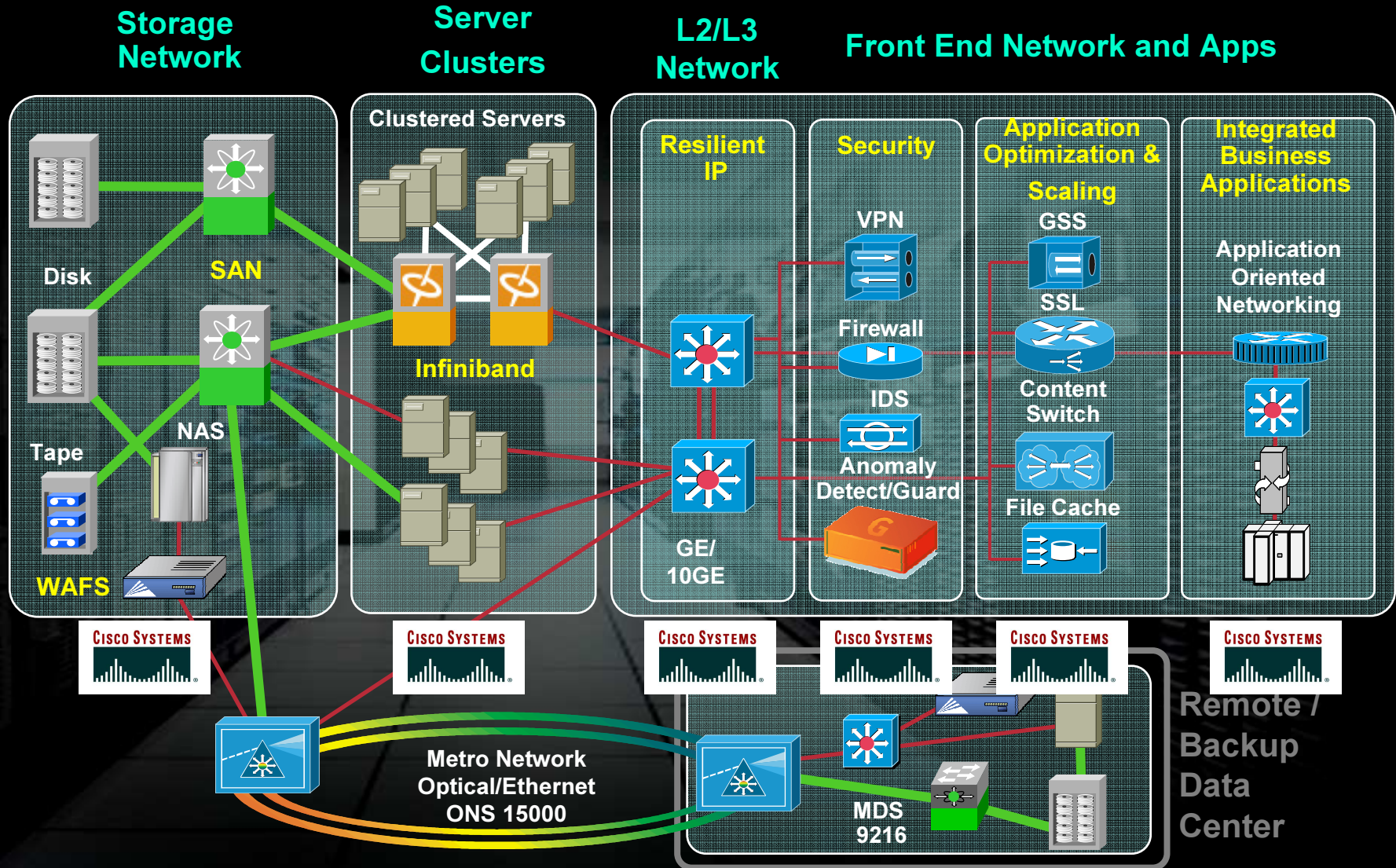
- **The DC will substantially grow! And host ever more business critical services.**
- **Optimization becomes more relevant (standards are great but they're slower and introduce more overhead).**
- **Application Level Security becomes essential (75% of new attacks are against applications).**
- **Intelligent/Application Aware Routing & service/message gateways (Message Level Routing) become essential.**
- **Disparate Protocols & Applications (above layer 3/TCP) must integrate!**
- **Standard Transport, Message, & Business Protocols will become ever more important.**
- **Simple & Complex Transformation (on the fly) will play a bigger role. Most common transformation: Messages over multiple mediums.**

Application Services: Pain Points

- **Application Monitoring/SLA**
- **Application Optimization**
- **Application Mgt/Virtualization**
- **Application Security**
- **Application Scaling**

Making the Network Application-Aware

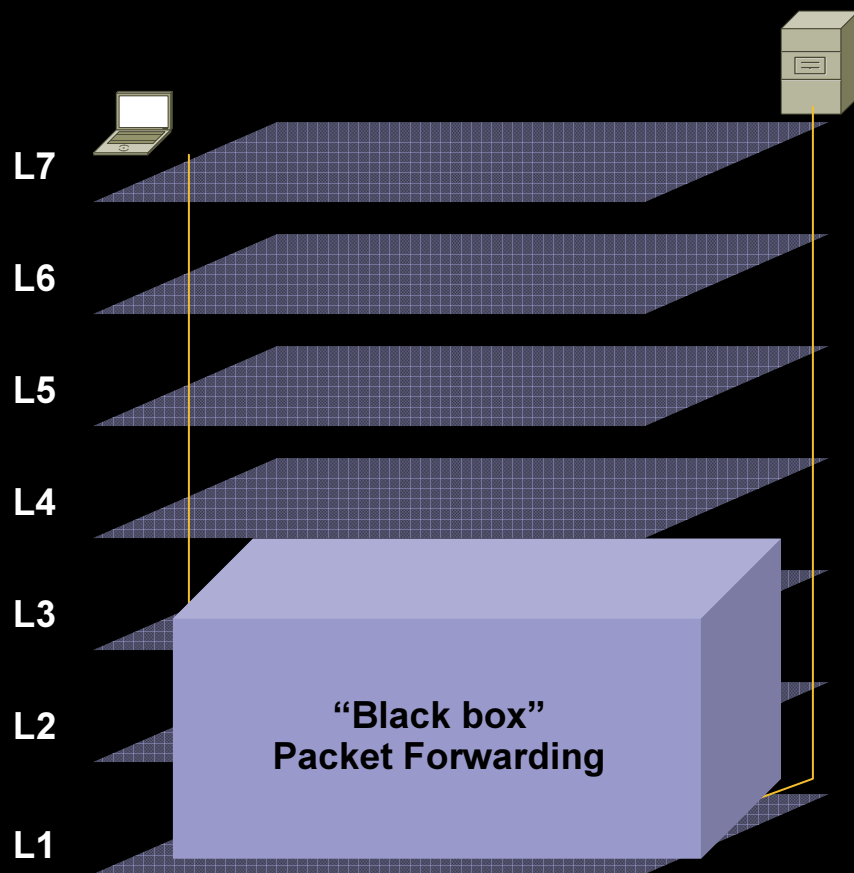
What Does Cisco Offer?



Network Paradigm Shift

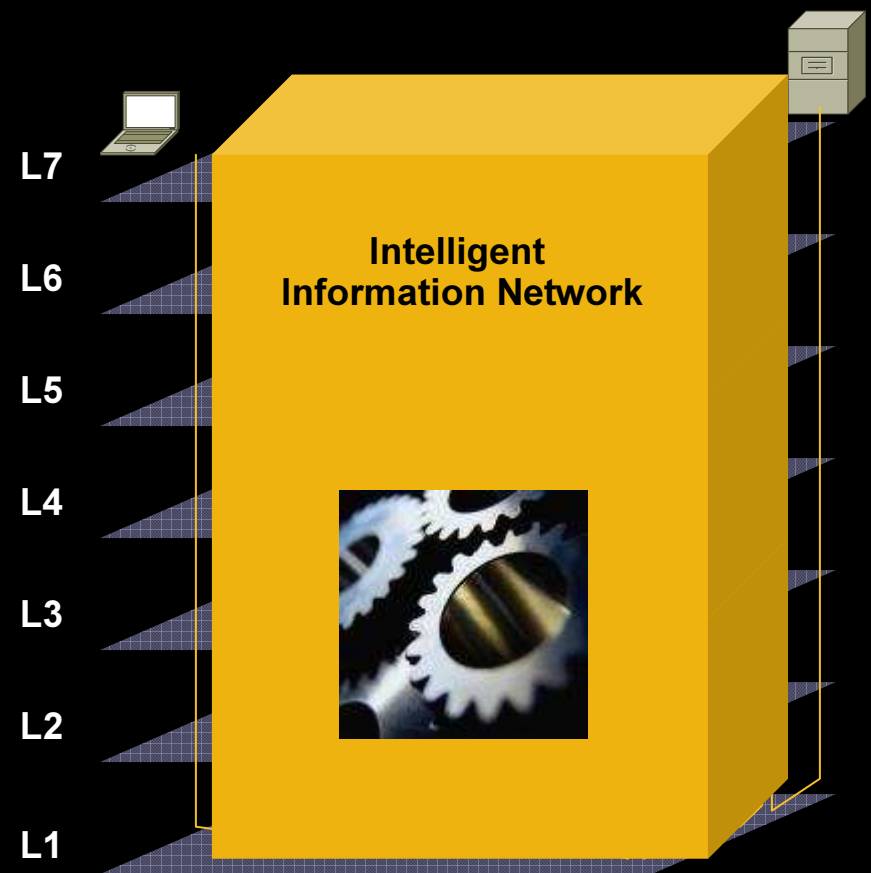
Old world

Network = packet forwarding



New world

Intelligent Information Network (IIN)
Service-Oriented Network Architecture (SONA)



Application Optimization

Why Optimization?

SampleServer;login;

19 characters!

However receiving application must know the following:

-Server Name = SampleServer

-Action = login

-Delimiter = ;

-EOL/EOF

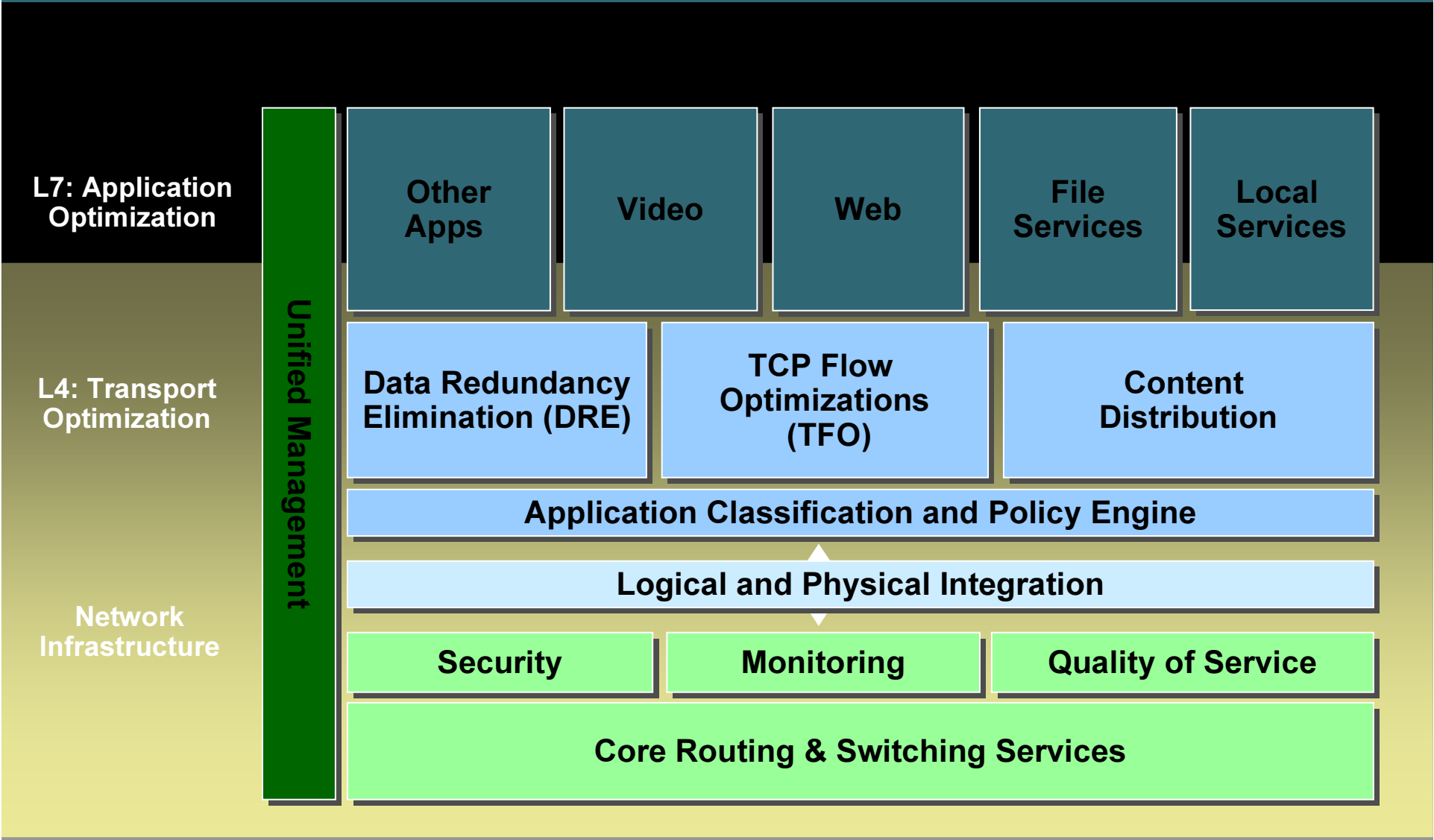
Why Optimization?

```
<?xml version="1.0" encoding="UTF-8" ?>
  <Request xmlns="urn:oasis:names:tc:xacml:1.0:context"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:1.0:context cs-xacml-schema-context-01.xsd">
    <Subject />
    <Resource>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
      DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>SampleServer</AttributeValue>
      </Attribute>
    </Resource>
    <Action>
      <Attribute AttributeId="ServerAction" DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>login</AttributeValue>
      </Attribute>
    </Action>
  </Request>
```

605 characters!

More Bandwidth! More Powerful Networking Gear! More need For Optimization! More Processing Power! More Storage!

Cisco WAAS Optimization Architecture



WAAS Accelerates Broad Range of Applications

Application	Protocol	Typical Improvement
File Sharing	<ul style="list-style-type: none"> • Windows (CIFS) • UNIX (NFS) 	<ul style="list-style-type: none"> • 2X-100X
Email	<ul style="list-style-type: none"> • Exchange (MAPI) • SMTP/POP3, IMAP • Notes 	<ul style="list-style-type: none"> • 2X-50X
Internet and Intranet	<ul style="list-style-type: none"> • HTTP, HTTPS, WebDAV 	<ul style="list-style-type: none"> • 2X-50X
Data Transfer	<ul style="list-style-type: none"> • FTP 	<ul style="list-style-type: none"> • 2X-50X
Software Distribution	<ul style="list-style-type: none"> • SMS • Altiris 	<ul style="list-style-type: none"> • 2X-100X
Database Applications	<ul style="list-style-type: none"> • SQL • Oracle • Notes 	<ul style="list-style-type: none"> • 2X-10X
Data Protection	<ul style="list-style-type: none"> • Backup Applications • Replication Applications 	<ul style="list-style-type: none"> • 2X-10X
Other	<ul style="list-style-type: none"> • Any TCP-based Application 	<ul style="list-style-type: none"> • 2X-10X

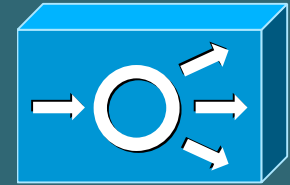
*** Performance improvement varies based on user workload, compressibility of data, and WAN characteristics and utilization. Actual numbers are case-specific and results may vary.**

Application Scaling & Virtualization

Why Scaling/Virtualization?

- **Application instances periodically seize to work.**
- **Number of concurrent transactions/users may require many instances of the same applications**
- **Rules for load balancing applications have become more complex.**
- **Application/service virtualization has become essential in order to simplify & automated provisioning.**

What Is ACE ?



Application Control Engine

Brand **new product line in the Cisco ANS portfolio**
Infrastructure simplicity in a single hardware platform,
ACE integrates

Content switching
SSL offload
Data center security features

The first ACE product is a **Cisco Catalyst® 6500 service module**, which comes in three flavors: 4Gbps, 8Gbps, and 16Gbps

The hardware supports **two field-replaceable daughtercards** for future hardware-accelerated application delivery functionality like HTTP compression

It delivers **application infrastructure control**, with features like virtual partitions and native role based access control (RBAC)

The Application Control Engine At-a-Glance

Application Infrastructure Control

- **Virtual Partitioning**
- **Hierarchical Management Domains**
- **Role-Based Access Control**

Application Performance

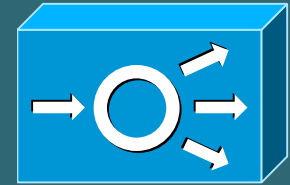
- **High Throughput (16Gbps)**
- **Maximum Scalability (350K CPS)**
- **Multi-tiered reliability, availability, and scalability**
- **Server Load Balancing**
- **Content Switching (L7 decisions and advanced stickiness)**

Application Security

- **Protocol-layer inspection**
- **TCP/IP Normalization**
- **Hardware-accelerated Protocol Control**
- **Access Control List (ACL) (up to 256K ACEs)**
- **DDoS Protection**

Infrastructure Simplification

- **Layer 2–7 Network Integration**
- **Functional Consolidation**
- **Application Network Management solution**
- **TCP Offload**
- **SSL Termination**
- **XML API**



ACE SLB Features

- **Predictors: Round Robin, Weighted Round Robin, Least connections, IP Hash, Connection Watermarks, Content Awareness**
- **Health Probes: L3 Ping, L4 UDP Data, HTTP GET, HTTP HEAD, DNS, POP, IMAP, Telnet, ICMP, TCP, UDP, ECHO, Finger, SMTP, RADIUS, LDAP, HTTP GET over SSL**
- **TCP Reuse: TCP connections are reused to minimize TCP setup and teardown on real (application) servers**
- **HTTP Redirection**
- **Persistence: Cookie, Cookie Insert, Offset & Length, Header Insert**
- **Redundancy: Inter-chassis (ACE modules in different Catalyst 6500), Intra-chassis (ACE modules in the same Catalyst 6500), or Inter-context (virtual partition) between applications. A mix of multiple active and standby contexts may run on a given ACE module**

Application Acceleration & Security

Web Application Acceleration

- **Optimize at Layer-7**
 - 2X–response time improvements**
 - 80% decrease in bandwidth requirements**
 - 80% fewer server cycles**
- **Stop application hacking**
 - Safely deploy applications**
 - Secure mission critical data**
 - Streamline operations**

**Secure, Fast & Reliable
Applications**



Cisco AVS 3120

Huge Lead in Acceleration Features

Functional Areas	AVS Acceleration Features
Latency Reduction	<ul style="list-style-type: none">▪ FlashForwarding*▪ Browser TCP multiplexing*▪ PDF download optimization▪ Response redirection control*
Bandwidth Reduction	<ul style="list-style-type: none">▪ GZIP Compression▪ Delta encoding*▪ Dynamic browser caching*▪ Dynamic image optimization▪ Flexible processing rules
Server Offload	<ul style="list-style-type: none">▪ TCP Offload▪ SSL Offload▪ RAM Caching▪ Dynamic caching*▪ Load-based caching*▪ Lazy request evaluation*▪ Single sign-on optimizations▪ XML merging/transformation

Delta Encoding

- **Web page caching is successful because many Web pages don't change and subsequent requests may be satisfied from the cache instead of the server.**
- **But some resources and content often change, which forces the re-retrieval of the modified page.**

Page will be marked as Non Cacheable

- **However, the modifications and changes are often minimal.**

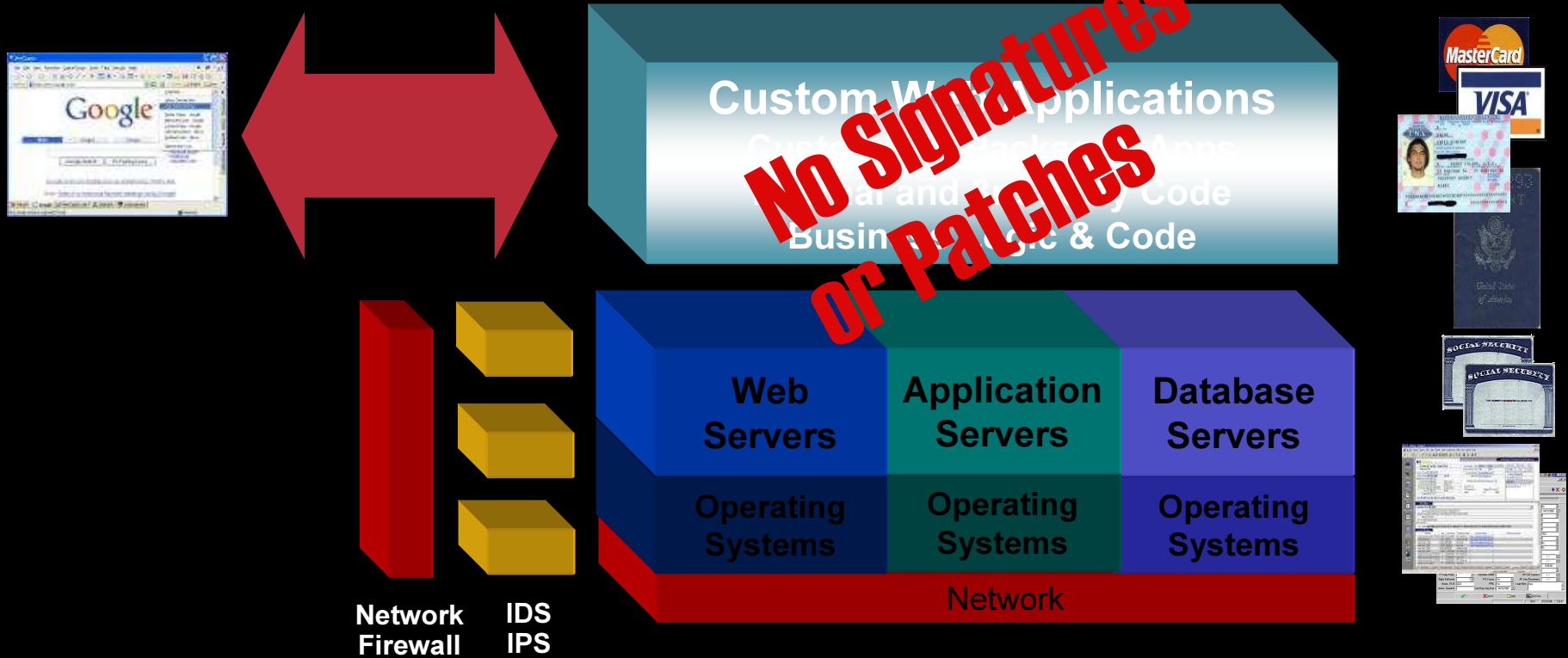
Often only a few bytes

- **Delta encoding delivers to the client only the *differences* between the cached (older) page and the new page.**

Often only a few bytes

Why Application security?

75% of Attacks Focused Here



Comprehensive Application Security is the Answer!

AVS Delivers Applications Securely

INSPECTS FOR:

SQL Injection
Cross-Site Scripting
Command Injection
Cookie/Session Poisoning
Application Reconnaissance
LDAP Injection
Buffer Overflows
Directory Traversals
Attack Obfuscation
Application Platform Exploits
Zero Day Attacks
Cookie Poisoning
Parameter Tampering



- **Bi – Directional Deep Inspection**
- **Positive & Negative Security**
- **Protocol compliance and anomaly detection**
- **Transaction logging and report for application security forensics**

Application Monitoring & Management

Why Application/Activity Management?

- **Distributed Applications are more difficult to manage.**
- **Policies enforced across applications are too costly.**
- **Distributed attacks have become far more common.**

Cisco AON Core Capabilities

Intelligent Messaging

- Reliable messaging
- Content based routing
- Transformation
- Protocol switching
- Message distribution
- Message load balance

Application-level Policies

- Authentication
- Authorization
- Encryption/Decryption
- Data integrity/
non-repudiation
- Digital signatures
- Centralized PKI mgt.

Business Event Visibility

- Event capture, filtering
- Logging for audit
- Automatic notification
- Policy controlled
- Feed to dashboards
- Link to Network events

Application Optimization

- Hardware Acceleration (SSL, Crypto, XML)
- Message level Caching and Compression
- High Availability, Failover, Load Balancing

Extensibility

- ADK (for custom adapters)
- SDK (for custom bladelets)
- AON Technology Partners

Application Networking Services! Where?

- **If you have applications running!! You may need one or more ANS technologies.**
- If you have branches!! You may need WAN Optimization
- If you have multiple or mission critical applications, you may need Content Switching & Load Balancing.
- If you're looking to improve application performance then you should consider SSL offloading, TCP offload, etc...
- If you have wireless! you may need RFID--Tracking.
- If you have network security, you may need Application-Level Security.

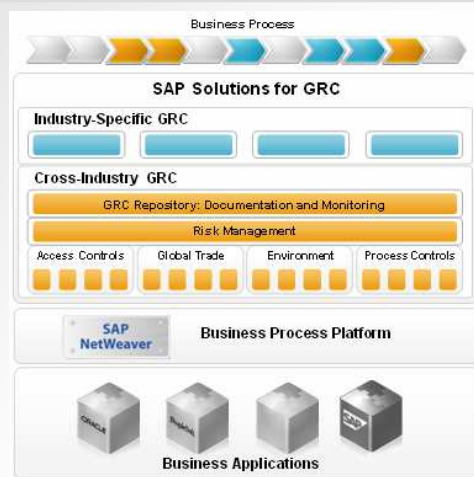
Questions!



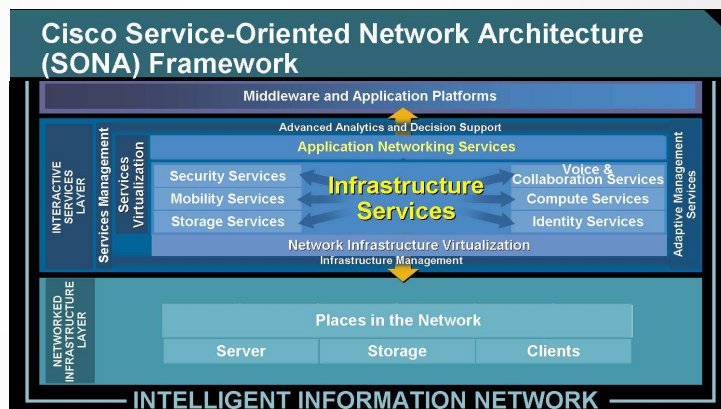
SONA/SAP Business Cases

- **Enable continuous monitoring and periodic testing of customer's Network IT Security environment in order to detect changes that may compromise IT Security compliance.**
- **Enable & Enforce Service Level Agreements (SLA) compliance.**
- **Enable non-intrusive protection of sensitive—personal & financial data exchanged across the network.**

SONA GRC Solution Overview



Cisco/SAP Adapter Layer



- Network-embedded GRC increases transparency and ability to manage risk effectively
- Shift to automatic controlled testing & simulations
- Aggregates and correlates multi-system, multi-application and multi-source information
- Provides predictive or early warning notifications
- Aligns controls with industry standards (e.g. COBIT)
- Delivers executive visibility into critical operational controls

Sample SONA/GRC Business Case



SAP GRC – Configuration Screens

The image displays three sequential screenshots of the YIRSA Process Controls configuration interface, accessed via Microsoft Internet Explorer. The browser address bar shows the URL: `http://172.21.52.138:50000/PC1/index.jsp`.

Top Screenshot: Main Dashboard
The interface features a navigation menu on the left with links for Home, Use Policy, Support, and User Login. The main content area includes a banner for "REAL-TIME COMPLIANCE REAL-TIME CONTROL" and a section titled "Why Confident Compliance?" with sub-sections for "Visibility" and "Control".

Middle Screenshot: Rules Designer
The "Rules Designer" screen provides a guided workflow for creating rules. It includes a "Rule Navigator" on the left and a central area with the following steps:

- Control List:** This step allows you to build and modify controls and associate them with required information.
- Define Rule:** In this section, you define what rules or system configurations are required to test the effectiveness of your controls.
- Build Rules:** Here, you build the rule parameters which produce the automated tests for your control.
- Define Test Period:** This allows you to determine the frequency of automated tests.

Bottom Screenshot: Application Set Up
The "Application Set Up" screen is divided into several sections:

- Inbox:** Contains links for My Tasks, My Documents, My Cases, and Workflow Inbox.
- Application Set Up:** Includes links for Organization Structure, Significant Account, Business Process, Test Plan, and Control Designer.
- Compliance Set Up:** Includes links for COSO Framework, Control Category, Control Type, and Deficiency Type.
- Case Management:** Includes links for Case List, Case List By Creation Date, Create Case, and Trend Analysis.

Network Event – Port Scanning

```
172.21.52.139 - default - SSH Secure Shell
File Edit View Window Help
SSH Secure Shell 3.2.0 (Build 267)
Copyright (c) 2000-2002 SSH Communications Security Corp - http://www.ssh.com/

This copy of SSH Secure Shell is a commercial version
licensed to CD-ROM customer, N/A.

Last login: Thu Jul 20 13:05:28 2006 from rtp-atrasi-vpnl.cisco.com
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# nmap -sS 172.21.52.0/24
```

```
172.21.52.139 - default - SSH Secure Shell
File Edit View Window Help
This copy of SSH Secure Shell is a commercial version
licensed to CD-ROM customer, N/A.

Last login: Thu Jul 20 13:05:28 2006 from rtp-atrasi-vpnl.cisco.com
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# nmap -sS 172.21.52.0/24

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host (172.21.52.0) seems to be a subnet broadcast address (returned 1 extra pi
ngs). Skipping host.
Interesting ports on (172.21.52.1):
(The 1596 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open       ssh
23/tcp    open       telnet
135/tcp   filtered   loc-srv
707/tcp   filtered   unknown
4444/tcp  filtered   krb524
```

SONA Device (IDSM Module) Captures Event

```

c:\ Telnet 172.21.52.136
Enter password:
Console> session 7
Trying IDS-7...
Connected to IDS-7.
Escape character is '^]'.
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto

If you require further assistance please contact
export@cisco.com.
SONA_IDSM2#
SONA_IDSM2#
SONA_IDSM2# show events

```

Intrusion Detection System (IDSM) monitoring events

Event Captured

```

c:\ Telnet 172.21.52.136
victim:
  addr: locality=OUT 172.21.52.18
  port: 0
victim:
  addr: locality=OUT 172.21.52.19
  port: 0
alertDetails: Traffic Source: 172.21.52.18

evAlert: eventId=1092711383356910623 severity=low
eventId=1092711383356910623
hostId: SONA_IDSM2
appName: sensorapp
appInstanceID: 1007
time: 2006/07/26 17:42:46 2006/07/26 17:42:46 UTC
intrusionAction: 0
vlan: 0
signature: sigId=2100 sigName=Net Sweep Echo subSigId=0 version=2.1.1
participants:
  attacker:
    addr: locality=OUT 172.21.52.189
    port: 8
  victim:
    addr: locality=OUT 172.21.52.18
    port: 0
--MORE--

```


SONA Device (CS MARS) Captures Event

The screenshot displays the Cisco Systems MARS (Malware Analysis Reporting System) interface. The main window shows a list of incidents with columns for Incident ID, Event Type, Matched Rule, Action, Time, Path, and Cases. A red callout bubble points to a specific incident entry, stating "Network Rule Triggered/ Incident Captured".

Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
11003523@	Inactive CS-MARS reporting device	System Rule: Inactive CS-MARS Reporting Device		Jul 20, 2006 12:00:02 PM PDT		
11003522@	Inactive CS-MARS reporting device	System Rule: Inactive CS-MARS Reporting Device		Jul 20, 2006 11:00:02 AM PDT		
11003521@	Inactive CS-MARS reporting device	System Rule: Inactive CS-MARS Reporting Device		Jul 20, 2006 10:00:02 AM PDT		
11003520@	Inactive CS-MARS reporting device	System Rule: Inactive CS-MARS Reporting Device		Jul 20, 2006 9:00:01 AM PDT		
11003519@	Inactive CS-MARS reporting device	System Rule: Inactive CS-MARS Reporting Device		Jul 20, 2006 8:00:01 AM PDT		

Network Rule Triggered/ Incident Captured

SONA Device (AON) Sends Notification over Unified Messaging to IP Phone

```
172.21.52.137 - default - SSH Secure Shell
File Edit View Window Help
SSH Secure Shell 3.2.0 (Build 267)
Copyright (c) 2000-2002 SSH Communications Security Corp - http://www.ssh.com/
This copy of SSH Secure Shell is a commercial version
licensed to CD-ROM customer, N/A.

slot3-kplus> sho log name aon.log tail
Press <CTRL-C> to exit...
20-Jul-2006 10:25:18 INFO [ObserverThread(com.cisco.aons.asg.phonepush.
PIHandler@1398044)] custombladelet CiscoTermInServiceEv (SEP00166F09B0F1)
```

```
172.21.52.137 - default - SSH Secure Shell
File Edit View Window Help
20-Jul-2006 11:18:05 DEBUG [MEC-Q-2] aons.mec.core In scopeInitiali
ze 0
20-Jul-2006 11:18:05 DEBUG [MEC-Q-2] aons.mec.core Operator Block I
d null
20-Jul-2006 11:18:05 DEBUG [MEC-Q-2] aons.mec.core Entering to find
associated opBlocks for scopeid 0
20-Jul-2006 11:18:05 DEBUG [MEC-Q-2] aons.mec.core Executing bladela
et - com.cisco.aons.bladelet.core.CreateMessage - 13
20-Jul-2006 11:18:05 DEBUG [MEC-Q-2] bladelet.CreateMessage Destinatio
n URI for this message is --> http://192.167.101.12:50000/CreateCase/Configl?s
tyle=document
20-Jul-2006 11:18:05 DEBUG [MEC-Q-2] aons.mec.buffer Created data rea
der for AONS Buffer[4131696]
20-Jul-2006 11:18:05 DEBUG [MEC-Q-2] aons.mec.core Correlation Id:
AAAAAAEMbxgwZQAAAwAAAAAy
20-Jul-2006 11:18:05 DEBUG [MEC-Q-2] aons.mec.core MessageHandler.s
etPriority(Message) Priority: 0
20-Jul-2006 11:18:05 DEBUG [MEC-Q-2] bladelet.CreateMessage Created
message : AONS-Id0.0.0.0@1152915091557--3-50
20-Jul-2006 11:18:05 DEBUG [MEC-Q-2] aons.mec.core Setting 13:AonsM
essage to be a ICloseable with hashCode -1322456795
20-Jul-2006 11:18:05 NOTICE [MEC-Q-2] bladelet.CreateMessage CreateMe
ssage executed successfully Bladelet=13:CreateMessage,MEC Id=MEC-ID-11529150
83758-6-79
```

SONA Device (IP Phone) Displays Event



Compliance Breach Notification is Displayed

Other Technology Solutions

- **Location Tracking.**
- **Unified Communication-CRM Integration.**
- **FIX Monitoring.**