Hotel Technology
next generation™

Hotel Property
Gateway Specification

Version 1.1

1 May 2013

Infrastructure & Device Forum

Infrastructure Resource Team

About HTNG

Hotel Technology Next Generation (HTNG) is a non-profit association with a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable hoteliers and their technology vendors to do business globally in the 21st century; to be recognized as a leading voice of the global hotel community, articulating the technology requirements of hotel companies of all sizes to the vendor community; and to facilitate the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hotels, and create a healthy ecosystem of technology suppliers.

Manufacturers and software providers shall not claim compliance with portions of the requirements of any HTNG specification or standard, and shall not use the HTNG name or the name of the specification or standard in any statements about their respective product(s) unless the product(s) is (are) certified as compliant to the specification or standard.

Permission is granted for implementers to use the names, labels, etc. contained within the specification. The intent of publication of the specification is to encourage implementations of the specification.

This specification has not been verified for avoidance of possible third-party proprietary rights. In implementing this specification, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed. Visit http://htng.org/ip-claims to view third-party claims that have been disclosed to HTNG. HTNG offers no opinion as to whether claims listed on this site may apply to portions of this specification.

The names Hotel Technology Next Generation and HTNG, and logos depicting these names, are trademarks of Hotel Technology Next Generation. Permission is granted for implementers to use the aforementioned names in technical documentation for the purpose of acknowledging the copyright and including the notice required above. All other use of the aforementioned names and logos requires the permission of Hotel Technology Next Generation, either in written form or as explicitly permitted for the organization’s members through the current terms and conditions of membership.

Table of Contents

1 Document History

Version	Date	Author	Comments
V0.36	2/10/2011	Team members	Initial Draft
V0.37	3/28/2011	Steve Berrey	Second major update
V0.38	4/12/2011	Jon Buenviaje	Reviewed and updated sections A1.1 to A4.2
V0.39	4/25/2011	Steve Berrey	Reviewed section A4.2 to A.# and updated and formatted contents
V0.40	4/26/2011	Team members	Reviewed 4.2 to 7.2 and made updates to each feature requirement
V0.41	5/10/2011	Team Members	Reviewed 7.2 to 16.1 and made updates to each feature requirement
V0.42	5/24/2011	Jon Buenviaje	Minor formatting and accepted changes
V0.43	6/7/2011	Team Members	Determined configurations from A1.1-A2.1
V0.44	6/30/2011	Team Members	Determined configurations from A2.1-A5.2
V0.45	7/13/2011	Team Members	Accepted changes and minor formatting
V0.46	7/19/2011	Richard Wagner	Updated A3.1 and general minor edits
V0.47	8/3/2011	Jon Buenviaje	Minor edits – accepted minor changes and deleted unnecessary comments
V0.48	8/12/2011	Team Members	Determined configurations from A5.2-A9.1
V0.49	8/26/2011	Team Members	Determined configurations from A6.1 and A-A9.1-A12.2
V0.50	9/2/2011	Team Members	Determined configurations from A12.2 – A15.1
V0.51	9/15/2011	Team Members	Updated Additional Information Section
V0.52	9/16/2011	Team Members	Reordered Feature Numbering Scheme
V0.53	10/20/2011	Carl Schlack	Added ISO Standards for Languages
V0.54	11/29/2011	HTNG	Comments noted in document for clarification
V0.55	05/15/2012	HTNG	Repositioned into best practice. Edited ability to be enabled/disabled on all features.
V0.56	07/27/2012	Team Members, Kylene Reese	Addressed feedback from HTNG management, Updated and formatted document
V0.57	07/30/2012	Kylene Reese	Updated terms and formatted document
V0.58	07/31/2012	Dick Wagner Greg Dawes	Added references, updated headings
V0.59	08/07/2012	Kylene Reese	Prepared document for Team review
V0.60	08/21/2012	Kylene Reese	Prepared for Team vote
V1.0	09/04/2012	Team Members	Version 1.0 Advanced Gateway Specification
V1.1	01/07/2013	Dick Wagner	Version 1.1 Combined Advanced and Basic Gateway
V1.11	03/13/2013	HTNG	Minor Edits – accepted minor changes and deleted unnecessary comments

2 Document Information

Document Purpose

The purpose of this document is to provide a best practice for implementation of a Hotel Property Gateway (HPG). Unlike existing high speed internet gateways that are currently being utilized for controlling and billing guest Internet access, the HPG is intended to provide a multitude of services and features for both guests and Hotel Staff. In addition, since smaller properties do not generally require all of the features required by a large hotel, the best practices for either a large hotel (hereafter referred to as advanced) or a small hotel (hereafter referred to as basic) are further defined.

Therefore, the intent of providing this best practice is to allow gateway vendors to develop products that can be deployed for use on hotel properties.

This best practice was developed by the HTNG Infrastructure Resource Team.

Scope

The scope of this document includes, directly or by reference, all information required to develop an HPG as described above. It does not include information needed to implement any other HTNG specifications. However, it should be noted that the information provided in this document is intended to support applications and products that utilize other HTNG specifications and that will also utilize the HPG.

Audience

The intended audience of this document includes developers of guest-facing high speed Internet gateways as well as hoteliers who are trying to acquire an HPG. In addition, the audience of this document could also be extended to vendors of gateway-like products that are not currently being deployed in the hospitality industry.

Document Terms

For the purpose of this document, the following terms have been defined:

Term	Definition
Access Control List (ACL)	A list of addresses in a firewall or router that is used to control inbound and outbound access. The ACL can be used to allow or deny access.
Active Directory	A technology created by Microsoft, based on Novell Directory and using modified versions of existing protocols and services, that provides a variety of network services.
Bandwidth Profile	A definition of the amount of bandwidth that needs to be assigned to a guest, controlling the maximum rate at which traffic can be sent and received on the WAN by that guest. The specific profile could be selected by a guest responding to a Splash Page indicating which profiles are available at the hotel.
Client Device	A device that connects to a network. Example client devices could include PCs, PDAs and smartphones.
Cyclic Redundancy Check (CRC)	A hash function designed to detect changes to raw computer data. A CRC is normally performed to guarantee that the data in question has not been changed or modified during storage or transmission. The detection of a CRC error indicates that the data has been

	modified or changed.
Domain Name System (DNS)	A hierarchical naming system built on a distributed database for computers, services or any resource connected to the Internet or a private network (Please refer to the following RFCs: 1035,1123, 2181).
Dynamic Host Configuration Protocol (DHCP)	A network protocol that is used to configure network devices so that they can communicate on an IP network (see Additional Information: Network Features) (Please refer to RFC 2131).
Dynamic Host Configuration Protocol (DHCP) Relay	An agent that routes a DHCP request to an external / remote DHCP server IP address. (Please refer to RFC 3046).
E-mail Relay Server	Server that provides a hotel user with the ability to relay e-mail messages (Simple Mail Transfer Protocol (SMTP)) from the user's client to e-mail servers outside the hotel.
File Transfer Protocol (FTP)	A standard network protocol used to transfer files from one host to another host over a TCP-based network (Please refer to RFC 959).
Firewall	Controls the incoming and outgoing network traffic by analyzing the data packets and based on a set of rules, determines whether it should be allowed through or not.
Graphical User Interface (GUI)	A type of user interface that allows users to interact with electronic devices using images rather than text commands.
Guest Access Code	The Guest Access Code (sometimes referred to as a conference code) is a code supplied by the property to the guest to allow the guest to access the High Speed Internet Access at a hotel. The Guest Access Code is typically provided to a guest in order for the guest to access the internet without purchasing the service from the hotel.
High Speed Internet Access (HSIA)	Broadband Internet access from the hotel.
Hotel Property Gateway (HPG)	HPG refers to this document, a best practice for implementation of a Hotel Property Gateway. The HPG is intended to provide a multitude of services and features for both guests and Hotel Staff.
Hotel Staff	Hotel employees.
Hypertext markup language (HTML)	(Please refer to RFC 1866.)
Hypertext Transfer Protocol Secure (HTTPS)	Encrypts web communications carried over HTTP. (Please refer to RFC 2660.)
Inbound	Typically refers to IP data that is entering the gateway from outside of the property.
Internet Protocol Security (IPSec)	A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. (Please refer to the following RFCs: 2401, 2412.)
Internet Protocol Television (IPTV)	A system through which television services are delivered using the Internet protocol suite over a packet-switched network.
Internet Protocol Version 4 (IPV4)	The fourth revision in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. (Please refer to RFC 791.)
Internet Protocol Version 6 (IPV6)	Internet Protocol that is designed to succeed IPV4. (Please refer to RFC 2460.)

Intrusion Detection System (IDS)	A device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station.
Layer 2 Tunneling Protocol (L2TP)	A tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs.
Lightweight Directory Access Protocol (LDAP)	An application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. (Please refer to the following RFCs: 2661, 3931.)
Local Area Network (LAN)	A computer network that interconnects computers in a limited area.
Management Information Base (MIB)	A virtual database used for managing the entities in a communications network.
Network Access Control (NAC)	An approach to computer network security that attempts to unify endpoint security technology, user or system authentication and network security enforcement.
Network Address Translation (NAT)	Translates a specific address from one subnet to another. Usually used for security reasons to hide private addresses from public addresses. (Please refer to RFC 2663.)
Network Time Protocol (NTP)	A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. (Please refer to RFC 5905.)
Outbound	Typically refers to IP data that is exiting the gateway.
Point-to-Point Tunneling Protocol (PPTP)	A method for implementing virtual private networks. (Please refer to RFC 2637.)
Port Address Translation (PAT)	Translates a specific address from one subnet to a single address that is shared by other translated addresses. Usually used for security to hide private addresses from public addresses. (Please refer to RFC 2663.)
Property Management System (PMS)	The system that manages guests and rooms at a hotel, including the tracking and settlement of guest charges.
Remote Authentication Dial-In User Service (RADIUS)	A networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. (see Additional Information: Authentication) (Please refer to the following RFCs: 2865, 2866.)
Roaming Rules	The definition of roaming rights for users and devices across the various hotel wired and wireless zones (i.e., guest rooms, conference space, public space).
Secure Sockets Layer (SSL)	Cryptographic protocols that provide communication security over the Internet. (Please refer to RFC 5246.)
Simple Network Management Protocol (SNMP)	An Internet-standard protocol for managing devices on IP networks. (Please refer to the following RFCs: 1155, 1157, 1213, 1441, 1442.)
Splash Page	Configurable Web page that is used to display terms, conditions and pricing information for Internet access, prior to providing access (except within a Walled Garden). Different Splash Pages may apply at different times, to different users or in different Zones.
System Log Protocol (SYSLOG)	A standard for computer data logging that separates the software that generates messages from the system that stores them and the software that reports and analyzes them.
Terminal Access Controller Access-Control System (TACACS)	A remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks (Please refer to RFC 1492.)

Transmission Control Protocol (TCP)	One of the core protocols of the Internet Protocol Suite, complementing the Internet Protocol (IP). (Please refer to the following RFCs: 793, 1122, 1323, 1379, 1948, 2018, 4614, 5681, 6298.)
Trivial File Transfer Protocol (TFTP)	A file transfer protocol notable for its simplicity; outlined in the Internet Engineering Task Force's RFC 1350.
Two-Way PMS Interface	An interface to PMS that allows two way communications between an application and PMS. That is, read/write access to PMS. It is typically used for such purposes as identifying guests, customizing their experience and posting charges to their guest room.
Virtual Private Network (VPN)	A private computer network that interconnects remote networks through primarily public communication infrastructures. (see Additional Information: VPN Support)
Walled Garden	A controlled area on a web server that can be used to provide specific information or access to defined web sites. It can be used to provide custom web pages for specific events or allow the hotel to allow the guest access to specific web sites (see Additional Information: Marketing).
Web Proxy	A server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers. The Web Proxy is the pointer to the proxy server that is installed in the user's web browser.
Wide Area Network (WAN)	A telecommunication network that covers a broad area and is typically the network access to the hotel.
Zone	Region in a hotel where wired/wireless coverage is confined. This is typically used to identify conference or public space that needs to be isolated from other conference/public spaces.

Referenced Documents

The following table shows the documents upon which this document depends:

Name	**Location**
IPV6	http://datatracker.ietf.org/wg/ipv6//

3 Business Process

The HPG best practice is intended to provide hoteliers and vendors with the requirements for a gateway product that can be used in hotels to provide gateway functionality for both guests and Hotel Staff. It should be noted that document applies to all sizes of hotels, as well as either guest use only, or for both guest and Hotel Staff use. However, the best practices for the development of an HPG for both large and small hotels will be presented. (As noted above, the HPG features that are required for a large hotel will be identified as “Advanced” and the features required for a small hotel will be identified as “Basic.”) The choice of deploying the “Advanced” or “Basic” features of the HPG will depend upon the needs of a given hotel.

Overview

The HPG is intended to provide hotels of any size with an appliance that can perform any or all of the following features to users or devices that are connected to any portion of a hotel network:

- Billing mechanism for guest use
- Bandwidth control of any or all devices passing through the gateway
- Effective management of the appliance by either the hotel or outsourced service provider
- Authentication of users or devices
- Support for pass through of user VPNs
- Support for network related functions (e.g., DHCP, NTP, etc.)

It should also be noted that the implementation of an HPG need not support all of the above mentioned features if that feature can be provided by another appliance (for example, a firewall).

Use Cases

Typical use cases for the HPG would be the following:

High Speed Internet Access (HSIA) for Guests

In the case of HSIA access for guests, the HPG would provide the hotel with ability to implement the following features:

- Multiple tiered access (selectable by guest)
- Bandwidth control of guest data ports
- Guest Splash Page editing (to allow hotel to customize Splash Pages to be hotel specific)
- Conference / meeting room functionality including conference administration
- Marketing features
- Integrated firewall and spam blocking
- Configure Ethernet ports for security, speed, autosensing and duplex
- Client isolation of all client-specific traffic that passes through the gateway

High Speed Internet Access (HSIA) for Hotel Staff

- Bandwidth control of Hotel Staff data ports
- Integrated firewall and spam blocking
- Gateway management

Gateway Functionality

Figure 1 presents a high-level diagram of the positioning of the HPG within a hotel. It should be noted that as indicated above, the deployment of a redundant HPG is dependent upon the particular hotel requirements and is not a mandatory requirement.

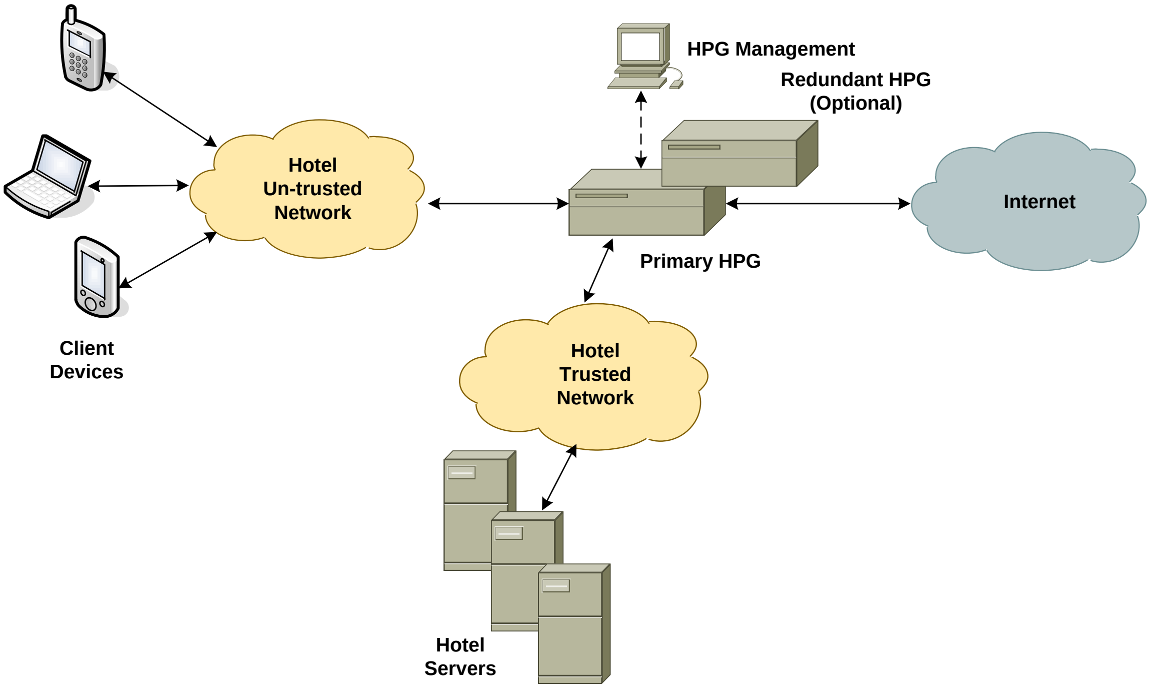

Figure 1:

From a high-level perspective, the HPG will contain the following features, functions and design considerations:

- Network engine for interconnecting clients with networks and subsequently to applications
- Scalable architecture (either through multiple server components or single server) to support small and large hotels
- Architecture that can be deployed worldwide
- Allow the property to use internal authentication sources (Active Directory, LDAP, Static databases) for authenticating Hotel Staff
- Provide LAN network services to clients, such as DHCP and VLAN assignment
- Provide firewall and IDS functions which allow the property to protect and isolate devices as well as protect the property from internal and external intrusion and control
- Provide ability for real time alarming and reporting
- Provide support for guest and Hotel Staff VPNs
- Provide ability to customize Splash Screens that are used to inform the guest on available Internet and local services
- Provide multiple billing methods, including PMS billing, credit card billing and other means of revenue generation

Behavior

Implementation of an HPG consists of inserting one or more gateways in-line between user devices and the hotel's external network (WAN). Installation of the vendor's HPG must be completely transparent to the hotel, and to clients utilizing the hotel's network. That is, no client device that works with an HPG may require reconfiguration or fail as the result of the addition of the HPG.

Gateway Interfaces

As a minimum, the HPG appliance must have two interfaces (inside and outside). However, the vendor appliance may provide support for either multiple inside and or multiple outside interfaces.

4 Detailed Gateway Requirements

The detailed advanced gateway requirements are presented below. For easy reference, each requirement is first grouped by function and then defined by specific categories. A description of each category is presented in the following table. In order to differentiate the features of the "Advanced" versus the "Basic" gateway, an "**A**" or "**B**" will be appended the feature number respectively. In the case where the feature applies to both, the letters "AB" will be appended to the feature number.

Category	Description
Feature Number	Number identifying the feature. The numbering scheme is defined as A + "Major_Category" + ". "+ "Sub_Category" + "-" "**A**", "**B**" or "**AB**" (for Advanced, Basic or Both Gateway) (e.g., A3.1- **A**).
Feature Name	Name of the Feature.
Feature Requirements	Detailed description requirements that need to be satisfied.
Use Case	Description of how the feature or requirement can be applied.
Comments	Additional comments to help clarify the feature or requirement.
Configurability	Indicates the range of functionality that needs to be supported.

Feature Number	**A1.1- AB**
Feature Name	**IP Provisioning and Connectivity – DHCP**
Feature Requirements	a) Must provide IP provisioning and connectivity for client (guest and Hotel Staff) devices with DHCP. This feature must always be enabled. b) The system administrator must be able to configure DHCP IP ranges and subnet masks, IP Gateway and DNS server addresses. This feature must always be enabled. c) Must provide support from 0 to 256 VLANs as well as the ability to configure DHCP scopes based on VLAN (e.g., for guests, Hotel Staff and others). This feature must have the ability to be enabled and disabled. d) Must support DHCP Relay. This feature must have the ability to be enabled or disabled.
Use Case	Applies to guest and Hotel Staff with DHCP request configured. All TCP/IP parameters (IP address, IP gateway, subnet mask and DNS servers) must be provided by the gateway.
Comments	Allows guest and Hotel Staff with IP enabled devices (with wired or wireless network adapters that are configured to obtain IP address automatically) to attach to the guest data network. (See **DHCP** under **Additional Information** for further clarification of this requirement.)

Feature Number	**A1.2- AB**
Feature Name	**IP Provisioning and Connectivity – Static IP**
Feature Requirements	a) Must provide IP provisioning and connectivity for client devices (guest and Hotel Staff) that have been configured with static IP addresses. This feature must have the ability to be enabled or disabled. b) Must provide the ability to support the Hotel Staff or guest's devices with pre-configured static IP addresses, subnet masks and IP gateway. This feature must have the ability to be enabled or disabled.
Use Case	Allows guest and Hotel Staff devices (with wired or wireless network adapters that are configured with a static IP address) to access the appropriate data network without reconfiguring their network settings.
Comments	Applies to guest and Hotel Staff with static IP parameters already configured. (See **Static IP** description under **Additional Information** for further clarification of this requirement.)

Feature Number	**A1.3- AB**
Feature Name	**IP Provisioning and Connectivity – Pre-Configured DNS**
Feature Requirements	Must provide IP provisioning and connectivity for a client device with preconfigured DNS entries. This feature must always be enabled.
Use Case	Allows client devices with wired or wireless network adapters that are configured with pre-set DNS entry to attach to the appropriate data network. The gateway should not override preconfigured DNS entries. The feature must also have the ability to assign an IP address (that is managed through the gateway) to the device.
Comments	Many corporate guests require preconfigured DNS to access corporate resources. (See Network Features description under **Additional Information** for further clarification of this requirement.) This may be required to support access to the enterprise assets via a VPN.

Feature Number	**A1.4- AB**
Feature Name	**IP Provisioning and Connectivity – Pre-configured Web Proxy**
Feature Requirements	The gateway must provide IP Provisioning and Connectivity for client devices (guest and Hotel Staff) with preconfigured web proxy entries. This feature must always be enabled.
Use Case	Allows client devices with web browsers preconfigured with a web proxy entry to attach to the appropriate data network. IP Provisioning must be flexible enough to provide unique connectivity for guests and associates and will be determined by the hotel requirements.
Comments	Many corporate guests require preconfigured Web Proxies for corporate controls. (See **Network Features** description under **Additional Information** for further clarification of this requirement.)

Feature Number	**A2.1- A**
Feature Name	**Configurable Splash Page**
Feature Requirements	The Splash Page configuration must provide the following features: a) Ability to enable or disable the Splash Page. This feature must always be enabled. b) Ability to provide local storage of HTML pages, which can be accessed by a web browser. This feature must have the ability to be enabled or disabled. c) Ability to redirect to specified remote or on-property server. This feature must have the ability to be enabled or disabled. d) Ability to customize gateway-hosted HTML pages that are editable by Hotel Staff. This feature must have the ability to be enabled or disabled. e) Ability to display and enforce acceptance of terms and conditions Splash Page. This feature must have the ability to be enabled or disabled. f) Ability to configure up to 128 user Zones. This feature must have the ability to be enabled or disabled. g) Must be able to edit a Splash Page once it has been created. This feature must have the ability to be enabled or disabled. h) Must support the following languages (This feature must always be enabled): *1.* English (Western ISO-8859-1) *2.* Chinese (Big5, EUC-CN, EUC-TW, GB2312) *3.* French (ISO-5559-1) *4.* German (ISO-5559-1) *5.* Japanese (EUC-JP, ISO-2022-JP, Shift_JIS) *6.* Korean (EUC-KR, ISO-2022-KR, KS_C_5601) 7. Spanish (ISO-5559-1) i) Hotel guest must be able to select available language on Splash Page. This feature must have the ability to be enabled or disabled.
Use Case	The Splash Page provides the property with the ability to provide multiple Splash Pages (with multiple URL links to other web sites) as well as to enforce acceptance of terms and conditions. The ability must also exist to allow the portal page to be turned on or off for a given Zone.
Comments	The method of configuring the Splash Page should be well defined and simple enough such that Hotel Staff can create and edit the page as well as import pages from an outside web development organization.

Feature Number	**B2.1-B**
Feature Name	**Configurable Splash Page**
Feature Requirements	The Splash Page configuration must provide the following features: a) Basic HTML b) Ability to provide local storage of HTML pages c) Ability to redirect users URL request to specified remote or on-property server d) Ability to customize gateway hosted HTML pages that are editable by hotel staff e) Ability to display and enforce acceptance of terms and conditions splash page f) Support for multiple user Zones (refer to document terms for definition of Zone)
Use case	The Splash Page would provide the property with the ability to provide a single portal page (with multiple URL links to other web sites) as well as provide the ability to enforce acceptance of terms and conditions. The ability must also exist to allow the portal page to be turned on or off for a given Zone.
Comments	The method of configuring the splash page should be well defined and simple enough such that hotel staff could easily create and edit the page as well as import pages from an outside web development organization.

Feature Number	**A3.1- AB**
Feature Name	**Guest Authentication**
Feature Requirements	This feature provides the mechanism for authenticating wired and wireless guest client device access to the data network. The authentication mechanism must provide support for the following capabilities: a) Two-way interface (see note below) into hotel PMS to verify guest. Minimum elements that need to be supported through a PMS query are guest name and room number. b) Access mechanisms must provide support for all of the following authentication methods: 1. Cookies (This access mechanism must always be enabled.) 2. Access or Promotion codes (This access mechanism must have the ability to be enabled and disabled.) 3. Username / password (This access mechanism must have the ability to be enabled and disabled.) 4. Support to Authenticate via at least four Roaming partners c) In the case of client device without a Web browser, authentication must be accomplishable via a manual process whereby a member of the Hotel Staff is given access to a gateway function that would support enabling the guest device by entering its MAC address. This feature must always be enabled. d) In the case where the client is connecting wirelessly, the client device shall be presented with a Splash Page that requires the user to enter either the guest room number and last name or an access code. The gateway should also provide a mechanism whereby the guest credentials would be used to determine from which hotel zone(s) the guest was allowed to be authenticated to use the Internet. This feature must always be enabled. e) The gateway must have the ability to interface with the property PMS to provide the following types of billing (this feature must always be enabled): 1. Wired bill to room 2. Wireless bill to room
Use Case	The client authentication feature provides the property with the ability to control access to the data network as well as roaming between wired and wireless within a given Zone. (See **Authentication** description under **Additional Information** for further clarification of this requirement.) If payment is required, a Splash Page displaying the payment information must appear.
Comments	HTNG Guest & Room Status Messaging specification is suggested.

Feature Number	**A3.2- AB**
Feature Name	**Guest Roaming**
Feature Requirements	This feature provides the mechanism for an authenticated guest to move throughout pre-defined zones without re-authenticating. The HPG must: a) Support multiple MAC addresses per device, i.e., a device connected first using a wireless MAC address must be recognized when it later connects with an Ethernet MAC address b) Support multiple devices per guest login c) Provide the capability to apply bandwidth policies per guest login or guest device d) Support Roaming Rules e) Be able to determine and limit the number of devices per guest login. The number should be less than 20. This feature must always be enabled.
Use Case	Guest is able to connect to network from guest room and then move to different areas of the hotel that are approved by the gateway, maintaining network connectivity.
Comments	None

Feature Number	**A4.1- A**
Feature Name	**Device Authentication – 802.1x**
Feature Requirements	This feature provides the mechanism for authenticating wired and wireless client device access to the pre-assigned data network. The authentication mechanism must provide the following capabilities: a) Two way interface into a directory data source (e.g. LDAP, Active Directory, SQL, etc.), directly or through a third party appliance b) Support for specifying the type (e.g. LDAP, SQL, etc.) and source of the directory data This feature must have the ability to be enabled and disabled.
Use Case	The device authentication feature provides the property with the ability to control access to various secure data networks as well as roaming between wired and wireless within a given zone. (See **Authentication** description under **Additional Information** for further clarification of this requirement.)
Comments	None

Feature Number	**A4.2- A**
Feature Name	**Device Authentication – Devices that do not support 802.1x**
Feature Requirements	This feature provides the mechanism for authenticating wired and wireless client device access to the pre-assigned data network. The authentication mechanism must provide all of the following capabilities: a) Access to a local database containing authorized MAC addresses of devices that are allowed to be connected to the secure network b) Mechanism to utilize the local database to authenticate the device to the network c) A user interface to manipulate (add/modify/delete/display) the local contents of the database This feature must have the ability to be enabled and disabled.
Use Case	The device authentication feature provides the property with the ability to control access to various secure data networks as well as roaming between wired and wireless within a given zone. (See **Authentication** description under **Additional Information** for further clarification of this requirement.)
Comments	None

Feature Number	**A5.1- AB**
Feature Name	**Gateway Administration – Access**
Feature Requirements	Administrative access to the gateway must be provided via the following mechanisms: a) HTTPS b) SNMP V3 This feature must always be enabled. Hotel Gateway administrative access must be via a secure GUI interface.
Use Case	Hotel administrative users use this feature to configure the features, to designate authorized devices and perform other tasks as documented elsewhere in this document.
Comments	Both protocols must be supported.

Feature Number	**A5.2- AB**
Feature Name	**Gateway Administration – Control**
Feature Requirements	Gateway must support all of the following security and authentication mechanisms: a) Local storage of administrator usernames and encrypted passwords b) Ability to require passwords to be reset at specified intervals (number of days specified by hotel) c) Ability to interface to external RADIUS and TACACS authentication servers for authentication of administrator usernames and passwords d) Ability to configure LAN and WAN access to the gateway for administrative control e) Ability to define the following gateway administrative user roles: 1. Full access (read/write) of all configurations, reporting, alarming and guest access code generation 2. Read access of all configurations, reporting, alarming 3. Read access of reporting and alarming 4. Guest access code generation This feature must always be enabled.
Use Case	Gateway administrative control must be enabled to manage secure access to the gateway administration tools.
Comments	None

Feature Number	**A6.1- AB**
Feature Name	**Public IP**
Feature Requirements	Gateway must be able to support the following Public IP features: a) Enable unique public IP addresses on guest devices (total number of addresses to be negotiated between hotel and carrier) b) IP address must be routable from guest device to Internet c) Maintain an IP address assigned to given guest device for length of registration d) Provide the following IP parameters for guest devices: 1. IP address 2. Subnet mask 3. IP gateway 4. DNS servers e) Revoke IP address from a device and reassign to another guest device f) Perform IP assignment automatically (without help desk interaction) g) Support IPV4 and IPV6 This feature must always be enabled.
Use Case	System must have the capability to provide a public IP address to a guest device.
Comments	The number of available IP addresses will be determined by the Internet Service Provider. The system must not have any restrictions as to how many static IP addresses can be assigned.

Feature Number	**A7.1- AB**
Feature Name	**User Access Control**
Feature Requirements	The following guest user access must be supported: a) Manually activate or de-activate connectivity to the wired or wireless network for a guest b) Manually change guest bandwidth profile c) Manual generation of network access code 1. Ability to define number of users that can connect to the network with the given access code d) Manually configure wired or wireless network connectivity through the gateway based on device MAC address e) Manually extend guest session time This feature must always be enabled.
Use Case	The system must provide an administrative interface for changing the services provided to the guests and Hotel Staff using the system. The feature provides the property with the ability to control user access to the network. That is, there may be situations where a user’s device cannot use the normal authentication method of connecting to the network and therefore needs to be allowed access without entering any credentials or access code.
Comments	None

Feature Number	**A7.2- AB**
Feature Name	**Basic Bandwidth Management**
Feature Requirements	The Gateway must be able to provide the following bandwidth management features: a) Ability to create Bandwidth Profiles (minimum of 100) that allow bandwidth management of traffic passing through gateway b) Ability to manage the following features of each Bandwidth Profile: 1. Incoming and outgoing combined bandwidth control of the data traversing the outside interface 2. Incoming and outgoing individual (by user) bandwidth control of the data traversing the inside interface 3. Ability to assign different levels of bandwidth by type (as defined by user role) of Hotel Staff connected to a given VLAN 4. Ability to assign access to the various bandwidth tiers per device This feature must always be enabled.
Use Case	System must provide capability to assign different bandwidth tiers (as defined by a bandwidth profile) which will cap the user's bandwidth rate preset in the Profile.
Comments	Bandwidth levels should be definable through the gateway administration function (see **Bandwidth Management** description under **Additional Information** for further clarification of this requirement).

Feature Number	**A8.1- AB**
Feature Name	**VPN Pass Through Support**
Feature Requirements	The gateway must allow: a) NAT traversal (NAT-T) to support the user's VPN (without disruption of service) b) The gateway must allow the following types of VPN to pass through: 1. PPTP 2. IPSec 3. L2TP 4. SSL This feature must always be enabled.
Use Case	Most of the guests who need to access to their corporate resources will use a VPN client. The gateway needs to support the most common VPN types as indicated in the description.
Comments	(See **VPN Support** description under **Additional Information** for further clarification of this requirement.)

Feature Number	**A9.1- AB**
Feature Name	**Firewall**
Feature Requirements	The gateway’s firewall must provide the following features: a) Ability to define the Access Control List (ACL) for all Ethernet ports on the gateway 1. Must include egress and ingress for all Ethernet ports 2. Ability to restrict and control access by TCP and UDP port numbers b) Ability to provide NAT and PAT between designated Ethernet ports c) Ability to provide client isolation by configured VLANs d) Ability to support different firewall configurations for each VLAN (That is, specific VLANs may need different firewall configurations.) This feature must always be enabled.
Use Case	As a set of rules, a firewall is used to filter incoming and outgoing packets based on type, source address and/or source interface. When configured on an interface, a firewall can prevent harmful traffic destined for the data network and between network users.
Comments	See **Security Features** description under **Additional Information** for further clarification of this requirement.

Feature Number	**A10.1- AB**
Feature Name	**Mail Relay**
Feature Requirements	The Gateway must have the following features: a) Ability to route SMTP e-mail traffic through the gateway to a specified e-mail relay server b) Ability to configure the relay server by DNS name This feature must always be enabled
Use Case	Allows guests to believe that they are sending e-mail from hotel through their preconfigured e-mail servers (though the e-mail is relayed through a hotel or service provider’s relay service)
Comments	Increasingly, Mail Relay services are primarily used by spamming viruses and bots, and prevent legitimate users that are attempting to send e-mail via secure or authenticated SMTP. Each property will need to analyze their users’ demographic, and decide whether to support or enable this feature locally.
Configurable	Ability to turn each individual component of the feature on or off.

Feature Number	**A11.1- A**
Feature Name	**Advanced Reporting and Logging**
Feature Requirements	The Gateway must provide the following capabilities: a) Provide an interface (GUI and API) to extract data collected or logged on the gateway b) Provide reporting functionality via a GUI locally or centrally c) Provide the following guest access reporting functionality: 1. Guest usage information: i. Date/time of logon ii. Packets/bytes in and out iii. IP address iv. MAC Address v. Port/VLAN 2. Connection source location/Zone 3. Number of authenticated users by time 4. Store a minimum of 30 days of usage records d) Provide the following management access logging information: 1. Administrative access and usage i. Source IP ii. Date/time of log in and log out iii. User ID 2. SYSLOG Messages 3. Support for SNMP traps using RFC standard MIBs (as provided by the gateway vendor). 4. CPU utilization on each of the gateway devices 5. Memory utilization on each of the gateway devices 6. Interface utilization on all active communication interfaces 7. Interface status 8. Interface errors i. Input errors ii. CRC errors iii. Output errors iv. Collisions v. Output drops 9. Store a minimum of 30 days of records. 10. Generate report by specified date and time. e) Provide export log files in at least one of the following file formats: i. CSV ii. Plain text iii. XML f) Generate and forward SYSLOG logging information 1. Store a minimum of 30 days of records 2. Generate report by specific data and time g) Firewall 1. Capture and log the following system and network information: i. Denied inbound access resulting from a particular Access Control List (ACL) being accessed on a specific Ethernet port ii. Denied outbound access resulting from a particular ACL being accessed on a specified Ethernet port iii. Administrative access to the firewall including all changes performed and by which administrative user iv. Outbound and inbound NAT and PAT translations This feature must always be enabled.

Use Case	Reporting and logging feature provides the property with the ability to: a) Effectively manage guest Internet access b) Provide current status information to make adjustments to the guest Internet service offering on items including: 1. Bandwidth consumption 2. Number of users 3. Current user status 4. Security and monitoring
Comments	(See **Logging** and **Reporting** descriptions under **Additional Information** for further clarification of this requirement.)

Feature Number	**B11.1-B**
Feature Name	**Basic Reporting and Logging**
Feature Requirements	a) Provide an interface to extract data collected or logged on the gateway b) Ability to store at minimum of 30 days of usage records c) Provide reporting functionality via a GUI interface locally, on the gateway. The gateway must provide the following reporting functionality: 1. Guest Usage information: date/time of logon, packets/bytes in and out, IP address, MAC Address, Port/VLAN 2. Connection Source Location/Zone 3. Number of users by time of day 4. Firewall logs d) Provide logging of the following: 1. Administrative access and usage (source IP, date/time of log in and log out) 2. SYSLOG Messages 3. Support for SNMP traps using standard MIBs or Enterprise MIBs e) Firewall features (as defined in B9.1) f) Provide the ability to export log files in non-proprietary format
Use case	Reporting and logging feature provides the property with the ability to: a) Effectively manage guest internet access b) Provide current status information to make adjustments to the guest internet service offering on items including: 1. Bandwidth consumption 2. Number of users 3. Current user status 4. Security and Monitoring
Comments	(See **Logging and Reporting** description under **Additional Information** for further clarification of this requirement.)

Feature Number	**A12.1- AB**
Feature Name	**Backup and Restore Gateway Configuration**
Feature Requirements	The gateway must provide the following capabilities: a) Generate and export a configuration file on an external device or static RAM (such that the file can be used to restore the gateway to a previous operational state) b) Specify location of backup files c) The backup/restore function must provide the following functionality: 1. Scheduled backups are configurable i. Recurring – with the ability to configure a daily, weekly and monthly interval ii. One-time – specifying the date and time 2. Manual backups on request 3. Restore command using exported configuration file from specified location 4. This feature must always be enabled.
Use Case	In the event of a failure or upgrade, a backup can be restored to provide complete functionality.
Comments	None

Feature Number	**A12.2- AB**
Feature Name	**Gateway Software Upgrade**
Feature Requirements	The gateway must provide the ability to upgrade the gateway software/firmware to any of the following: new releases, current releases and previous releases (as determined by the manufacturer). This feature must always be enabled.
Use Case	When new software functionality is available, the gateway firmware is upgraded locally or remotely.
Comments	None

Feature Number	**A12.3- A**
Feature Name	**Failover and Redundancy**
Feature Requirements	The gateway must provide the ability to: a) Support two load balance servers, or a primary and a secondary server, allowing for automated failover b) Provide a manual cutover to a secondary gateway c) Support stateless failover without interruption of user registrations. This feature must always be enabled.
Use Case	During a server failure, gateway functionality is provided by an alternate server without interrupting the traffic flow of the guest and associates.
Comments	None

Feature Number	**A13.1- AB**
Feature Name	**Pass Through List**
Feature Requirements	Prior to guest authentication, the gateway must be able to provide the following capabilities: a) Creation and editing of a pass through list containing the following: 1. A list of specific IP addresses (single or range) 2. A list of domain names (Specific URL or Wildcard URLs) b) Allow the guest to access any specific IP address or domain name in the pass through list c) Ability to enable redirection to a specific URL when pass through list is violated, which may instruct Guest to perform some other operation (for example, call the front desk) This feature must have the ability to be enabled and disabled.
Use Case	Hotels that allow free access to web sites for users before or without authentication.
Comments	This is often referred to as a Walled Garden. If Splash Pages and Hotel Staff content are not hosted locally, their URLs need to be listed in the pass through URL list. (See **Marketing** description under **Additional Information** for further clarification of this requirement.)

Feature Number	**A14.1- A**
Feature Name	**Storage Expansion**
Feature Requirements	The gateway must be able to provide the following a) Ability to increase the file storage on an as needed basis through at least one of the following: 1. USB drive 2. SSD 3. HDD 4. Network drive 5. Remote network accessible storage b) Ability for the system to automatically recognize the size of the file storage device This feature must always be enabled.
Use Case	In the event that the standard gateway configuration (disk storage) does not provide sufficient mass storage that the property requires to save lagging information, the ability to add addition mass storage would allow a hotel to increase the memory to satisfy their specific requirements. In addition, increased storage will provide the ability to log data longer than the required 30 days.
Comments	The amount of storage required will depend upon the property size and owners' logging requirements.

Feature Number	**A15.1- AB**
Feature Name	**Network Interface Protocol Support**
Feature Requirements	The gateway must be able to support the following protocols a) TCP/UDP on all gateway Ethernet ports b) Internet Protocol V4 on all gateway Ethernet ports c) Internet Protocol V6 on all gateway Ethernet ports that are attached to the property's Wide Area Network equipment This feature must always be enabled. Devices may need to connect using a variety of current and future protocols.
Use Case	Devices may need to connect using a variety of current and future protocols. This will satisfy the future requirement to allow the gateway to interface with IPV6 wide area networks.
Comments	It is assumed that the provider of the Wide Area Network equipment will require the support of IPV6 before the hotel requires support of IPV6.

5 Additional Information

Contained in this section is a list of additional information that should be referenced as part of the requirements presented above. The information provides the reader with additional insight into the requirements presented in the detailed advanced gateway requirements section and provides best practices for the development of the HPG.

VPN Support

A Virtual Private Network (VPN) is a communications network tunneled through another network and dedicated for a specific network. A common application is secure communications through the Internet. The HPG should provide support the VPN connection types outlined in this section.

Point-to-Point Tunneling Protocol (PPTP)

PPTP was developed by Microsoft and is the most widely supported VPN method among Windows clients. PPTP is built into Windows operating systems.

Layer 2 Tunneling Protocol (L2TP)

L2TP is an extension of PPTP from Microsoft and Layer 2 Forwarding (L2F) from Cisco.

IP Security (IPSec)

IPSec is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. IPSec also includes protocols for cryptographic key establishment.

IPSec with Authentication Header (AH)

The IPSec Authentication Header (AH) protects entire IP packets, including IP headers, against modification in transit.

Supported VPNs

The HPG should allow any VPNs to be passed through the gateway.

Authentication

The HPG should provide a mechanism to authenticate users and/or devices that are attempting to connect to the network and/or the HPG. Contained in this section is a description of the available authentication mechanisms as well as which back-end authoritative databases may be supported.

Authentication Method

Table 1 presents a list of currently in-use authentication mechanisms that the HPG may have to support.

Table 1: Authentication/Encryption Methods

Authentication/Encryption Methods	Description
Remote Authentication Dial-In User Service (RADIUS)	RADIUS uses the AAA concept to manage network access where AAA is defined as Authentication, Authorization and Accounting. The Radius protocol is defined in the Internet Engineering Task Force's RFC 2865 and RFC 2866.
802.1x	IEEE 802.1x is an IEEE standard for port-based network access control, and part of the IEEE 802 (802.1) group of protocols. It provides authentication to devices attached to LAN ports, establishing or preventing port access based on the results of the authentication.
Kerberos	Kerberos is a computer network authentication protocol which allows individuals communicating over a non-secure network to verify identities to one another in a secure manner. Kerberos is defined in the Internet Engineering Task Force's RFC 4120.
Digital Certificates	Digital Certificates consist of either public key certificates or identity certificates, which are electronic documents that incorporate a digital signature to bind together a public key with an identity. In a typical public key infrastructure (PKI) scheme, the signature will be that of a certificate authority (CA).
Media Access Control (MAC)	The address that is a quasi-unique identifier that is attached to a network adapter.
Two-Factor Authentication	A mechanism whereby a second authentication can be requested. The second factor can be provided by a number of products including Entrust, Verisign, etc.
Secure Socket Layer (SSL)	A cryptographic protocol that provides secure communications on the internet. SSL is defined in the Internet Engineering Task Force's RFC 2246.
Terminal Access Controller Access-Control System (TACACS)	A remote authentication protocol that is used in UNIX systems and Cisco devices. TACACS allows a remote device to communicate with an authentication server in order if the user is allowed access to the device. TACACS is defined in the Internet Engineering Task Force's RFCs 1492 and 0927.

Authoritative Authentication Data Sources

Where applicable, the Authentication methods presented in Table 1 typically require one or more of the authoritative data sources presented in Table 2 to perform a successful authentication.

Table 2: Authentication Data Sources

Authoritative Authentication Sources	Description
Active Directory (AD)	An implementation of LDAP directory service by Microsoft for use within the Windows environment. It provides central authentication and authoritative services for Window-based computers.
Lightweight Directory Access Protocol (LDAP)-supported databases	An application protocol for querying and modifying directory services. LDAP is usually a front-end query tool that is provided as part of an overall directory. LDAP is defined in the Internet Engineering Task Force's RFC 4510.
Local Database	A local database would be contained and managed on the HPG appliance. The database should have the ability to store username, device name and password.

Network Features

The HPG should provide support for the network features defined in this section.

DHCP

The Dynamic Host Configuration Protocol (DHCP) is a protocol used by network devices (clients) to obtain various parameters necessary for the clients to operate in an Internet Protocol (IP) network. The DHCP services must have the ability to provide different DHCP scopes for devices that are placed on different VLANs.

The DHCP protocol is defined by the Internet Engineering Task Force's RFCs 1534, 1541, 2131, 2132 and 3315.

Static IP

Static IP addressing is the ability for a given IP address to be assigned to a given device. In many cases, the device will also require that in addition to assigning the static IP address that a subnet mask and next hop gateway also be configured.

VLAN Tagging

Since VLANs designate separation of networks coexisting on common wires, gateways must sync up with DHCP servers to be able to allocate a variety of address space and still be able to route them. The gateway must be able to assign devices to shared and unique VLANs as necessary. This can be done by any of the following: physical port, MAC recognition, NAC.

The VLANs are defined by the Internet Engineering Task Force RFCs 3069, 4554 and IEEE 802.1Q.

MAC recognition

Fixed devices such as telephones, set-top boxes and room controls need virtual segmentation from un-trusted equipment. The segmentation allows for these devices to communicate with other devices. The gateway accomplishes this by having the vendor portion of the MAC or even the entire address recognized and assigning these devices their proper VLAN via the VLAN hash table.

Lease timers

Lease timers offer a way of maintaining effective duration control. This can greatly assist in eliminating bandwidth theft and unauthorized use of the network. Users can re-authenticate via several methods including the use of a cookie.

DHCP Relaying

DHCP relaying should be available including option 82 & option 43 as defined in the Internet Engineering Task Force's RFC 3046.

NTP

NTP services may be enabled. NTP works best when at least two time sources are available. This allows both for drift as well as redundancy.

TFTP Support

In order to support many dynamic devices on the network such as VoIP phones, TFTP protocol (as outlined in the Internet Engineering Task Force's RFC 1350) should be passed, and a TFTP server should be included as an optional feature.

Marketing

Walled Garden

A walled garden, with regards to media or marketing content, refers to a closed set or exclusive set of information services provided for users. This is in contrast to providing consumer's access to the open Internet for content and e-commerce. An example is where an unauthenticated user is given access to a limited environment, or specific URLs, for the purpose of setting up an account, viewing marketing material or browsing pre-authentication portal pages. Post-authentication, they are allowed out of the walled garden and into the Internet.

The HPG should have a location for entering walled garden IPs and/or URLs for unfettered, pre-authenticated viewing access.

Login Portals

Login portals are customizable portals for guest connectivity to multiple services based on location, policy and cost.

There will be different log-ins for different zones (for example, there will be different log-ins for the conference room and the guest room).

Multi-Language Support

The HPG should have the ability to support multiple languages on guest facing screens.

Logging and Reporting

HPG logging and reporting generally includes the following:

Configurations

In order to provide sufficient detail for logging and reporting, the logging function should have the ability to configure the following logging parameters:

a) Which of the available logging items should be logged
b) Logging interval (between 5 minutes and 1 hour)
c) Length of time that the logging data should be stored on the gateway (function of available disk space)
d) Defined thresholds for alarming of available logging items
e) Defining baseline values of available logging items
f) Define e-maile-mail address, SNMP community strings and SYSLOG location for alarming

Logging

The HPG should have the ability to log and timestamp the following items:

a) CPU utilization on each of the gateway devices
b) Memory utilization on each of the gateway devices
c) Interface utilization on all active communication interfaces
d) Interface status
e) Interface errors (e.g. input errors, CRC errors, output errors, collisions, output drops.

Reporting

The HPG should have the ability to provide the following tabular reports:

a) 95th percentile interface utilization at minimum poll intervals
b) Exception reporting that identifies devices exceeding pre-defined thresholds
c) Reporting of baseline values for CPU utilization, memory utilization and interface utilization along with values for time period of interest

Alarming

The HPG should have the ability to generate real-time alarms to all of the following communication mechanisms:

a) E-mail address
b) SNMP
c) SYSLOG