Cisco AVVID Network Infrastructure Overview

Organizations operating large networks increasingly seek an enterprise-wide infrastructure to serve as a solid foundation for emerging technologies such as IP telephony and storage.

Technological Framework for Cisco AVVID

Cisco *Architecture for Voice, Video and Integrated Data* (AVVID) is the key enterprise network architecture from Cisco Systems. It is designed on open standards principals to deliver the flexibility, reliability and essential network enablers that position enterprises to become agile and adaptable. This network architecture also allows organizations to plan effectively for network upgrades and enhancements.

Cisco *AVVID Network Infrastructure* provides the technological foundation for Cisco AVVID. It is analogous to a foundation of poured concrete and steel-reinforcement over which an industrial-strength structure stands. Without this foundation, there is no unifying system tying the applications together. With it, a scalable, resilient networking structure can be built supporting an enterprise's entire suite of communications requirements.

Cisco AVVID Network Infrastructure provides an enterprise foundation that combines IP connectivity with high performance, security and availability. Although layering application solutions such as voice or video networks may require changes to the infrastructure, this architectural approach provides the basis for optimizing design principles and practices.

Because network requirements differ, specific variations in topology (mesh or hub-and-spoke), media (Frame Relay or Asynchronous Transfer Mode [ATM]), and overall network (LAN, WAN, or MAN) must be factored into each implementation. Cisco AVVID Network Infrastructure provides the design flexibility to handle these varying requirements.

Building a Foundation for Resilient Networks

The premise of *resilience* is a central theme of Cisco AVVID and Cisco AVVID Network Infrastructure. This theme can be split into four general layers of emphasis: *network resilience*, *communications resilience*, *applications resilience*, and *business resilience*.

- *Network Resilience*—The intelligence of the network provides adaptability, flexibility, and distributed response to single points of failure. The dimensions of network resilience include physical redundancy (links and nodes) and mesh-based network design. However, Cisco substantially enhances common-sense design principles with key Cisco IOS capabilities—including resilient routing, switching, IP services, and Multiprotocol Label Switching (MPLS)

- *Communications Resilience*—IP-based communications benefit directly from network resilience. By building a converged network infrastructure, organizations can cost-effectively deploy diverse communications such as IP telephony, telecommuting, video conferencing, and unified messaging that increases and enhances contact with customers, partners and suppliers even in the event of disruptions.
- *Applications Resilience*—Networked applications directly benefit from network and communications resilience. For example, applications resilience is facilitated by Cisco AVVID Network Infrastructure design elements such as distributed data center designs, data center recovery, and remote data replication.
- *Business Resilience*—Workplace resilience is achieved through the distribution of workers among multiple, dispersed settings. Technologies that enable telecommuting, desk sharing, office hoteling, and employee mobility are essential for ensuring optimal productivity during disruptions.

Business resilience represents the next phase in the evolution from traditional, place-centric enterprise structures to highly virtualized, people-centric organizations that enable people to work anytime, anywhere. When built from the infrastructure up, business resilience allows organizations to respond quickly, decisively, and effectively to unforeseen and unpredictable forces.

Why Implement a Cisco AVVID Network Infrastructure?

The global economy's evolving business climate requires organizations large and small to adopt information management systems that promote adaptability and resilience while ensuring stability throughout the communications infrastructure. In this new business environment, how do companies continue to thrive and survive? Companies must harness the power of the Internet and an effective network infrastructure to yield productivity and profitability gains.

This is where Cisco Systems can help. Cisco AVVID Network Infrastructure delivers the design principals to enable essential transformational technologies. These technologies are vital to optimizing the integration of mission-critical applications within a *converged* networking environment.

Significant productivity gains can be enhanced by developing a converged network environment capable of handling an organization's entire suite of communications applications, while extending services to remote sites, telecommuters and mobile employees.

This assertion was recently reinforced in the results of a survey of voice and data professionals conducted by META Group:

- Almost 70 percent of respondents believe that converging their networks will realize substantial to moderate infrastructure savings
- 50 percent of respondents expect substantial to moderate administrative cost savings
- 60 percent of respondents expect to achieve substantial to moderate toll bypass savings

Cisco AVVID network infrastructure provides the tool set to integrate disparate and changing organizational elements smoothly and securely—to create a more efficient communications environment. Today's business reality is about getting back to the basics of profit, cash flow and productivity. Cisco AVVID can help harness the power of networking to enable productivity applications that drive these business constants.

Only those organizations that strategically leverage networks to combine business and innovative technology solutions will succeed in the new Internet economy. With this kind of instinctive approach, organizations are positioned to drive profitability and improve customer loyalty through increased productivity.

Cisco AVVID Network Infrastructure Components—Intelligent Network Services

Network managers who design and build networks to support solutions such as voice and video must first consider the components that allow networks to operate properly. The individual devices or nodes often become the focus of an organizations's design decisions. However, a single element—whether switch, router, or any other networking device—is only one component of the overall network. It is increasingly important to focus on how the devices connect, what features and protocols are used, and how they are used to form the foundation for what can be placed on top of the network. If the foundation is unstable, layering technology solutions over the network creates additional problems.

By creating a robust foundation of basic connectivity and protocol implementation, Cisco AVVID Network Infrastructure addresses five primary concerns of network deployment: *high availability, quality of service (QoS), security, mobility and scalability.*

High Availability

Determining how resilient a network is to change or disruption is major concern for network managers. This assessment of network availability is critical. It is essential that every network deployment emphasizes availability as the very first consideration in a baseline network design.

Availability must be viewed from the user's perspective. To the user, the network is down regardless of whether an application fails, a router dies, or a piece of fiber is cut. Key availability issues to address include:

- *Hardware Redundancy*—This is often the first level of redundancy in the network. Cisco offers, in its modular products for example, options for redundant supervisor engines and dual in-line power supplies. This often provides the first backstop against a network failure.
- *Protocol Resiliency*—Good design practices dictate how and when to use protocol redundancy, including load-sharing, convergence speed, and path redundancy handling. Contrary to popular belief, if some redundancy is good, more redundancy is not necessarily better.
- *Network Capacity Design*—Good design practices include capacity planning. How much traffic can a connection handle in the worst case? Ascertaining that a link can handle double the traffic when a redundant link fails must be considered. Capacity planning must be included during the network design phase to ensure the smooth integration of new technologies (such as video conferencing).

With Cisco AVVID Network Infrastructure solutions for hardware redundancy and protocol resiliency, combined with effective planning, high availability of network resources can be optimized.

Quality of Service (QoS)

Voice, video, and mission-critical data applications are important underlying productivity tools that make a business successful. Ensuring that these applications are effectively delivered requires skillful traffic management—particularly within the context of an integrated networking solution. *Quality of Service* (QoS) is a key Cisco AVVID network infrastructure enabling capability for such an environment.

Application Considerations for QoS

The specific QoS requirements for given applications are generally determined by three parameters: *latency*, *jitter*, and *loss*. Depending on the type of application to be implemented over a Cisco AVVID Network Infrastructure, the importance and effects of these considerations can differ.

For example, while one-way latency for voice or video conferencing should be no more than 150 to 200 ms, streaming video can tolerate up to 4 to 5 second latency. Similarly, jitter is not an issue for streaming video, while it should be limited to 30 ms for voice and video conferencing applications.

Bandwidth effects will also differ. For example, to support video conferencing, the minimum bandwidth guarantee is the size of the video-conferencing session plus 20 percent (a 384 Kbps video-conferencing session requires 460 Kbps guaranteed priority bandwidth). Voice requires 17-to-106 Kbps of guaranteed priority bandwidth per call (depending on the sampling rate, codec and Layer 2 overhead), while 150 bps (plus Layer 2 overhead) per phone of guaranteed bandwidth is required for Voice Control traffic.

Although planning requirements certainly vary depending on application, Cisco AVVID Network Infrastructure capabilities have the flexibility to concurrently support QoS requirements of voice, streaming video, video content distribution, video conferencing, and mission critical data traffic—all carried over a common IP-based networking environment.

Security

Security must be treated as an integral element of any Cisco AVVID network. An organization's communications network is the basic environment connecting all users, servers, applications and service providers. Implementing a robust security suite provides the best defense against possible information loss, tampering, or productivity disruption. Cisco's security suite emphasizes three key areas: *internal* network security, *external* network security, and the *identity* of users and applications to ensure proper policy assignment.

- *Internal Network Security*—Ensuring that your internal network is secure includes tracking physical, endpoint, application and Layer 2 security issues.
- *External Network Security*—External network security focuses on securing the interface between an organization's internal network and the outside world (the Internet edge).
- *Network Identity*—In considering a network's overall security scheme, it is essential to establish a framework that allows the network administrator to implement identity-based network access control and policy enforcement, right down to the user and individual access port level.

Cisco AVVID Network Infrastructure capabilities present a formidable array of both device-based and server-based security applications and features. Access control lists (ACLs), firewalls, server-based authentication, intrusion detection systems, and virtual private network capabilities can be integrated into a seamless security environment. Together, these capabilities provide an adaptable, resilient safety zone to ensure secure data transport, voice communications, and shared application access.

Enterprise Mobility

Mobility is often defined as providing ubiquitous connectivity to the mobile user, independent of devices and access technologies. But *enterprise* mobility goes beyond simply allowing users to roam from building to building with a laptop, or connecting to the Internet at the local cybercafe. Creating an enterprise network that facilitates organizational mobility involves embedding the environment with an infrastructure capable of integrating an underlying flexibility and security to promote scalable networks—while ensuring continuity as networks move through transitions or expand and contract based on business needs.

A key concept in understanding the way a seamlessly mobile environment fits into the enterprise network is *convergence*. Convergence involves the integration of security capabilities with underlying infrastructure elements, and an organization's strategic movement to IP as the single common technology supporting mission critical enterprise communications applications (voice, video, data and storage). The convergence toward an IP-based infrastructure is central to promoting true organizational mobility.

Cisco AVVID Network Infrastructure technologies enable the mobile enterprise via *Mobile IP* and *Extensible Authentication Protocol (EAP)-Cisco Wireless LANs*.

Scalability

A network must be able to scale from where it is today to where it might be in the future. For example, a network administrator might need to design the WAN to support only 50 branch offices today. However, over a year's time, 50 more branches might require connectivity. The design, IP address management, features, and WAN link speeds must all be able to provide this connectivity and additions without massive redesign of the network.

The key to successful long-term network scalability is to select and implement equipment to minimize network reconfiguration and device turnover downstream. That means ensuring that network interface cards will have the appropriate capacity to handle upgrades to media capabilities (such as from 10/100 Mbit Ethernet to 1000 Mbit Ethernet) or deployment of hardware acceleration features.

Planning for these changes requires that organizations be prepared to support emerging technologies and networked applications as they are implemented. Networks must be able to handle increased demand required by new networking capabilities. Building a network over a Cisco AVVID Network Infrastructure provides a framework of intelligent network services (high availability, security, QoS, and mobility) capable of effective long-term scalability.

Cisco AVVID Network Infrastructure: Foundation of the Converged Network

Industry studies, such as META's recent survey of telecom and data management professionsals, indicate widespread agreement that most Enterprise networks will converge around IP-based architectures within the next 3-to-5 years. Figure 1 illustrates a generalized network for such a converged network. Equipment costs, management efficiencies, and long-term operational cost benefits all combine to ensure that, while not every implementation will be identical, almost every large-scale voice, video, and data network will be built over a common IP environment. Ensuring that such a system is truly resilient and capable of delivering on the promise of productivity gains will hinge on investing in the right systems in the context of the right network design.

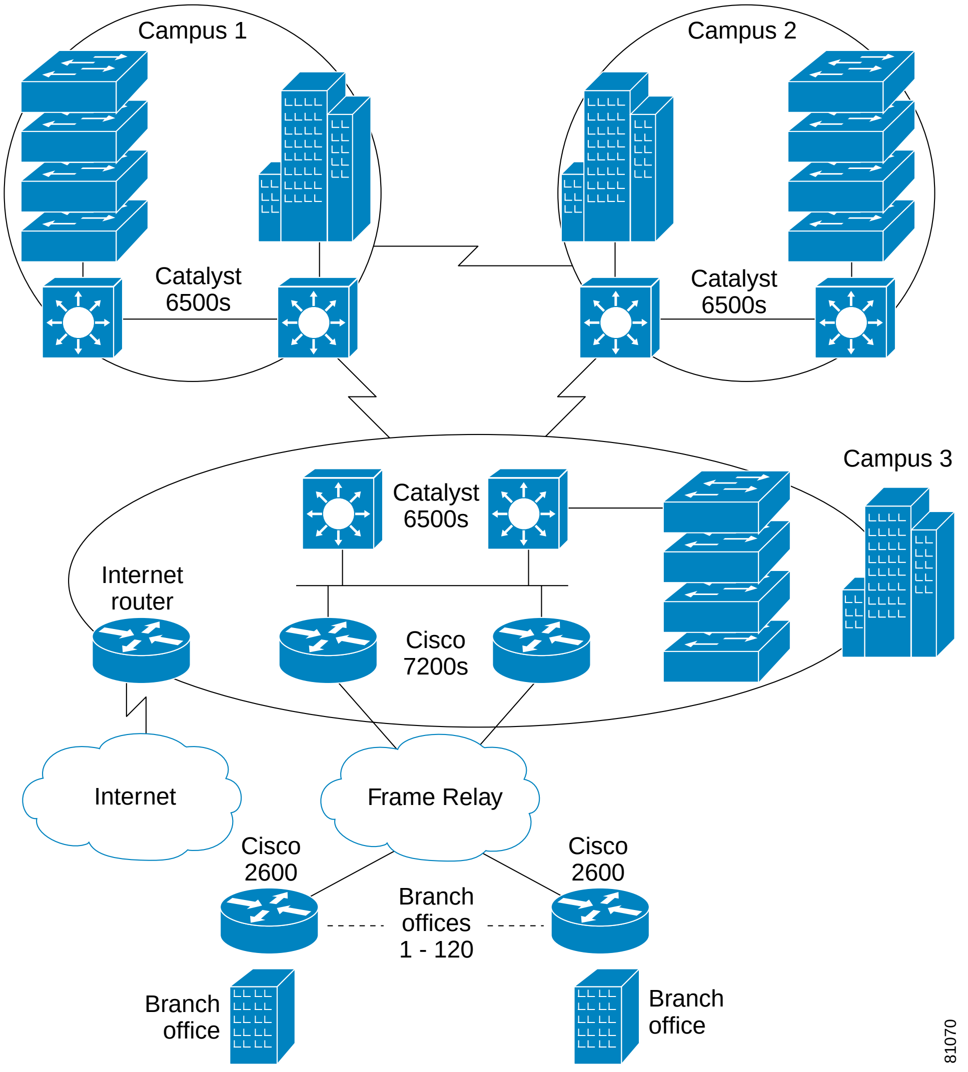
Cisco AVVID Network Infrastructure intelligent network services provide the stable platform of high availability, QoS, security, mobility, and scalability that will prepare networks to support emerging technologies. For more information for Cisco AVVID Network Infrastructure contact your Cisco Account Manager.

For more information on Cisco AVVID Network Infrastructure, please visit the following websites:

- Cisco employees: http://wwwin.cisco.com/ent/ese/
- Cisco partners: http://www.cisco.com/partner/avvid_sol/cani.html

Figure 1

Example Cisco AVVID Network Infrastructure Environment



Cisco Systems

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe