Cisco Medical-Grade Network

Providing Foundational Architectures for Healthcare

Cisco Medical-Grade Network

The Cisco® Medical-Grade Network (MGN) provides the network foundation and architectures that enable advanced clinical applications and biomedical devices to operate in a protected, interactive, resilient, and responsive environment. These characteristics are detailed within the MGN architecture, which is based on the best practices of a robust healthcare environment.

Cisco's Medical-Grade Network provides an end-to-end framework for the healthcare industry and allows integration and interoperability at each functional area to optimize interactions among healthcare participants, processes, applications, and hardware components. This includes areas such as Acute Care campus networks, ambulatory clinics, remote clinicians, and data centers.

Within the Cisco MGN, diverse business and clinical communications are facilitated and integrated throughout the continuum of care. The Cisco MGN supports:

- Communication needs for clinicians, patients, administrators, and partners
- Healthcare regulatory requirements for patient privacy and data security
- Healthcare's unique information, technology, bandwidth, and integration challenges
- Anytime, anywhere information capture and access for wired and wireless applications and devices
- Converged data, voice, and video networks enhancing patient care and collaboration
- Identity- and policy-based security from inside the network to beyond organizational walls
- Transfer and storage of large amounts of data created by healthcare applications

Cisco Smart+Connected Health Solution Portfolios

- **Cisco Connected Imaging Solutions**
  Solutions that optimize imaging workflow and image access
- **Cisco Care-at-a-Distance Solutions**
  Solutions that offer face-to-face communication unbounded by distance, physical location, or setting
- **Cisco Clinical Workflow Solutions**
  Solutions that streamline workflows and improve communication among clinicians
- **Cisco Healthcare Technology Foundations**
  End-to-end healthcare IT infrastructure solutions that provide the technology foundations to enable security, reliability, and regulatory compliance
- **Cisco Smart Healthcare Facility Solutions**
  Services that enable hospitals to reduce the capital and operating expenses of healthcare facilities

www.cisco.com/go/mgnfoundation
www.cisco.com/go/mgnfdz

Resilient

Single points of failure are eliminated and rapid convergence architectures and technologies are used throughout the network. Advanced technologies are used to maximize uptime for mission-critical applications such as Electronic Health Records (EHRs), Picture Archiving and Communications Systems (PACS), and biomedical devices.

Protected

In order to secure Protected Health Information (PHI) and other patient confidential information, the Cisco Security Framework provides an industry-proven architecture. This provides the foundation for meeting global healthcare security specification such as HIPAA, PCI, PIPEDA, 95/46/EC, HITRUST, and Red Flags Rule.

Interactive

Through the use of Cisco technologies, clinicians, physicians, payers, and patients are able to interact with the healthcare network. Utilizing wired and wireless technologies, the Internet, and remote access solutions, authorized individuals are able to access critical clinical information. Patients are able to interact with their care providers, resulting in an enhanced patient care model.

Responsive

The network needs the flexibility to quickly respond to changing demands. These demands range from regulatory requirements and security to new clinical systems and devices. The Cisco MGN is elastic in its ability to respond to the needs for increased bandwidth, quality of service, security, and regulatory compliance.

Acute Care Campus Environment

Protected
Secure and Automated Device Access
Biomedical and IT devices are dynamically identified and the network automatically provisioned for the proper medical network. Unauthorized devices are denied access and are reported back to a central management system.

Cisco Network Admission Control (NAC) performs posture assessment and checks PC and workstation antivirus and software patch levels.

Signature- and behavior-based antivirus solutions protect desktop and clinical workstations against day-zero attacks and data loss.

Interactive
Wireless/Unified Communications
The Cisco Medical-Grade Network optimizes the infrastructure to support wireless devices and unified communications applications.

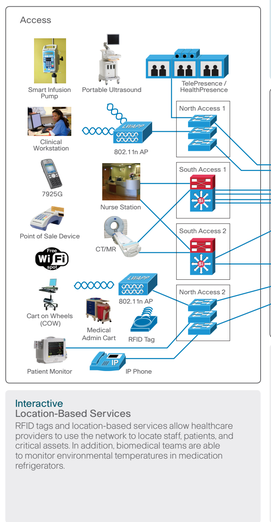
Wireless access is available to clinicians, physicians, contractors, and patients/visitors through Cisco's industry-leading, highly secure wireless architectures.

Clinicians utilize Cisco Unified Communications and Cisco TelePresence for consults, screen sharing, and online collaboration to increase productivity and help reduce errors.

Responsive
Quality of Service
High-priority applications such as voice, patient monitoring, and various biomedical devices are given high-priority QoS classification and treatment throughout the network.

Access Layer

The access layer provides the intelligent demarcation between the network infrastructure and the computing devices. It provides a security, QoS, and policy trust boundary and is a key element in enabling multiple services.

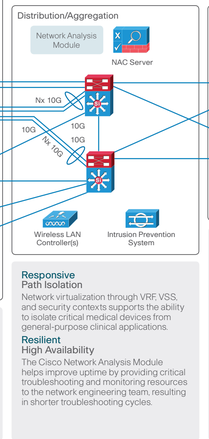


Distribution/Aggregation Layer

The distribution layer acts as a services and control boundary between the access layer and the network core. It protects the core from high-density peering and provides policy services for traffic flows within the access-distribution block.

The distribution layer uses Layer 3 switching for its connectivity to the core of the network and either Layer 2 or Layer 3 services for its connectivity to the access layer.

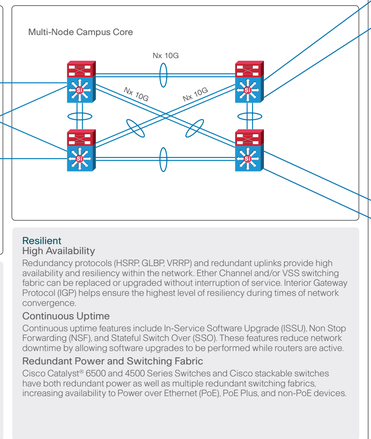
Network services contained within the distribution layer include wireless LAN controllers, network analysis, network access controllers, and intrusion prevention appliances.



Core

The campus core is the network infrastructure that provides access to network communication services and resources to end users and devices spread over a single geographic location. Its architectural design promotes non-blocking, rapid convergence, and ultra high non-stop availability.

The core is the cornerstone of the entire campus network, providing connectivity between end users and data.



Interactive
Location-Based Services
RFID tags and location-based services allow healthcare providers to use the network to locate staff, patients, and critical assets. In addition, biomedical teams are able to monitor environmental temperatures in medication refrigerators.

Responsive
Path Isolation
Network virtualization through VRF, VSS, and security contexts supports the ability to isolate critical medical devices from general-purpose clinical applications.

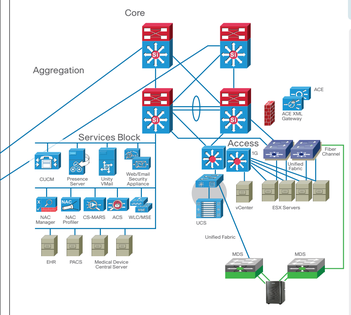
Resilient
High Availability
The Cisco Network Analysis Module helps improve uptime by providing critical troubleshooting and monitoring resources to the network engineering team, resulting in shorter troubleshooting cycles.

Resilient
High Availability
Redundancy protocols (HSRP, GLBP, VRRP) and redundant uplinks provide high availability and resiliency within the network. Ether Channel and/or VSS switching fabric can be replaced or upgraded without interruption of service. Interior Gateway Protocol (IGP) helps ensure the highest level of resiliency during times of network convergence.

Continuous Uptime
Continuous uptime features include In-Service Software Upgrade (ISSU), Non Stop Forwarding (NSF), and Stateful Switch Over (SSO). These features reduce network downtime by allowing software upgrades to be performed while routers are active.

Redundant Power and Switching Fabric
Cisco Catalyst® 6500 and 4500 Series Switches and Cisco stackable switches have both redundant power as well as multiple redundant switching fabrics, increasing availability to Power over Ethernet (PoE), PoE Plus, and non-PoE devices.

Data Center



Cisco Data Center Solutions

Cisco data center solutions provide the connectivity to physical and virtualized data center resources including EHR and PACS servers, blade servers, virtualized machines, and SAN/NAS environments. The infrastructure supporting these services includes application servers, storage media, routers, switches, load balancers, and application acceleration devices.

Resilient
The data center is designed for high resiliency through use of redundant pairs of switches and modules. Single points of failure are eliminated for software and hardware within the data center.

Interactive
Voice, Video, Data Servers
Voice, video, and data communication servers provide the unified communications platform to enable clinical staff, IT users, patients, and partners to communicate more effectively.

Application servers host EHRs, PACS, medical device information, and clinical applications.

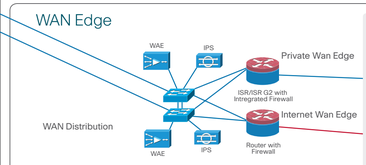
Responsive
Cisco Unified Computing System
The Cisco UCS platform unites compute, network, storage access and virtualization into a cohesive system to reduce total cost of ownership and increase business agility.

VMware ESX servers virtualize healthcare applications and server storage/networking. This increases hardware utilization, provides more efficient use of processing, and lowers total cost of ownership.

The modular switching platform provides 10 Gigabit Ethernet and unified fabric in the data center, delivering scalable, continuous operation and transport flexibility.

Protected
Compliance, Collection, and Correlation
Cisco Secure Access Control Server (ACS), an industry-leading AAA platform, also supports RADIUS, NAC, and directory services enabling healthcare facilities compliance with regulatory requirements. Infrastructure-based network telemetry, AAA firewall, and IPS event data is centrally collected and correlated for threat identification and mitigation.

WAN Edge



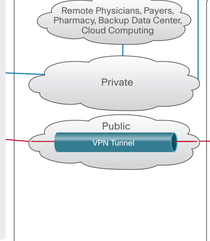
WAN Edge

The WAN edge aggregates WAN links, which connect geographically distant clinics, ambulatory facilities, remote clinicians, payers, and backup data centers to the central data center. The WAN can be either privately owned by the facility or provided by a public service provider.

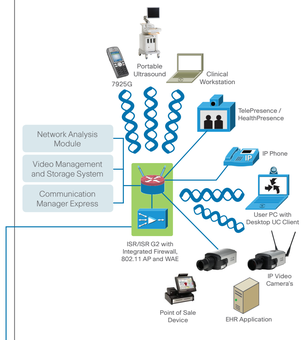
Protected
Secure WAN and Remote Connectivity
Edge firewalls and IPS/IDS are used to meet specific regulatory requirements such as HIPAA, Payment Card Industry Data Security Standards (PCI DDS), and HITRUST. Firewalls provide granular access control and connectivity to branch physician offices, practices, payers, and disaster recovery data centers. Remote physicians use authenticated and encrypted access methods such as Secure Sockets Layer (SSL) and IP Security (IPSec) VPN.

Responsive
Wide Area Application Services (WAAS)
Cisco Wide Area Application Engines (WAEs) reduce the WAN bandwidth of PACS imaging viewing, retrieval, and storage functions. WAAS uses optimized caching, transport flow optimization (TFO), and compression to reduce traffic bandwidth across WANs.

Resilient
Enhanced Availability and Resiliency
Hardened devices add high-availability, dual-homed links to help ensure optimal service and network availability.



Ambulatory Care



Ambulatory Care

Ambulatory Care facilities include doctors' offices and large specialty clinics. In smaller facilities a single Integrated Services Router can provide all of the network services. The Cisco Medical-Grade Network will provide comparable services to those provided in a larger facility.

Resilient
Survivable Remote Site Telephony (SRST) provides local telephony services in the event that connectivity to the centralized Cisco Unified Computing System fails.

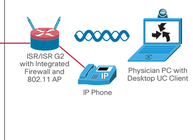
Responsive
Cisco WAAS
Cisco WAAS minimizes IP protocol overhead, optimizes specific applications, and provides data compression over WAN links from the clinic to the main acute care facility.

Interactive
Cisco TelePresence and Cisco HealthPresence Solutions
Cisco TelePresence and Cisco HealthPresence™ solutions allow real-time meetings between patients and doctors at different locations. The Cisco HealthPresence solution captures patient physiological information and transmits the data instantaneously for immediate physician review. This technology is ideal for telemedicine based applications.

Interactive
Cisco ISR and ISR G2
Cisco Integrated Services Routers (ISR) and ISR Generation 2 (ISR G2) provide a high-performance extension of the hospital's data, video, collaboration, and telephony environment from the hospital to the clinic, allowing caregivers the same experience in the clinic as the hospital.

Protected
Endpoint Security
Signature- and behavior-based antivirus solutions protect desktop and clinical workstations against day-zero attacks and data loss.

Remote Clinician



Remote Clinician

The Medical-Grade Network provides the clinician's home or small office with the same core network services that are provided in larger facilities.

Interactive
Cisco Virtual Office
Cisco Virtual Office provides a simple, secure extension of the hospital's data, video, collaboration, and telephony services to the clinician's home or small office.

Interactive
Unified Communications Endpoints
Cisco Unified Communications phones and desktop clients provide an extension of the healthcare organization's Unified Communications infrastructure, allowing remote workers to interface and collaborate as though they were onsite.

Protected
VPN Technologies
VPN technologies provide enterprise-ready encryption to remote clinicians. The Cisco Secure Desktop VPN prevents protected health information from being cached locally on the remote device.