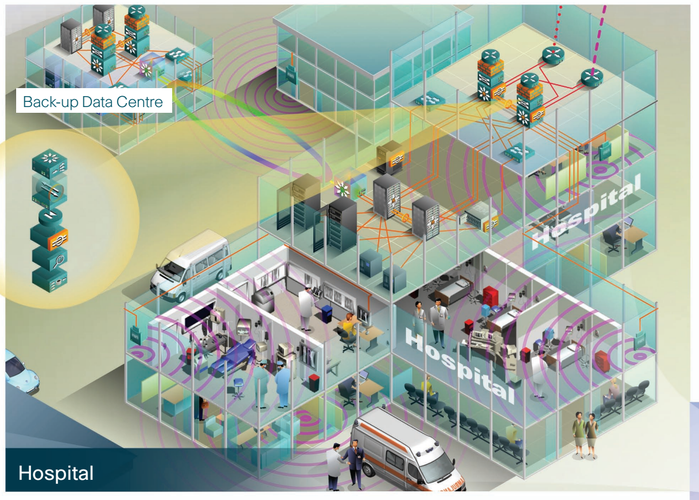
Cisco Connected Health



Cisco's Connected Health network architecture enables the secure sharing of information – from patient records, to MRI images, bed availability and billing data – between clinicians, health administrators, facilities and individuals. It uses a virtualised network, rather than multiple single-user networks, enabling diverse health entities to collaborate and communicate without conflict.

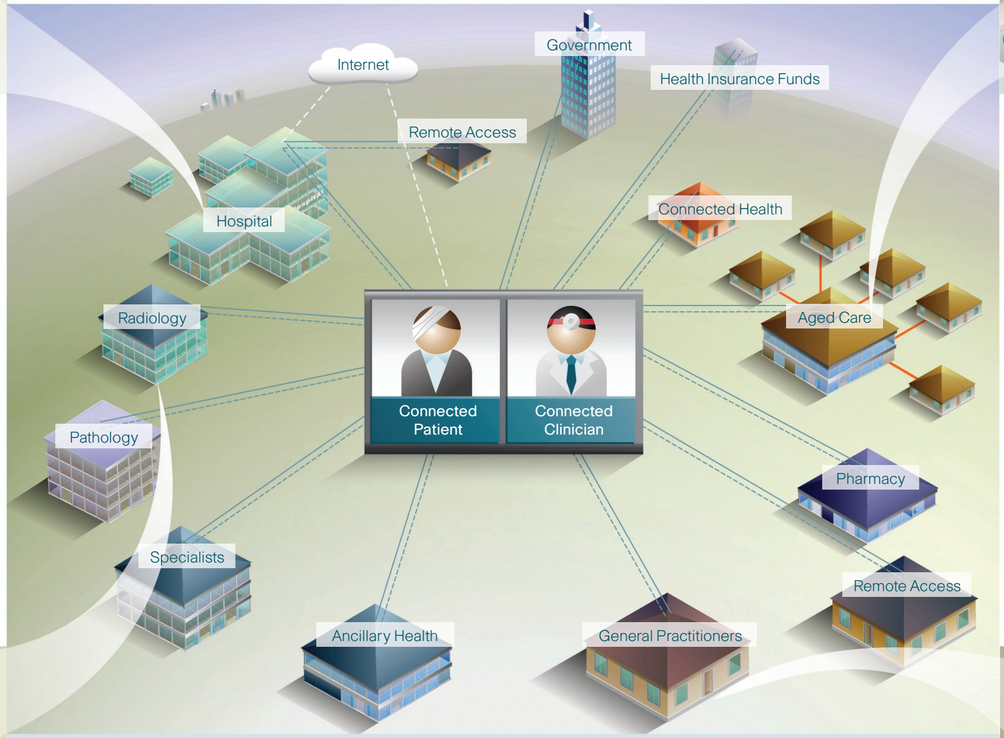
The Cisco Medical-Grade Network delivers the high levels of availability, resiliency, security and auditability demanded by a Connected Health community, as well as the full range of mobility solutions.

Providing a Secure, Collaborative Hospital Environment

- Wireless mobility enables staff to securely access patient data, medical imaging, up-to-date drug databases and essential information across the entire hospital.
- The single network supports high-speed voice, video and data applications without congestion. Multiple virtual networks can be created, making it easy to manage applications and access levels according to the user requirements.
- The network is protected from inside and out against attacks. Robust authentication identifies anyone attempting to connect and then denies or authorises their level of access. Rogue devices are immediately identified and shut down. Viruses and worms are isolated before they can even penetrate the network.
- Robust resiliency measures ensure that the network and applications are kept operational during maintenance work. Failsafe, fully redundant systems keep the network functioning during unforeseen events such as power outages.

Enabling Efficient, Collaborative Radiology Services

- Large image files can be securely stored and transmitted at high-speed. This means they can be viewed wired or wirelessly from the hospital or remote locations using PCs, notebooks or handhelds, enabling doctors and radiologists to collaborate – regardless of location – and provide faster, more accurate diagnoses.
- The network also supports IP transcription making it easy for doctors and radiologists to transcribe patient records remotely using speech-to-text technology.
- High level security ensures patient privacy and compliance with confidentiality requirements. Twenty-four hour system availability with high levels of resiliency enables continual care services, even during power failures or major disruptions.

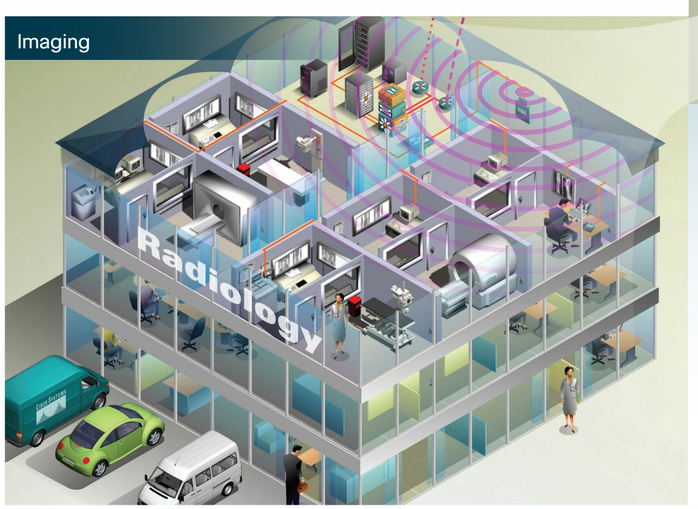


Improving the Safety and Quality of Aged Care

- Providing a secure and safe environment is essential in order to keep residents mobile and housed in self-care accommodation, rather than in acute care facilities.
- Residents can teleconference with GPs and specialists, providing easy access to medical care. 'Nurse Alert' buttons worn on pendants or wrist straps can be activated wirelessly.
- Radio Frequency Identification (RFID) bracelets can be worn by dementia patients to unobtrusively improve safety by preventing them from wandering into danger.
- The network can monitor for abnormal water or lighting usage and alert staff in case a resident needs help.
- User-pays services such as cable television and low-cost calls can be offered.

Supporting Effective Tools and Secure Access in General Practice

- GPs can reliably view patient data – from medical images to records – and securely communicate by phone or videoconference over the one network with specialist staff, colleagues and the patient from the surgery, on the road or from home, if required.
- Secure email and secure messaging are provided at all times.
- Practice surveillance is a low cost add-on to this network, and applications that allow for prescribing support, and even voice-recognition and automatic transcription, operate seamlessly.
- GPs in remote locations can enjoy the same secure access to high-speed applications and functionality in metropolitan practices, and can update their medical education.
- Patients can make appointments.



Technical Details

Hospital Care

Availability – physical, device, network and application failure-resilient design, in-service hardware and software upgrades, configuration and operating system rollback.
Security – security at user, device, access, transport, server and application layers throughout the total hospital network. In-band and out-of-band network management.
Resiliency – 10GE EtherChannel, rapid convergence, granular end-to-end QoS, Virtualised Infrastructure per Hospital organisational sub-unit - VLANs, service engines, etc.

Data Centre and Remote Data Centre

Availability – scalable design, performance (80Gbps trunking), multi-pathing to storage/server and application load balancing, network-based content caching and distribution.
SAN and disaster recovery – network and compute resource efficiency, virtualisation of storage infrastructure, tiered storage, end-to-end visibility, synchronous/asynchronous replication over protocol independent transport (FC, FCoE, FCoIP, iSCSI, FCoWDM, FCoSDH, ESCONoWDM, ESCONoSDH), call home support.
Security – virtualised data centre infrastructure – network, storage, remote data centre and multi-service transport. Data Centre services are protected by wire speed encryption of inter and intra-data centre traffic, intrusion detection, secure management control.
WAN – centralised application hosting via distributed application and file acceleration services.

Wide Area Network and Connected Health VPN Interconnection

Availability – resilient and redundant WAN and Connected Health VPN connections.
Security – protection of devices, network and servers from viruses/worms/denial of service attack, host and network-based intrusion detection.
Policy – user admission control, traffic rate limiting by traffic type and destination.
Management – network traffic analysis, SLA monitoring and alarming filtering, QoS enforcement.
Mobility – remote user access with location identification and presence.

General Practice

Availability – highly available access to Connected Health VPN content and the Internet.
IP Communications - voice, video and data health messaging, communications and conferencing integrated into practice management system.
Security – secure roaming access to surgery information and security systems.

Imaging

Availability – high performance virtualised storage, scalable, fault tolerant, secure access.
Disaster recovery – synchronous/asynchronous back-up to the remote facilities.
IP Communications – voice, video and data health messaging, communications and conferencing integrated into PACS/RIS systems.
Security – protect imaging modalities and networks from internal and external attack, replicated and partitioned data with secure remote clinical access.

Aged Care

Flexibility – rapid and cost effective deployment of resident services (voice, video, data, monitoring).
Availability – physical, device, network and application failure-resilient design.
Security – security at user, device, access, transport, server and application layers throughout federated aged care sites.
Resiliency – redundant WAN and Connected Health VPN connections.
Mobility – WiFi mobility across campus.