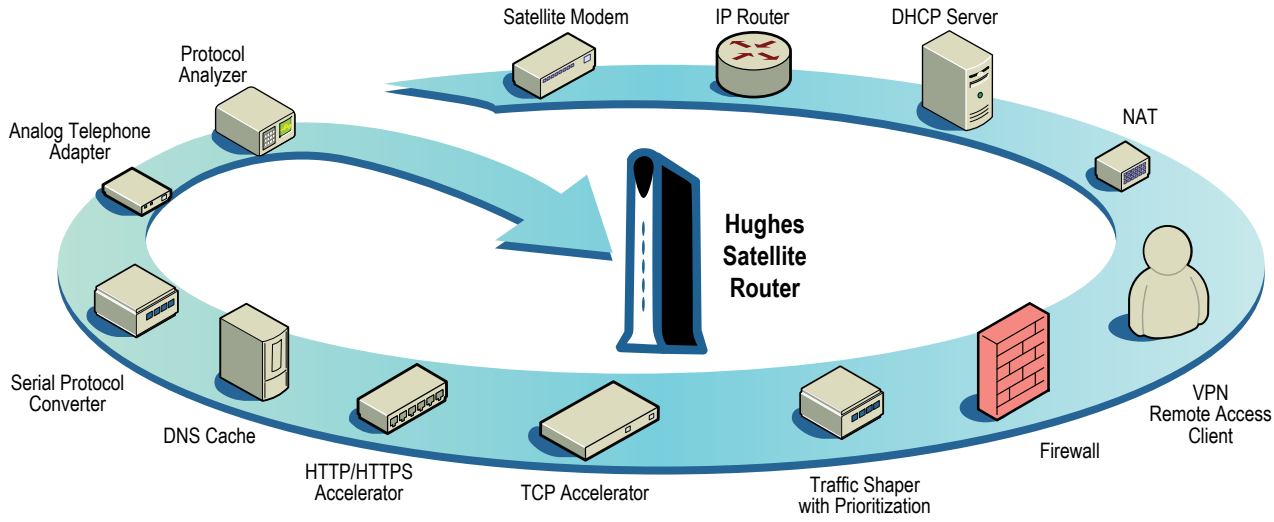
HUGHES

Key Features of Hughes HN/HX Broadband Satellite Routers

As illustrated, the Hughes family of HN/HX broadband satellite routers incorporates the combined functionality of a satellite modem and a full-featured Internet protocol (IP) router. Optimized for satellite communications and fully compliant with the global IPoS/DVB-S2 standard, its comprehensive suite of built-in features addresses performance, security, and operational requirements.



HN/HX Overview

Fully IP compliant, all HN/HX broadband satellite routers interoperate directly with other routers on the remote LAN through standard IP protocols, eliminating the need for an external router. System performance and efficiency are optimized at network, transport, and application layers. For high availability networks with transport diversity, (for example, combining satellite, DSL, and frame relay technologies), HN/HX routers employ features that enable transparent failover and selective IP forwarding to alternate paths, and can be combined with VPN Automatic Dial Backup for increased redundancy.

The Hughes family of HN/HX routers is designed to support a wide variety of terminal devices via Ethernet LAN ports, synchronous/asynchronous serial ports, and analog telephony interfaces. In addition to providing IP connectivity for native IP devices, integrated serial protocol conversion enables legacy serial devices to effectively operate over an IP network. Similarly integrated voice functionality enables connected analog telephones, facsimile machines, and voice-band data modems to operate as VoIP devices with voice QoS (Quality of Service) guarantees. Hughes HN/HX routers also employ optimization capabilities for third-party VoIP and videoconferencing equipment, and provide efficient pre-allocation of bandwidth resources based on codec usage.

Hughes HN/HX Systems employ several information assurance techniques to safeguard the integrity and confidentiality of data and to adhere to PCI compliance requirements, including conditional access control and two-way IPSec encryption. Hughes HN/HX routers offer additional network defenses through built-in firewall features.

Hughes is a leading provider of managed network services in the US, and that experience is reflected in the extensive diagnostic and troubleshooting capabilities built into the HN/HX family of routers. A Web interface shows router and system information in a way that is easy to understand and use. The diagnostic system offers multiple levels of information for end users and support personnel. New capabilities and improvements are continually under development, and software upgrades are typically delivered over the network and automatically installed with less than a minute of service disruption.

IP Stack/Service Features

Hughes HN/HX Systems provide high-speed IP satellite connectivity between corporate headquarters and/or the Internet and multiple remote sites.

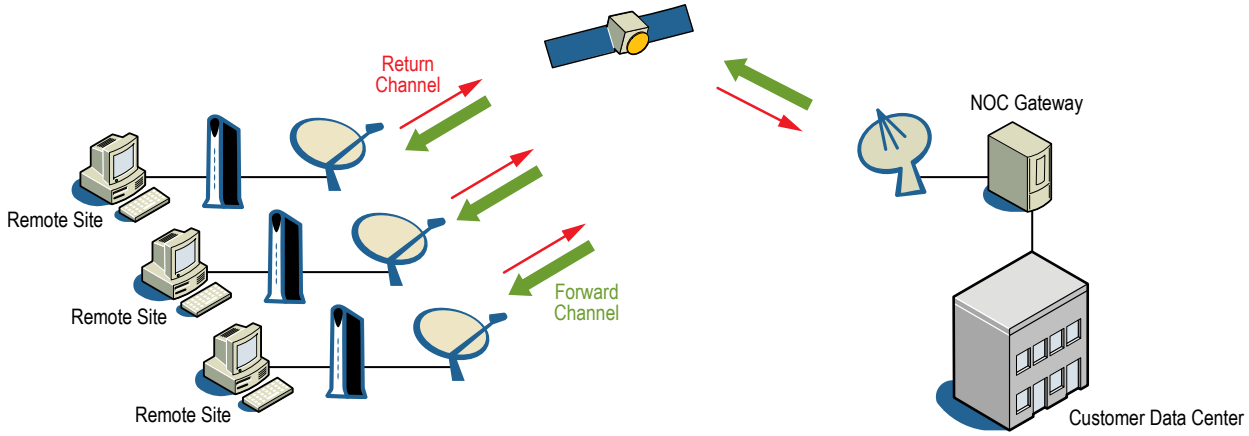


Figure 1. System Overview

HN/HX Systems include a variety of standard and specialized IP features designed to optimize space segment and minimize latencies for IP networking protocols and services. All common unicast and multicast IP protocols, including TCP and UDP and the protocols carried on top of them (HTTP, SSL, RTP, SIP, etc.), are supported. The multicast capability works transparently with hosts and routers running IGMPv1 (RFC 1112), IGMPv2 (RFC 2236), and IGMPv3 (RFC 3376), and includes support for the source-specific multicast filtering available with modern operating systems. Because satellite networks efficiently carry multicast communications, HN/HX Systems can bring a multicast solution to a network that is otherwise not optimized for multicast communications (for example, DSL networks). Additionally, remote sites can be defined as receive-only for applications that do not require a return path (for example, IPTV).

HN/HX Systems are capable of transmitting IP multicast traffic originating at a remote site across a return channel to the NOC. At the NOC, the traffic can be forwarded to a customer's data center, back over the forward channel to the customer's other remote sites, or both. The IP multicast packets can be prioritized relative to other inbound data.

HN/HX Systems can provide a completely private network or full access to the public Internet. HN/HX routers are available with one or two LAN ports that can be configured to support multiple IP subnets.

Network Address Translation

All Hughes HN/HX routers provide a Network Address Translation (NAT) service which conforms to RFC 3022 and includes support for a variety of ALGs including IPSEC and PPTP. NAT allows a single device, such as a router, to act as an agent between the Internet (or a public network) and the local (or private) network. HN/HX routers support NAT and Port Address Translation (PAT), which is sometimes referred to as Network Address and Port Translation (NAPT). Port Address Translation (PAT) allows users to send data traffic from multiple IP devices on the router LAN using a single address.

Simple NAT enables enterprise customers to cut over to the Hughes HN/HX network without changing their existing remote networks. By using static translation tables, it also makes servers on the router LAN accessible from the WAN side.

If the Hughes router is configured for port address translation, it can be configured for Port Forwarding. Port Forwarding is the mapping of traffic received by the router on a given port to a particular IP address/port number on the router LAN. Mappings can be specified as either TCP or UDP. Port Forwarding is useful for allowing connectivity initiated from the NOC to NATed remote hosts.

Each LAN port on a Hughes router can be configured independently for NAT services.

Devices with private and public IP addresses can coexist on the LAN interfaces of HN/HX routers. Each router manages two separate IP subnets; one is NAT-enabled and is mapped via NAPT to an IP address from the second public IP subnet. This capability provides the benefits of public addressing to specific devices, while allowing the use of private addressing for other devices on the LAN.

DHCP Server/DHCP Relay

Hughes HN/HX routers provide a standards-compliant implementation of Dynamic Host Configuration Protocol (DHCP) Server and Relay. The DHCP Server manages the automatic assignment of IP addresses to devices on the router LAN. When enabled, the DHCP service responds to a DHCP request by assigning an IP address, a subnet mask, up to two Domain Name Server (DNS) IP addresses, and a default gateway IP address. The DHCP Server can also be configured to assign a DNS domain name, up to two WINS Server IP addresses, WINS scope, and WINS node type. Network Time Protocol (NTP) is also supported by HN/HX routers and is used to ensure that leases are managed across router restarts.

The DHCP service can be configured with disjoint address pools, so that certain IP addresses on the LAN can be statically assigned based on MAC address while others are given out via DHCP.

Hughes HN/HX routers implement a DHCP Relay feature that allows a device on the router LAN to obtain IP addresses and other information, such as initial bootstrap program and DNS IP address, from an enterprise DHCP server rather than from the router. DHCP requests received by the router from devices on its LAN are forwarded through the spacelink and NOC gateways to an enterprise DHCP server. The responses are carried over the spacelink to the router and sent out the LAN port from which the requests were received. The DHCP relay function allows relaying to multiple DHCP servers in the enterprise network.

Each LAN port on a Hughes router can be configured independently for DHCP services.

LAN Features

Hughes HN/HX routers are available with one or two LAN ports. Dual LAN ports can be configured for operation as two independent LAN segments, or as a single LAN segment operating in a hub-like mode.

VRRP

The HN/HX router participates in the IETF standard Virtual Router Redundancy Protocol (RFC 3768) with other routers on the remote LAN. Increased availability is achieved through VRRP by creating a virtual router consisting of a group of cooperating physical routers that share a virtual MAC and IP address. The physical routers elect and monitor a master router to service requests. If the master router fails, another group member assumes its responsibilities. The use of a virtual router makes router switchovers transparent to the IP hosts at the site. The HN/HX router supports up to three VRRP routers on each LAN interface and can be made a master for one or more of the VRRP routers. It advertises itself via VRRP messages only if the satellite link is up and functional, and can optionally require a successful end-to-end ping connectivity test as a criteria for “up and functional.”

When multiple paths exist to a remote site, mechanisms are needed to support switching from one path to another in the event of a failure and for sharing the load between the paths when both are available. A typical VRRP configuration is to define two virtual routers, each with a different default master router. This provides the ability to implement load sharing by having different end hosts use a different default router while still providing transparent recovery if one router fails.

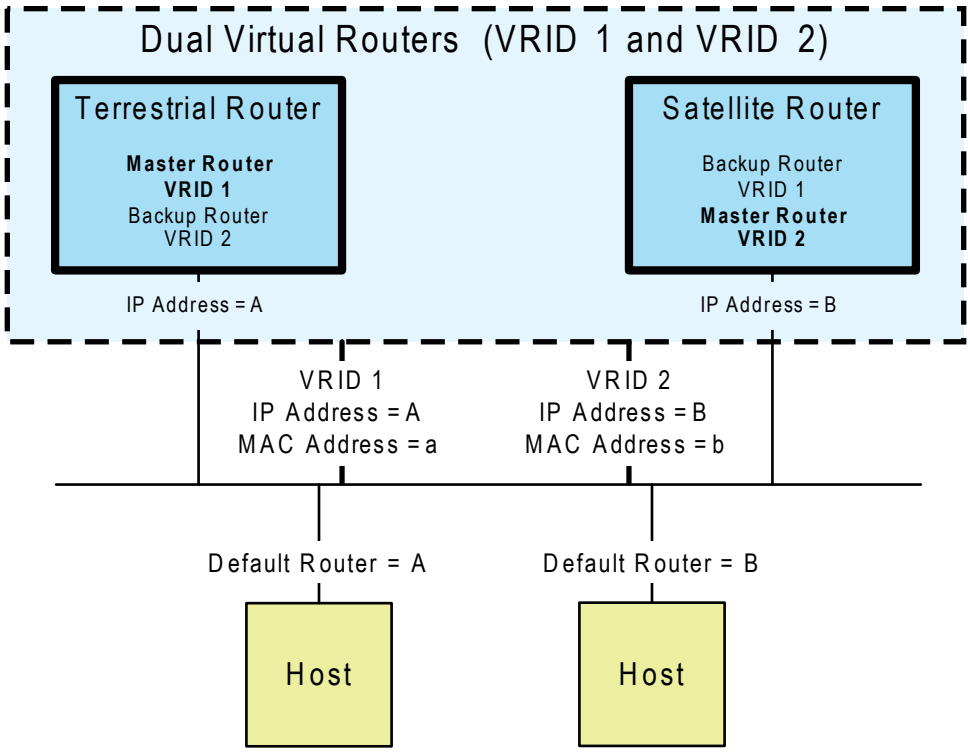


Figure 2. Dual Virtual Routers for Load Sharing

VLAN Tagging

When connected to an Ethernet VLAN switch, the Hughes HN/HX router provides VLAN routing support to devices at the remote site. The LAN subnet served by the router is divided into smaller subnets, and each subnet is assigned a VLAN tag; the subnet containing the router IP address is considered a "native" VLAN and does not use a VLAN tag. The router connects to the Ethernet switch's VLAN Trunk (802.1q enabled) port and is configured with the same VLAN configuration as the switch. Up to 8 VLANs can be configured on the router and switch. The router is responsible for inter-VLAN routing at the site as well as providing access to the Enterprise LANs and/or the Internet based on Access Control Lists (ACLs) configured in the router. See the Access Control List subsection for more information on ACL rules. The router inserts the appropriate VLAN tags into outgoing Ethernet packets and removes VLAN tags from incoming LAN packets.

VLANs can be used as a mechanism for segregating intracustomer traffic. For example, point-of-sale traffic and Internet kiosk traffic could be tagged using different VLAN IDs. Since VLAN IDs correspond to subnets, the source IP address can be used in the HN/HX System to perform VLAN traffic prioritization and path selection.

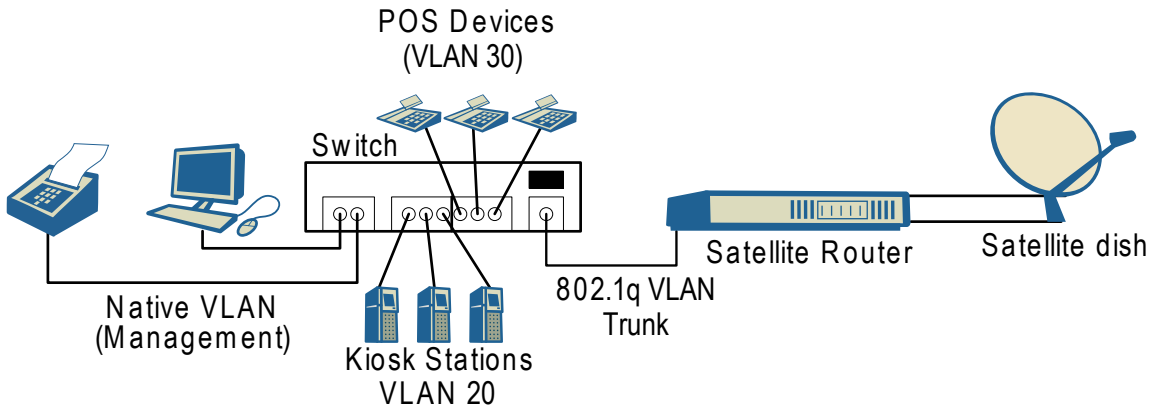


Figure 3. VLANs for Segregating Traffic

HN/HX Systems employ a feature called End-to-End VLAN Propagation which extends VLAN tagging support by carrying the VLAN tags over the satellite between the router and NOC Gateway. This is useful when a remote customer site has multiple networks, each needing to communicate with different customer intranet host servers (See Figure 4). End-to-End VLAN Propagation also supports terrestrial network infrastructures configured to prioritize certain VLAN IDs. VLAN definitions can be flexibly defined as either disjoint or overlapping subnets, and VLAN IDs can be translated between a router set of VLAN IDs and a NOC Gateway set. The mapping of 802.1p packet bits to IP header DSCP values is also supported. Several mechanisms for VLAN traffic prioritization are provided by the HN/HX Systems as identified in the Prioritization Section.

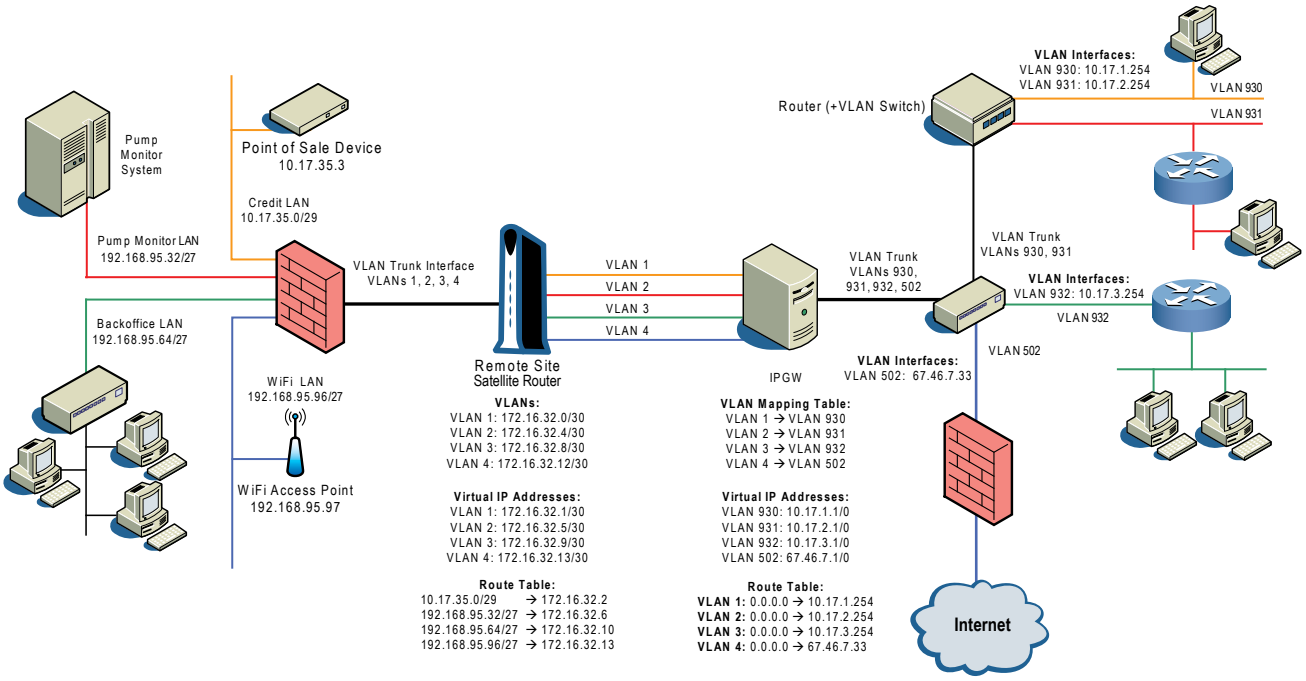


Figure 4. End-to-End VLAN Tagging Application

IP Routing Features

Routing protocol support by the HN/HX Systems enables network interoperability.

RIP and BGP

Dynamic routing allows routers to manage the routing of messages in circumstances where there may be multiple paths available for a given address. The HN/HX Systems exchange RIPv2 or BGP4 (Border Gateway Protocol) routing messages with external routers to determine what paths are available in the network and which path should be used. A proprietary routing protocol (BRP) is used internally to optimize the exchange of routing messages over the spacelink between the Hughes routers and NOC Gateways.

With dynamic routing the HN/HX Systems can effectively coexist in a network with multiple paths between the remote devices and the enterprise LANs, for example, when a terrestrial link and a satellite link exist to each site. Dynamic routing is useful even when the satellite is the only path to the site. If a site has multiple LAN subnets separated by an external router, only the subnet attached to the Hughes router is known. Dynamic routing allows other subnets to be learned, eliminating the need for extensive manual configuration.

The HN/HX Systems are capable of generating and receiving RIPv1 messages per RFC 1058 and RIPv2 messages per RFC 2453. Hughes' routers support IRDP per RFC 1256 in order to support various router failovers and initial router discovery. The HN/HX Systems can coexist with BGP-enabled systems and provides a BGP aware path between a remote network (or Autonomous System in BGP terms) and a corporate data network (or AS in BGP terms). BGP is a routing protocol that is increasingly being used in large networks since it offers a much larger set of capabilities compared to RIPv2 and other protocols. For instance, BGP is commonly used in MPLS networks because it allows the MPLS tags to be carried within the BGP protocol. With the BGP feature, the Hughes router and NOC Gateway operate as BGP edge routers and exchange routes with their BGP peers. The routing protocol between the Hughes router and NOC Gateway remains as BRP.

Figure 5 shows a portion of a typical customer network divided into multiple autonomous systems. A NOC Gateway and its associated satellite routers is part of a single AS, the "HN AS." The "Enterprise Remote Site AS" and the "Enterprise Data Center AS" are additional autonomous systems. Connectivity is shown between the Enterprise Remote AS and the Enterprise Data Center AS via a terrestrial service provider with the HN/HX Systems acting as alternate and redundant paths.

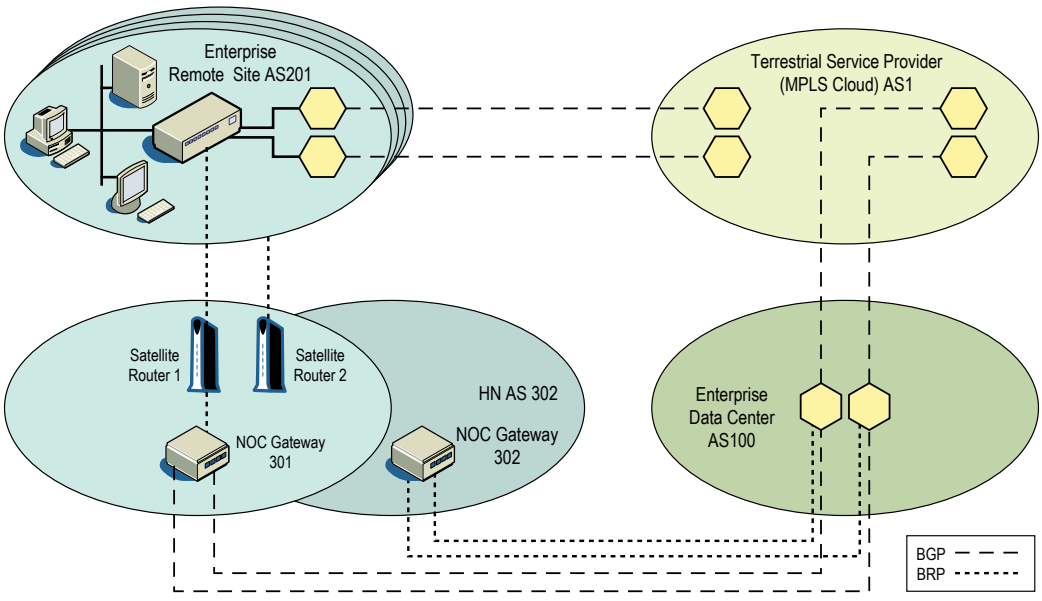


Figure 5. Use of BGP within an Intranet with Satellite

Policy-based Routing

Policy-based Routing (PBR) allows the Hughes HN/HX router to selectively forward some IP traffic to an alternate path instead of sending all the traffic over the single path selected by the dynamic routing protocol. Up to three next hop routers can be configured for each LAN interface. All clauses available in the ACL rules are applicable for Policy-based Routing. See the Access Control List subsection for details on ACL rules. The next hop routers can be defined as always available or available only if responding to periodic ping requests or sending RIP messages.

PBR also allows a backup router to be specified from the list of next hop routers. Traffic is forwarded to the backup router whenever the spacelink status goes down unless the Hughes VPN Automatic Dial Backup (VADB) feature is enabled.

PBR is frequently used in conjunction with VRRP. The combination of VRRP and PBR provides the ability to support load sharing based on application type while still providing transparent recovery if one of the routers fails. A typical deployment scenario is a network with diverse transport (for example, satellite and DSL) as shown in Figure 6 with policy rules defined to favor the terrestrial path for TCP traffic and the satellite path for UDP or multicast traffic.

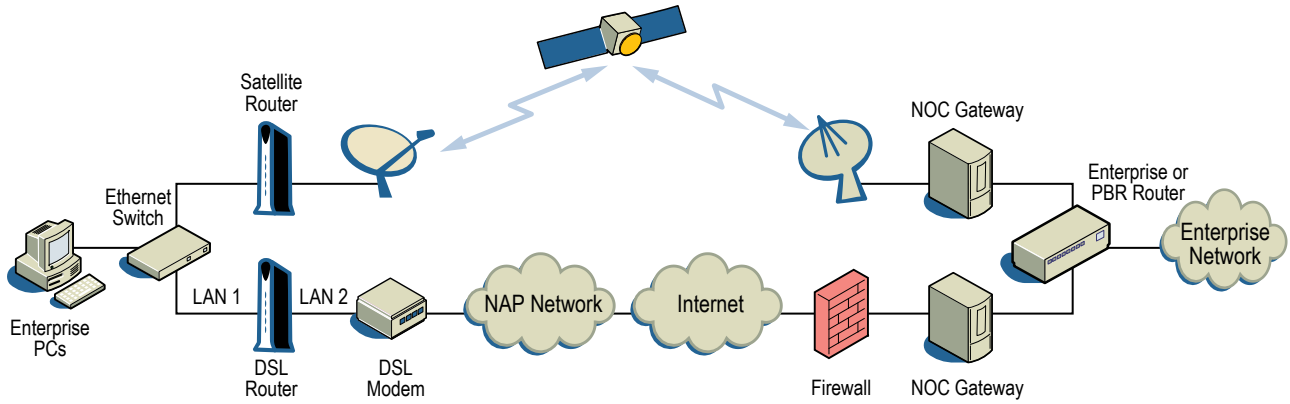


Figure 6. High Availability Network with Satellite and Terrestrial DSL Transport

Firewall Features

HN/HX Systems provide the following network safeguards to protect the LANs connected to the Hughes HN/HX router and ensure optimal use of the satellite bandwidth.

Access Control List (ACL)

Hughes HN/HX routers have an embedded firewall functionality that controls traffic coming in or going out of its LAN and satellite interfaces. ACLs can be defined for each interface to restrict the reception and/or transmission of packets based on: Source IP address range, Destination IP address range, TCP/UDP port number, IP Protocol type, ICMP Message type, and Diffserv code point (DSCP) bits. The rules can be configured such that they apply to individual routers or groups of routers. Rules can optionally be configured via the router's local Web Interface. Detailed information regarding packet discards is available through the Web Interface. The ACL capability provides maximum flexibility for different firewall needs. For example, rules can be defined to block all traffic from a single PC on the LAN or a set of PCs on the same subnet; block Internet or intranet access for a subset of devices on the LAN; limit FTP access to only one machine on the local LAN; drop UDP traffic destined to or originating from specific ports, or all UDP traffic except DNS lookups, or all ICMP traffic, etc.

The Hughes Policy-based Routing (PBR) feature, described in the Policy-based Routing subsection, is built on top of the ACL method. Each ACL rule has an additional parameter that specifies the next hop router to which a packet is forwarded in case the rule is applied to a packet.

Fenced Internet

The Fenced Internet Access (FIA) service is an option that provides a mechanism for enterprise customers to restrict remote site access to a limited number of specifically approved Internet sites. URL white lists can be defined to restrict Web browsing from remote LANs to only permitted sites, IP addresses, and domains. Separate white lists can be constructed for each of the router's LAN interfaces and can restrict access to URLs based on Source IP address range. Different lists of approved sites can be supported for multiple subsets of a customer's remote sites.

Since FIA identifies and filters traffic at the remote site, it brings the added benefit of bandwidth savings over a customer data center filtering solution.

Virus Protection

Hughes HN/HX routers contain a Virus Protection feature designed to supplement other virus protection mechanisms in use throughout the network. The Virus Protection feature monitors traffic received on the router's LAN interfaces for specific signatures and blocks them if they match the signature. Traffic monitoring is based on three filters: a protocol/port filter, an attribute filter, and a subnet filter. The protocol filter identifies specific protocol packets and destination or source ports that should be monitored. The attribute filter defines the transmit activity that identifies a suspected virus (for example, a unique destination IP address rate in packets per second over a specified monitoring interval). Multiple protocol filters may share a common attribute filter. The subnet filter identifies the Destination IP address range to be blocked.

The router's local Web interface indicates when virus activity is detected and provides detailed information about the data being monitored including host IP address, protocol, port, and time correlation.

MAC Address White Lists

The MAC Address White List feature limits access to the HN/HX router to an approved list of MAC addresses. Traffic from any source not present in the MAC list for that port is dropped.

Per-port white lists can be configured for a total of 32 MAC addresses.

High Performance

The HN/HX Systems offer advanced performance enhancing features that maximize performance and network efficiency.

TCP Performance Enhancing Proxy

Performance Enhancing Proxy (PEP) software features improve the throughput and response time of TCP applications while minimizing the required bandwidth. All Hughes routers implement the PEP feature, which includes bidirectional TCP spoofing, acknowledgement reduction, message multiplexing, data and header compression, and prioritization.

Full function outbound and inbound TCP spoofing is provided, using a split TCP connection approach. The TCP connection is fully terminated on each side of the satellite link with the Hughes PBP, a proprietary PEP backbone protocol optimized for satellite, used in between. PEP dynamically determines available bandwidth and packet loss and automatically adjusts to match current conditions. PEP spoofs the three-way TCP connection handshake so that data can be forwarded without waiting for end-to-end connection establishment. A feedback mechanism, implemented as part of the backbone protocol, is provided for each direction to allow maximum buffer utilization. Packets dropped on the local LAN are retransmitted locally. Multiple TCP connections are multiplexed onto a single backbone connection so a single backbone protocol ACK can acknowledge the data of multiple TCP connections. Up to four backbone connections may be used in parallel to each Hughes router, and each may be tuned to support different classes of service/priorities for different traffic types.

Compression

HN/HX Systems provide IP/TCP/UDP/RTP header compression and payload compression in both inbound and outbound directions.

A standard TCP/IP header is 40 bytes per packet, and most of that information is redundant for a given session. Header compression suppresses any redundant information, reducing the bandwidth required for the header. This compression capability requires that a large number of the fields either do not change or change only in expected ways. Inbound header compression compresses TCP/IP headers from 40 bytes to 10–12 bytes, reducing typical bandwidth usage by 15–-20%. The inbound compression algorithm is a Hughes-extended version of RFC 1144. Multiple types of IP headers can be compressed, including IP headers, UDP headers, TCP headers, RTP headers, and Hughes' PBP headers.

Outbound header compression compresses IP, UDP, and RTP headers using the header fields that do not change or change in predictable ways. The outbound compression algorithm is based on RFC 3095, Robust Header Compression, and the Hughes inbound header compression algorithm. IP/UDP/RTP headers for RTP packets (types G.729 and G.723.1) are compressed. With outbound header compression, the size of the IP/UDP/RTP headers becomes 5 bytes from 40 bytes. With an average RTP payload size of 20 bytes, the expected compression ratio for IP/UDP/RTP packets is 35/(40+20) = 58.3 %.

PEP packet payload compression uses the V.44 lossless compression algorithm. V.44 is an ITU standardized compression technology based on a Hughes-patented compression algorithm. The PEP stateful compression implementation takes advantage of the guaranteed, in-order delivery service provided by the PEP backbone protocol. Stateful compression is able to take advantage of redundancy in all messages being sent instead of only redundancy within a message, thus providing significantly better compression ratios. Compression ratios of up to 12:1 are achieved.

HN/HX Systems feature IP Payload Compression for UDP Packets utilizing the IP Payload Compression Protocol (IPComp) per RFC 3173 to compress UDP traffic (for example, DNS, BRP, SNMP, Multicast traffic) using a lossless, stateless compression algorithm. The bandwidth savings is a function of traffic type. Bandwidth usage for typical DNS request traffic will be reduced by 10%, DNS responses by 30%, and SNMP traffic by 50%.

Prioritization

With any network it is vital to apply prioritization to ensure that business-critical applications do not suffer due to bandwidth contention with non-vital applications. Hughes HN/HX Systems can be configured to prioritize inbound and outbound traffic based on IP traffic characteristics (for example, by protocol type, IP addresses, port ranges, and other header fields). This allows prioritization based on a machine or application level.

HN/HX Systems maintain four forward channel priorities and four return channel priorities. The four queues carry PEP and non-PEP traffic. Inbound prioritization uses an extra, special queue for handling Constant Bit Rate (CBR) traffic, such as Real-time Transport Protocol (RTP) and facsimile. Packets from the CBR queue are transmitted before packets from any of the priority queues. CBR traffic is also prioritized higher than other traffic in the outbound direction.

PEP classes of service and non-PEP traffic can be mapped to the four forward and return channel priorities. Packet delivery prioritization is based on Protocol Type, Source IP address range, Destination IP address range, TCP/UDP port number, TCP options, ICMP type, Diffserv code point (DSCP) bits, and VLAN ID. Furthermore, the Hughes router supports the capability to preserve and/or modify the DSCP bits and VLAN IDs.

TurboPage HTTP/HTTPS Acceleration

TurboPage Web acceleration increases the speed of Web page loading. All Hughes HN/HX routers support the TurboPage feature that maintains a persistent TCP connection across the spacelink to one of multiple farmed TurboPage servers at the NOC. Persistent TurboPage connections ride on top of the TCP PEP connections and therefore get the full benefit of PEP acceleration. Similar to the benefits of PEP backbones, the TurboPage persistent and pipelined connections between downstream and upstream proxies reduce delays and maximize bandwidth efficiency.

The TurboPage server parses HTML documents and HTTP responses, prefetches the referenced Uniform Resource Locators (URLs), and forwards the information over the satellite link. The prefetched content is then cached by the HN/HX router for immediate response as the user's browser processes the Web page and requests delivery of content.

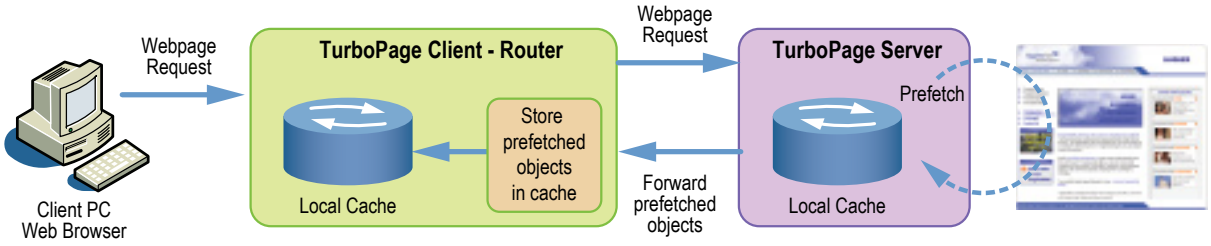


Figure 7. TurboPage Acceleration

TurboPage also optimizes delivery of Web content by compressing HTTP/HTTPS traffic. A stateful compression algorithm is used, producing compression ratios on the order of 15 to 1 for request and response headers. In the outbound direction, stateful compression is used to produce further optimization on compressible objects (for example, HTML, cascading style sheets, JavaScript).

SSL Bridging is a TurboPage feature that provides acceleration for secure (HTTPS) Web pages while maintaining SSL protection of secure Web page data across every communications link on which the data is carried.

DNS Caching

All Hughes HN/HX routers include a DNS caching proxy, which reduces Web page response time by eliminating the satellite round-trip required for a domain name lookup. The DNS caching proxy receives and processes DNS requests and caches the DNS responses. When the TurboPage server prefetches Web page URLs, it also sends the corresponding DNS information to the router. In addition to maintaining resolved domain names that were either visited by the user or prefetched by TurboPage, the router's DNS cache can be preconfigured with entries that never expire or are preloaded from a multicast server.

Network Security

HN/HX Systems can employ several information assurance techniques to safeguard the integrity and confidentiality of data transported through the system.

Conditional Access

Access to the forward channel is restricted by means of the HN/HX System conditional access mechanism. Each Hughes HN/HX router is manufactured with a unique key. The key is used by the HN/HX System to authenticate the satellite router when it is commissioned. The unique key is also used to distribute conditional access "session" keys for receiving unicast and multicast traffic from the forward channel. The latter ensures that only the intended terminal (or terminals, in the case of multicast traffic) can receive the forward channel traffic.

IPSec Encryption

HN/HX Systems provide standards-based IPSec per RFCs 4302, 4303, and 4305; Advanced Encryption Standard (AES) per RFCs 3686, 2404, and 3566; and Internet key exchange (IKE) support per RFC 2409 for encrypting user data traffic and managing encryption keys. The IKE protocol is used to automatically generate and maintain 128- or 256-bit session keys to set up an IPSec tunnel between a Hughes HN/HX router and an enterprise network endpoint. The IPSec tunnel rides over top of the Hughes network conditional access protected forward channel. The complete IP packet is tunneled, protecting the IP information as well as TCP/UDP and above. The tunnel supports all unicast IP traffic, including serial protocols and voice. Satellite acceleration is implemented prior to encryption, thereby preserving the benefits of satellite acceleration in a secure configuration. IPSec is compatible with the Hughes VADB, Secondary Forward Channel, and NOC Diversity features; the IPSec tunnel automatically switches over to the VPN dial backup network or alternate satellite path when a satellite link failure is detected.

The Hughes security kernel included in the satellite router is FIPS 140-2 level 1 certified.

HN/HX Systems provide the necessary protections to adhere to PCI-compliance requirements.

Integrated Serial and Voice Support

HN/HX Systems include integrated serial protocol conversion allowing legacy serial devices to effectively operate over an IP network. In addition to providing optimizations for VOIP devices, Hughes HN/HX routers have built-in support for analog telephones, facsimile machines, and voice-band data modems that enable them to operate as VoIP devices.

Serial Protocols

Serial protocol support extends network boundaries to serial devices connected to the Hughes router and to serial hosts connected to enterprise LANs. Hughes has extensive experience with X.25, SDLC, BSC, and ASYNC networking that has been applied to integrating the legacy protocol support with the HN/HX Systems advanced IP networking capabilities. Satellite router models are available with support for up to four synchronous/asynchronous connections. The following protocol conversions are supported:

- X.25 Remote ⇔ X.25 Host
- X.25 Remote ⇔ XOT Router
- SDLC Remote ⇔ SDLC Host
- SDLC Remote ⇔ LLC Host
- LLC Remote ⇔ LLC Host
- XPAD Remote ⇔ X.25 Host
- XPAD Remote ⇔ XOT Router
- DPAC 3201 Remote ⇔ X.25 Host
- BSC DSPAD Remote ⇔ X.25 Host
- BSC Remote ⇔ IP Host
- ASYNC Remote ⇔ IP Host.
- SLIP Remote ⇔IP Host

Flexible configuration options are offered to meet customer specific protocol requirements.

The serial connections are carried over IP connections and therefore benefit from the PEP performance enhancing features.

Voice over IP

Optimizations for carrying Voice over IP (VoIP) traffic are provided by the HN/HX Systems. VoIP traffic is dynamically detected by the Hughes router's Session Initiation Protocol (SIP) plug-in, and bandwidth resources are efficiently preallocated based on codec usage. VoIP and other constant bit rate data (for example, videoconferencing) can be recognized and prioritized based on Source IP address range, Destination IP address range, TCP/UDP port number, TCP options, ICMP type, and DSCP bits. In addition to supporting third- party VoIP devices, Hughes HN/HX router and appliance models are available that connect to standard analog voice and fax devices and establish VoIP connections on their behalf. These connections are automatically prioritized as Constant Bit Rate (CBR) traffic. In addition, the codec sampling size is optimized for satellite usage to provide high-quality voice over the satellite.

Operations and Support Features

Hughes HN/HX routers have been designed with an emphasis on ease of use and supportability. A Web interface shows information about the router, its connected devices, and the overall system in a way that is easy to use and understand. The Web interface and front bezel LEDs provide a clear indication as to whether the router is operating normally. And if the router is functioning in a degraded mode, the failure is identified and resolution actions are indicated. In addition to providing guidance to the end user, the Hughes router contains extensive diagnostic and troubleshooting capabilities intended for support personnel to effectively identify and resolve local or system problems.

Web Interface

The Hughes HN/HX router's built-in Web server is accessible using a Web browser from any connected computer. It is password protected and highly customizable. Extensive help is provided through local links and configurable links to other network Web servers.

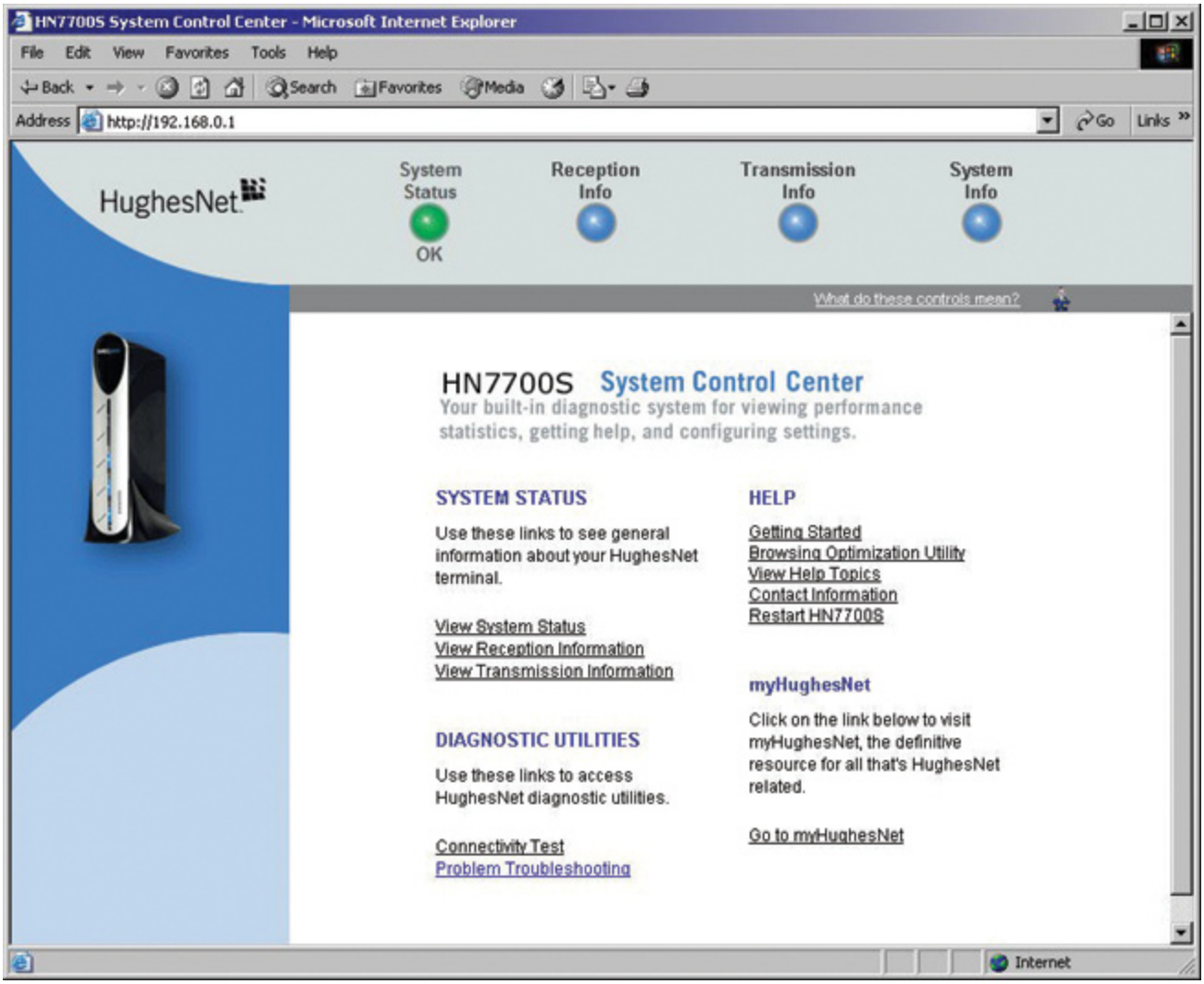


Figure 8. Built-in Web Server

Diagnostics

A connectivity test link is presented on the Web Interface that can be used to verify connectivity between the router and NOC Gateway. An optional Problem Troubleshooting link is available to support end-user troubleshooting.

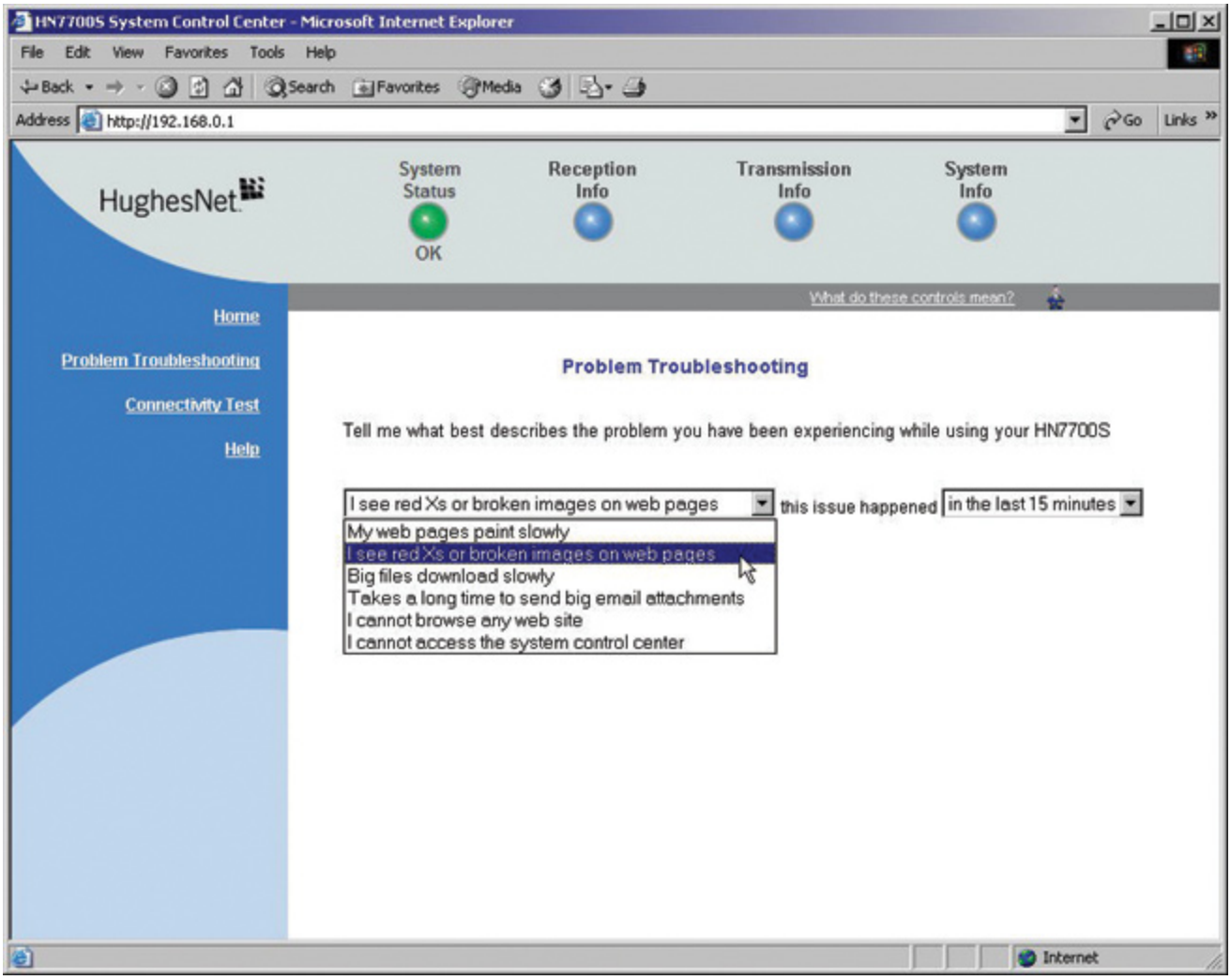


Figure 9. Problem Troubleshooting Web Page

Advanced diagnostics are provided, which identify a set of configurable system problems that are automatically detectable by the Hughes HN/HX router via configurable statistics maintained in the router. The problem detection is done on two configurable monitoring intervals (for example, 5 minutes, and 1 hour). Figure 10 shows the Advanced Hourly History page presenting the system problem(s) detected in each 1-hour interval in the previous 24 hours. Clicking on a Green Check or Red X displays the detailed statistics page for the selected interval.

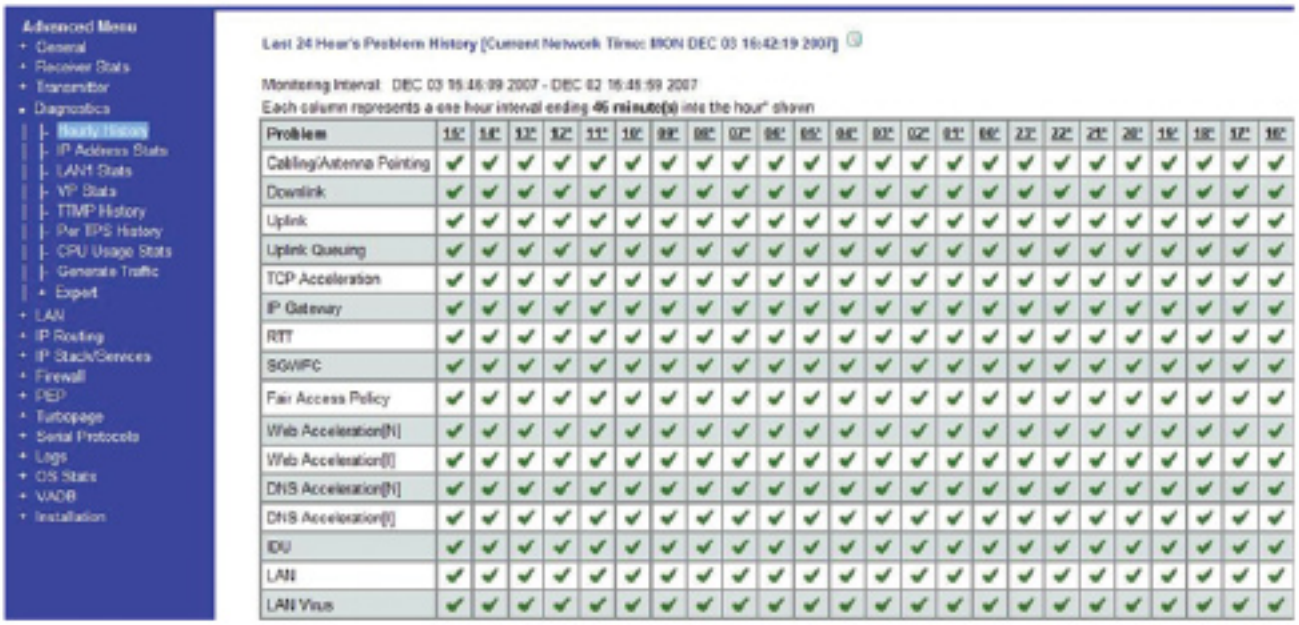


Figure 10. Advanced Diagnostics Hourly History Web Page

Diagnostic data and backup statistics can be archived to the router's permanent file system and periodically uploaded to a FTP server.

Troubleshooting Capabilities

In addition to its comprehensive automatic diagnostics, the Hughes HN/HX router provides detailed module level statistics and tools useful to support personnel. A ping test utility initiates pings from within the router, and a browsing test initiates HTTP gets to a configurable URL list while measuring response times. An input filter utility looks at all IP packets received from LAN ports and maintains statistics on the number of TCP/UDP packets received for each destination port number and the number of other packet types received.

A packet capture utility provides the ability to capture various packets sent and received on each of the router's interfaces. As illustrated in Figure 11, the utility provides flexible configuration of the data to be captured. The packet dump output is a PCAP formatted file, which can be analyzed by popular protocol analyzer applications to accurately display network, transport, and application dissections. This built-in utility can eliminate the need for on-site personnel to deploy and capture interface traces.

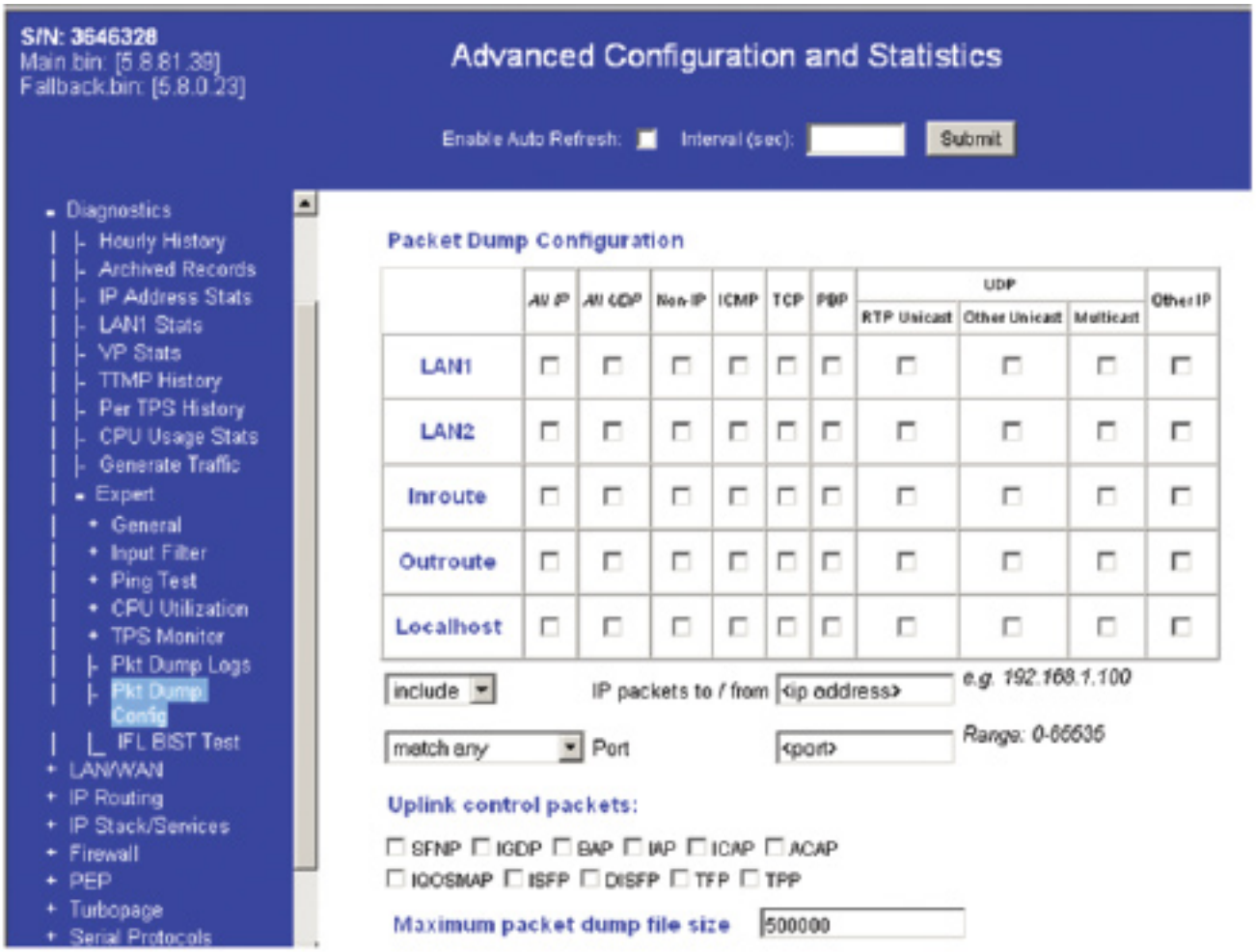


Figure 11. Built-in Packet Capture Utility

The Hughes HN/HX router maintains detailed event logs with local and GMT time correlation in its permanent file system. Events can optionally trigger the sending of SNMP traps to one or more trap servers.

Hughes HN/HX routers include FTP and Telnet hosts useful to support personnel for remote troubleshooting and retrieval of diagnostic and log files. A built-in RADIUS client feature can be enabled to authenticate incoming FTP or Telnet sessions via a remote RADIUS Server. If not required, local and remote HTTP, FTP, and Telnet access can be disabled.

Application Programming Interface

Hughes HN/HX routers support HTTP and socket-based Application Programming Interfaces (APIs) to provide seamless integration with third- party applications and subsystems such as motorized antennas for mobile applications and PC customer care programs.

Configuration and Management

The Hughes management system provides centralized configuration and management for Hughes HN/HX routers, including software upgrades. A network operator is able to upgrade the configuration of software for thousands of remote sites with a simple single process, and the upgrade is automatically installed with less than a minute of service disruption.

HN/HX Systems employ a NOC Diversity feature which allows HN/HX routers to be managed by two different NOCs, providing geographic diversity. In the event of a NOC failure, the routers can be managed from the secondary NOC. NOC diversity also provides the ability to temporarily force routers to the alternate NOC in order to balance the load on NOC components.

HN/HX routers include a standards-compliant SNMP agent. The SNMP agent responds to queries from SNMP managers configured via the Hughes management system. Up to 10 entries can be configured with SNMP Manager IP Address, Community String, and Read or Write Access Mode.

The router's Web Interface optionally supports configuration of features that may be better managed by the local user, for example, Port Forwarding and ACLs.

Acronym List

ACL	Access Control Lists	NAPT	Network Address and Port Translation
AES	Advanced Encryption Standard	NAT	Network Address Translation
ALG	Application Layer Gateway	NOC	Network Operation Center
API	Application Programming Interfaces	NTP	Network Time Protocol
AS	Autonomous System	PAT	Port Address Translation
BGP	Border Gateway Protocol	PBR	Policy-based Routing
BRP	Broadcast Routing Protocol	PCAP	Packet Capture
BSC	Binary Synchronous Communication	PEP	Performance Enhancing Proxy
CBR	Constant Bit Rate	POS	Point of Sale
DHCP	Dynamic Host Configuration Protocol	PPTP	Point-to-Point Tunneling Protocol
DNS	Domain Name Server	QoS	Quality of Service
DPAC	Datapac	RFC	Request for Comments
DSCP	Diffserv Code Point	RIP	Routing Information Protocol
DSPAD	IBM 3270 Display System PAD	RTP	Real-Time Transport Protocol
DSL	Digital Subscriber Line	SDLC	Synchronous Data Link Control
FIA	Fenced Internet Access	SIP	Session Initiation Protocol
FTP	File Transfer Protocol	SLIP	Serial Line Internet Protocol
GMT	Greenwich Mean Time	SNMP	Simple Network Management Protocol
ICMP	Internet Control Message Protocol	TCP	Transmission Control Protocol
HTTP	Hypertext Transfer Protocol	UDP	User Diagram Protocol
HTTPS	Hypertext Transfer Protocol Secure	URL	Uniform Resource Locator
IETF	Internet Engineering Task Force	VADB	VPN Automatic Dial Backup
IKE	Internet Key Exchange	VLAN	Virtual LAN
IP	Internet Protocol	VoIP	Voice over IP
IPComp	IP Payload Compression Protocol	VPN	Virtual Private Network
IPSec	Internet Protocol Security	VRID	Virtual Router Identification
ITU	International Telecommunication Union	VRRP	Virtual Router Redundancy Protocol
LAN	Local Area Network	WAN	Wide Area Network
LLC	Logical Link Control	WINS	Windows Internet Name Service
MAC	Media Access Control	XOT	X.25 Over TCP
MPLS	Multiprotocol Label Switching		

Appendix A RFCs Supported

The RFCs in the following table are supported by Hughes HN/HX broadband satellite routers. Enhancements are continuously being introduced, so this list should not be considered as being complete.

IP Protocol RFCs	
RFC 791 (IPv4)	RFC 792 (ICMPv4)
RFC 793 (TCP)	RFC 768 (UDP)
RFC 959 (FTP)	RFCs 854/855 (Telnet)
RFC 1112 (IGMPv1)	RFC 2236 (IGMPv2)
RFC 3376 (IGMPv3)	RFC 1661 (PPP)
RFC 2516 (PPoE)	RFC 1157 (SNMP)
Routing Protocol RFCs	
RFC 1058 (RIPv1)	RFC 2453 (RIPv2)
RFC 1256 (IRDP)	RFC 3768 (VRRP)
RFCs 1519/4632 (CIDR)	RFCs 1771/1772/4271 (BGP)
RFC 1997 (BGP Communities Attribute)	RFC 2842 (Capabilities Advertisement)
RFC 2385 (BGP use of TCP/MD5)	RFC 2796 (BGP Route Reflection)
RFC 2439 (BGP Route Flap Dampening)	RFC 2918 (BGP Route Refresh Capability)
RFC 4360 (BGP Ext. Communities Attribute)	RFC 3065 (AS Confederations for BGP)
IP Services RFCs	
RFC 3022 (NAT)	RFC 1939 (E-Mail: POP)
RFC 3501 (E-Mail: IMAP)	RFC 3461 (E-Mail: SMTP)
RFCs 2131 (DHCP)	RFCs 3046 (DHCP Relay)
Performance Features RFCs	
RFC 1349 (TOS)	RFC 3173 (IPComp)
RFC 2616 (HTTP)	RFC 2474 (DSCP)
RFC 3051 (V.44 Compression)	RFC 2818 (HTTPS)
RFC 3095 (Robust Header Compression)	RFC 1144 (Header Compression)
Network Security RFCs	
RFCs 4302 (IPsec: AH)	RFCs 4303 (IPsec: ESP)
RFC 4305 (ESP/AH Crypto Requirements)	RFC 1321 (MD5)
RFC 1829 (DES)	RFC 1851 (3DES)
RFC 2085 (HMAC-MD5)	RFC 2404 (HMAC-SHA-1)
RFC 2409 (IKE)	RFC 3566 (AES-XCBC-MAC-96)
RFC 3686 (AES)	RFCs 4346/4366 (SSL/TLS)

Proprietary Statement