



IP/VPN

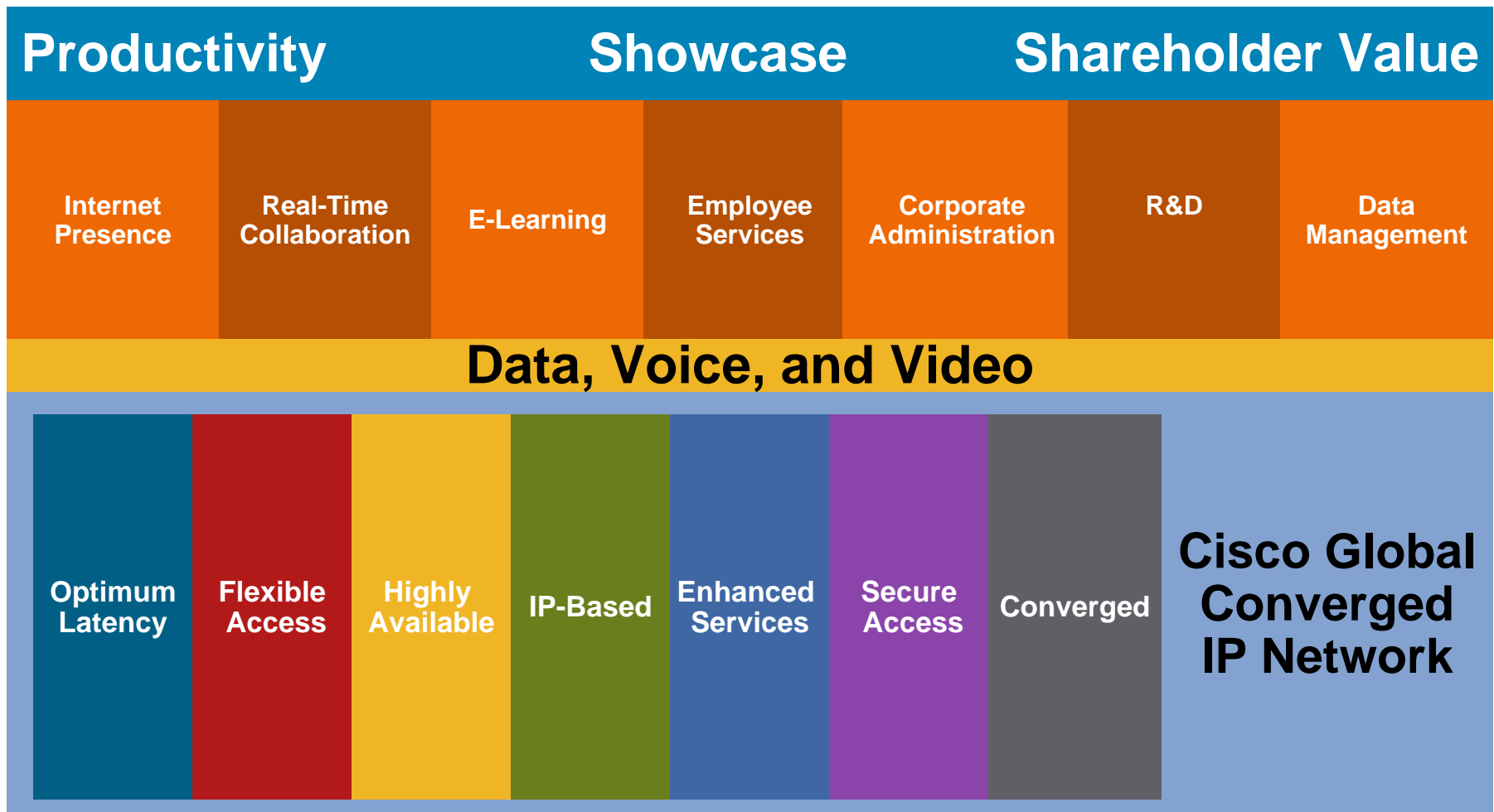
Cisco on Cisco Technology Tutorial



Dipesh Patel

IT Engineer, Cisco IT

Cisco's Intelligent Network Infrastructure Delivering Value Through the Network



Cisco's Intelligent Network Infrastructure

Direction: Leverage Enterprise Class IP/VPN

- **Transport benefits: effectively out-tasks the core**

Provides virtual “any-to-any”—optimal latency support for real-time applications (collaboration, video, telephony)

Easy to implement and support, leverages core SP engineering activity - no need to engineer a mesh of interconnection links between sites

Reduces bandwidth management efforts from a link-by-link basis to site-by-site



Established
2001

Cisco's Intelligent Network Infrastructure

Direction: Leverage Enterprise Class IP/VPN (Contd..)



Established
2001

- **In-cloud services**

Access to other services—services that can be leveraged in the 'cloud' via IP without extra facilities (VoIP PSTN, hosted telephony, Internet connectivity, etc.)

- **Key service requirements**

Must be a “drop-in replacement” for existing L1/L2 WAN networks, including support for routing protocols, multicast, QoS transparency

Sufficient footprint to take advantage of any-to-any topology

Cisco's Intelligent Network Infrastructure

Direction: Leverage Enterprise Class IP/VPN

- **Support for enhanced IP services**

 - Transparency for QoS markings

 - Native support for Multicast

- **Flexible access**

 - Network view is same from all points

- **Network Management**

 - Routing simplified / non-hierarchical

 - SP has Layer 3 reachability thus can take on more network operational tasks

Cisco's Intelligent Network Infrastructure

Direction: Leverage Enterprise Class IP/VPN (Contd..)

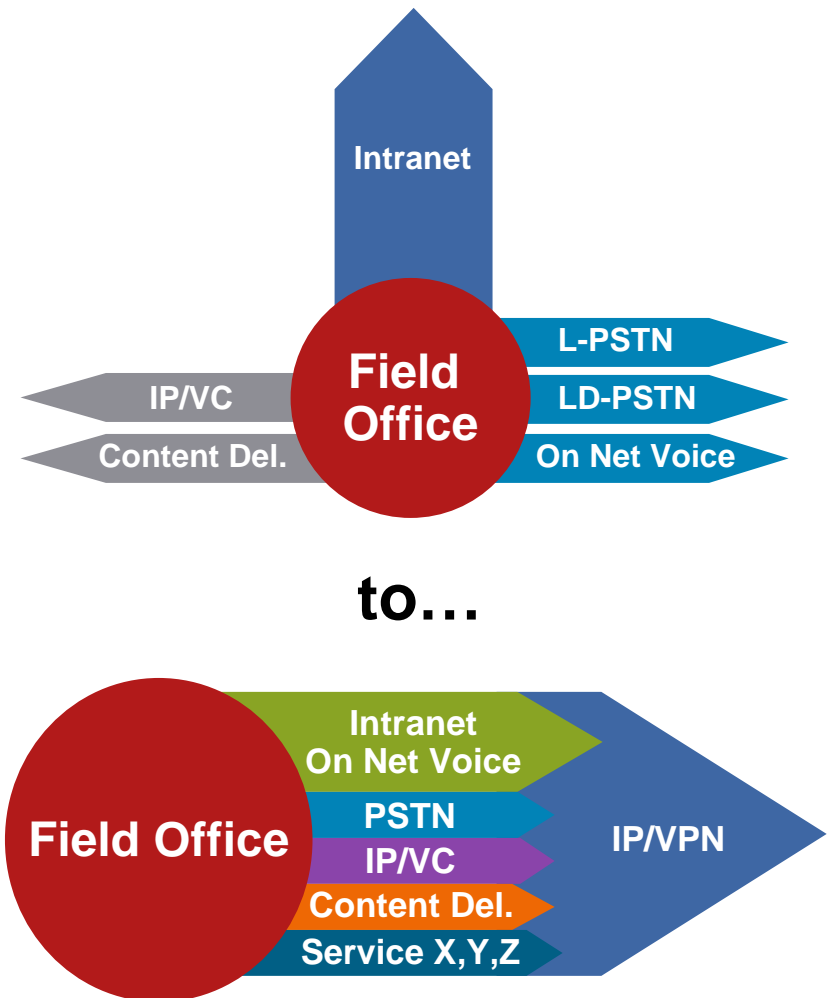
- **Capacity planning**

SP's can provide detailed class of service usage and traffic pattern trending

Cisco's Intelligent Network Infrastructure

Direction: Convergence of Pipes

- Converge to common facilities for most services by using in-cloud SP services or consolidating to hub sites
- Leverage SP partners' core services and economies of scale to make infrastructure management less complex

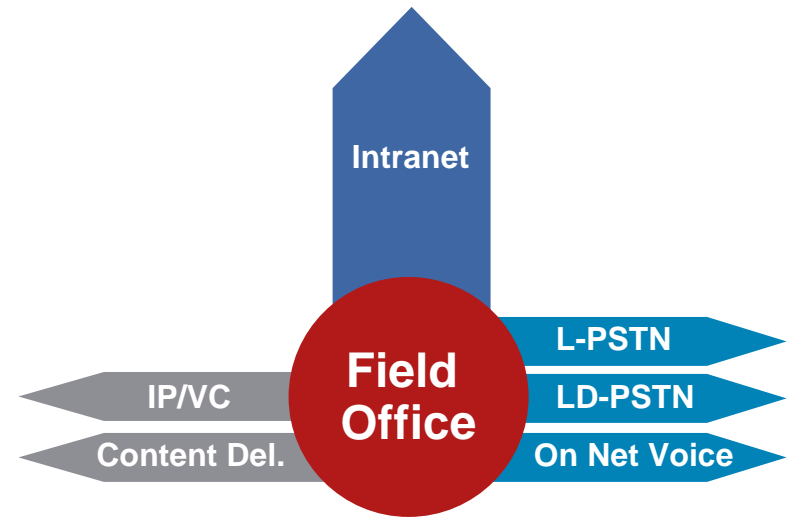


Cisco's Intelligent Network Infrastructure Direction: Convergence of Pipes (Contd..)

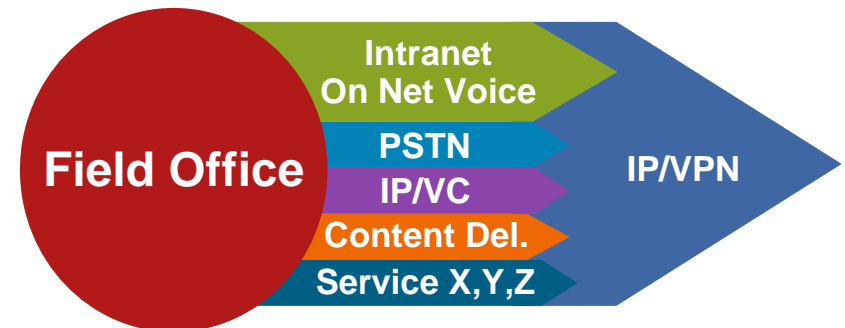
- Challenges/barriers today

Economies of scale for integrated services (for example access to the PSTN via VoIP) are still under development

“Bandwidth mentality”



to...



Hurdles to IP/VPN Adoption



IP/VPN Roadblock #1: Pricing

- Pricing for early IP/VPN services was fairly high; most SPs compared it with a full-mesh, frame-relay, or ATM network
- Cisco IT and other enterprises really do not need a full-mesh network, but would like the advantages that the technology provides
- Changing: service providers are restructuring their pricing for adoption; recent bids are demonstrating savings compared to existing TDM networks

IP/VPN Roadblock #2: Transparency

- “Drop-in replacement” service requires transparency - interaction with and preservation of:
 - Enterprise QoS policy:** must support multiple classes of service aligned with enterprise QoS policy and preserve enterprise markings for end-to-end QoS
 - Enterprise IP routing policy and protocol:** should integrate with existing network without having to re-engineer routing policy and/or retrain engineer/support base on new protocols
 - Enterprise IP multicast infrastructure:** should natively support IP multicast and avoid maintenance and scale issues with a special tunnel overlay
- Changing through enterprise demands, Cisco IT partnerships with Cisco R&D, and new feature support

IP/VPN Roadblock #3: PE Coverage

- Early IP/VPN services touted significant coverage but relied upon a small number of provider edge IP nodes and ATM/FR access backhaul
 - Example: one early service used only five PE nodes in US; latency from site-to-site was better on our private network for support of real-time apps
- Changing through SP service evolution to IP services network and gradual service expansion; most providers now offer good coverage in their focus region(s)

IP/VPN Roadblock #4: Unmanaged CE Service

- Early IP/VPN service offerings only supported a completely managed service, including the CE routers
- Cisco IT (along with other enterprises) are concerned about the loss of visibility into the state of the WAN
- Cisco IT was also concerned about our ability to deploy new features and functionality at WAN edge, where many new features are most applicable
- Changing through customer demand to SPs; most SPs now offer unmanaged CE service

IP/VPN Roadblock #5: Inter-provider VPN

- Many enterprises (including Cisco IT) have expressed a desire for more resiliency in the network
- Deploying IP/VPNs involves taking more of a risk - enterprises can no longer combine multiple service provider circuits to form a resilient network
- Ideally, enterprises like Cisco IT would like to leverage multiple SPs that are interconnected to provide a higher level of availability in case of one SP failing
- Cisco IT is finding this one is harder to change
 - Not a technology problem

Cisco WAN Strategy

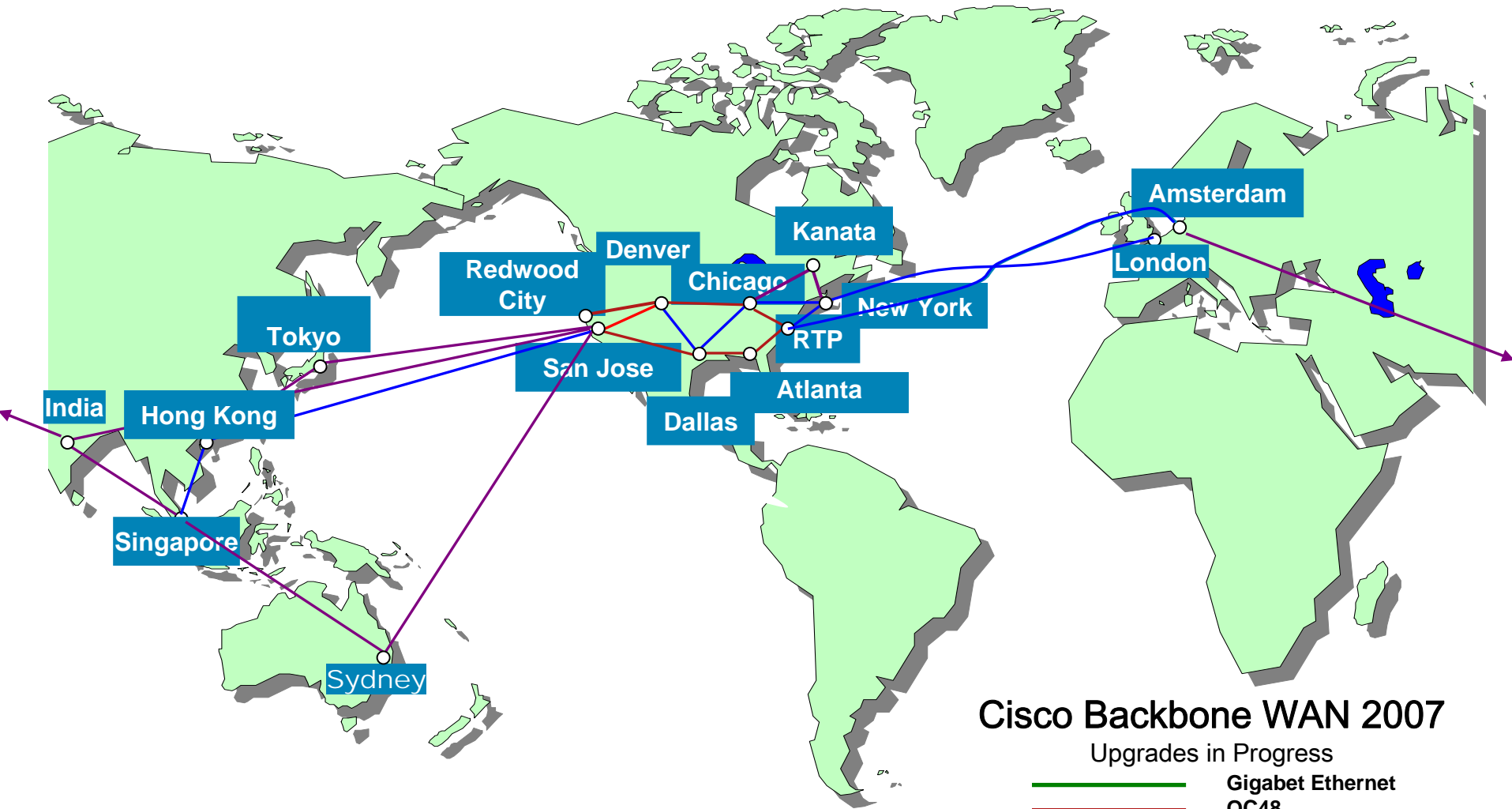


Global WAN Strategy

- Cisco to maintain a TDM based backbone for major offices worldwide. Otherwise known as CAPNet
- Utilise IDC/Hosting centers as major node points for connecting regions
- Regional WAN networks to span off this backbone network to allow for maximum flexibility
- Regional WAN topology to be dictated by market factors and SP capabilities
- Primary choice of topology for regional WAN's is IP/VPN where the capability exists to meet Cisco's needs

Backbone Network WAN

Updated Aug 2007



Cisco Backbone WAN 2007

Upgrades in Progress

-  Gigabet Ethernet
-  OC48
-  OC3 – OC12
-  DS3 – OC3

Regional WANs (IP/VPN or TDM)

- Europe
- Middle East
- Africa
- Latin America
- North America
- China
- India
- AsiaPacific

Cisco's IP/VPN requirements

- Must have:

- QoS transparency end to end

- QoS with at least 4 classes of service and

- Support for Multicast in native form

- Proactive & Reactive monitoring

- Nice to have

- Support for EIGRP PE to CE

- Co-managed CE solution

- CoS reporting & capacity planning

IP/VPN SP Selection - factors

- Financials
- Reach & node density
- Cisco powered
- Capabilities
- Operating Support System (OSS)
- Performance & capacity
- InterVPN agreements
- SLA Commitments

Latency

- Latency is a primary measure of end user performance
- Most important for real/interactive traffic
- IP/VPN Service providers should aim to provide estimated Latency times

Example Latency Matrix

	Site 1	Site 2	Site 3	Site 4	Site 5	Site 6	Site 7	Site 8	Site 9	Site 10	Site 11	Site 12	Site 13	Site 14
Site 1	0	96	88	139	42	82	35	34	164	138	76	80	1	84
Site 2	92	0	263	110	12	138	140	4	20	100	-8	250	-30	235
Site 3	88	331	0	110	12	134	132	0	16	104	223	246	2	231
Site 4	139	110	106	0	65	-80	239	57	73	142	94	102	10	98
Site 5	38	12	8	30	0	4	70	24	40	50	92	5	-19	5
Site 6	82	188	184	100	8	0	194	0	16	80	72	180	-36	76
Site 7	-28	148	108	163	62	102	0	54	70	154	92	96	-11	100
Site 8	34	-4	0	57	24	0	226	0	32	42	-11	-7	1	-7
Site 9	46	16	16	73	40	16	102	32	0	62	9	184	17	13
Site 10	138	108	104	146	54	88	214	58	62	0	88	112	78	92
Site 11	76	-29	223	94	96	117	96	-7	5	84	0	183	-9	224
Site 12	88	250	246	98	5	180	100	-7	188	108	175	0	-12	187
Site 13	1	2	2	14	17	-8	17	9	29	78	-9	20	0	3
Site 14	80	235	231	98	100	121	212	-3	13	142	220	187	-33	0

Colour	Round Trip Time (ms)
Light Blue	Improves 20ms above what we have today
Yellow	Improves between 1 and 20ms above what we have today
Orange	Is below current performance (<0ms))

Latency (Contd..)

- Latency of IP/VPN can reveal underlying infrastructure (e.g. lack of P/PE node density, asymmetric routing etc)
- Figures can be used as part of SLA agreements to ensure SP accountability

Example Latency Matrix

	Site 1	Site 2	Site 3	Site 4	Site 5	Site 6	Site 7	Site 8	Site 9	Site 10	Site 11	Site 12	Site 13	Site 14
Site 1	0	96	88	139	42	82	35	34	164	138	76	80	1	84
Site 2	92	0	263	110	12	138	140	4	20	100	-8	250	-30	235
Site 3	88	331	0	110	12	134	132	0	16	104	223	246	2	231
Site 4	139	110	106	0	65	-80	239	57	73	142	94	102	10	98
Site 5	38	12	8	30	0	4	70	24	40	50	92	5	-19	5
Site 6	82	188	184	100	8	0	194	0	16	80	72	180	-36	76
Site 7	-28	148	108	163	62	102	0	54	70	154	92	96	-11	100
Site 8	34	-4	0	57	24	0	226	0	32	42	-11	-7	1	-7
Site 9	46	16	16	73	40	16	102	32	0	62	9	184	17	13
Site 10	138	108	104	146	54	88	214	58	62	0	88	112	78	92
Site 11	76	-29	223	94	96	117	96	-7	5	84	0	183	-9	224
Site 12	88	250	246	98	5	180	100	-7	188	108	175	0	-12	187
Site 13	1	2	2	14	17	-8	17	9	29	78	-9	20	0	3
Site 14	80	235	231	98	100	121	212	-3	13	142	220	187	-33	0

Colour	Round Trip Time (ms)
Light Blue	Improves 20ms above what we have today
Yellow	Improves between 1 and 20ms above what we have today
Orange	Is below current performance (<0ms))

Cisco IT EMEA IP/VPN Implementation



Cisco's Intelligent Network Infrastructure

Europe WAN FY'03/04: IP/VPN

- **Our implementation**

- Primary IP/VPN service to most EMEA locations with a primary service provider

- Hard-to-reach EMEA sites connected to Cisco hub sites via traditional access (leased line)

- Secondary IP/VPN service to key EMEA hub locations for resilience with a second service provider

Cisco's Intelligent Network Infrastructure

Europe WAN FY'03/04: IP/VPN (Contd..)

- **Key implementation features**

“Unmanaged” service: Cisco maintains control of the customer edge router configuration for new features, network visibility; SP has limited management access to troubleshoot and maintain

“Transparent” service: service provides “drop-in” network with transparency so that Cisco's network retains its integrity and does not have to be designed around individual SP offerings

Cisco's Intelligent Network Infrastructure

IP/VPN Benefits Realized: EMEA

- TCO reduction

Five dedicated WAN staff consolidated with remainder of network support staff, **effort reduced ~ 20-30%**

Capacity planning efforts reduced as granularity shifted from per-circuit to per-site

Network engineering efforts reduced as Cisco effectively leverages SP's network planning process

Troubleshooting efforts reduced as Cisco leverages service provider processes

Network availability improved

Average daily downtime has been reduced from 6.3 to 2.3 minutes through proactive co-management of service

Network reliability has improved as number of priority 1 WAN cases have decreased

Cisco's Intelligent Network Infrastructure

IP/VPN Lessons Learned: EMEA

- Given nearly equivalent bandwidth and Cisco's bandwidth requirements, raw bandwidth costs between IP/VPN and circuit costs were within 10% of each other
- We were one of the first major enterprise implementations of IP/VPN on this scale: network engineering effort was greater in shaping service offering with our service providers (one-time effort)
- IP/VPN troubleshooting can be slightly more complex - it helps if enterprise engineers understand the basics of MPLS VPN (although not required)
- Migration plan is important to ensure continued service throughout the transition

Q and A



Further Resources



Cisco on Cisco Website

<http://www.cisco.com/go/ciscoit>



Call to get Product, Solution and Financing Information

1-800-745-8308 ext. 4699



Order Resources

<http://cisco.com/en/US/ordering/index.shtml>

