WAN and Application Optimization Technical Overview

April 2008

Agenda

- Customer Challenges

- Vision for Cisco WAN and Application Optimization

- Solution Components

     Monitoring and Instrumentation

     Classification

     Optimization

     Control

     Network Management

- Putting it Altogether

     Branch Deployment

     Data Center Deployment

     Network Management

- Best Practices

- Summary

Customer Challenges

Perspectives on Key Application Delivery Challenges

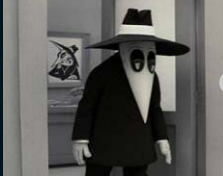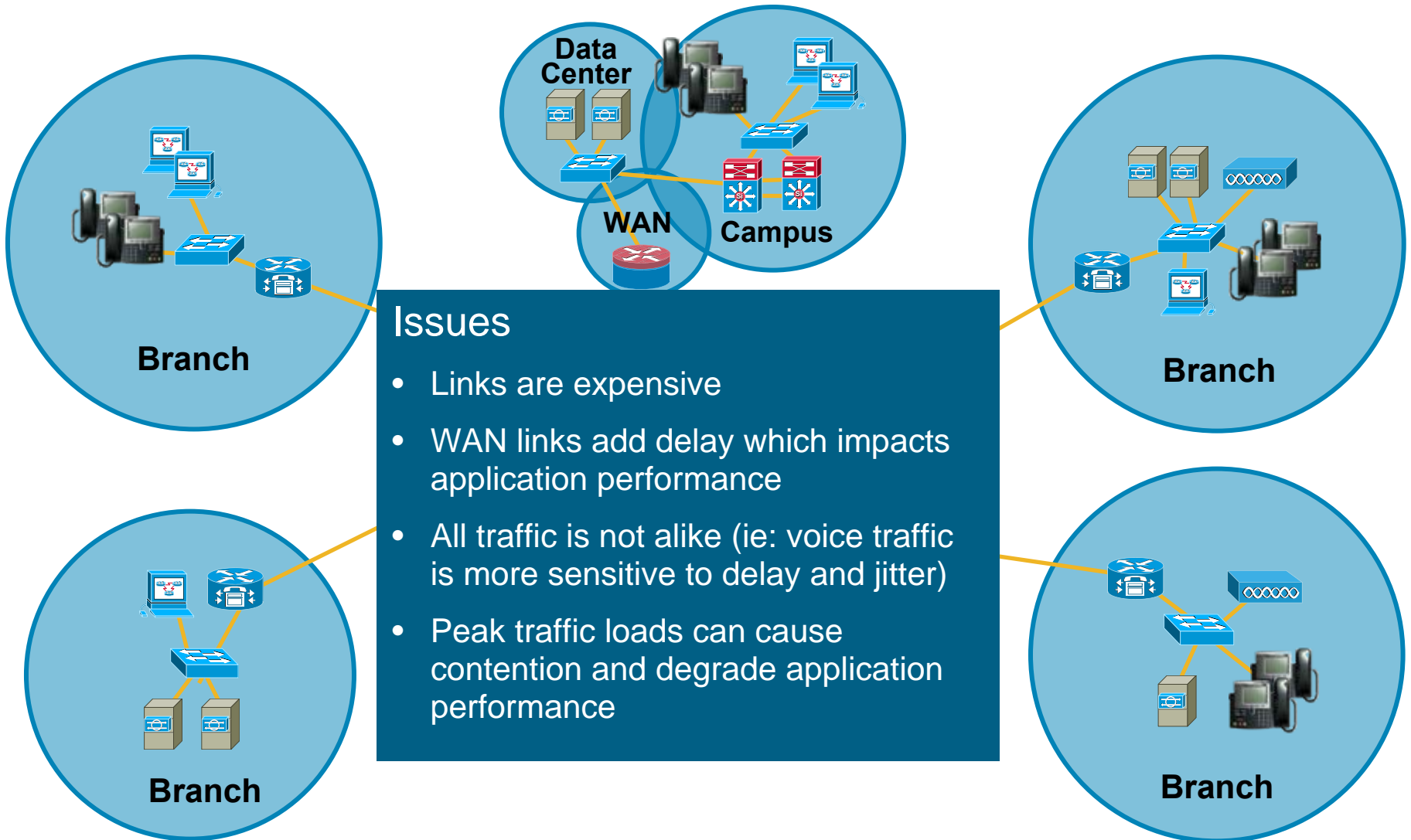|	
CxO	"Need to control operations and capital costs, and at the same time introduce new services" "IT needs to better support the business"
Apps/ Servers	"Deliver LAN-like response times" "Chatty protocols,a bandwidth upgrade is not always the answer"
Ops	"Often no coordination between developers, server administrators and network engineers" "IT infrastructure centralization"
SecOps	"Compliance and regulations driving consolidation of servers and applications" "Protect the applications and data from attack"
Work Force	"Increasingly located outside of HQ, but expect the same response time when connected remotely"
Network	"Web-based applications put significant burdens on the network"

Things to Look Out for in the WAN

Data Center

WAN

Campus

Branch

Branch

Branch

Branch

Issues

- Links are expensive

- WAN links add delay which impacts application performance

- All traffic is not alike (ie: voice traffic is more sensitive to delay and jitter)

- Peak traffic loads can cause contention and degrade application performance

Vision for Cisco WAN and Application Optimization

Application Optimization Process

Profile and Baseline

- **Profile:** Understand current traffic patterns and resource utilization levels providing visibility to applications and services needing optimization

- **Baseline:** Establish baseline performance metrics for applications and resources (links, servers, etc.)
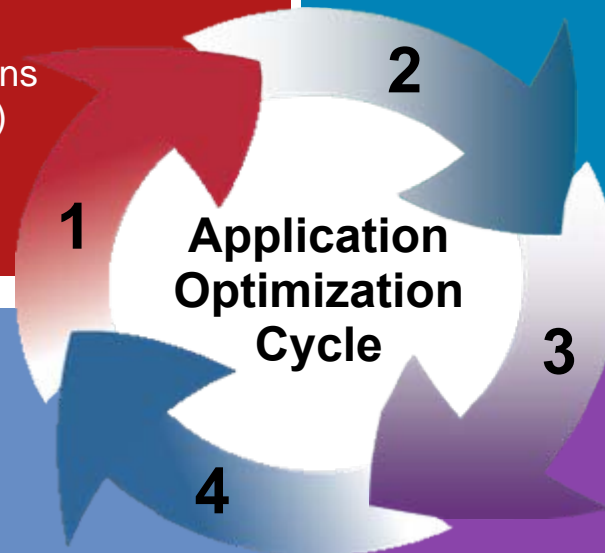
Optimize

- Apply optimization techniques to meet performance objectives

  Application/protocol optimization

  Bandwidth optimization (compression, caching, etc.)

  Path optimization

  Congestion management and avoidance (QoS)

1   **2**

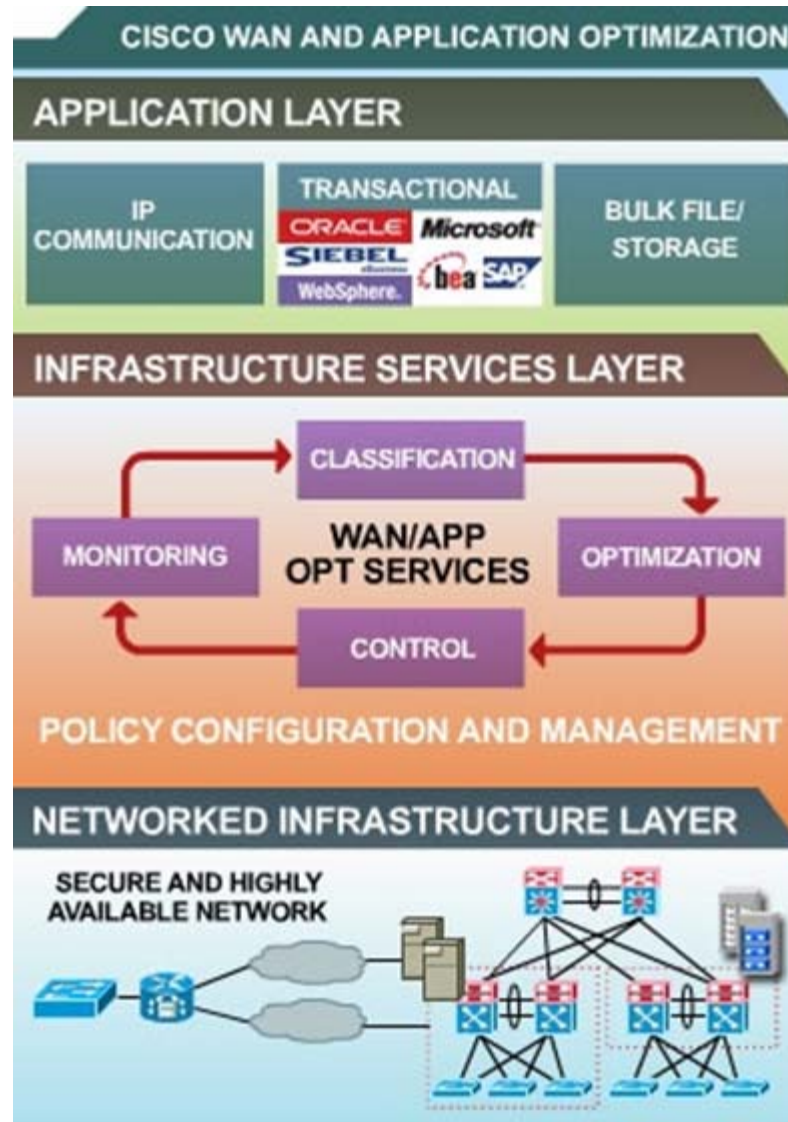**Application Optimization Cycle**

4   **3**

Evolve

- **Applications and Services:** Roll out new ones and remove the obsolete

- **Users:** Add new users

- **Topology:** Add/remove:

  Sites and subnets

  Links
  Equipment

Operate

- **Assess:** Quantify effectiveness of optimization techniques

- **Tune:** Fine-tune the network and optimization parameters

- **Troubleshoot:** Investigate and address performance problems

Enterprise WAN and Application Optimization Framework
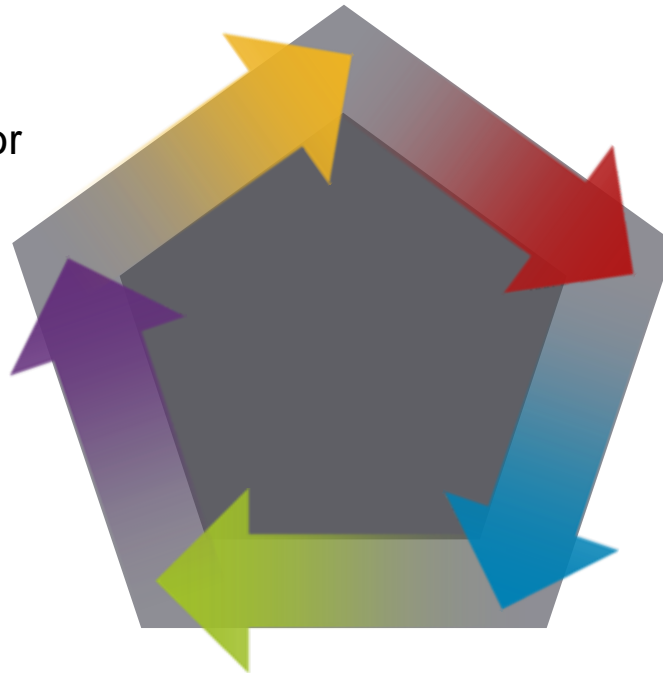
Solution Components: Overview

WAN and Application Optimization System Description

Monitoring and Instrumentation

- Visibility into network and application behavior
- Response time measurements

Network Management

- Centralized monitoring and reporting
- Configuration management
- Troubleshooting

Classification

- Automatic application recognition
- Traffic flow/application recognition
- Categorizing traffic based on policy

Optimization

- Application acceleration
- Application offload
- Reduce WAN traffic
- Reduce application latency
- Select the optimal path

Control

- Provide fair access for business-critical traffic
- Control non-business critical traffic
- Enforcement of business policies and priorities

Solution Components

Monitoring and Instrumentation	Classification	Optimization	Control	Network Management
• NetFlow to characterize and analyze traffic flows • IP SLA for active response time measurements • NAM for passive response time measurements • WAAS Flow Agent	• NBAR for protocol discovery, full packet, stateful inspection and enables application of QoS policies to traffic flows	• WAAS for data redundancy elimination, TCP Flow optimization • PfR for path optimization • ACE for server offload, connection management and server load balancing	• Cisco IOS® QoS to provide fair access for business-critical traffic • Cisco IOS Firewall for critical asset protection	• NetQoS for centralized monitoring and reporting • NAM for granular troubleshooting and conversation analysis

WAN Design (DMVPN, MPLS-VPNs, etc.)

Business-Ready Branch Overview

Product Portfolio

- Cisco 800/1800/2800/3800 Series Integrated Services Router
- Cisco WAN Area Application Services (WAAS)

Architecture Features

- Integrated security
- QoS
- Redundant WAN backup
- Path optimization
- Bandwidth optimization
- Path optimization
- Application acceleration
- Network and application visibility

Technologies

- Firewall
- DMVPN
- NBAR
- QoS (Quality of Service)
- Performance Routing (PfR)
- Data Redundancy Elimination
- TCP Flow optimization
- CIFS optimization
- NetFlow
- IP SLA

Business-Ready Data Center Overview

Product Portfolio

- Cisco 7X00 Series Gateway
- Cisco Catalyst® 6000 Switch
- Cisco Wide Area Application Service (WAAS)
- Cisco Application Control Engine (ACE)
- Cisco Catalyst 6000 Firewall Service Module (FWSM)
- Cisco Catalyst 6000 Network Analysis Module (NAM-2)
- NetQoS ReporterAnalyzer and SuperAgent

*Data Center technologies

Architecture Features

- End-to-end security
- QoS
- High Availability
- Path optimization
- Bandwidth optimization
- Path optimization
- Application acceleration
- Network and application visibility
- Server offload*
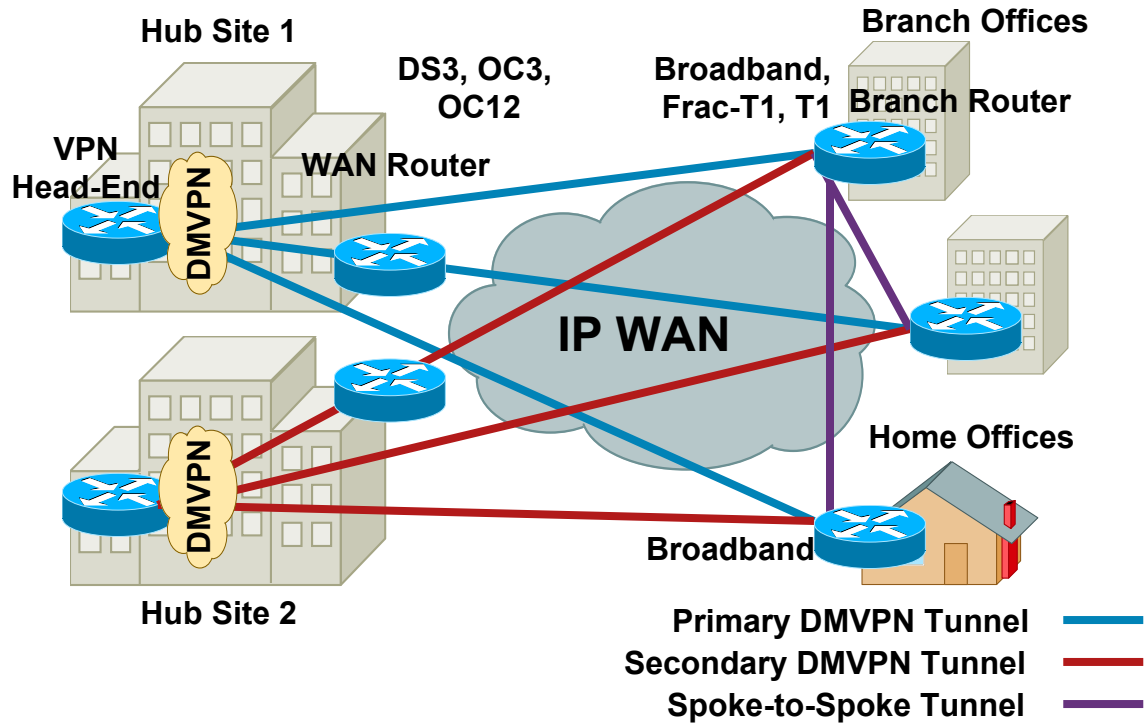- Network management*

Technologies

- Firewall
- DMVPN
- NBAR
- QoS
- Performance Routing
- Data redundancy elimination
- TCP Flow optimization
- CIFS 0ptimization
- NetFlow
- IP SLA
- Server load balancing*
- Connection management*

WAN Designs

Dynamic Multipoint VPNs

Hub Site 1

DS3, OC3, OC12

Branch Offices

Broadband, Frac-T1, T1 **Branch Router**

VPN Head-End

WAN Router

DMVPN

IP WAN

Home Offices

DMVPN

Broadband

Hub Site 2

Primary DMVPN Tunnel	———
Secondary DMVPN Tunnel	———
Spoke-to-Spoke Tunnel	———

	Head-End		**Branches**	
Routing Control Plane	Dynamic Routing	NHRP	Dynamic Routing	NHRP
GRE Control Plane	Multipoint GRE		Multipoint GRE	
IPsec Control Plane	Tunnel Protection	DPD	Tunnel Protection	DPD

Key Features:

- Multipoint GRE (mGRE)
- Dynamic IGP Routing (EIGRP, OSPF, etc.)
- NHRP

Good for:

- Customers already using routing
- IP only branch offices
- IP Multicast requirements
  Hub and spoke only
- Customers with dynamic partial or full mesh requirements

Solution Components: Monitoring and Instrumentation

Monitoring and Instrumentation Essentials

Application Monitoring

- Full recognition
- Metrics collection
- Application performance baselining

Device Monitoring

- Bandwidth utilization
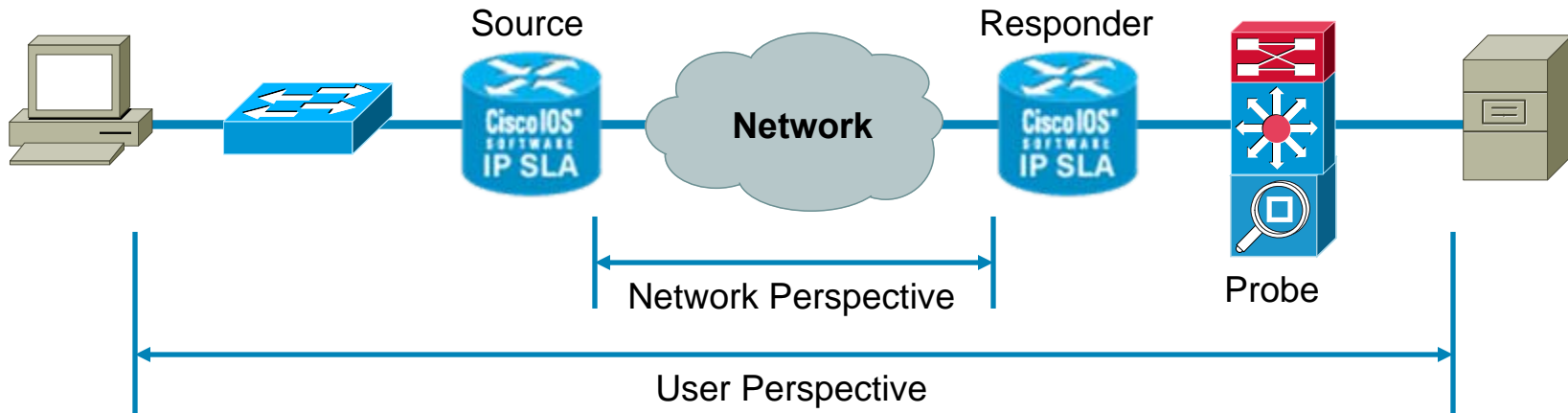- Topologies coverage (MPLS, VLAN, etc.)

Network Monitoring

- Flow analysis
- Quantifiable bandwidth utilization
- Network utilization baselining

Service Level Management

- Active response time measurements
- Passive response time measurements

Response Time Measurement

Active Agent

- Sampling Method

  Synthetic/active

- Collection Method

  Embedded agents instead of external probes

- Perspective of Measurement

  Network perspective

- Scope of Measurement

  End-to-end/path

Passive Agent

- Sampling Method

  Observing the traffic passively

- Collection Method

  External probes

- Perspective of Measurement

  Network perspective and user perspective

- Scope of Measurement

  End-to-end/path
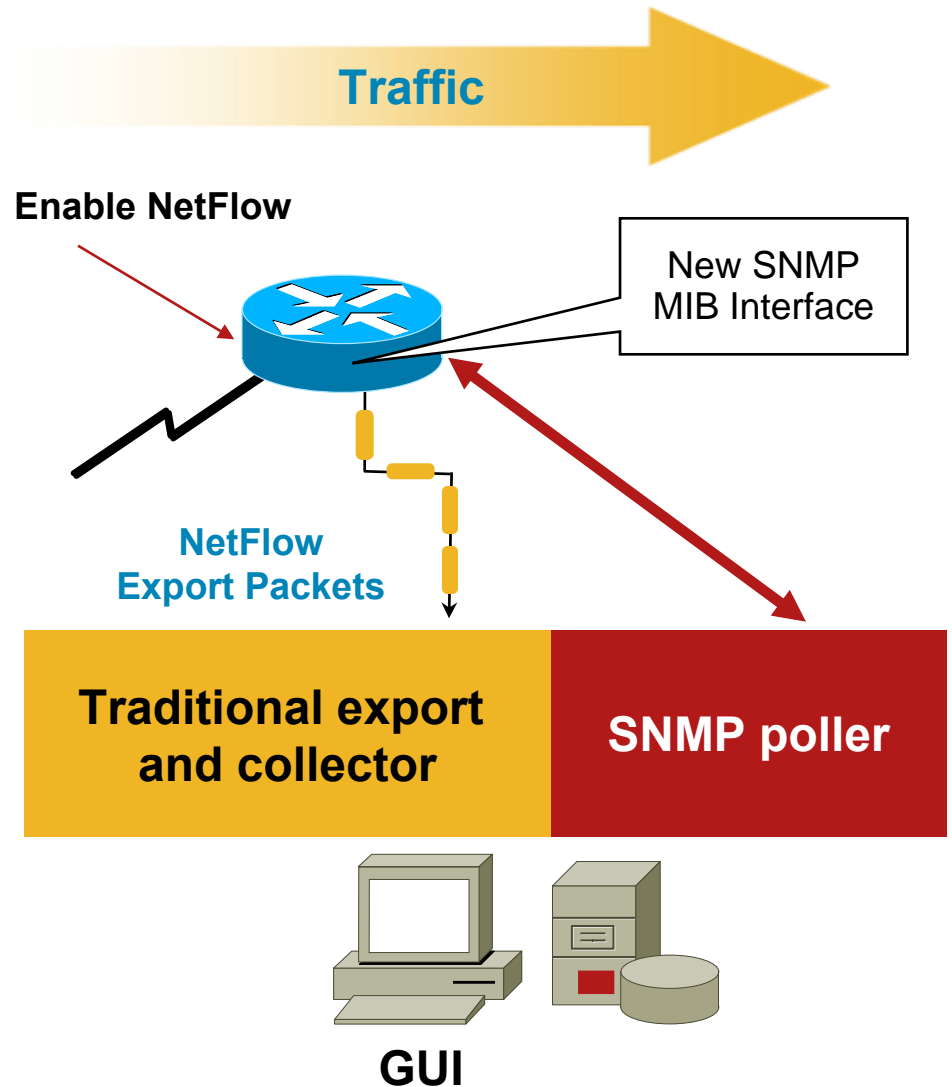
Solution Components Monitoring and Instrumentation

Component	Solution Function
NetFlow	Characterize and analyze traffic flows
IP-SLA	Actively gather performance measurements using synthetic traffic
NAM Instrumentation	Passively gather traffic and performance data for troubleshooting
WAAS Flow Agent	Facilitate correct performance reporting for optimized traffic

Principle Use of NetFlow

Solutions	Description
Analyze new applications and their network impact	▪ Identify applications and network load
Reduction in peak WAN traffic	▪ Measure WAN traffic improvement ▪ Understand who is utilizing the network and top talkers
Troubleshooting and understanding network pain points	▪ Diagnose slow network performance, bandwidth hogs and bandwidth utilization in real time
Detection of unauthorized WAN traffic	▪ Avoid costly upgrades by identifying the applications causing congestion
Security and anomaly detection	▪ NetFlow can be used for anomaly detection, worm diagnosis
Validation of QoS policies	▪ Confirm that appropriate bandwidth has been allocated to each application class

NetFlow is Defined by Seven Unique Keys

1. Source IP address
2. Destination IP address
3. Source port
4. Destination port
5. Layer 3 protocol type
6. TOS byte (DSCP)
7. Input logical interface (ifIndex)

Traffic

Enable NetFlow

New SNMP MIB Interface

NetFlow Export Packets

Traditional export and collector

SNMP poller

GUI

Solution Components - Monitoring and Instrumentation

Component	Solution Function
NetFlow	Characterize and analyze traffic flows
IP-SLA	Actively gather performance measurements using synthetic traffic
NAM Instrumentation	Passively gather traffic and performance data for troubleshooting
WAAS Flow Agent	Facilitate correct performance reporting for optimized traffic

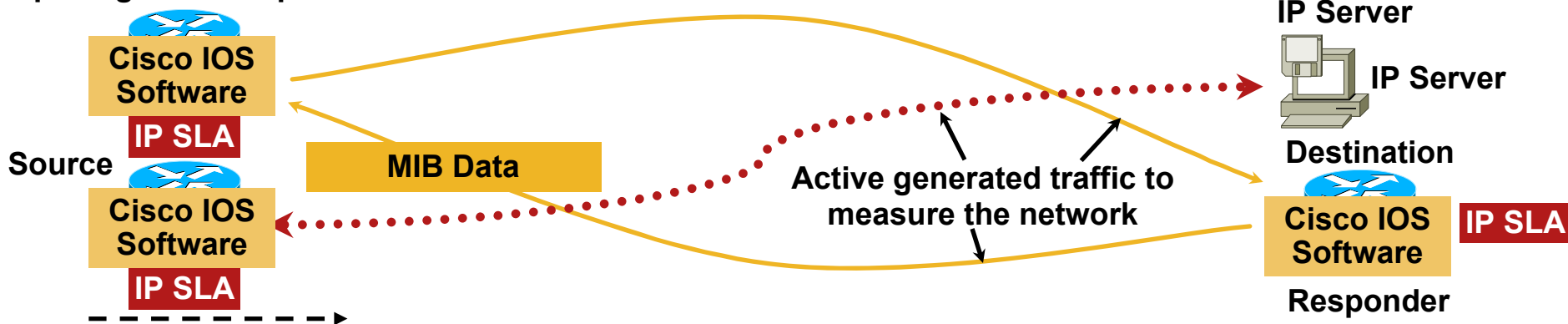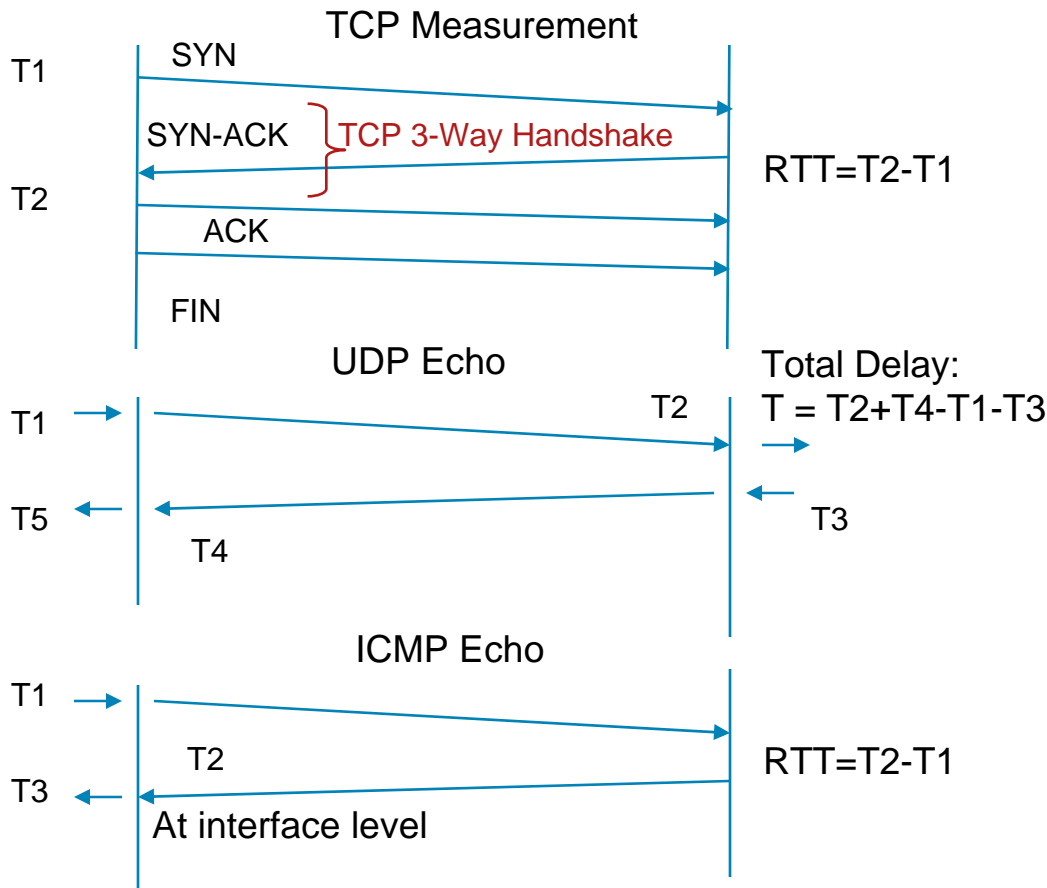# Multi-Protocol Measurement and Management with Cisco IOS IP SLAs

Uses

Availability	Network Performance Monitoring	VoIP Monitoring	Service Level Agreement (SLA) Monitoring	Network Assessment	Multiprotocol Label Switching (MPLS) Monitoring	Trouble-shooting

Measurement Metrics

Latency	Packet Loss	Network Jitter	Dist. of Stats	Connectivity

Operations

Jitter	FTP	DNS	DHCP	DLSW	ICMP	UDP	TCP	HTTP	LDP	H.323	SIP	RTP

Defined packet size, spacing CoS and protocol

Cisco IOS Software

IP SLA

Source

MIB Data

Cisco IOS Software

IP SLA

IP Server

IP Server

Destination

Active generated traffic to measure the network

Cisco IOS Software

IP SLA

Responder

Measuring TCP Response Times: Active Mode (Cisco IOS IP-SLA)

Jitter, packet loss, latency, voice quality

Sender   Responder

Network

TCP Measurement

T1 — SYN →

SYN-ACK } TCP 3-Way Handshake

RTT=T2-T1

T2

ACK →

FIN →

UDP Echo

Total Delay:
T = T2+T4-T1-T3

T1 →   T2

T5 ←   T3

T4

ICMP Echo

T1 →

RTT=T2-T1

T2

T3

At interface level
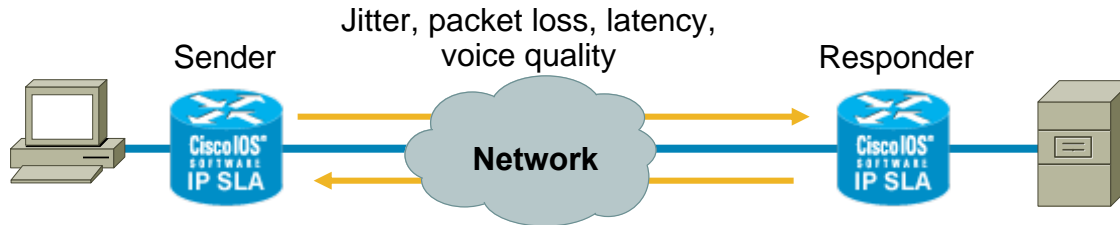
- Voice Deployment

  Cisco IOS IP SLAs provide comprehensive tools for voice deployment, including hardware-based VoIP measurements, MOS scores, H323/SIP integration

- Service Level Agreement Validation

  Cisco IOS IP SLAs are a frequently used tool by Service Providers to monitor customer SLAs, and by Enterprises to validate that they are getting the service provided

- High Availability for Mission-Critical Systems

  Cisco IOS IP SLAs integrate with policy-based routing, OER, HSRP and Embedded Event Manager (EEM) for automated problem resolution

Solution Components - Monitoring and Instrumentation

Component	Solution Function
NetFlow	Characterize and analyze traffic flows
IP-SLA	Actively gather performance measurements using synthetic traffic
NAM Instrumentation	Passively gather traffic and performance data for troubleshooting
WAAS Flow Agent	Facilitate correct performance reporting for optimized traffic

Cisco Network Analysis Module Overview


- **Cisco Network Analysis Module (NAM)**

  Embedded module for Cisco routers and switches, delivering both **NAM instrumentation** and **NAM network management** features (see network management section)

  In this solution, NAM-2 is deployed on the Cisco Catalyst 6000

- **NAM instrumentation collects data needed for detailed troubleshooting and conversation analysis**

  Per conversation TCP application response time metrics

  Detailed conversation data collection that allows interactive drill-down to individual conversations experiencing problems
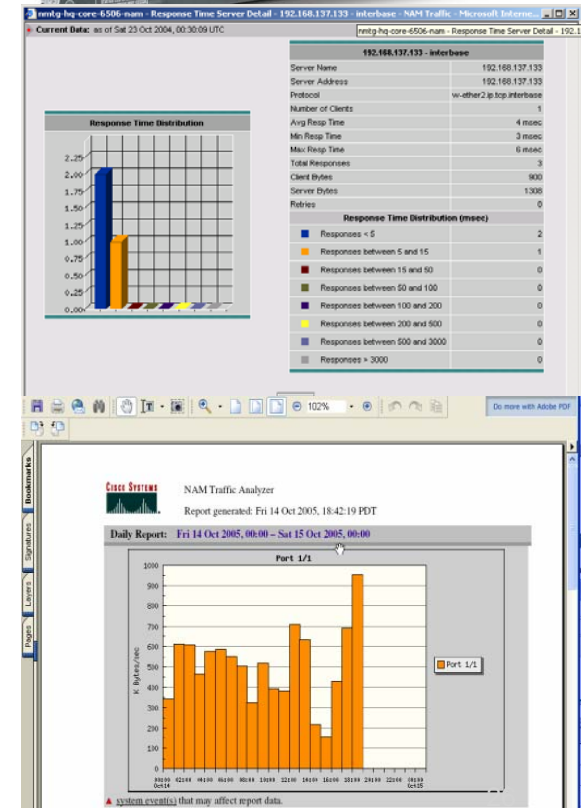
NAM Passive Measurements
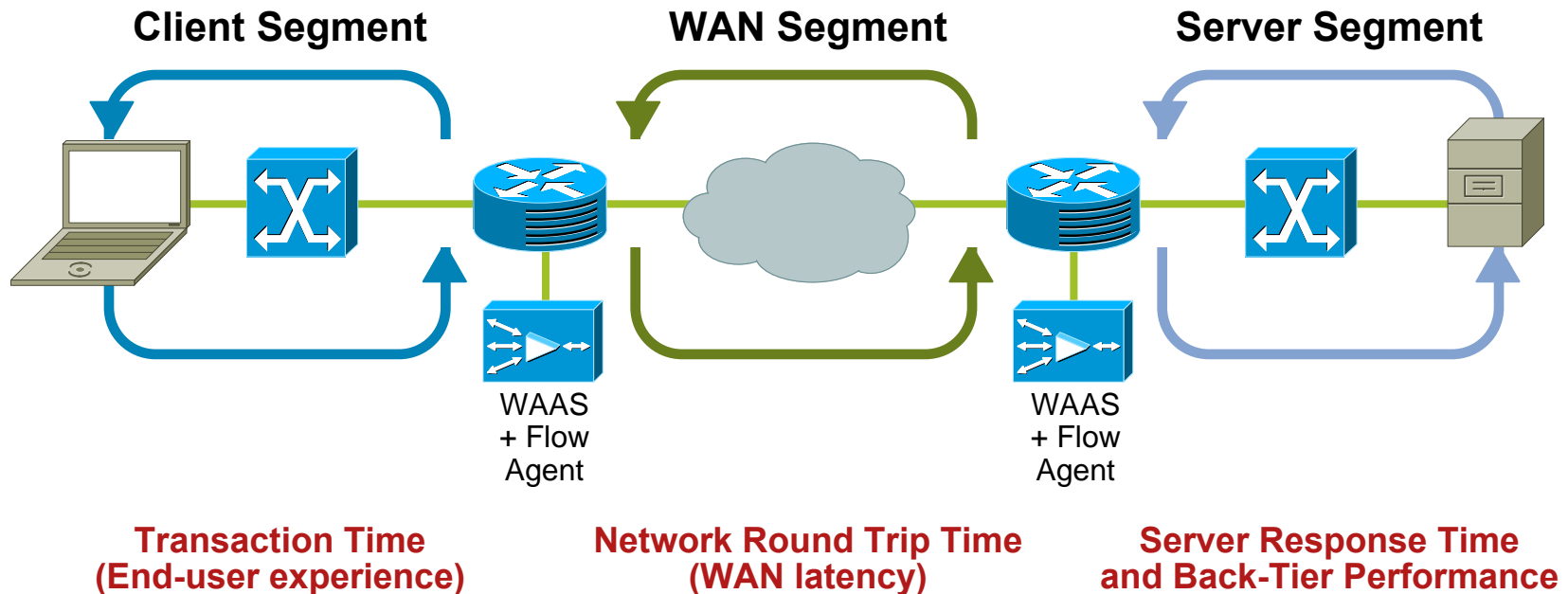
TCP Response Time Metrics

Metric Relative to	Metric	Description
Networks	**Network Delay (ND)**	The client-server roundtrip delay during TCP connection setup
	Client Network Delay (CND)	The roundtrip time between NAM and client during TCP connection setup
Servers	**Application Delay (AD)**	The time it takes the application server to start responding to a request from the client
	Server Network Delay (SND)	The roundtrip time between NAM and server during TCP connection setup
	Number of clients	Number of clients connecting to a server in the data center
	Number of connections	Number of connections connecting to a server in the data center
Applications	**Transaction Time (TT)**	The time it takes to complete a client-server application transaction
	Number of transactions	Number of client-server application transactions seen

Solution Components - Monitoring and Instrumentation

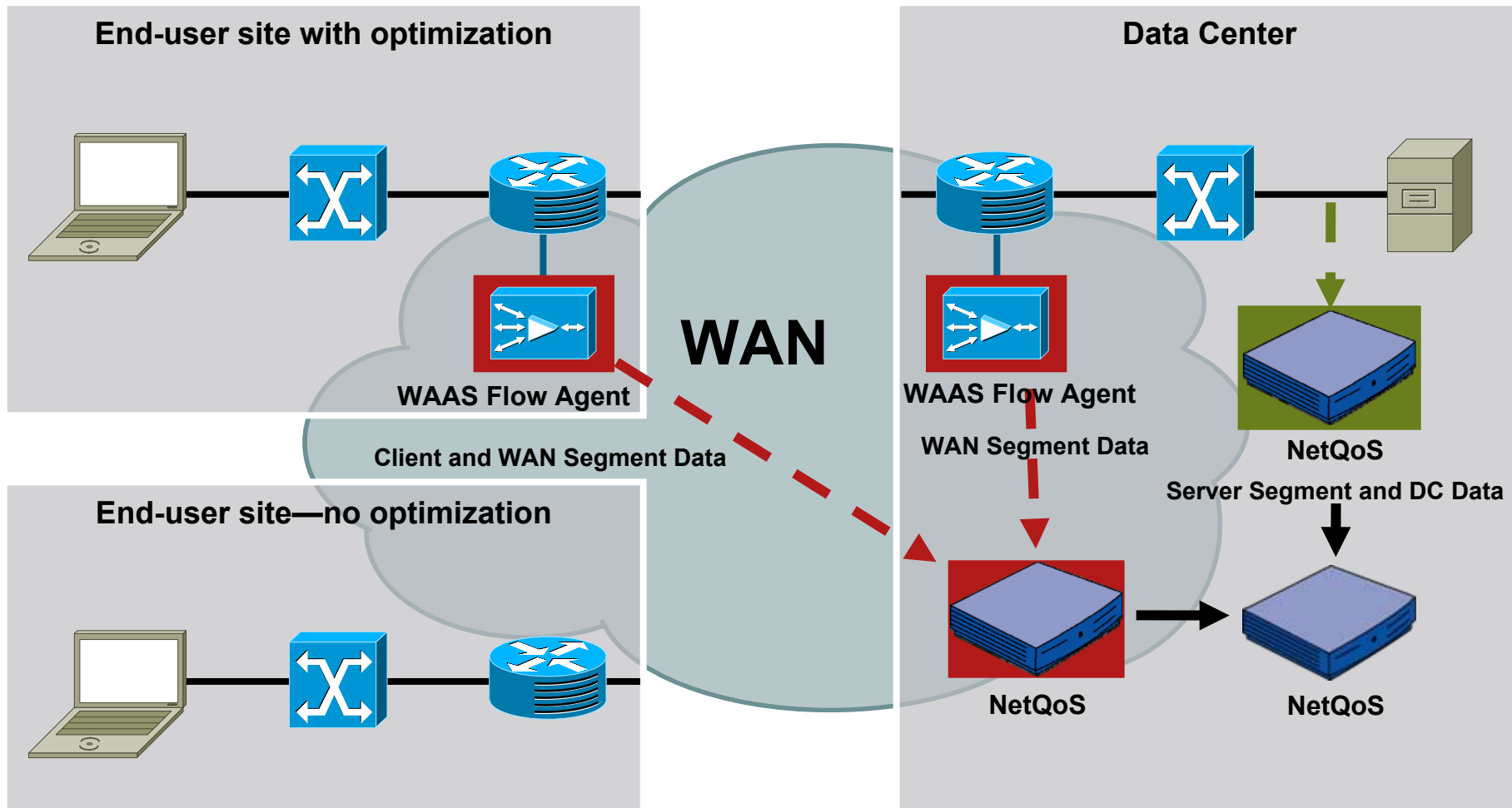| Component	Solution Function
NetFlow	Characterize and analyze traffic flows
IP-SLA	Actively gather performance measurements using synthetic traffic
NAM Instrumentation	Passively gather traffic and performance data for troubleshooting
WAAS Flow Agent	Facilitate correct performance reporting for optimized traffic

WAAS Flow Agent: Optimized Environment Monitoring

- WAN Optimization breaks the TCP session between client and server into three segments, each with different transactions

Client Segment   **WAN Segment**   **Server Segment**

WAAS + Flow Agent   WAAS + Flow Agent

Transaction Time (End-user experience)   **Network Round Trip Time (WAN latency)**   **Server Response Time and Back-Tier Performance**

- Cisco WAE flow agent enables accurate reporting of optimized traffic performance over the client, WAN and server segments without any additional remote instrumentation
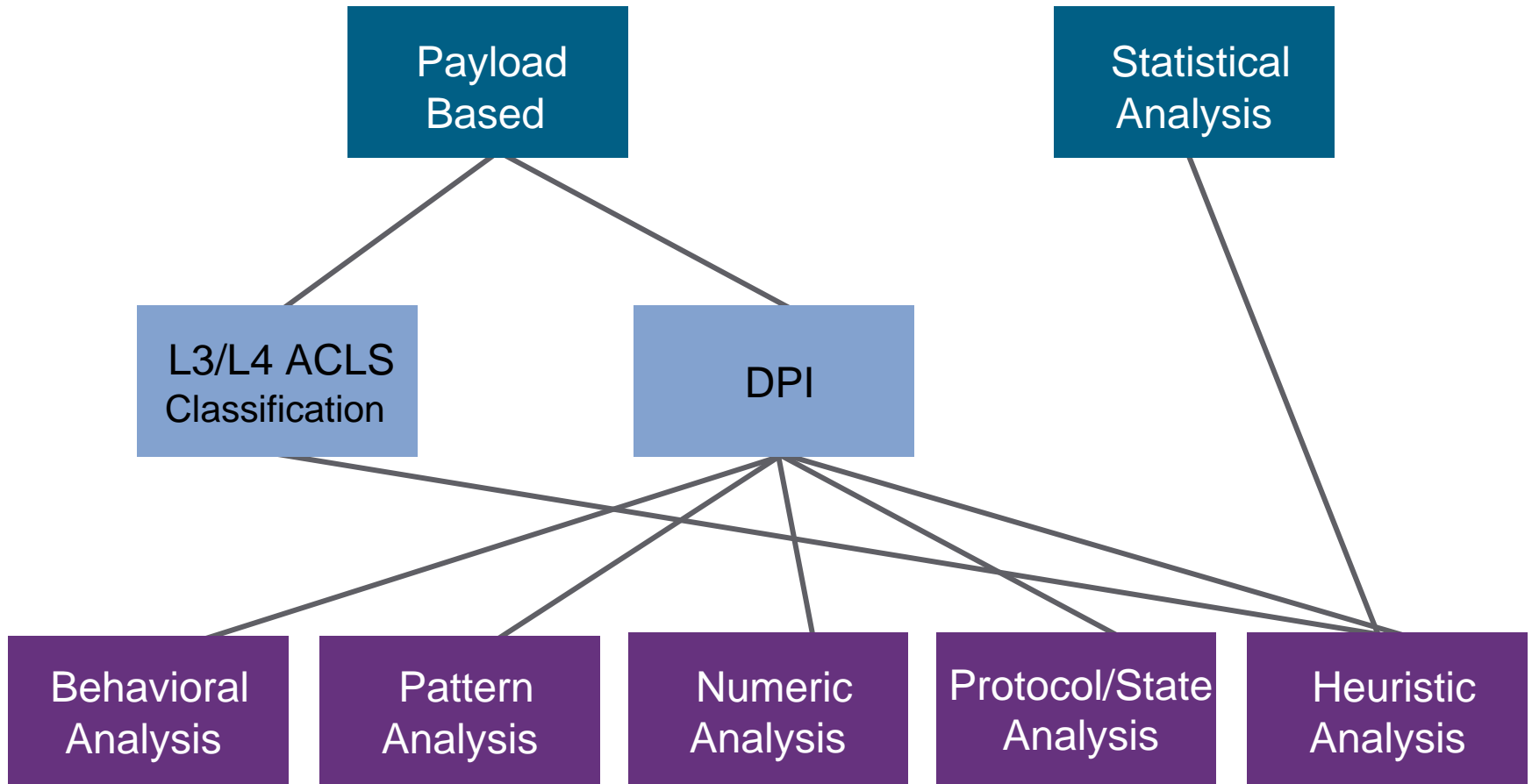
WAAS Flow Agent: Export to NetQoS

End-user site with optimization

Data Center

WAAS Flow Agent

WAAS Flow Agent

Client and WAN Segment Data

WAN Segment Data

WAN

End-user site—no optimization

NetQoS

Server Segment and DC Data

NetQoS

NetQoS

WAAS Flow Agent Data Feed

SPAN or VACL Data Feed

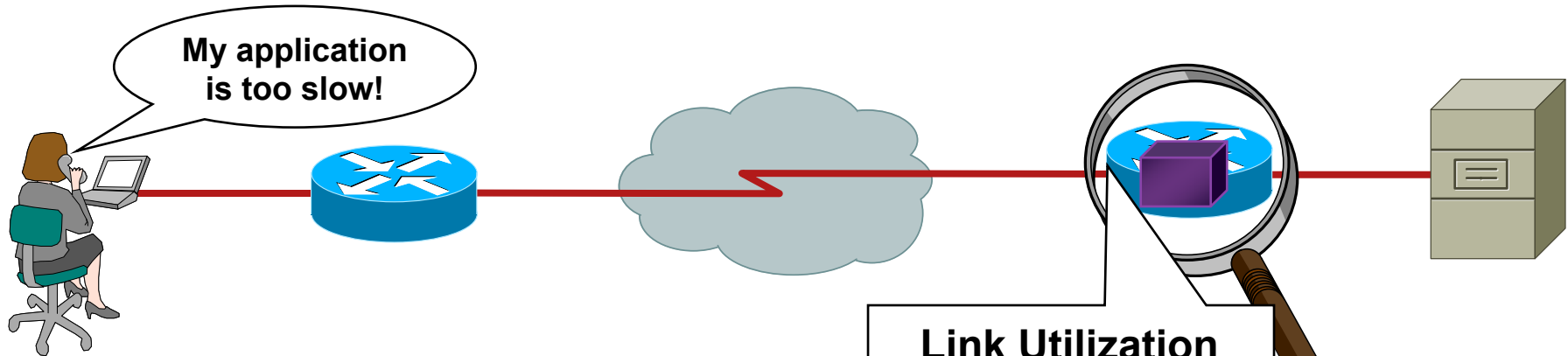# Solution Components: Classification

Classification Methods

How to Identify Applications

- Well known protocols can be classified by L3 and L4 fields

    IP Protocol-based services (non-UDP/non-TCP protocols)

    EGP, ICMP, GRE, IPsec, etc.

    UDP and TCP protocols

    DNS, Finger, Gopher, http, https, ntp, PCAnywhere, RIP, etc.

- But, what about applications that are not well-known?

Link Utilization

Citrix	**5%**
Telnet	**5%**
HTTP	**90%**
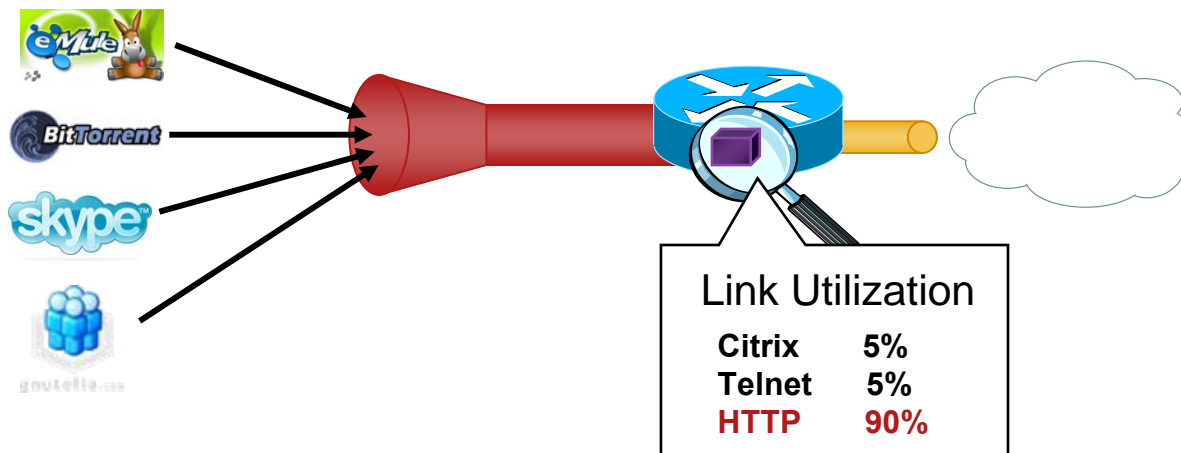
Network Based Application Recognition (NBAR) Overview

My application is too slow!

Link Utilization

Citrix	25%
Netshow	15%
Fasttrack	10%
FTP	30%
HTTP	20%

- Full-packet, stateful inspection identifies traffic type

- Protocol discovery analyzes multi-packet behavior and application signatures

- Enables application of QoS policies to traffic flows

Mark Citrix as interactive traffic and police FTP assure bandwidth for Citrix!

NBAR:
Stateful Application Intelligence

Real-Time Application Visibility

- Protocol Discovery: Discover what apps are running on the network with real-time statistics

- Per-interface, per-protocol, bi-directional statistics

    bit rate (bps); packet count; byte count

- SNMP accessible for centralized monitoring

- Supported by partner products (Concord/CA, InfoVista, Micromuse/IBM) and MRTG

Link Utilization
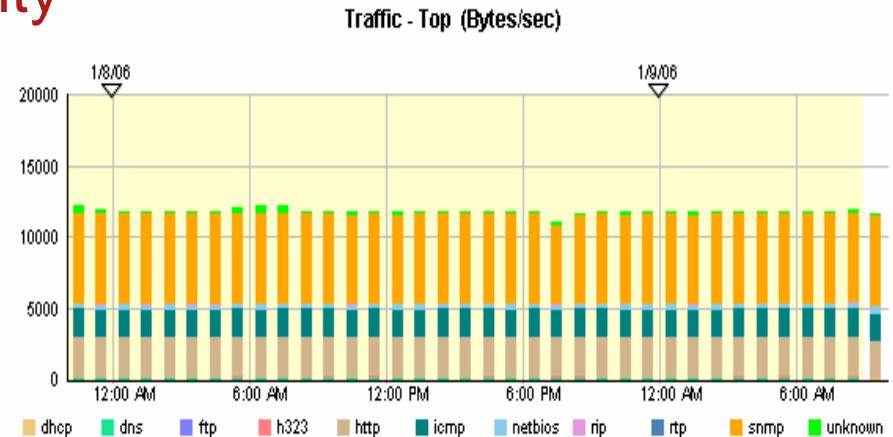
Solution Components: Optimization

Optimization Techniques

WAN Design/Secure Transport

Layer 7 Optimization

HTTP Compression

Application Acceleration
(CIFS, MAPI, etc.)

Layer 4 Optimization

TCP Stack Optimization

Layer 4 Payload Compression
(Data redundancy elimination)

Layer 3 End Point Optimization and Server Selection

DNS-Based Optimization
Anycast Addressing

Layer 7 Redirection
Server Load Balancing*

Path Optimization
Advanced load balancing, application best path selection, WAN problem migration

Pre-Positioning
VoD, Web, CIFS

Stream Splitting
Multicast
Multicast translation and unicast stream splitting

*Data Center technology

Not in this phase

The WAN is a Barrier to Consolidation

- Applications generally perform well in LAN environments as few barriers exist to application performance
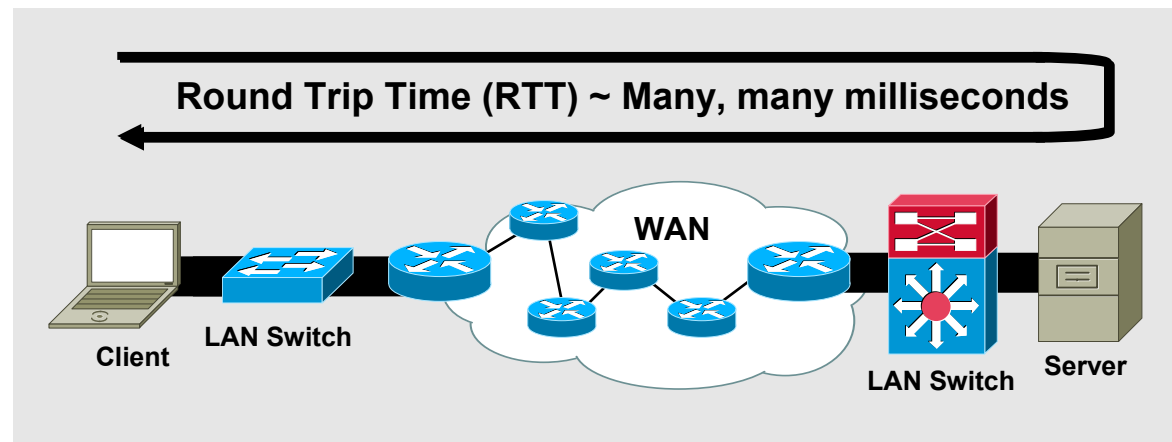
  - High bandwidth

  - Low latency

  - Reliability

Round Trip Time (RTT) ~ 0 mS
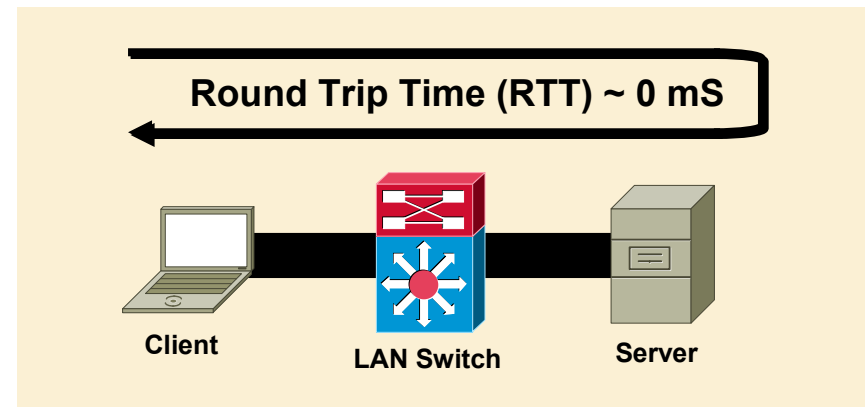
Client   **LAN Switch**   **Server**

- WAN characteristics hinder performance and consolidation efforts

  - Congested

  - Low bandwidth

  - Excessive delay

  - Packet loss

Round Trip Time (RTT) ~ Many, many milliseconds

**Client**   **LAN Switch**   **WAN**   **LAN Switch**   **Server**

Solution Components
Optimization

Component	Solution Function
WAAS	Application acceleration, advanced compression, and TCP optimization for WAN traffic
ACE	DC server load balancing and offload, application acceleration, with integrated security
PfR	Adaptive routing guided by application performance, for dynamic application path selection, network problem migration, and active load sharing

Cisco WAAS:
Overcomes the WAN

- Cisco WAAS overcomes application performance problems in WAN environments and enables server consolidation
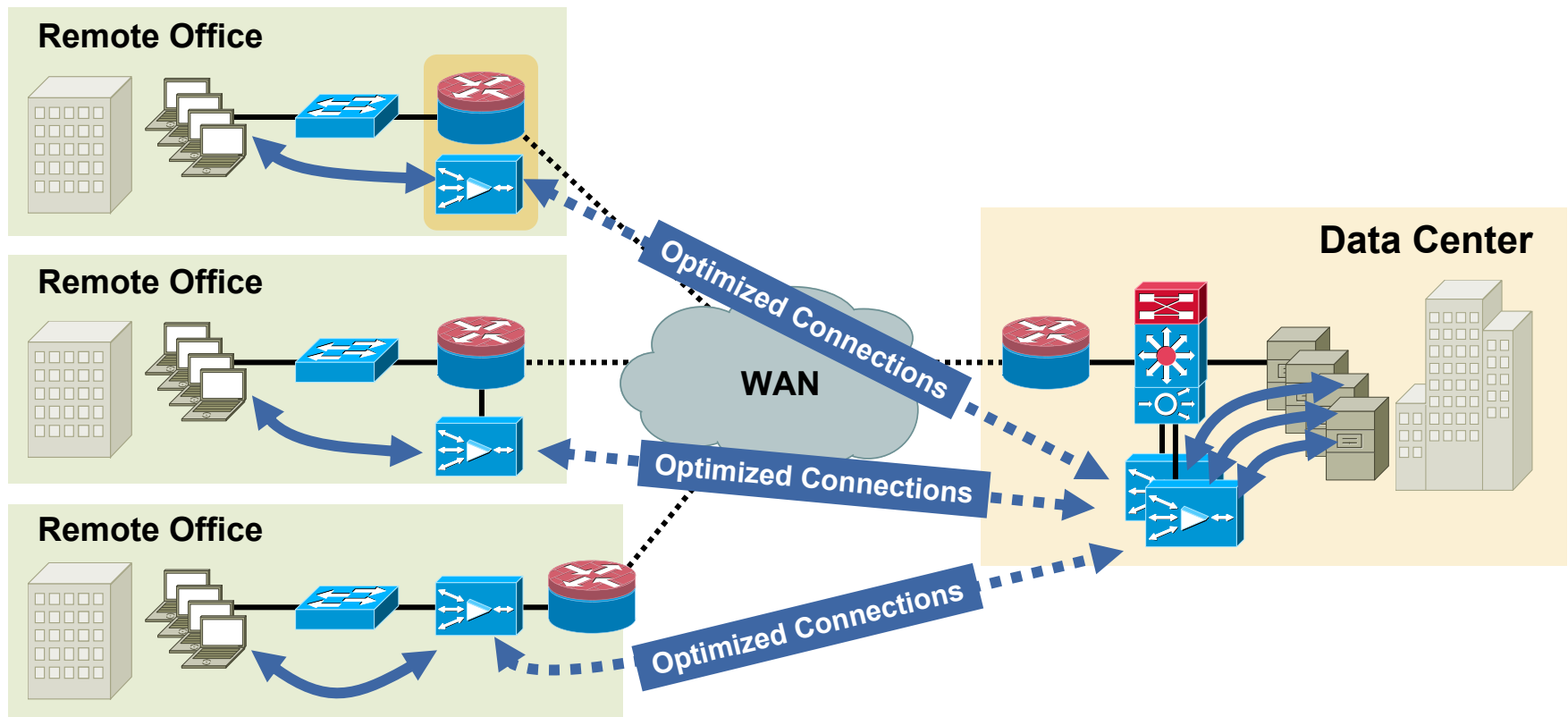
Cisco WAAS: Seamless Integration

Transparency Ensures Compliance with Critical Network Features
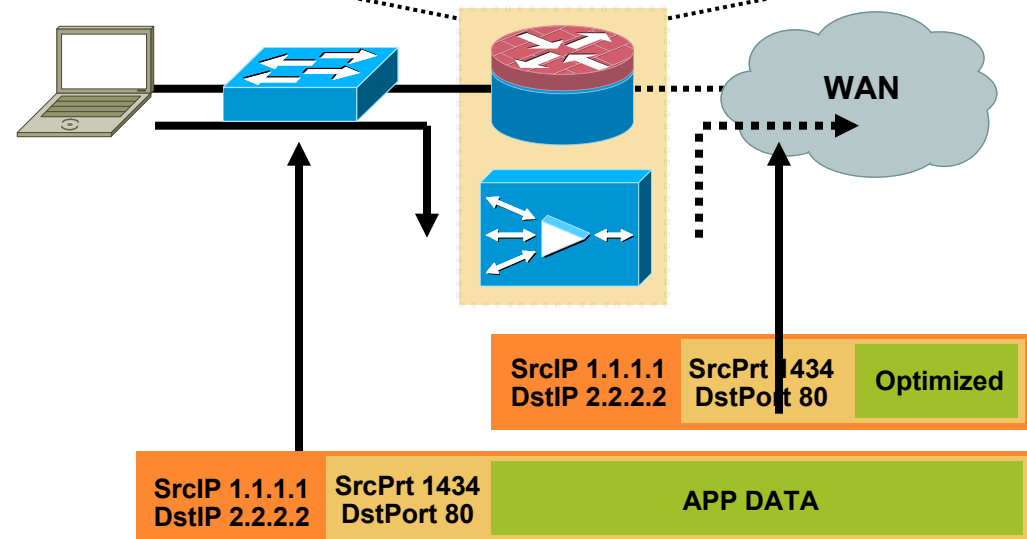
- **Quality of Service (QoS)**
  - Classification, NBAR, marking
  - Policing, shaping, queuing, WRED
  - LFI, header compression

- **Network Management**
  - NAM, NetFlow, NetQoS
  - NetQoS, IP SLA

- **Security**
  - Cisco IOS Firewall, IDS, IPS, ACL, VPN

- **Optimized Routing**
  - Network Path Affinity (NPA)
  - Performance Routing, PBR

Cisco Integrated Services Router

- Quality of Service (QoS)
- Network Analysis/NetFlow
- Cisco IOS Firewall
- Intrusion Prevention
- Performance Routing (PfR)
- Policy Based Routing (PBR)
- IP Service Level Agreements
- VPN

Cisco Wide Area Application Services

- Application acceleration
- Advanced compression
- Transport optimization
- Wide area file services

WAN

| SrcIP 1.1.1.1 DstIP 2.2.2.2 | SrcPrt 1434 DstPort 80 | Optimized |

| SrcIP 1.1.1.1 DstIP 2.2.2.2 | SrcPrt 1434 DstPort 80 | APP DATA |

WAAS Optimization

LAN TCP Behavior

Window scaling large initial Windows congestion mgmt improved retransmit

TFO

LAN TCP Behavior

Email

WAAS

Email

LZ .... **LZ**

DRE **DRE** **DRE**

Synchronized DRE Context
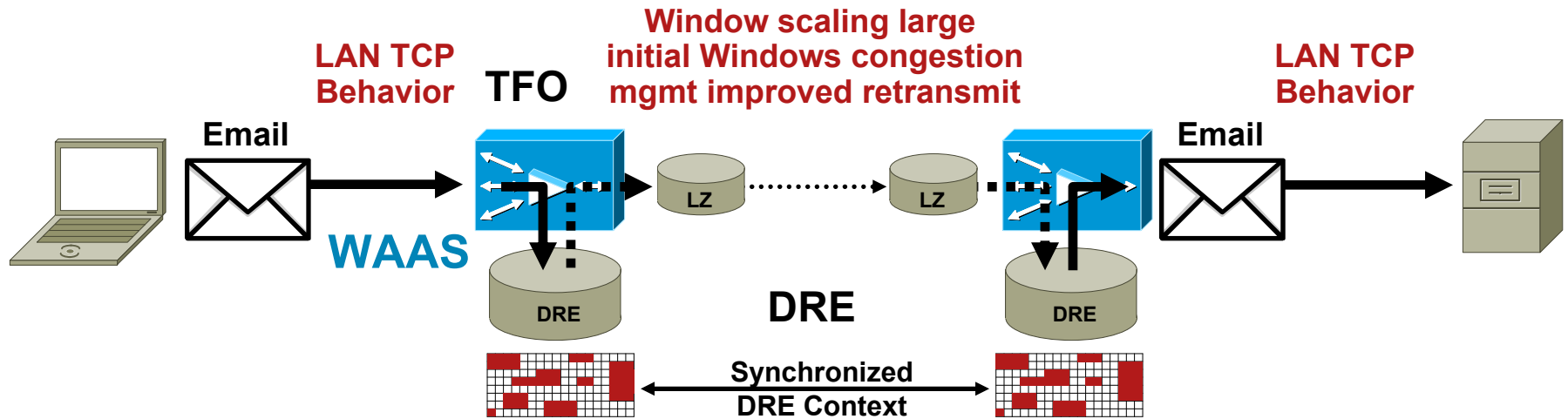
- L7 Optimization

    Application and protocol awareness

    WAASv4 application accelerators

    CIFS (Windows File Services) and Windows printing

    Intelligent server offload

- Advanced Compression

    Data redundancy elimination

    Persistent LZ compression

- TCP Optimization

Solution Components
Optimization

Component	Solution Function
WAAS	Application acceleration, advanced compression, and TCP optimization for WAN traffic
ACE	DC server load balancing and offload, application acceleration, with integrated security
PfR	Adaptive routing guided by application performance, for dynamic application path selection, network problem migration, and active load sharing

Available:
Key to Continuity

Available

Load Balancing Support
- SIP
- Extended RTSP
- Radius
- RDP
- Generic Protocol Parsing

Enhanced Predictors
- Adaptive algorithms
- Least loaded
- Least bandwidth

General SLB
- Kal-AP
- HTTP header rewrite
- Partial server farm failover
- Application-based probes
- SNMP-based probes
- UDP fast age

- **Application-Aware Load Balancing**

  Load balances the clients request to the best available application with an understanding of the application traffic

- **Application Awareness Predictor**

  The ACE queries and monitors application performance and critical resources before load balancing

- **Large Scale Load Balancing**

  Enables infrastructure scalability and resilience between multiple sites

Application-Aware Load Balancing

- ACE provides application-layer load balancing capabilities for the following protocols
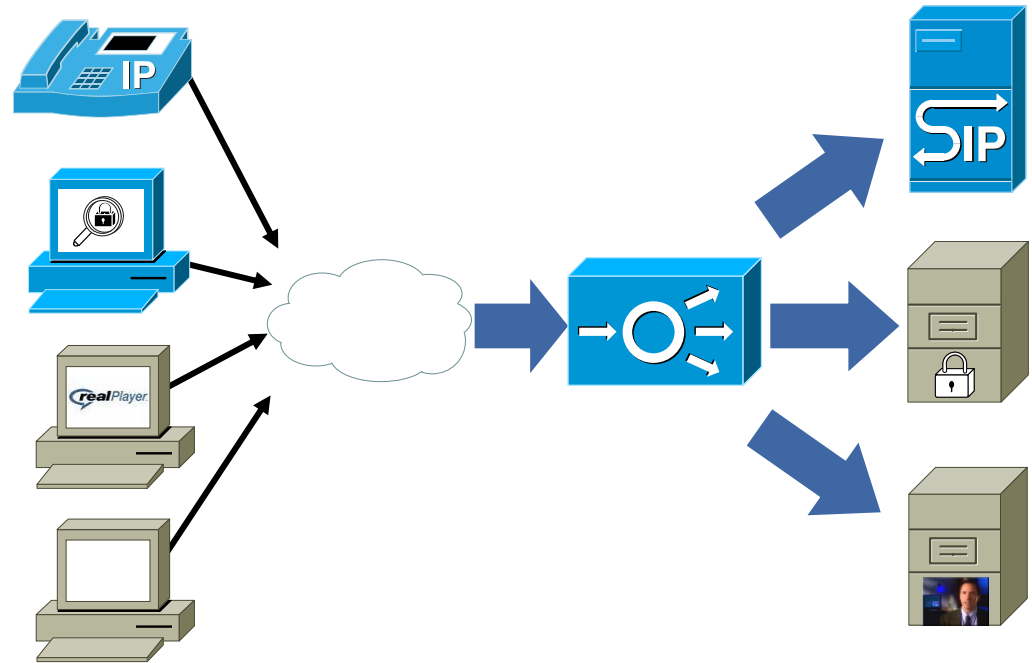
  SIP

  Extended RTSP

  Radius

  RDP

  Generic Protocol Parsing

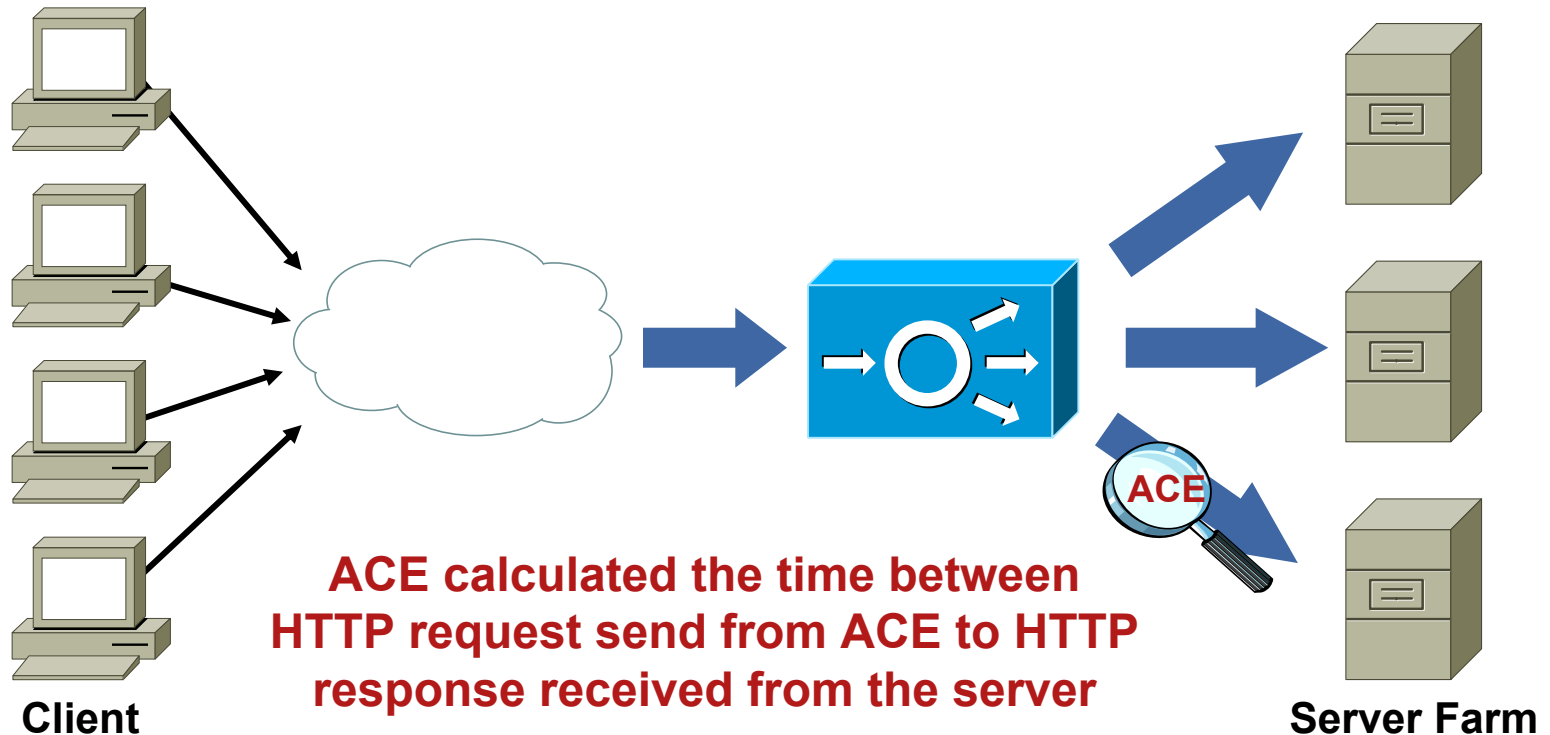 HTTP Content Load Balancing

- Health monitoring probes available for these protocols

Enhanced Predictors

Adaptive Response Predictor

- With Adaptive Response Predictor, server with the lowest average response time is preferred by ACE on new connections

ACE calculated the time between HTTP request send from ACE to HTTP response received from the server

Client

Server Farm

Solution Components
Optimization

Component	Solution Function
WAAS	Application acceleration, advanced compression, and TCP optimization for WAN traffic
ACE	DC server load balancing and offload, application acceleration, with integrated security
PfR	Adaptive routing guided by application performance, for dynamic application path selection, network problem migration, and active load sharing

What Is Cisco Performance Routing (PfR)?

- Performance-based adaptive routing

- Application best path selection
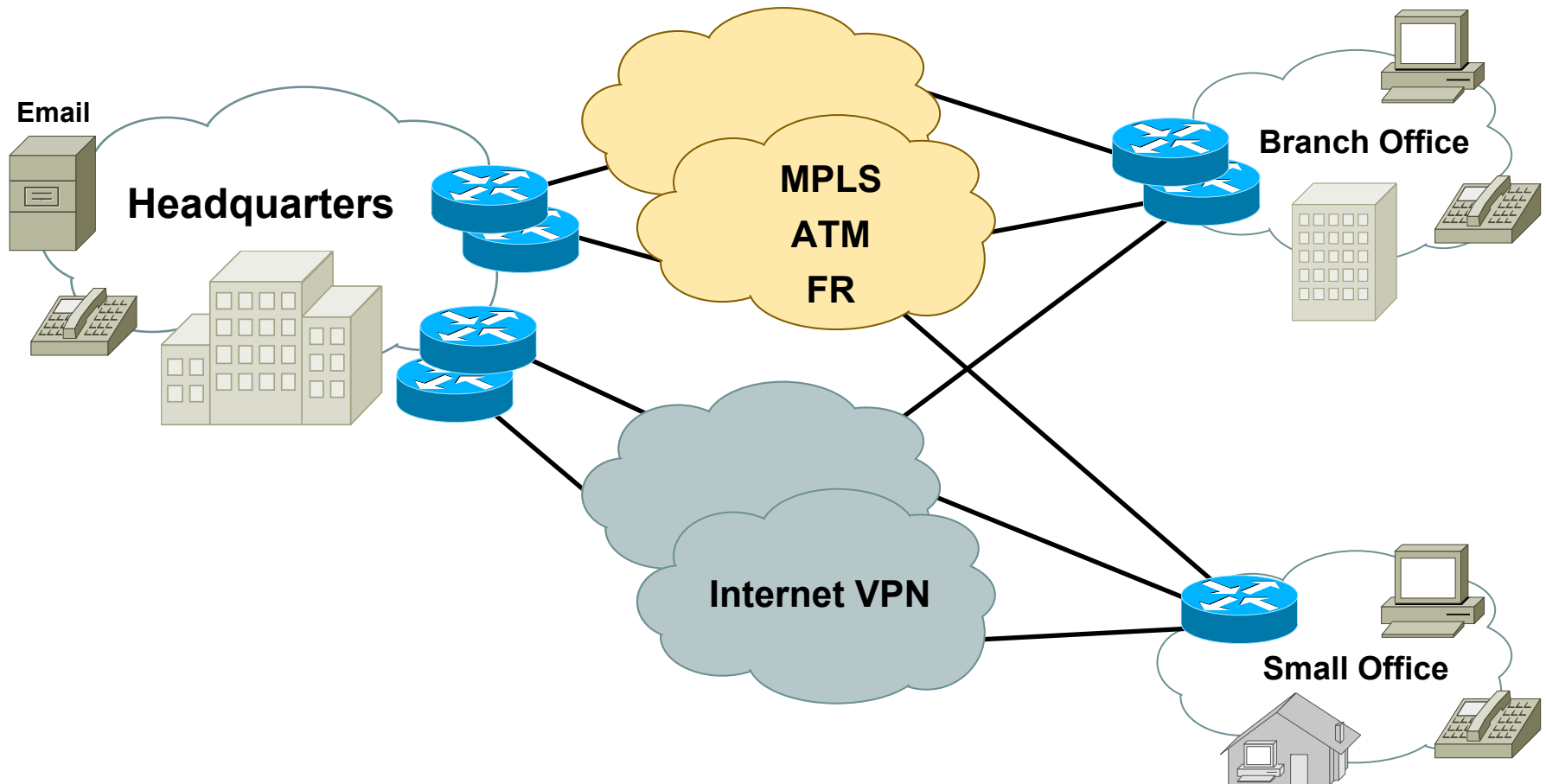
- Network problem mitigation

- Active load sharing

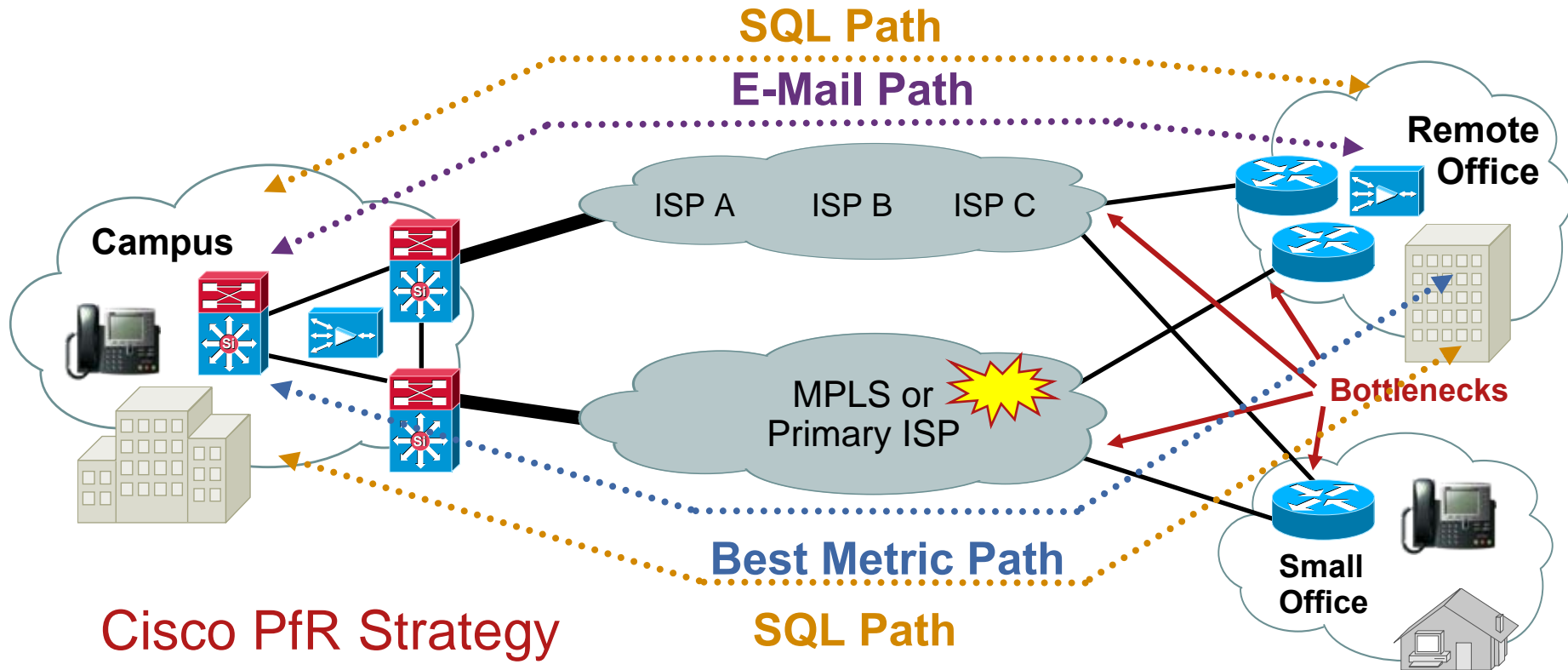# Enterprise WAN Challenge

**Two Paths
Two Providers** → **WAN Availability**

Email

Headquarters

MPLS
ATM
FR

Branch Office

Internet VPN

Small Office

Cisco Performance Routing Enterprise WAN

Optimize by:
reachability, delay, loss, jitter*,
MOS*, throughput, load, and cost

SQL Path

E-Mail Path

Remote Office

ISP A   ISP B   ISP C

Campus

Bottlenecks

MPLS or
Primary ISP

Best Metric Path

Small Office

Cisco PfR Strategy

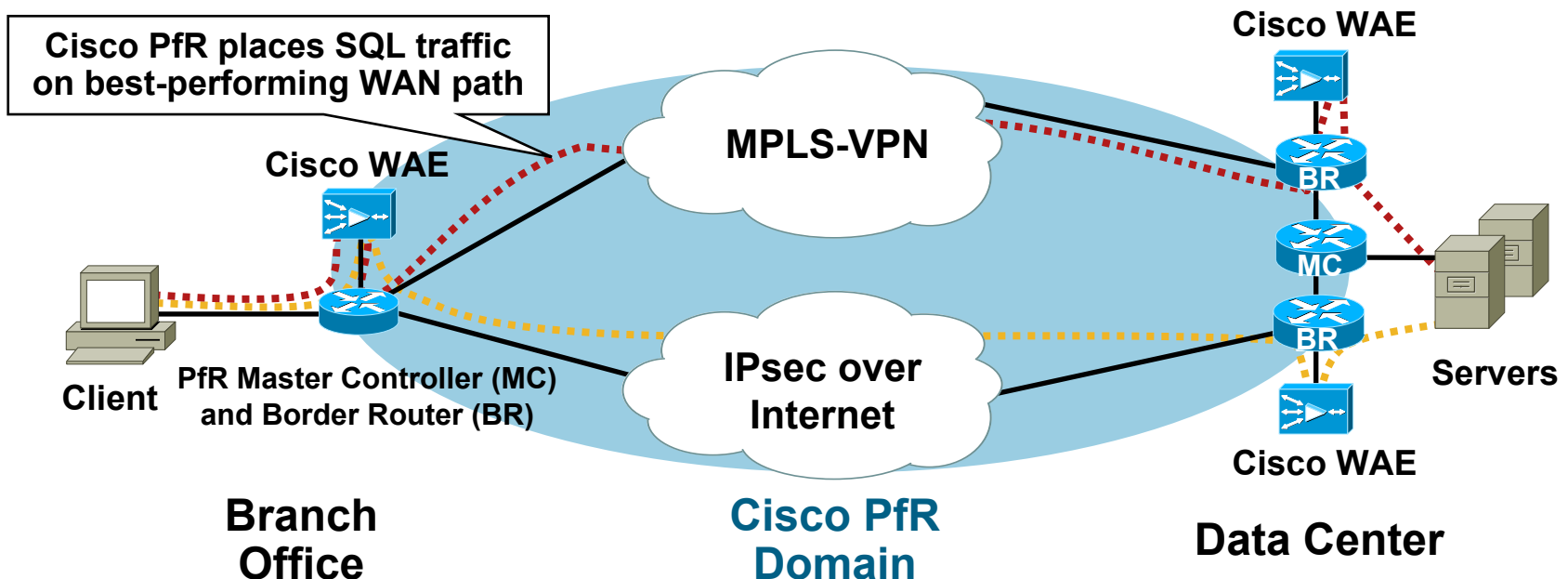**SQL Path**

- Best path based upon policy and real-time performance metrics
- Adaptive routing based upon application performance criteria
- Active load balancing to fully utilize all paths

Cisco PfR and Cisco WAAS Integration Adaptive WAN-Optimized Network

- Cisco Wide Area Application Services (WAAS) optimizes the TCP session

- Cisco PfR monitors and optimizes WAN path selection

- Cisco WAAS network transparency allows individualized session placement by Cisco PfR over best WAN path

Cisco PfR places SQL traffic on best-performing WAN path

Cisco WAE

Cisco WAE

MPLS-VPN

BR

MC

BR

IPsec over Internet

Servers

Cisco WAE

Client

PfR Master Controller (MC) and Border Router (BR)

Branch Office

Cisco PfR Domain

Data Center

Solution Components: Control

What is Quality of Service?

Two Perspectives

- ## The User Perspective

  Users perceive that their applications are performing properly

  Voice, video, and data

- ## The Network Manager Perspective

  Need to manage bandwidth allocations to deliver the desired application performance

  Control delay, jitter, and packet loss

Different Types of Traffic Have Different Needs

- **Real-time applications especially sensitive to QoS**
  - Interactive voice
  - Video conferencing
- **Causes of degraded performance**
  - Congestion losses
  - Variable queuing delays
- **The QoS challenge**

  Manage bandwidth allocations to deliver the desired application performance

  Control delay, jitter, and packet loss

Application Examples	Sensitivity to QoS Metrics		
	Delay	Jitter	Packet Loss
Interactive Voice and Video	Yes	Yes	Yes
Streaming Video	No	Yes	Yes
Transactional/ Interactive	Yes	No	Yes
Bulk Data, Email, File Transfer	No	No	No

Need to manage bandwidth allocations

Quality of Service Operations

How do QoS Tools Work?

Classification and Marking

Queuing and (Selective) Dropping

Post-Queuing Operations

Robust Cisco IOS QoS Behavioral Model

Match conditions keyword: class-map	Policy actions keyword: policy-map		
Classification	Pre-Queuing	Queuing and Scheduling	Post-Queuing
▪ Classify Traffic	▪ Immediate Actions	▪ Congestion Management and Avoidance	▪ Link Efficiency Mechanisms
Match one or more attributes (partial list—see notes): ▪ ACL list ▪ CoS ▪ DSCP ▪ Input-interface ▪ MAC address ▪ Packet length ▪ Precedence ▪ Protocol ▪ VLAN	▪ Mark (Set QoS values) ▪ Police ▪ Drop ▪ Count ▪ Estimate bandwidth	▪ Queue-limit ▪ Random-detect ▪ Bandwidth ▪ Fair-queue ▪ Priority ▪ Shape	▪ Compress header ▪ Fragment (Link fragmentation and interleaving, Layer 2)

Robust Cisco IOS QoS Behavioral Model (Cont.)

Match conditions keyword: class-map	Policy actions keyword: policy-map		
Classification	Pre-Queuing	Queuing and Scheduling	Post-Queuing
Most accelerators only provide a limited set of classification capabilities largely based on IP addresses and port numbers	Cisco IOS Software has extensive, integrated QoS capabilities to optimize delivery of voice, video and data traffic Support for many underlying network technologies ▪ Frame Relay, ATM, MPLS, SONET, and IP routed networks Most accelerators do not have the robust QoS feature set The Cisco QoS behavioral model is the conceptual framework underlying the Modular QoS CLI (MQC). The model and the MQC provide a way to implement QoS consistently on Cisco routers and switches, irrespective of the implementation details of those platforms; accelerators do not have the capability.		

Solution Components: Network Management

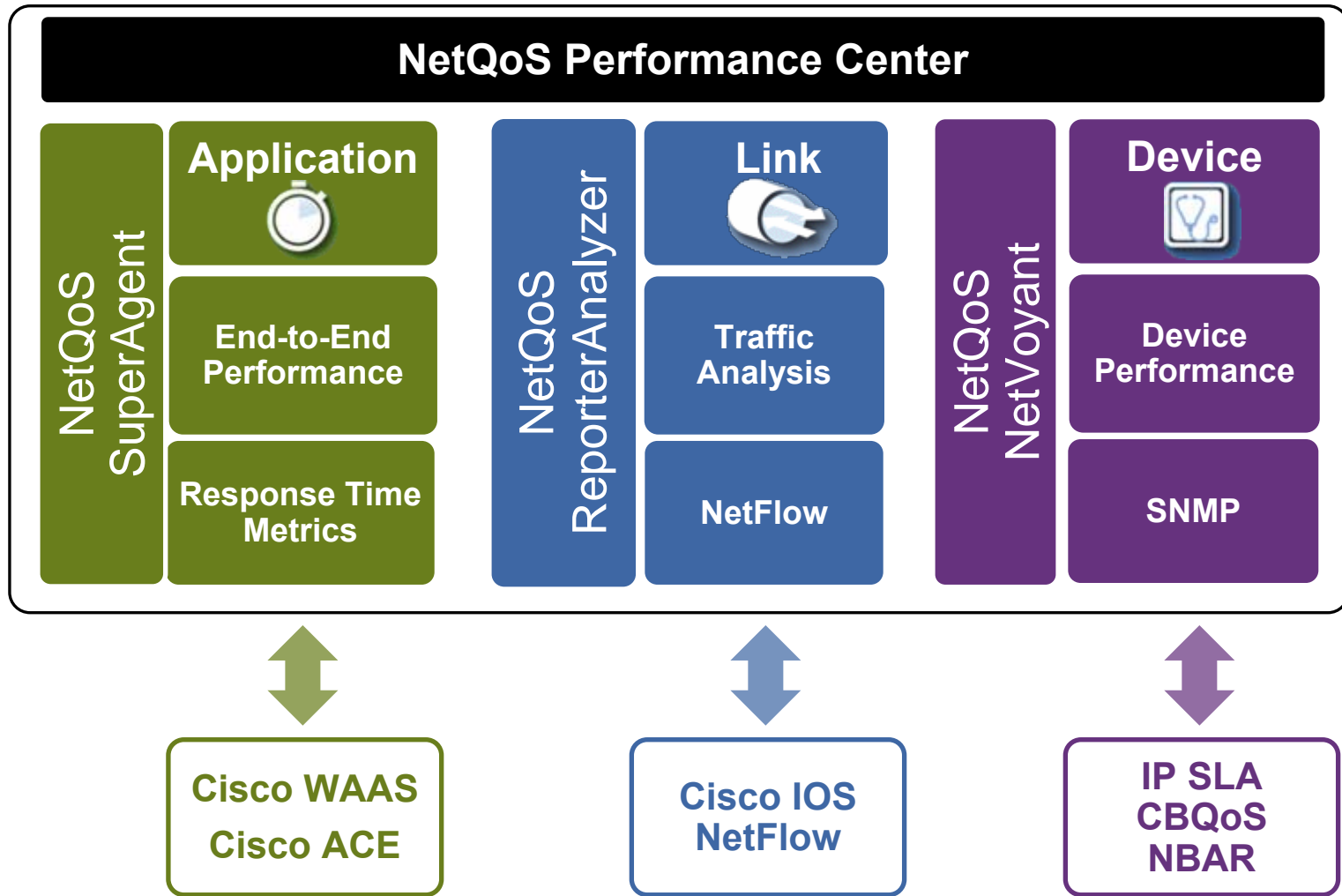# Solution Components

Network Management

Component	Solution Function
NetQoS Product Suite	Centralized monitoring of WAN and application traffic and its performance
NAM Management	Centralized, interactive troubleshooting and granular conversation analysis

Centralized Monitoring Reporting: NetQoS

NetQoS Performance Center

NetQoS SuperAgent		NetQoS ReporterAnalyzer		NetQoS NetVoyant	
	Application		**Link**		**Device**
	End-to-End Performance		**Traffic Analysis**		**Device Performance**
	Response Time Metrics		**NetFlow**		**SNMP**

| **Cisco WAAS Cisco ACE** | **Cisco IOS NetFlow** | **IP SLA CBQoS NBAR** |

One-source network performance management for Cisco infrastructure

NetQoS Complements Cisco Technologies

Cisco Technology	NetQoS Supporting Value	Customer Advantage
WAAS WAN Optimization **ACE Load Balancing**	- End-to-end performance monitoring - NetFlow traffic analysis - SNMP device performance monitoring	- Identify the best deployment candidates - Accurately size and configure each deployment - Maintain visibility for troubleshooting - Prove WAAS and ACE return on investment
Cisco IOS NetFlow	- NetFlow traffic analysis - Anomaly detection - Usage-based IT cost allocation	- Solve performance problems faster - Optimize the Cisco infrastructure for performance - Provide business insight to control IT costs
QoS	- End-to-end performance monitoring - NetFlow traffic analysis	- Eliminate unnecessary WAN costs - Optimize the Cisco infrastructure for performance - Prove QoS policy effectiveness
IP SLA, CBQoS, NBAR	- SNMP device performance monitoring	- Simplify management and reporting - Solve performance problems faster - Prove Cisco infrastructure performance - Provide business insight to control IT costs

Joint Solutions Provide Higher Value

Business Driver	Customer Initiative	NetQoS Supporting Technology	Customer Advantage
Data Center Consolidation	▪ WAN Optimization ▪ ACE Deployment	▪ End-to-end performance monitoring ▪ NetFlow traffic analysis ▪ SNMP device performance monitoring	▪ Accurately size and configure each deployment ▪ Prove the ROI of WAAS and ACE ▪ Maintain visibility for troubleshooting
Router as Integrated Service Platform	▪ NetFlow ▪ IP SLA ▪ QoS ▪ CBQoS ▪ NBAR	▪ NetFlow traffic analysis ▪ SNMP device performance monitoring ▪ End-to-end performance monitoring ▪ Usage-based IT cost allocation ▪ Anomaly detection	▪ Fully leverage the economy, scalability of Cisco-embedded technologies ▪ Simplify management and reporting ▪ Provide business insight to control IT costs

Solution Components

Network Management

Component	Solution Function
NetQoS Product Suite	Centralized monitoring of WAN and application traffic and its performance
NAM Management	Centralized, interactive troubleshooting and granular conversation analysis

Cisco NAM: Granular Troubleshooting and Conversation Analysis

- **Real-time visibility for troubleshooting**

  Apply filters in real-time—no need to pre-configure data-sources, servers, and applications

- **Granular traffic and performance views**

  Drill-down to individual conversations, with data points collected over short intervals

  Short- and long-term traffic and performance reports on specific conversations and hosts, to avoid masking conversation behavior by aggregation
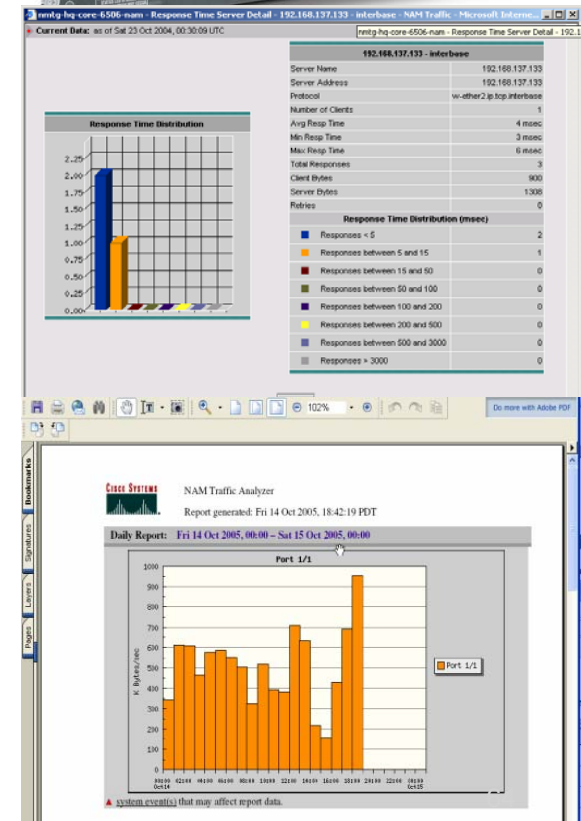
- **Performance analytics**

  TCP application response time metrics, DiffServ QoS, as well as voice and video metrics

- **Packet capture for post-event analysis**

  User-defined threshold-based packet capture, filters and decodes
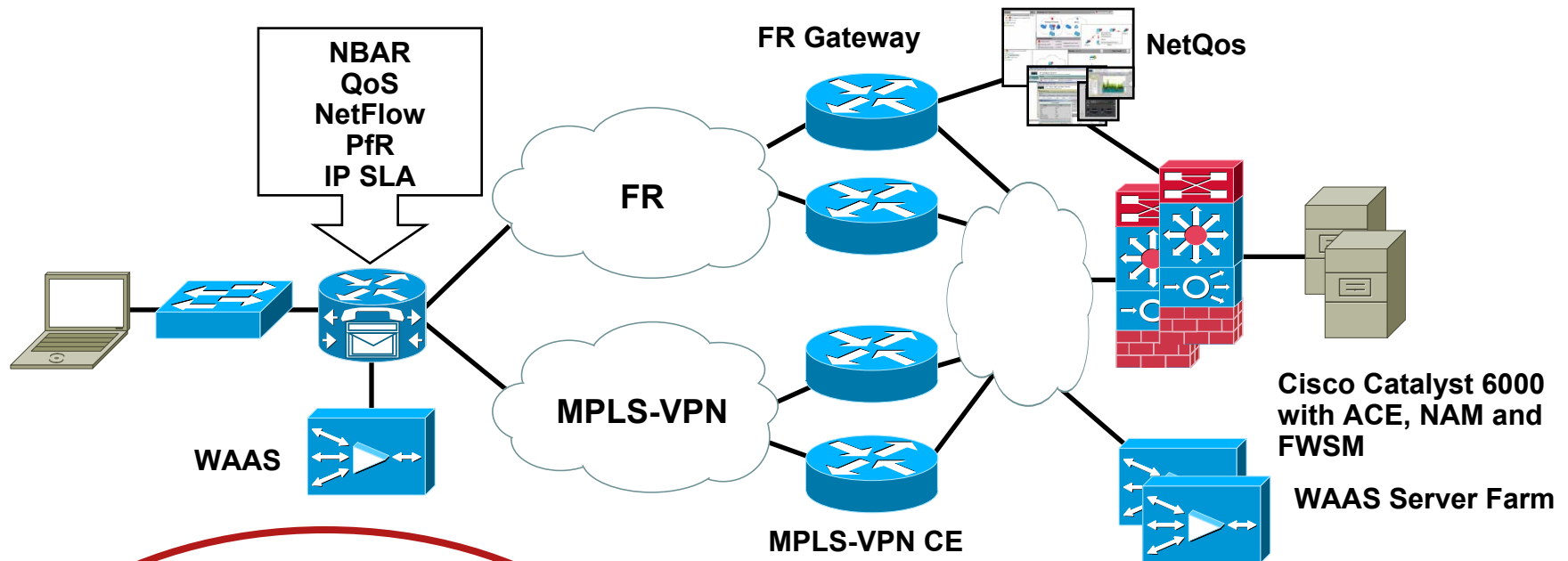
- **Remote NetFlow processing**

  Remote NetFlow processing to support determination of conversation paths

Putting It All Together: Branch Deployment

WAN and Application Optimization Use Case

NBAR
QoS
NetFlow
PfR
IP SLA

FR Gateway

NetQos

FR

WAAS

MPLS-VPN

MPLS-VPN CE

Cisco Catalyst 6000 with ACE, NAM and FWSM

WAAS Server Farm

Branch

- WAAS to optimize TCP based traffic
- NBAR to enable protocol discovery
- QoS to prioritize business critical traffic
- PfR to place traffic on best performing WAN path based upon application criteria
- NetFlow and IP SLA to monitor traffic

Data Center

- WCCP to load balance the WAAS server farm
- ACE to load balance the application server farm
- PfR to place traffic on best performing WAN path based upon application criteria
- Firewall (FWSM) deployed in the data center
- NAM for granular troubleshooting
- NetQoS for centralized monitoring and reporting

Packet Flow

Branch View

FR

ISR

NBAR+QoS

WCCP

PfR

QoS

LAN

Based on DSCP setting the SP will act on the SLA

NBAR uses deep packet inspection to identify the application

Modifies DSCP (TOS Byte) to Application ID

QoS can selectively rate-limit or drop undesirable traffic

MPLS-WAN

Packet Flow

Branch View

LAN

NBAR+QoS

WCCP

ISR

PfR

QoS

FR

MPLS-WAN

WCCP redirects packet to WAAS WAE device

Packet Flow

Branch View

FR

LAN

NBAR+QoS

WCCP

IP TCP payload

ISR

PfR

QoS

Note: NBAR should be configured on the LAN link to perform input classification before the traffic Is redirected to WAE

WAE compresses payload and preserves the DSCP information

pl$9ad

MPLS-WAN

Packet Flow

Branch View

FR

MPLS-WAN

LAN

NBAR+QoS

WCCP

PfR

QoS

ISR

Note: Effectively use DSCP to 'glue' the egress functions like PfR and QoS

PfR has been monitoring/polling multiple paths

PfR uses DSCP to identify the application, then maps packet to best path for optimization

IP TCP pl$9ad

Packet Flow

Branch View

FR

MPLS-WAN

NBAR+QoS

WCCP

PfR

QoS

IP

TCP

pl$9ad

LAN

ISR

QoS on egress
interface does final
control
on packet

Header
compression, LFI,
delay, etc. applied

Packet Flow

Branch View

FR

LAN

NBAR+QoS

WCCP

PfR

QoS

IP TCP pl$9ad

ISR

PfR determines that the MPLS-WAN is the appropriate route

MPLS-WAN

Packet Flow
Branch View

FR

LAN

NBAR+QoS

WCCP

PfR

QoS

ISR

IP TCP pl$9ad

PfR moves traffic to alternate

Excessive Loss

MPLS-WAN

Putting it
All Together:
Data Center
Deployment

WAN and Application Optimization Use Case
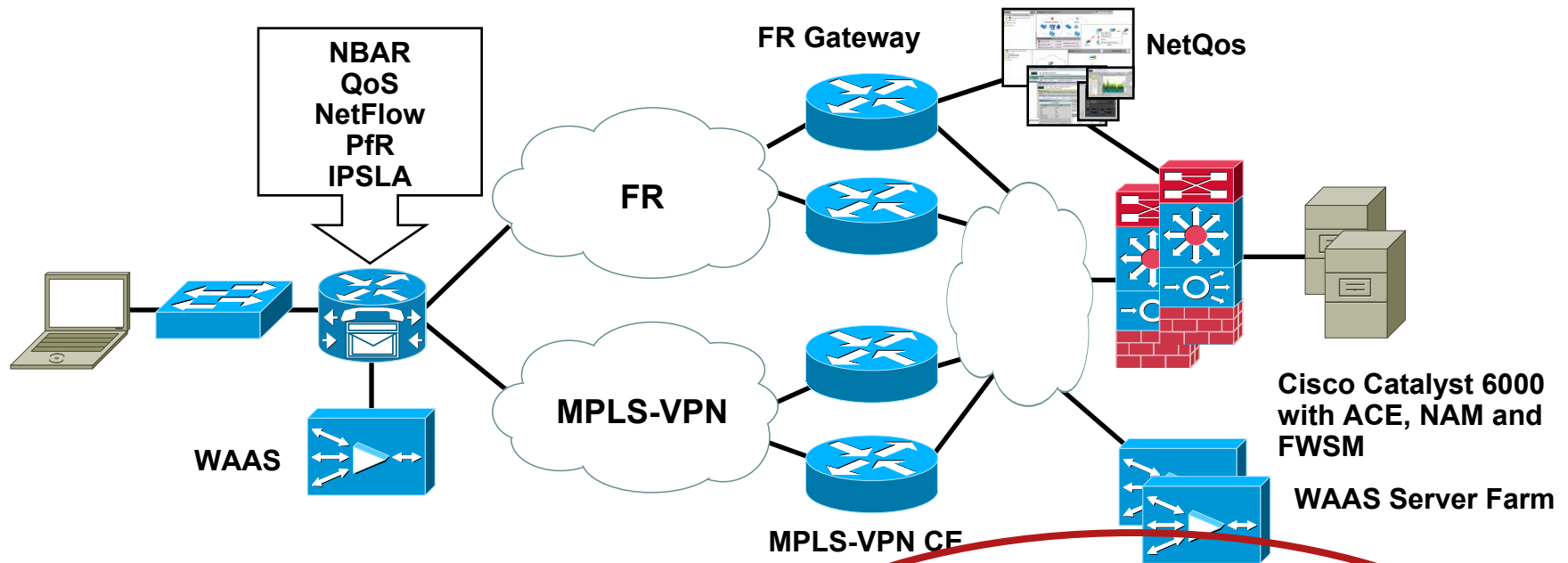
NBAR
QoS
NetFlow
PfR
IPSLA

FR Gateway

NetQos

FR

MPLS-VPN

WAAS

MPLS-VPN CE

Cisco Catalyst 6000 with ACE, NAM and FWSM

WAAS Server Farm

Branch

- WAAS to optimize TCP based traffic
- NBAR to enable protocol discovery
- QoS to prioritize business critical traffic
- PfR to place traffic on FR or MPLS-VPN path depending on corporate policies
- NetFlow and IPSLA to monitor traffic

Data Center

- WCCP to load balance the WAAS server farm
- ACE to load balance the application server farm
- Firewall (FWSM) deployed in the data center
- NAM for granular troubleshooting
- NetQoS for centralized monitoring and reporting

Data Center: WAAS at WAN Edge

Logical View

WCCP redirects packet to WAAS WAE device

Packets pass through to server farm load balanced by ACE

Packets are mirrored to NAM/NetQOS for monitoring

WAN Edge Router

Distribution Switch

Server Farm

WCCP

Firewall

ACE

SPAN/ VACL

Packets inspected by Firewall

NetQoS SuperAgent Collector

WAE

NAM Analyzer
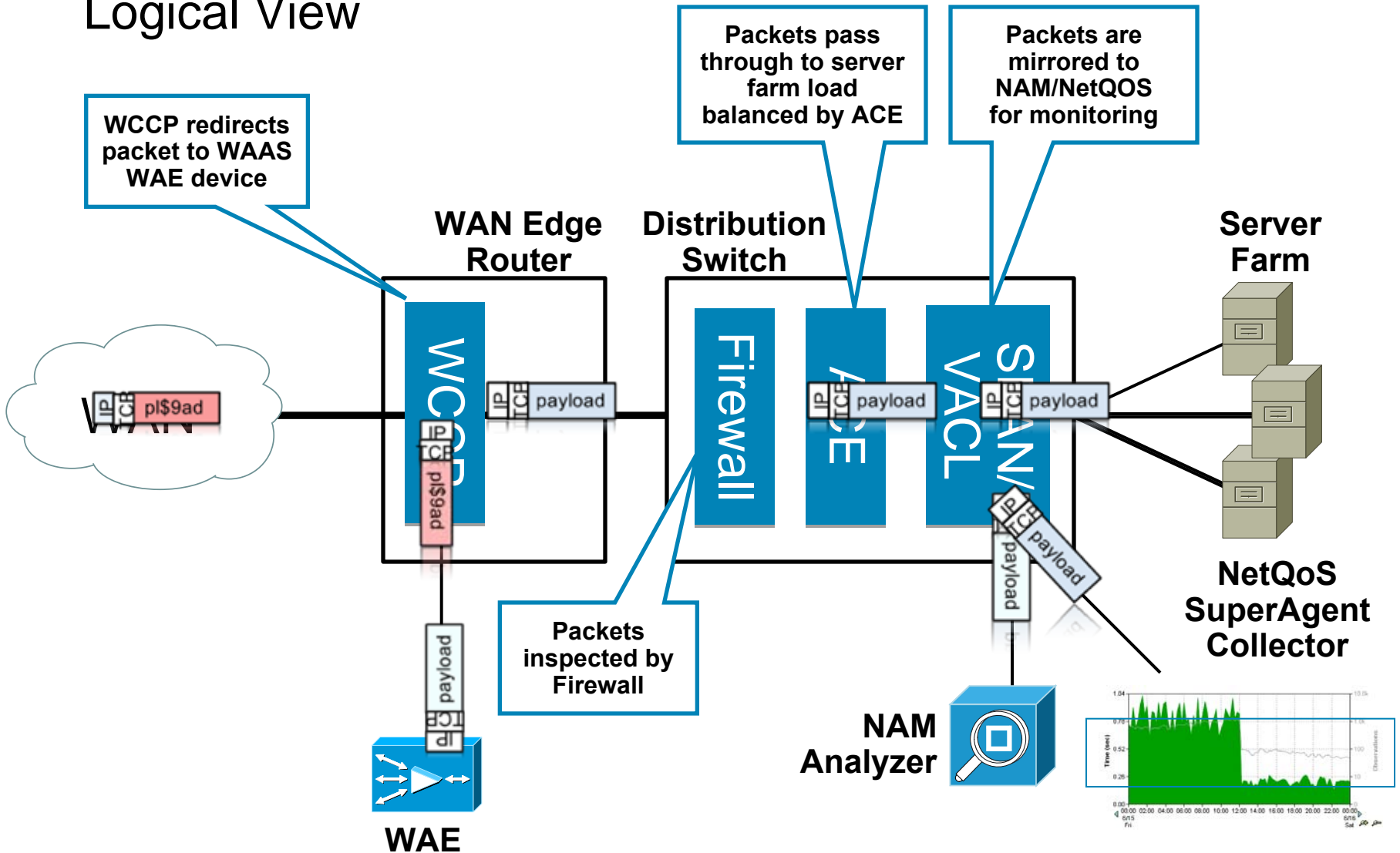
Data Center: WAAS at Distribution Layer

Logical View

WCCP redirects packet to WAAS WAE device

Packets pass through to server farm load balanced by ACE

Packets are mirrored to NAM/NetQOS for monitoring

Distribution Switch

Server Farm

WAN Edge Router

Firewall

WCCP

ACE

SPAN/VACL

WAAS optimized packets inspected by Firewall

NetQoS SuperAgent Collector

NAM Analyzer

WAE
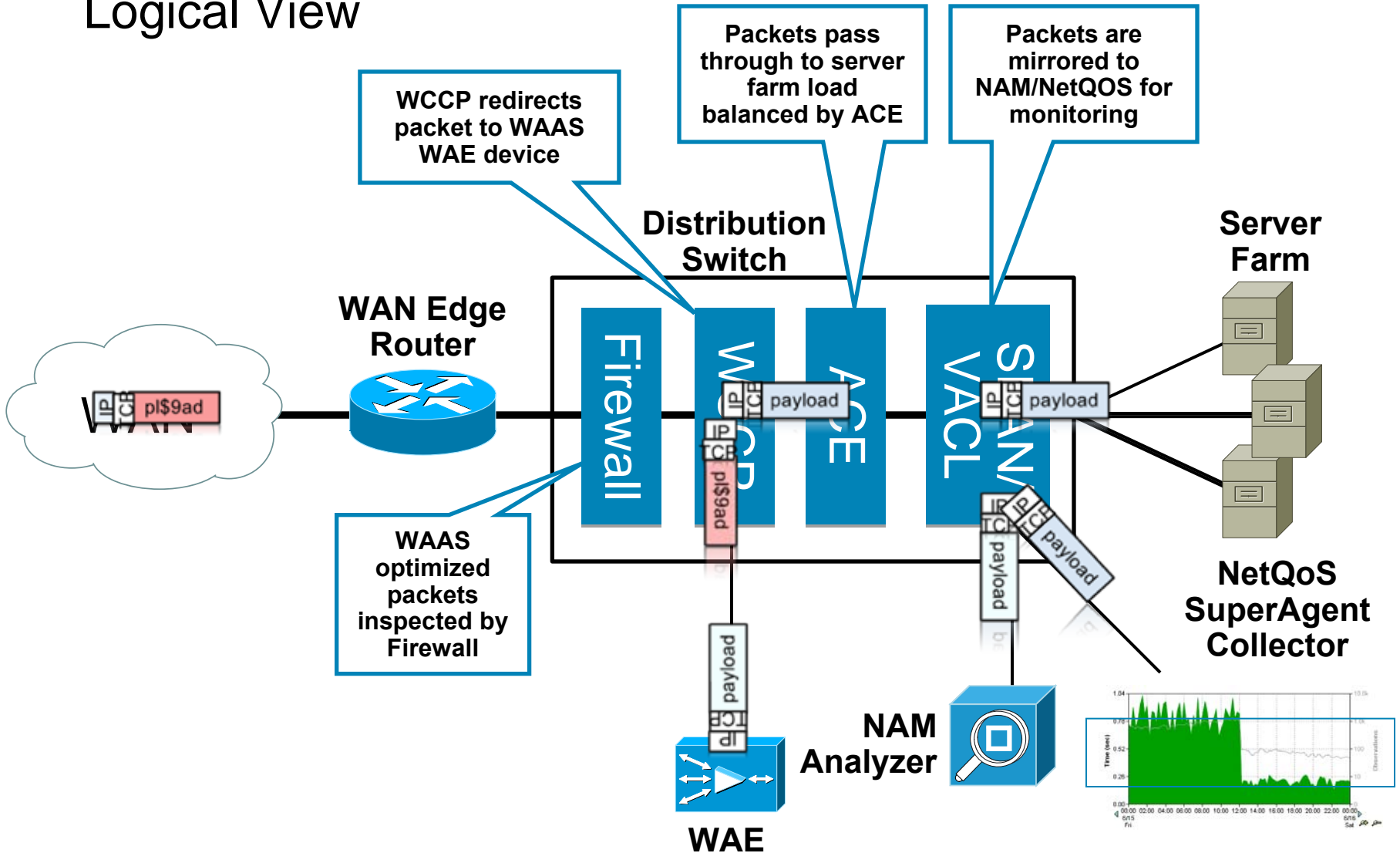
Data Center:
ACE to Load Balance WAAS

Server Farm Logical View

WAAS optimized packets inspected by Firewall

ACE to load balance between WAE farm and server farm

Packets are mirrored to NAM/NetQOS for monitoring

Distribution Switch

Server Farm

WAN Edge Router

Firewall

ACE

SPAN/VACL

payload

payload

WAN

pl$9ad

pl$9ad

payload

payload

payload

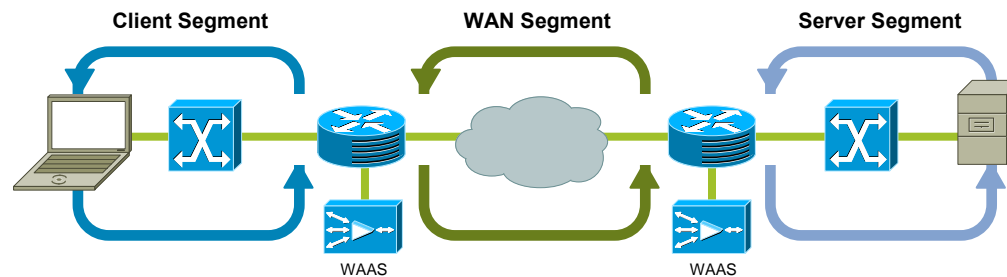NetQoS SuperAgent Collector

WAE

NAM Analyzer
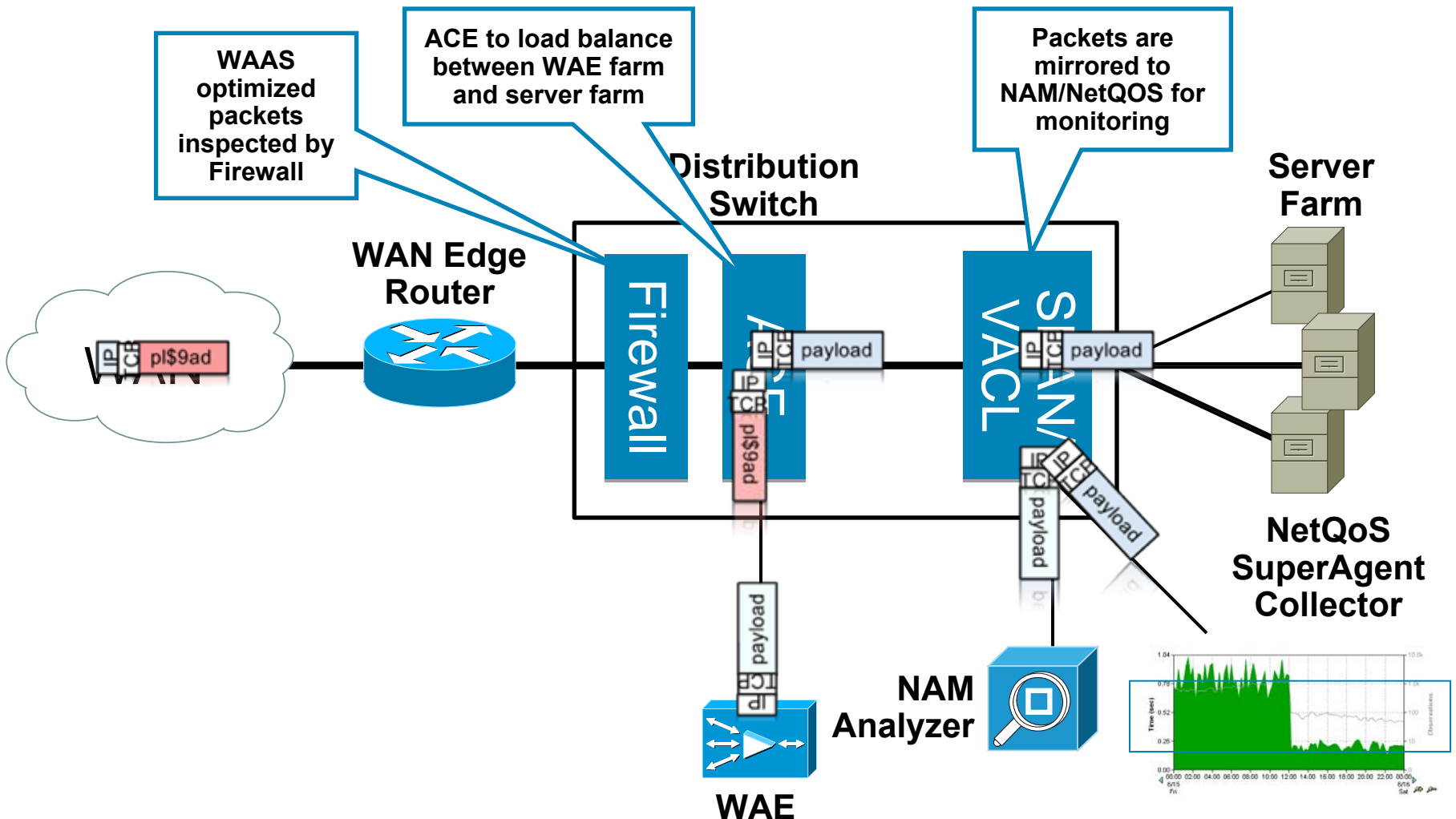
Network Management

Network Management Segment Visibility

- WAN Optimization breaks the TCP session between client and server into three segments, each with different transactions

Client Segment   **WAN Segment**   **Server Segment**

WAAS   WAAS

- NetQoS Recommendations

    Server segment

        SPAN/VACL at Data Center (DC) distribution switch to NetQoS SuperAgent Collector

    Client and WAN segment

        WAAS Flow Agent exports to NetQoS SuperAgent
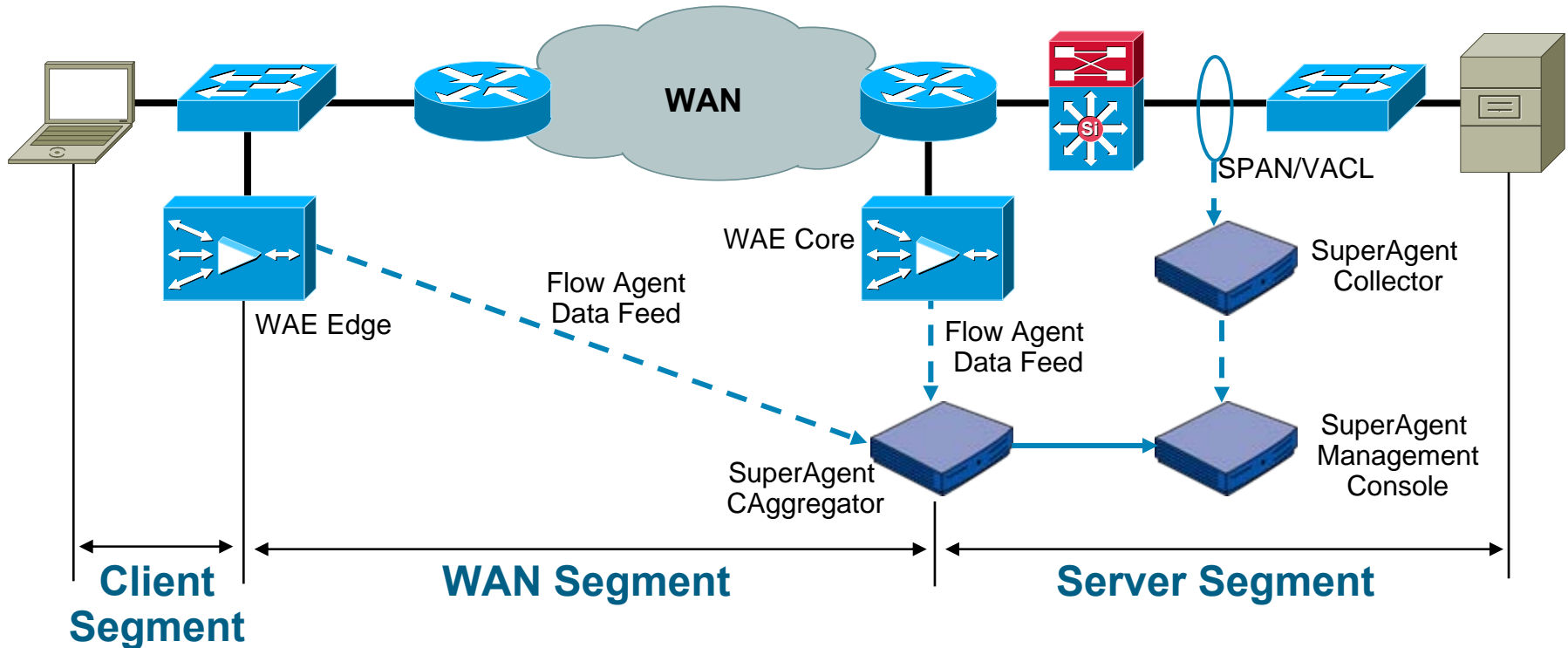
- NAM Recommendations

    Server segment

        SPAN/VACL at DC distribution switch to NAM

    WAN segment

        NetFlow export to NAM

- Target interesting traffic only for scalability (NAM + NetQoS)
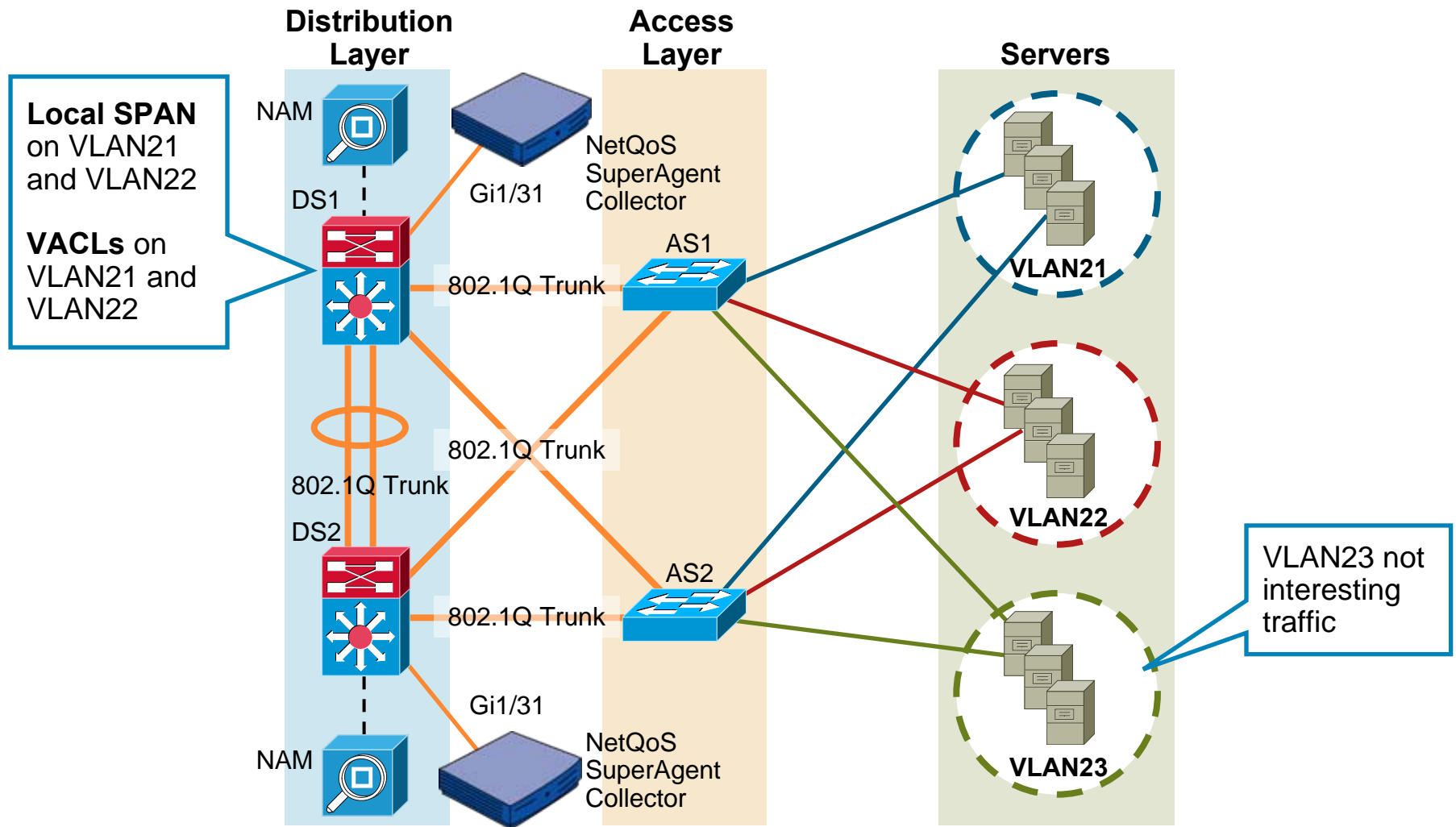
NetQoS SuperAgent Collection Overview

- Cisco WAE flow agent to collect metrics on client and WAN segments
- SuperAgent Collector for server response time metrics (as supposed to metrics collected by the core WAAS agent)

  SPAN/VACL allows you to captures traffic that is not seen by WAAS

  Typically, SuperAgent Collector is placed close to the server, hence more accurate server metrics
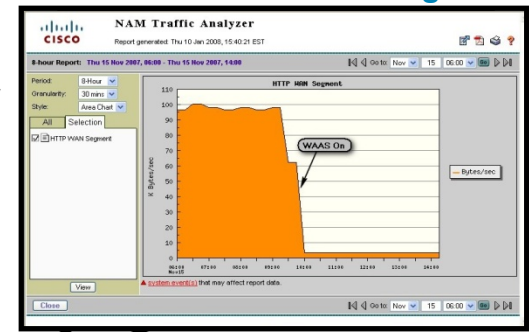
NetQoS SuperAgent and NAM Server Segment Deployment

Distribution Layer

Access Layer

Servers

NAM

Local SPAN on VLAN21 and VLAN22

VACLs on VLAN21 and VLAN22

DS1

Gi1/31

NetQoS SuperAgent Collector

AS1

802.1Q Trunk

VLAN21

802.1Q Trunk

802.1Q Trunk

DS2

AS2

802.1Q Trunk

VLAN22

VLAN23 not interesting traffic

Gi1/31

NAM

NetQoS SuperAgent Collector

VLAN23

- Single SPAN session with multiple destinations (NAM + NetQoS)

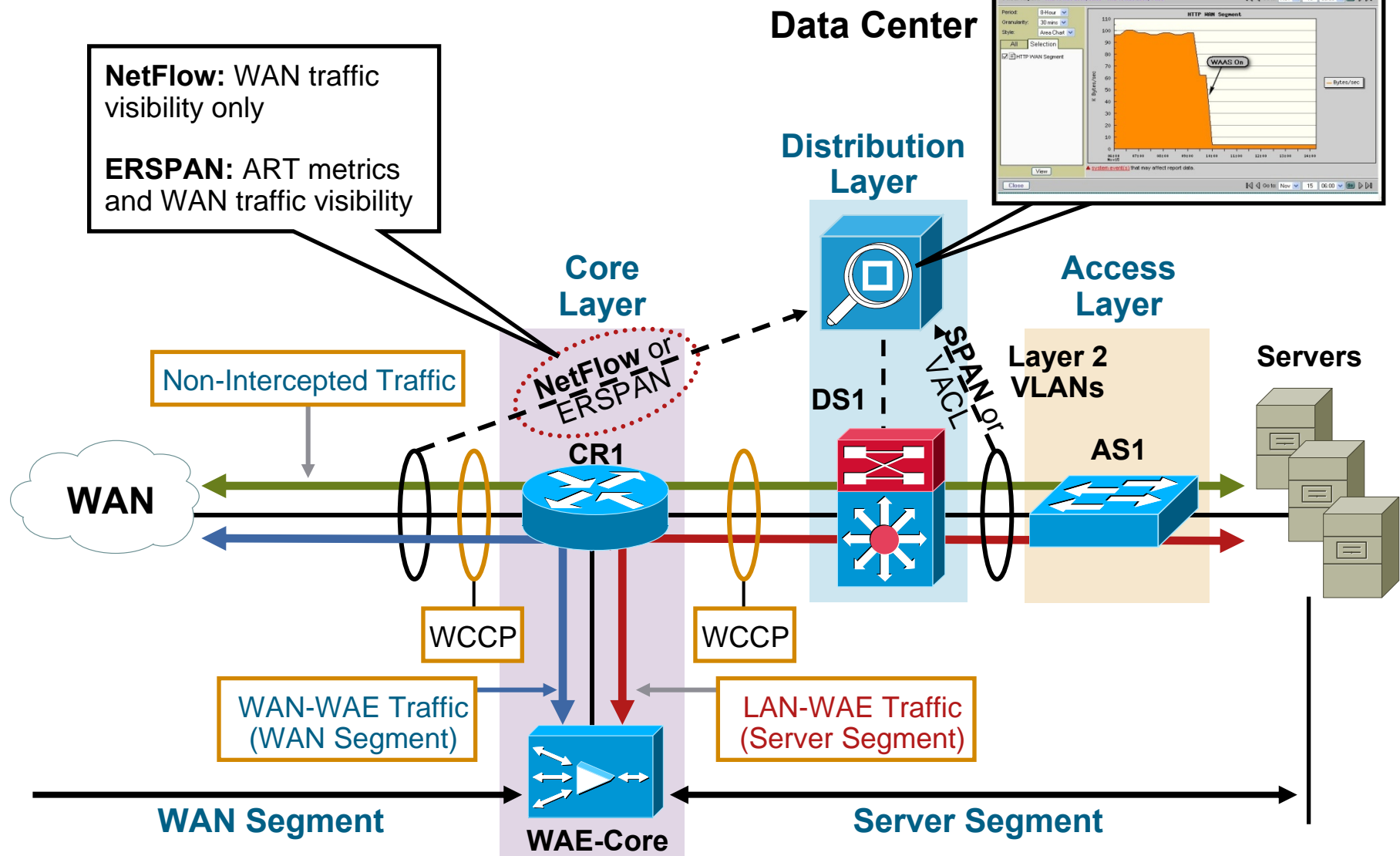- For granular traffic analysis, use VACLs as a flexible alternative (NAM + NetQoS)

NAM: Traffic Volume on WAN Segment

Traffic Volume on WAN Segment

Data Center

NetFlow: WAN traffic visibility only

ERSPAN: ART metrics and WAN traffic visibility

Distribution Layer

Core Layer

Access Layer

NetFlow or **ERSPAN**

Non-Intercepted Traffic

WAN

CR1

DS1

SPAN or **VACL**

Layer 2 VLANs

Servers

AS1

WCCP

WCCP

WAN-WAE Traffic (WAN Segment)

LAN-WAE Traffic (Server Segment)

WAN Segment

WAE-Core

Server Segment

Best Practices

Application Optimization Best Practice

Profile and Baseline

- **Profile:** Understand the traffic patterns and resource bottlenecks, enabling the user to prioritize links and protocols to be optimized

- **Baseline:** Establish baseline performance metrics for applications and resources (links, servers, etc.)
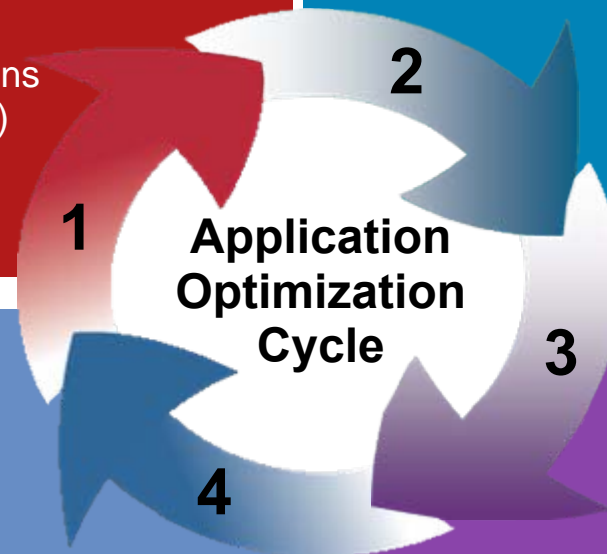
Optimize

- Apply targeted optimization features to meet performance objectives

    Application/protocol optimization

    Bandwidth optimization (compression, caching, etc.)

    Path optimization

    Congestion management and avoidance (QoS)

Evolve

- **Applications:** Roll out new applications and services

- **Users:** Add new users

- **Topology:** Add/remove

    Sites and subnets

    Links
    Equipment

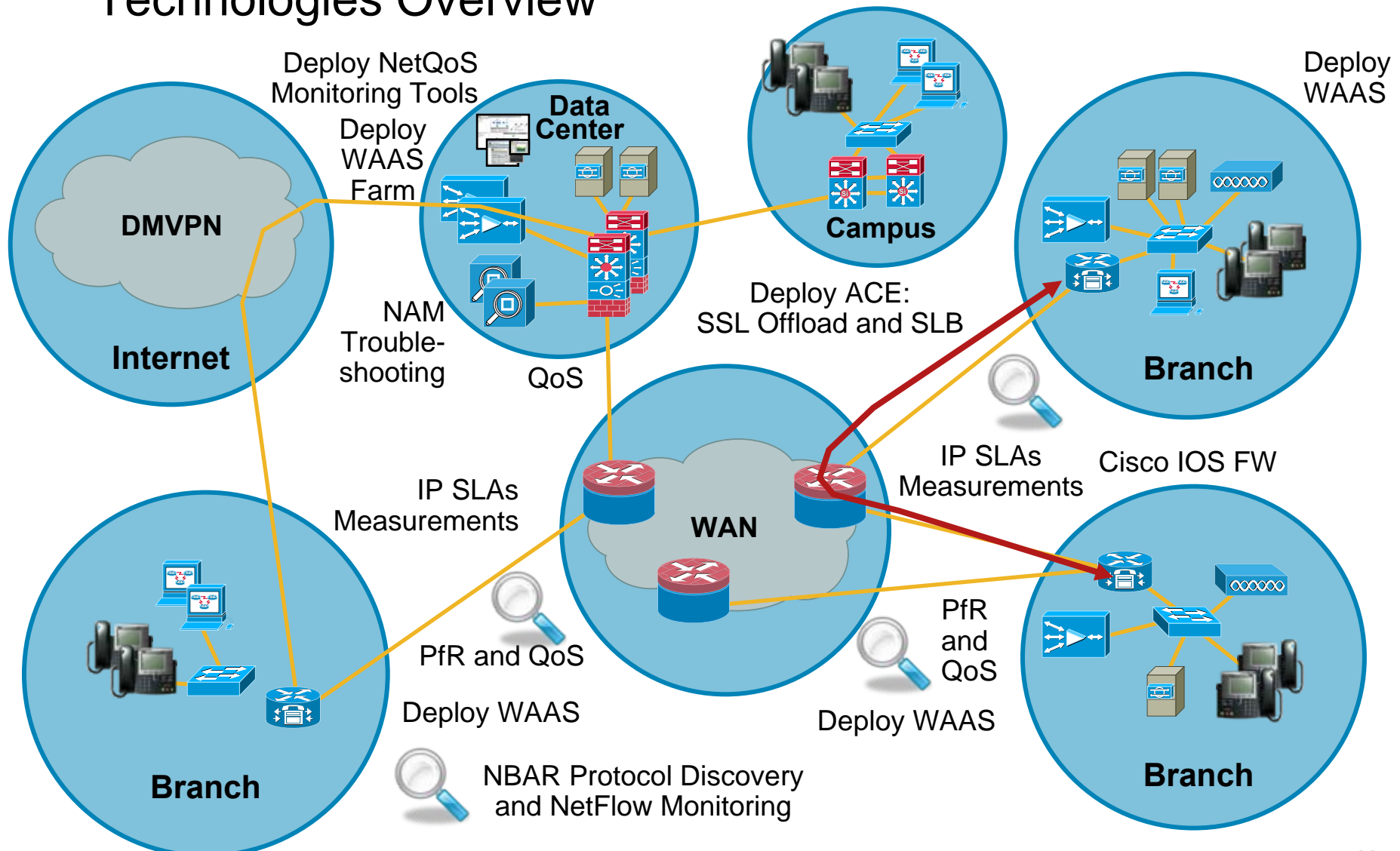**Application Optimization Cycle**

1 2 3 4

Operate

- **Assess:** Quantify effectiveness of optimization techniques

- **Tune:** Fine-tune the network and optimization parameters

- **Troubleshoot:** Investigate and address user performance problems

WAN and Application Optimization

Technologies Overview

Deploy NetQoS Monitoring Tools

Deploy WAAS Farm

Deploy WAAS

Data Center

DMVPN

Internet

NAM Trouble-shooting

QoS

Campus

Deploy ACE: SSL Offload and SLB

Branch

IP SLAs Measurements

Cisco IOS FW

WAN

IP SLAs Measurements

PfR and QoS

PfR and QoS

Branch

Deploy WAAS

Deploy WAAS

NBAR Protocol Discovery and NetFlow Monitoring

Branch
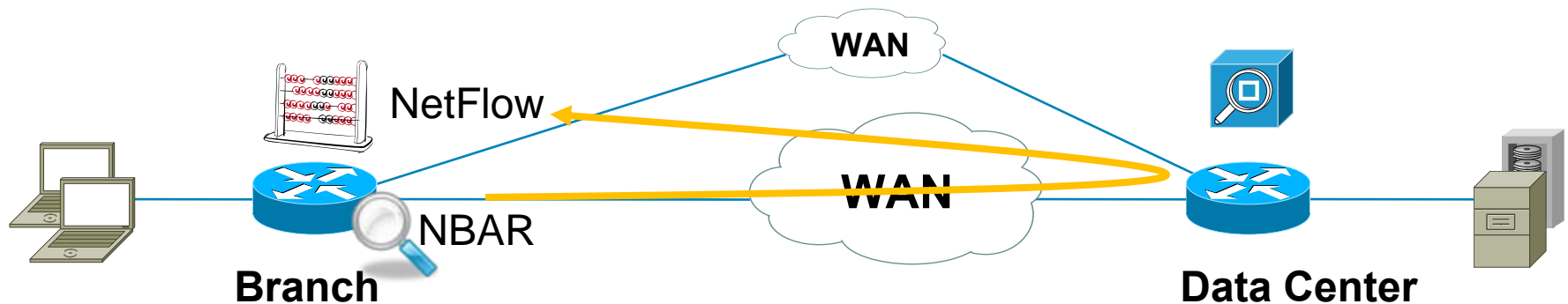
Profile and Baseline

Measure What You Can Improve

- NetFlow for accounting traffic: rate of traffic, link utilization, who is talking to who, capacity planning

- NBAR protocol discovery for identifying additional protocols

- IP SLA for measuring path characteristics

- PfR in learn mode for automating multi-path baselining

- NAM and NetQoS to measure response times

- WAAS Flow-Agent to measure optimized traffic times

NetFlow

NBAR

Branch

WAN

WAN

Data Center

Profile and Baseline

- Use **NetQoS** to gather the historical traffic and measured performance data, and to profile and baseline the network and applications

- Talk with server/applications maintainers to understand pain-points and SLA requirements of applications

    Bandwidth needed, delay thresholds, uptime, etc.

Optimize

- Map objectives to **QoS** policies

  Map voice traffic to priority queue

  Critical business traffic to dedicated bandwidth

  Scavenger traffic restricted and controlled

  AutoQoS can recommend initial policy, adjust to meet needs

- Apply **WAAS** to significantly accelerate response times, while significantly improving throughput

- Apply **ACE** for improved data center server performance

- Apply **PfR** to optimize applications over WAN and track WAN performance

- Internet-based **DMVPN** may provide alternate paths for non-critical traffic

Operate

- Assess

  Use **NetQoS** baselining and historic reporting to assess the overall performance of the newly optimized traffic

- Tune

  Use **NetQoS** to identify opportunities for tuning the optimization

- Troubleshoot

  Use **NAM** to isolate individual customer performance problems, and to carry out detailed investigations using its granular and interactive conversation analysis capability

Evolve

- After the profiling, baselining, optimization, assessment and tuning, the network now works well for the current applications and topology

- Incrementally deploy new applications, new sites, and implement necessary topology changes

- Iterate the Application Optimization Best Practice cycle

Summary

Business Ready Architectures Enable Optimal Application Performance

Tight integration of WAN optimization devices and Cisco infrastructure enable all components to work together as an effective system

Cisco Advantages

- Superior breadth and depth of tools and techniques working together
- Cooperation with security components to protect your business against disruption
- The systems approach provides integration resulting in substantial savings
- Deliver a credible and simple management solution

Comprehensive suite of products and technologies to improve the reliability, performance and delivery of applications securely

Deliver Business Advantage

- **Systems Approach:** Uses the network to

  Baseline application traffic

  Gain end-to-end visibility

  Optimize applications

  Control and protect business critical traffic

- **Integrated Solution:** Integrating services to ensure secure and reliable end-to-end networks

- **Ready for New Applications:** Provides an architectural framework to meet changing business needs

- **Sustainable and Adaptable:** Supports business growth and agility

- **Verified Detailed Design Guidance:** Facilitates more reliable and predictable customer deployments

Additional Resources

- For more information

  http://www.cisco.com/go/wanopt

  http://www.cisco.com/go/datacenter

  http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html

- Contact/mailing alias

  info-wanopt@cisco.com