Allied Telesis
Healthcare Network Construction Guidebook
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare Network Solution</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Outline of a Healthcare Network</td>
<td>4</td>
</tr>
<tr>
<td>Importance of the network</td>
<td>4</td>
</tr>
<tr>
<td>Main requirements in designing a healthcare network</td>
<td>5</td>
</tr>
<tr>
<td>Non-stop Network</td>
<td>7</td>
</tr>
<tr>
<td>Network bandwidth and QoS (Quality of Service)</td>
<td>7</td>
</tr>
<tr>
<td>Data capacity</td>
<td>7</td>
</tr>
<tr>
<td>Network bandwidth and cost of LAN devices</td>
<td>8</td>
</tr>
<tr>
<td>QoS (Quality of Service)</td>
<td>9</td>
</tr>
<tr>
<td>Redundancy and proactive measures to overcome network failures</td>
<td>10</td>
</tr>
<tr>
<td>Core switch redundancy</td>
<td>10</td>
</tr>
<tr>
<td>Comparison of redundancy of communication</td>
<td>11</td>
</tr>
<tr>
<td>Loop protection</td>
<td>12</td>
</tr>
<tr>
<td>Secure and Reliable Network</td>
<td>13</td>
</tr>
<tr>
<td>Security</td>
<td>13</td>
</tr>
<tr>
<td>Importance of security; both physical and human factors</td>
<td>13</td>
</tr>
<tr>
<td>Threats to network security</td>
<td>14</td>
</tr>
<tr>
<td>Network authentication</td>
<td>15</td>
</tr>
<tr>
<td>External network (Internet) connection</td>
<td>19</td>
</tr>
<tr>
<td>Inter-regional cooperative healthcare network</td>
<td>20</td>
</tr>
<tr>
<td>Effective use of Wireless LAN</td>
<td>21</td>
</tr>
<tr>
<td>Security in Wireless LAN</td>
<td>21</td>
</tr>
<tr>
<td>Install and operation of Wireless LAN</td>
<td>22</td>
</tr>
<tr>
<td>Ease of Operation</td>
<td>23</td>
</tr>
<tr>
<td>Critical issues for network operation</td>
<td>23</td>
</tr>
<tr>
<td>SNMP (Simple Network Management Protocol)</td>
<td>24</td>
</tr>
<tr>
<td>Measures against system failures; device failures, incorrect wiring</td>
<td>24</td>
</tr>
<tr>
<td>Use of SNMP</td>
<td>25</td>
</tr>
<tr>
<td>IPv6</td>
<td>26</td>
</tr>
<tr>
<td>Network Configuration Example</td>
<td>27</td>
</tr>
<tr>
<td>Network configuration for hospitals with fewer than 100 beds</td>
<td>28</td>
</tr>
<tr>
<td>Network configuration for hospitals with more than 100 and fewer than 200 beds</td>
<td>30</td>
</tr>
<tr>
<td>Network configuration for hospitals with more than 200 beds (i)</td>
<td>32</td>
</tr>
<tr>
<td>Network configuration for hospitals with more than 200 beds (ii)</td>
<td>34</td>
</tr>
</tbody>
</table>
At the end of the 20th century, computers and the technology field overall began embracing the idea of being ‘open.’ With this, we saw the development of new interoperable platforms and the advent of more healthcare-focused technologies, such as the computerization of roentgenography, CT, and sonography scanning and x-ray communications tools. At the same time, centralized computer systems downsized and tools such as electronic medical charts began operating on standard software such as Windows and UNIX.

Meanwhile, with the explosive spread of the Internet, hospital networks began standardizing on IP (Internet Protocol) and shifting away from more conventional protocols, such as SNA. It has now become possible for individual hospitals to operate on a single IP network, as the systems have become more convenient and economical. However, as electronic medical charts have become more commonplace, hospital operations have shifted to a paperless environment where all the information is managed as electronic data. This means if the network shuts down, all medical treatment stops.

Furthermore, the network, which is set up across all corners of a hospital, is large-scale and increasingly complex. The global penetration of Windows, UNIX, and IP networks has rendered them more inexpensive, but security issues are now more of a concern.

In keeping with these developments in hospital network administration, this booklet explains important features about hospital network construction based on three key concepts: ‘Non-stop Network,’ ‘Secure and Reliable Network,’ and ‘Ease of Operation.’
**Importance of the network**

Today, hospitals generally conduct business with use of multiple integrated healthcare information systems. However, a network does not exist for each system; rather, it must be designed, constructed, and operated as a single, common infrastructure.

Since a network system failure can lead directly to entire hospital routines and operations coming to a halt, a ‘Non-stop Network’ is one of the most important components within hospital administration.

Meanwhile, as a result of the explosive spread of Internet in the latter half of the 1990’s, previously closed IP networks became more open and inexpensive. This has made the technology more readily available, but at the expense of exposing a variety of security vulnerabilities. As a result, hospital networks dealing with highly personal information are required to design and adopt ‘Safe and Reliable Networks.’

Based on recent advancement in healthcare technology, most networks are expected to be established as regional alliance infrastructures among many hospitals to ensure maximum security and reliability.
Main requirements in designing a healthcare network

Non-stop network

- Network bandwidth and QoS
  Large volumes of image data, such as from CTs and MRIs, are mainly accessed from the radiography section. Additionally, data or applications handled by various medical information systems run via the network. Therefore, it is important to pay attention to bandwidth in order for large volumes of data transmission to be carried out efficiently, quickly, and easily. By using QoS (Quality of Service) practices, it becomes possible to give increased priority to processing the data to minimize delay, even within a limited bandwidth system.

- Redundancy and preventive measures against system failures
  If a hospital network stops suddenly, running applications shut down. Therefore, a network system failure is a serious problem directly linked with system-wide hospital applications such as accounting or medical services. In order to construct a ‘Non-stop Network,’ it is necessary to ensure network device and path redundancy and enhance its reliability. By doing so, it becomes possible to keep network downtime at a minimum in the event of system failure.

Sometimes a problem caused by human error may cause the entire network to shut down. It is also important to take measures to prevent unnecessary trouble, particularly network loops, when constructing a non-stop network.

Secure and reliable network

- Importance of security
  If personal or critical information is leaked or compromised, such as electronic medical charts, it can be very damaging to patients. Together with physical management (such as antitheft devices, limiting access to patients’ rooms) using PCs and the server, the following measures must be taken on the network system:
  - Security measures are based on the proper control of various IT devices. For example, the possibility of computer virus infections must be minimized, since they can be caused by private PCs brought in from outside, unauthorized access via the Internet from outside the network, or even from within the hospital LAN. Therefore, firewall or virus protection is needed for the Internet, and network authentication must be in place to prevent the use of unauthorized PCs for LAN-related problems.
  - When constructing a regional alliance-based healthcare network via the Internet, it is necessary to build a VPN (Virtual Private Network). By doing so, even with access to public networks like the Internet, the virtual tunnel with encrypted communication safely connects all the LAN terminals.

The security measures above are not automatic, but are established as post-installation steps. Following a strict protocol on a daily basis is crucial for their success.

- Effective use of Wireless LAN
  Today, in a hospital that includes patient rooms, the use of Wireless LAN (WLAN) technology is growing as people use laptops and other devices. While WLAN service is an effective way of providing Internet access to inpatients as a hospital amenity, adequate security measures must be taken when implementing an open LAN environment.
Ease of operation

- Early detection and restoration of system failures with the improvement in system functions of operation and control

By constantly monitoring network devices, early detection of a system failure can facilitate a quick recovery. For improvements in operation and control performance, it is highly important to use SNMP (Simple Network Management Protocol).

- Consideration of shift to IPv6-based Network

With the development and the expansion of the Internet over the last few years, the remaining available IP addresses under IPv4 will likely become exhausted. Acquiring a new IPv4 global address is estimated to be even more difficult by 2011. Although IPv4 is the current standard, it is necessary to support two versions of IP to meet the next-generation IP standard, such as IPv6, when selecting network devices.
Network bandwidth and QoS (Quality of Service)
When constructing a network, it is necessary in advance to determine the size of all hospital data communication requirements and data-access frequency, and to take possible staff and patient increases into consideration.

Data capacity
One of the most important aspects of network design is securing enough capacity to support a large volume of data communication during peak periods. Listed below are the main data types and sizes streaming throughout a network. A network design is required to take into account handling large data volumes of data and access frequency.

### Examples of Data Capacity

<table>
<thead>
<tr>
<th>Text data</th>
<th>Image data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receipt, prescription order receipt</td>
<td>MRI</td>
</tr>
<tr>
<td>Tens of kbytes (hundreds of kbits)</td>
<td>Approx. 500kbytes * 100 sheets (400Mbits per one inspection)</td>
</tr>
<tr>
<td>E-mail with a large number of characters</td>
<td>Chest X-ray</td>
</tr>
<tr>
<td>Approx. 20kbytes (160kbits)</td>
<td>Approx. 30Mbytes (one sheet: 240Mbit)</td>
</tr>
<tr>
<td>E-mail with a large number of characters</td>
<td>Echo</td>
</tr>
<tr>
<td>Approx. 20kbytes (160kbits)</td>
<td>Approx. 300kbytes * 10 sheets (24Mbits per one inspection)</td>
</tr>
<tr>
<td>E-mail with a large number of characters</td>
<td>Web (top page of Japan Health, Labor and Welfare Ministry)</td>
</tr>
<tr>
<td>Approx. 20kbytes (160kbits)</td>
<td>Approx. 240kbytes (2Mbits)</td>
</tr>
</tbody>
</table>

Although much depends on the capability of individual PCs and applications, a chest radiograph image normally takes three seconds at 100Mbps and may be received at up to 0.3 seconds in 1Gbps. The impact of bandwidth expansion from 100Mbps to 1Gbps can be dramatic and significant.

In addition, as the above chart indicates, when medical image data like X-rays or MRI flow through 100Mbps-LANs, interference occurs with the other data communication, such as a delay in processing time.
Network bandwidth and cost of LAN devices

The cost of network devices is determined by the selection of 1Gbps or 10Gbps speeds for the main line connecting core and floor switches, or 1Gbps or 100Mbps for the branch line connecting floor and edge switches.

Listed here are the examples of cost comparisons of the entire network system.

Notes: These prices are only for switches and optical modules, not including cables. These prices are calculated based on Allied Telesis standard price.

Condition: Comparisons with actual design for a general hospital with approximately 600 beds
- Core switch redundancy
- Floor switch (6 units)
- Edge switch (20 units) calculated with a switch and AT-SFP/XFP optical module
QoS (Quality of Service)
QoS is a technology giving priority to specific traffic and securing a fixed level of response throughput.

Usually, a switch processes packets in an entry sequence format; when traffic is heavy, delays occur; in the worst case the packet itself is lost or destroyed. With QoS features, priority processing of audio/video traffic is made possible and maximum communications traffic can be controlled to minimize the risk of sound and video traffic delay and packet destruction.

The switch receiving a packet identifies the data and carries out the QoS processing.

QoS processing is classified roughly into priority control and bandwidth control. Priority control processes the high-priority packets first through multiple processing buffers with different levels of priority. Meanwhile, bandwidth control is managed by securing enough bandwidth and by controlling high-traffic data.
Redundancy and proactive measures to overcome network failures

Core switch redundancy

Star topology is commonly adopted for LANs residing inside buildings. Since star topology is constructed based on core switches, it is important to create core-switch redundancy to ensure stable operation without the network shutdown.

Multiple methods exist for redundancy, including making the power supply and management modules redundant inside the chassis, or even the chassis itself redundant.

<table>
<thead>
<tr>
<th>Network Devices Types and Comparison of Redundancy Function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Chassis type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Modular type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Box type</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Comparison of redundancy of communication

Chassis redundancy uses redundant protocols to automatically switch to standby equipment in the event of system failure.

Redundant protocols include not only a standard protocol, but also a vendor-specific protocol which covers the shortcomings of standard protocols. Therefore, we can make decisions that take into account the function, bandwidth, and ease of operation.

**STP (Spanning-Tree Protocol):** When making a path redundant by using several Layer 2 switches on a LAN, STP provides path redundancy while preventing undesirable loops in a network.

<table>
<thead>
<tr>
<th>1. Active/standby configuration</th>
<th>2. Active/standby distributed configuration</th>
<th>3. Stack configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Diagram" /></td>
<td><img src="image2" alt="Diagram" /></td>
<td><img src="image3" alt="Diagram" /></td>
</tr>
</tbody>
</table>

With redundancy configuration by STP or single VLAN, one device stands by and does not operate.

An efficient operation is possible by distributing master/slave switches with VLANs. However, that may make the setting and design more complex.

In stack configuration, load distribution is possible even with a single VLAN configuration. Also, setting and design are very easy. Note: Link aggregation connection between distribution switches.
**Loop protection**

In network operations, a system administrator is most troubled by human errors, yet these mistakes can be alleviated by device functionality.

Common errors arise as desktop PC switches are detached, cables are connected and disconnected on a daily basis based on floor layout changes, and PCs are carried in or out of their original locations.

Examples of desktop-switch failures:
- Cable-related failures (e.g. connector comes out of RJ-45 plug)
- Network device breakdown (e.g. if it gets wet)
- Terminal setting errors, duplication of IP
- Loop failures

Loop failures frequently appear to be human-made, such as an unintentional connection error by users. For example, a loop failure occurred when one hospital staff member inserted an extra LAN cable into the switch. This can lead to larger problems, such as an entire network breakdown. Therefore, some measures have to be taken into account to minimize the effect on the entire system.

Loop-preventive functions such as ‘Loop Guard’ and ‘ForceMDI’ can automatically detect a loop and shut down a port – making it possible to create a loop-preventing design.

---

**Comparison of loop defense functions**

<table>
<thead>
<tr>
<th>Method</th>
<th>Summary</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC address slashing</td>
<td>Detecting frequently changing registered ports with the same MAC address and blocking ports at the time the loop occurs.</td>
<td>High price</td>
</tr>
<tr>
<td>LDF</td>
<td>Determining whether the receiving LDF is a loop; if so, it takes action, such as blocking ports.</td>
<td>Relatively low price</td>
</tr>
<tr>
<td>Rate limit</td>
<td>Presetting the traffic rate; if it receives excessive traffic, it detects a loop and takes action, such as blocking ports.</td>
<td>Relatively low price</td>
</tr>
<tr>
<td>ForceMDI</td>
<td>Force ports to MDI or MDI-X (ForceMDI function); preventing linkup caused by improper cable connections.</td>
<td>Low price</td>
</tr>
</tbody>
</table>
Secure and Reliable Network

Security

Importance of security: both physical and human factors

‘System security’ is normally focused on system-related factors such as firewalls, but physical factors such as locking a server room and password non-disclosure policies are also important.

Security-related accidents often occur in the absence of sufficient security measures. As listed below, this is like leaking water from the lowest point when pouring it into a barrel. Eventually, lack of security measures in any of several factors can lead to serious accidents.

For example, if a PC connected to the network is placed where patients or visitors can come and go, it could lead to serious problems, such as someone using a PC improperly. Additionally, personal information may be compromised if a PC is stolen, so a physical measure like a wire lock is required.

To protect confidential data, certain types of access need to be restricted to authorized users inside the hospital. Additionally, authorized users must strictly follow security rules, such as not disclosing their IDs or passwords to anyone without authorization.

As mentioned above, security is not guaranteed by merely installing a security system. Establishing, communicating, and enforcing proper security rules based on potential and actual risks affecting daily operation is essential.

Examples of security rules:
- Prohibiting personal PCs in the hospital
- Password setting/encryption with e-mail attachment
- Set a password to screen-saver
Threats to network security
As the following diagram shows, unauthorized entry from the outside and malicious internal access may lead to data being falsified, leaked, or lost. Such risks must be understood so security measures can be properly designed, operated, and managed.

From a security standpoint, even if the external network connection (Internet connection) is physically separated from the healthcare information network, both networks can be connected if there are two network interfaces in PCs.

However, separation of two networks is not always entirely safe because there is still a risk of virus infection or the malicious use of external memory devices such as a USB stick. Since there are tradeoffs between convenience and safety in security measures, integrated security must be in place that treats the entire hospital as one integrated network infrastructure.

Apart from a regular Internet connection, there may be connection points outside the network that on occasion are attached to the system, such as those used for medical device maintenance.

All staff members must be trained to recognize the danger of potential hacking and strictly follow security rules.
Network authentication

One of these network security measures is authentication. This is a function that allows authorized personnel only to access information depending upon each person’s access level. Although an authentication application function can restrict access, the danger of tapping via an unauthorized terminal is still a risk. In addition, establishing network authentication eliminates unauthorized terminals (making it impossible to access a network) and improves security.

There are two types of authentication functions for switches:
- Port security function
- Terminal authentication function

Furthermore, when an unauthorized terminal tries to connect to the network, it is possible to notify system administrators through switch log information, SNMP TRAP, and the RADIUS server.

MAC address

This is 6byte (48-bit) address assigned to LAN interfaces or network devices. The first three bytes are assigned by IEEE (The Institute of Electrical and Electronics Engineers) standards, and the latter half of the three bytes are assigned by each manufacturer to avoid duplication. This address uniquely identifies each node on a network and corresponds with Layer 2, the data link layer of the OSI Reference Model. A MAC address is different from a Layer 3 IP address, and is a unique address for each device. It is also known as a ‘hardware address’.

RADIUS (Remote Authentication Dial in User Service)

RADIUS is a networking protocol providing centralized authentication, authorization, and accounting (tracking consumption of network resources by users) management for computers to connect and use network services. Originally, it was developed for user authentication of a remote connection through a dial-up connection, but now, it is widely used as a general authentication protocol in wired and Wireless LANs. Radius protocol is defined in IETF (Internet Engineering Task Force), RFC (Request for Comments) 2865.

IEEE 802.1x

IEEE 802.1x is an IEEE standard for port-based network access control and is part of the IEEE 802.1 working group (higher-layer LAN protocols) of networking protocols. It provides an authentication mechanism for network terminals, and is becoming more widely used as both wired and wireless network authentications and for managing a ‘quarantined’ network.

<table>
<thead>
<tr>
<th>Comparison of Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
</tr>
<tr>
<td>Port security</td>
</tr>
<tr>
<td>Terminal authentication</td>
</tr>
</tbody>
</table>
**Port security function**

Even a relatively low-cost switch can provide port security functions, so the security system can be enforced inexpensively. In cases where terminals are added or transferred, it is necessary to change settings.

**Terminal authentication function**

Different from port security, an authentication process is established using RADIUS, not by the unit itself. This provides ease-of-operation, such as not having to change authentication devices settings even if terminals are added or transferred. In addition, a recent product provides three authentication methods within one authentication switch. It allows an authentication network to be constructed more flexibly.

---

### Comparison of Authentication Method

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Summary</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.1x</td>
<td>Authenticate with use of a client supported IEEE 802.1x. It can authenticate by both user account and certificate.</td>
<td>Some older OSs need other client software.</td>
</tr>
<tr>
<td>MAC</td>
<td>Authentication with use of a terminal MAC address.</td>
<td>Even printers and complex devices are available.</td>
</tr>
<tr>
<td>Web</td>
<td>Authenticate users by a Web browser.</td>
<td>Since any terminals with a browser are available, it can authenticate regardless of OSs.</td>
</tr>
</tbody>
</table>
**VLAN**

VLAN is a function to divide a LAN virtually into multiple networks. In many cases, one VLAN represents one user group. With restricting communication between VLANs, it can ensure a constant level of security between intergroup communications. Generally, VLAN is classified according to a switch port, and when a terminal is transferred, it becomes necessary to change the switch setting.
**Dynamic VLAN**
As laptops become more common, there is increased demand to access data on the same VLAN from different places, rather than from a fixed location. Dynamic VLAN has a function to dynamically assign VLAN to a PC with a link to an authentication function based on MAC addresses and user IDs. This enables users to participate in the original VLAN group regardless of their physical locations. In addition, even if a PC is moved, it is not necessary to change switch settings.

**Multiple dynamic VLAN**
The switch supports multiple dynamic VLAN, which can assign different VLANs to each user using one physical port. This function enables integration of authentication switches into one unit and is inexpensively configured with edge switches.
The chart below compares authentication costs using edge switches and integrated authentication switches with multiple dynamic VLAN function.

**Condition:**
- 200 units of authentication terminals
- 20 units of edge switches

### Authentication Costs

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Type and number of switches</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>By an edge switch</td>
<td>1 unit of floor switch; 20 units of edge switches are integrated 20 units of authentication edge switches</td>
<td>Approx. $27,000</td>
</tr>
<tr>
<td>By one integrated authentication switch</td>
<td>1 unit of authentication floor switch; 20 units of edge switches are integrated 20 units of authentication packet transmission edge switches</td>
<td>Approx. $13,500</td>
</tr>
</tbody>
</table>

**External network (Internet) connection**

An Internet-accessible environment is always exposed to external threats. Therefore, unauthorized access from the outside must be restricted by all possible means. Since the use of P2P software like ‘Winny’ could be the cause of an information leak, traffic from within must also be monitored.

### Comparison of Main Security Devices

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Summary</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall/Intrusion Detection System (IDS)</td>
<td>Packet filtering, monitoring of session state.</td>
<td>Protection from outside attacks and detection of hackers (the most common measure).</td>
</tr>
<tr>
<td>Intrusion Prevention System (IPS)</td>
<td>It is possible to prevent attacks targeting an OS weakness, by checking the communicating information in the upper layer</td>
<td>Detection and blocking of P2P traffic, such as ‘Winny’ and ‘Share.’</td>
</tr>
<tr>
<td>Unified Threat Management (UTM)</td>
<td>An all-inclusive security product with multiple security functions: firewall, antivirus, intrusion detection, and anti-spam.</td>
<td>Integrated, low-cost security for small and medium-sized companies.</td>
</tr>
</tbody>
</table>
Inter-regional cooperative healthcare network

In recent years, medical technology advancement has caused shortages of medical specialists. Consequently, a regional center hospital and other hospitals/clinics in the region must cooperate at higher levels, as healthcare organizations are becoming more differentiated. In order to ensure and support cooperation among regional hospitals, including medical services, the use of a network in a regional center hospital as the network core is required. Some networks use Internet-type public services because of economic reasons; in these cases, additional security measures are required beyond general external connections.

In keeping with this, VPN is becoming more commonplace as a network that safely connects with the outside virtual world. There are two primary VPN connection methods: IPSec and SSL.

**VPN (Virtual Private Network):** This technology enables connection of specific points safely through a virtual encrypted tunnel on a public network like the Internet, using cryptographic technology. VPN provides a connection between multiple LANs or remote access to a LAN from an external terminal.

<table>
<thead>
<tr>
<th>Comparison of VPN Functions</th>
<th>IPSec VPN</th>
<th>SSL VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation and control</strong></td>
<td>It is necessary to buy devices and VPN software and to change the setting every time a new hospital joins the network.</td>
<td>This makes management easier since there is no need to add a device or change settings each time a new hospital is added.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Secure communication is ensured via VPN.</td>
<td>Secure communication is ensured via VPN.</td>
</tr>
<tr>
<td><strong>Others</strong></td>
<td>- Since there are many relatively inexpensive products, lower-cost configuration is possible if there are a few bases - Two-way communication is possible - In many cases, this function is mounted on firewall or routers</td>
<td>- The initial installation cost is high - Basically, it is one-way communication - Authentication function for connection availability based on a client’s security status (Security patch, OS, etc.)</td>
</tr>
</tbody>
</table>
Effective use of Wireless LAN
As laptop and handheld terminal use has increased with the increasingly widespread use of electronic medical charts, Wireless LANs are becoming more commonplace in hospitals. Wireless LANs have made it easier for hospitals to provide Internet access to patients as an amenity. As long as Wireless LAN access points support dynamic VLAN, it is possible to activate several networks using a single wireless access point.

Security in Wireless LAN
As Wireless LANs establish transmission with electrical wave impulses, without cables, it raises the risk of hacking and interception by a third party. For this reason, encryption and authentication are essential for establishing wireless connections between wireless terminals and access points.

As far as encryption schemes used at original wireless points are concerned, ‘WEP’ was the standard and considered mainstream, but it has lately become regarded as less secure due to vulnerability and security issues caused by malicious third parties deciphering codes.

Today’s wireless access points support ‘WPA2’ that uses a robust encryption scheme (AES: Advanced Encryption Standard) to reduce vulnerability. In addition, by integrating an IEEE 802.1x authentication function, secure wireless networks are more easily constructed.
Install and operation of Wireless LAN
When a Wireless LAN device is installed and established, it is necessary to take into account radio-wave interference, and ease of control and operation for a large quantity of wireless access points as well as security.

If radio-wave interference occurs, it may delay transmission or cause errors. With proper access channel design and construction, radio-wave interferences can be prevented. But if there are a large number of wireless access points, it becomes more necessary to prevent radio-wave interferences due to the number of available channels.

Preliminary research before setting of wireless access point:
- Install a trial wireless access point, then check its terminal communication condition.
- Confirm the setup position of a wireless access point using a site-survey tool.

Functions contained in wireless access points:
- Interference avoidance by automatic channel management function of a wireless access point.
- Interference avoidance by using a Wireless LAN switch system.

It is possible to construct a secure Wireless LAN network by conducting preliminary research on its communication condition and installation environment, including the use of wireless device functions.
Ease of Operation

Critical issues for network operation
Maintaining stable, uninterrupted operation is essential for network infrastructures.

Therefore, it is necessary to consider network configuration, wiring design, device setting, and overall network environment improvements at all times to be able to respond to unexpected failures and interruptions.

- Secure the space for network device setting
- Check power supplies
- Check wiring connection
- Keep terminal and network device well-organized

If the cable is connected to the unused port, all communication can be potentially wiretapped because of shared hub use. In addition, performance issues can be a concern.

There is a possibility of loop failure by incorrect wiring connections due to loose cable management.

With devices not placed on a rack, the switch is inconveniently located and difficult to replace. In addition, it can be affected by heat and insufficient exhaust space.

With only one core switch, the entire hospital network operation is dependent upon its operation, and might break down in the case of failure.
SNMP (Simple Network Management Protocol)

Measures against system failures; device failures, incorrect wiring

If network monitoring cannot be conducted, such as by using non-SNMP-compliant products, administrators must check PCs, cables, and LAN switches individually when terminal users report connection errors. This causes problem resolution to take significantly longer, especially when there are numerous hospital floors covering a large area. SNMP significantly helps alleviate this problem.

SNMP (Simple Network Management Protocol): This is a protocol for network control and management, such as controlling configuration, performance, and fault monitoring.

This is a standardized protocol as defined in RFC (Request for Comments) 1157 of IETF (Internet Engineering Task Force).
Use of SNMP
To ensure stable network system operation, early detection of unusual activities and prompt response is essential. In a hospital, there are many devices connected to the network throughout the infrastructure, including hospital terminals, servers, and printers. In the case of device failure, measures should be taken immediately to minimize any impact on the system. Quick recovery efforts nearly always shorten system down-time.

In network operation and management, it is important to constantly monitor network device conditions, such as performance and communication; this makes it possible to detect failures and conduct recovery work at early stages. In order to constantly monitor network devices, each device needs to correspond to an SNMP function. Additionally, intensive remote monitoring and control is accomplished using SNMP-compatible devices in conjunction with network-monitoring servers.

SNMP Compatible Devices

<table>
<thead>
<tr>
<th>Type</th>
<th>Compatibility</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network device (intelligent)</td>
<td>Yes</td>
<td>Layer 3 switch, router, firewall are compatible.</td>
</tr>
<tr>
<td>Network device (non-intelligent)</td>
<td>No</td>
<td>Low-cost edge switch (dumb switch) is incompatible.</td>
</tr>
<tr>
<td>PC, server, printer, UPS</td>
<td>Yes</td>
<td>Windows system is compatible with installation of SNMP service program.</td>
</tr>
</tbody>
</table>

* Some inexpensive printers or UPS are incompatible

Network monitoring and control

This displays network composition clearly in the network tree/map so that failure points can be checked visually. It allows recovery actions to take place at early stages.
- Condition monitoring with Ping and SNMP
- Device error alerts with icons changing colors
- Optional automatic e-mailing to administrators control

Statistical information can be checked and displayed as graphs.
- SNMP MIB information device display
- Packet and error count, MAC table display

Display device conditions in colors.

Each device can be controlled in detail. When clicking on a device displayed in the network map or tree, the device front panel activates as a GUI to allow intuitive control.
IPv6
As a result of IPv4 addresses becoming exhausted, there is growing interest in a shift to IPv6. Carriers already support IPv6 in their new service offerings, and Windows Vista and Windows 7 also supports it as a standard.

For now, IPv4 is still the mainstream in a LAN, however, in creating and constructing new networks it’s necessary to consider IPv6 compatibility and support.

One of the greatest advantages of IPv6 is ease of management. Since IP addresses are automatically generated from MAC address on PCs in the network, it reduces an administrator’s burden in assigning IP addresses without having to use a DHCP server.

When shifting to IPv6 from IPv4, especially in environments where there are many terminals such as PCs and medical devices, it is better to install a dual-stack switch supporting both IPv4 and IPv6. Then a gradual shift to IPv6 can take place.
Based on the points noted previously, listed below are some examples of network configuration by hospital scale.

### Sample Requirements in Network Composition

<table>
<thead>
<tr>
<th>Hospitals with fewer than 100 beds</th>
<th>Hospitals with more than 100 and fewer than 200 beds</th>
<th>Hospitals with more than 200 beds (i)</th>
<th>Hospitals with more than 200 beds (ii)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration 1</strong></td>
<td><strong>Configuration 2</strong></td>
<td><strong>Configuration 3</strong></td>
<td><strong>Configuration 4</strong></td>
</tr>
<tr>
<td>Functions to be used</td>
<td>Functions to be used</td>
<td>Functions to be used</td>
<td>Functions to be used</td>
</tr>
<tr>
<td>- Layer 3 routing</td>
<td>- Layer 3 routing</td>
<td>- Layer 3 routing</td>
<td>- Layer 3 routing</td>
</tr>
<tr>
<td>- Network monitoring (SNMP)</td>
<td>- VLAN</td>
<td>- VLAN</td>
<td>- VLAN</td>
</tr>
<tr>
<td>- Core switch redundancy</td>
<td>- Core switch redundancy</td>
<td>- IEEE 802.1x MAC authentication</td>
<td>- IEEE 802.1x MAC authentication</td>
</tr>
<tr>
<td>- Network monitoring (SNMP)</td>
<td>- Network monitoring (SNMP)</td>
<td>- Network monitoring (SNMP)</td>
<td>- Network monitoring (SNMP)</td>
</tr>
<tr>
<td>Regional medical care cooperation</td>
<td>n/a</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Service for patients using network</td>
<td>n/a</td>
<td>Internet access service for inpatients</td>
<td>Internet access service for inpatients</td>
</tr>
<tr>
<td>Communication bandwidth</td>
<td>Communication bandwidth</td>
<td>Communication bandwidth</td>
<td>Communication bandwidth</td>
</tr>
<tr>
<td>(Wired part)</td>
<td>High-speed (1 Gbps)</td>
<td>High-speed (1 Gbps)</td>
<td>High-speed (1 Gbps)</td>
</tr>
<tr>
<td>Price (LAN device)</td>
<td>Approx. $40,000</td>
<td>Approx. $100,000</td>
<td>Approx. $270,000</td>
</tr>
<tr>
<td>Expandability</td>
<td>Backbone speed can be easily increased by adding modules to core switches. Modules can be compatible for optical fiber.</td>
<td>Internet access service in a hospital ward is possible based on high-capacity communication bandwidth on each floor.</td>
<td>It is easy to expand communication ports by adopting a high-capacity ports-configurable device as a core switch. (A single unit is expandable up to 96 ports.)</td>
</tr>
</tbody>
</table>

**Key points in selection**

- In terms of cost, it can back up communications devices without duplicating wiring and devices.
- By using Gigabit Ethernet for all the wired networks (not including wireless), network stability is secured.

- It ensures redundancy of core switches and optically duplicates the backbone.
- By using Gigabit Ethernet for all the wired networks (not including wireless), network stability is secured.

- It ensures network stability and security at a high level, including core switch and backbone duplication, providing broadband access and employing network authentication.
- The firewall supports UTM* functions in order to meet various Internet threats.
  *UTM: antivirus, anti SPAM, web filtering, attack detection and prevention

- It ensures stability and security of network at a high level, including inside the core switch redundancy, providing broadband access, and employing network authentication.
- The firewall is compatible for UTM* functions in order to meet various Internet threats.
  *UTM: antivirus, anti SPAM, web filtering, attack detection and prevention

- It is easy to expand communication ports by adopting a high-capacity ports-configurable device as a core switch.
- (A single unit is expandable up to 192 ports.)
Network configuration for hospitals with fewer than 100 beds

Requirements:
- Create a high-speed Gigabit (1Gbps) network (except wireless parts)
- Allow network connection from every room in a hospital
- Use a Wireless LAN in a hospital ward to allow doctors and nurses to access internal hospital information systems regardless of their location
- Secure, economical efficiency and ease-of-operation

Conditions:
- Number of departments: 5
- Number of beds: 50
- Number of PCs: 50
- Number of medical inspection devices: 5
- Servers: 5 (total)

*Desktop switches are not included in this composition
Hospitals with fewer than 100 beds

Points for network design

- **Gigabit network**
  All wired parts in the LAN, from core to desktop switches, are secured by Gigabit bandwidth (1 Gbps).

- **Network using Layer 3 switch**
  A network can be logically segmented by each section using Layer 3 switches, such as accounting and reception, medical care, to keep data properly compartmentalized and prevent unnecessary data from other sections affecting specific areas. In addition, by adding VLAN, network configuration can be managed easily and flexibly in case of future growth and/or subdivision of departments within a hospital.

- **Wireless LAN used in a hospital ward**
  In a hospital ward, a 24-hour response is required for patients. Therefore, doctors and nurses need to be able to wirelessly connect to read charts and update patient information. (This configuration uses PoE (Power over Ethernet) enabled switches that allow electrical power to be transferred to wireless access points, and eliminates the need for the power supply construction.)

- **Early detection of failures and recovery work through network monitoring**
  Since each network device supports SNMP, it is possible to remotely check individual device communication and condition using network monitoring software (SwimSuite). This way, even if failure occurs, the fault point and communication levels can be visually confirmed, enabling early detection and quick recovery. In addition, since communications ports can be also monitored, unauthorized connections are easily detected. This means network monitoring functions are used effectively not just for quick recovery, but also for security.

- **Inexpensive and secure network**
  In order to save costs, backup devices can substitute for devices duplication.
  To simplify ease of operation, each floor switch is unified and related to a product of the same series. Additionally, each floor’s switch settings are saved to backup devices to enable fast response and minimized network downtime in the event of a system failure.
Network configuration for hospitals with more than 100 and fewer than 200 beds

Requirements:
- Create high-speed Gigabit (1Gbps) network
- Allow network connection from every room in a hospital
- Use a Wireless LAN in a hospital ward to allow doctors or nurses to access internal hospital information systems regardless of their location
- Minimize network downtime caused by circuit error and device failure

Conditions:
- Number of departments: 7
- Number of beds: 150
- Number of PCs: 180
- Number of medical inspection devices: 10
- Servers: 8 (total)

*Desktop switches are not included in this composition*
Hospitals with more than 100 and fewer than 200 beds

Points for network design

- **Gigabit network**
  All wired parts in the LAN, from core to desktop switches, are secured by Gigabit bandwidth (1 Gbps).

- **Network by using Layer 3 switch**
  A network can be logically segmented by each section using Layer 3 switches, such as accounting and reception, medical care, to keep data properly compartmentalized and prevent unnecessary data from other sections affecting specific areas. In addition, by adding VLAN, network configuration can be managed easily and flexibly in case of future growth and/or subdivision of departments within a hospital.

- **Wireless LAN used in a hospital ward**
  In a hospital ward, a 24-hour response is required for patients. Therefore, doctors and nurses need to be able to wirelessly connect to read charts and update patient information. (This configuration uses PoE (Power over Ethernet) enabled switches that allow electrical power to be transferred to wireless access points, and eliminates the need for the power supply construction.)

- **Early detection of failures and recovery work through network monitoring**
  Since each network device supports SNMP, it is possible to remotely check individual device communication and condition using network monitoring software (SwimSuite). This way, even if failure occurs, the fault point and communication levels can be visually confirmed, enabling early detection and quick recovery. In addition, since communications ports can also be monitored, unauthorized connections are easily detected. This means network monitoring functions are used effectively not just for quick recovery, but also for security.

- **Core switch and backbone duplication**
  Uninterrupted network operation inside a hospital can be ensured by using redundant core switches (VCS: Virtual Chassis Stacking), even if an accident occurs in any one of the core switches. With dual cable wiring between core switches and floors, or between core switches and important medical practice points, even if a cable breaks, communication can be ensured with the one remaining cable. This path duplication is important in areas such as medical examination rooms, reception, or accounting where electric chart system shutdown would be catastrophic. Additionally, this configuration is very economical since these two duplicated paths are commonly available at the same time.
Network configuration for hospitals with more than 200 beds (i)

Requirements:
- Create high-speed Gigabit (1Gbps) network
- Operate as the core of a hospital in regional healthcare, and share healthcare information with other regional healthcare facilities
- Allow network connection from every room in a hospital
- Provide Internet connection service to hospital wards or open spaces to patients
- Authenticate network by using RADIUS server (IEEE 802.1x, MAC authentication)

Conditions:
- Number of departments 15
- Number of beds 350
- Number of PCs 450
- Number of medical inspection devices 30
- Servers 15 (total)

*Desktop switches are not included in this composition
Hospitals with more than 200 beds (i)

Points for network design

- **Gigabit network**
  All wired parts in the LAN, from core to desktop switches, are secured by Gigabit bandwidth (1Gbps).

- **Network by using Layer 3 switch**
  A network can be logically segmented by each section using Layer 3 switches, such as accounting and reception, medical care, to keep data properly compartmentalized and prevent unnecessary data from other sections affecting specific areas. In addition, by adding VLAN, network configuration can be managed easily and flexibly in case of future growth and/or subdivision of departments within a hospital.

- **Wireless LAN used in a hospital ward**
  In a hospital ward, a 24-hour response is required for patients. Therefore, doctors and nurses need to be able to wirelessly connect to read charts and update patient information. (This configuration uses PoE (Power over Ethernet) enabled switches that allow electrical power to be transferred to wireless access points, and eliminates the need for the power supply construction.)

- **Early detection of failures and recovery work through network monitoring**
  Since each network device supports SNMP, it is possible to remotely check individual device communication and condition using network monitoring software (SwimSuite). This way, even if failure occurs, the fault point and communication levels can be visually confirmed, enabling early detection and quick recovery. In addition, since communications ports can also be monitored, unauthorized connections are easily detected. This means network monitoring functions are used effectively not just for quick recovery, but also for security.

- **Network by using VPN**
  A regional healthcare network must be designed with the expectation of an increase in access points. By using a high-performance firewall, it becomes possible to establish 250 IPSec VPN connection available points.

- **Internet access service for patients**
  Information leaks and virus infections to the internal information system are prevented by preventing patients access to the internal network. Moreover, in view of user privacy, using a multiple VLAN function prevents direct communication among patients.

- **Network connection by using an authentication function**
  By the setting of a user ID and a password for access to a network, public (non-hospital staff) access can be blocked. Switches at each floor that support IEEE 802.1x or MAC authentication are used, and PCs or printers are connected to information sockets available in each room. Input of an ID and a password on PCs is required by a switch using the IEEE 802.1x function. Then, after the ID and the password are authenticated by RADIUS server, the switch opens a port to allow connection with the internal hospital information system. As for a device which cannot input an ID and password, such as a printer, the access to the internal network is controlled by MAC authentication. Thus, network security is ensured by preventing unauthorized terminals from accessing the internal network.

- **Core switch and backbone duplication**
  Uninterrupted network operation inside a hospital can be ensured by using redundant core switches (VCS: Virtual Chassis Stacking), even if an accident occurs in any one of the core switches. With dual cable wiring between core switches and floors, or between core switches and important medical practice points, even if a cable breaks, communication can be ensured with the one remaining cable. This path duplication is important in areas such as medical examination rooms, reception, or accounting where electric chart system shutdown would be catastrophic. Additionally, this configuration is very economical since these two duplicated paths are commonly available at the same time. Furthermore, distinguished from the second configuration using box switches as stated on page 31, modular switches are used in this configuration since numerous ports can be configured in the modular switch—enabling economical operation and network expandability.
Network configuration for hospitals with more than 200 Beds (ii)

Requirements:
- Create high-speed Gigabit (1Gbps) network
- Operate as the core of a hospital in regional healthcare, and share healthcare information with other regional healthcare facilities
- Allow network connection from every room in a hospital
- Provide Internet connection service to hospital wards or open spaces to patients
- Authenticate network by using RADIUS server (IEEE 802.1x, MAC authentication)

Conditions:
- Number of departments: 15
- Number of beds: 350
- Number of PCs: 450
- Number of medical inspection devices: 30
- Servers: 15 (total)

*Desktop switches are not included in this composition*
Hospitals with more than 200 beds (ii)
Points for network design

- **Gigabit network**
  All wired parts in the LAN, from core to desktop switches, are secured by Gigabit bandwidth (1 Gbps).

- **Network by using Layer 3 switch**
  A network can be logically segmented by each section using Layer 3 switches, such as accounting and reception, medical care, to keep data properly compartmentalized and prevent unnecessary data from other sections affecting specific areas. In addition, by adding VLAN, network configuration can be managed easily and flexibly in case of future growth and/or subdivision of departments within a hospital.

- **Wireless LAN used in a hospital ward**
  In a hospital ward, a 24-hour response is required for patients. Therefore, doctors and nurses need to be able to wirelessly connect to read charts and update patient information. (This configuration uses PoE (Power over Ethernet) enabled switches that allow electrical power to be transferred to wireless access points, and eliminates the need for the power supply construction.)

- **Early detection of failures and recovery work through network monitoring**
  Since each network device supports SNMP, it is possible to remotely check individual device communication and condition using network monitoring software (SwimSuite). This way, even if failure occurs, the fault point and communication levels can be visually confirmed, enabling early detection and quick recovery. In addition, since communications ports can also be monitored, unauthorized connections are easily detected. This means network monitoring functions are used effectively not just for quick recovery, but also for security.

- **Network by using VPN**
  A regional healthcare network must be designed with the expectation of an increase in access points. By using a high-performance firewall, it becomes possible to establish 250 IPSec VPN connection available points.

- **Internet access service for patients**
  Information leaks and virus infections to the internal information system are prevented by preventing patients access to the internal network. Moreover, in view of user privacy, using a multiple VLAN function prevents direct communication among patients.

- **Network connection by using an authentication function**
  By the setting of a user ID and a password for access to a network, public (non-hospital staff) access can be blocked. Switches at each floor that support IEEE 802.1x or MAC authentication are used, and PCs or printers are connected to information sockets available in each room. Input of an ID and a password on PCs is required by a switch using the IEEE 802.1x function. Then, after the ID and the password are authenticated by RADIUS server, the switch opens a port to allow connection with the internal hospital information system. As for a device which cannot input an ID and password, such as a printer, the access to the internal network is controlled by MAC authentication. Thus, network security is ensured by preventing unauthorized terminals from accessing the internal network.

- **Core switch and backbone duplication**
  By installing two unit functions (modules) into one unit, a core switch can increase its own availability and achieve stronger stability. With inside the unit redundancy, the connection between modules is duplicated to ensure an alternate path. This also allows high-speed switching in circuit resistance time (designed target level: 1 second) using real-time hardware conditions. In addition, all power supplies and fans can be duplicated. As a redundancy between core and floor switches, link aggregation helps to achieve high-speed switching.