RanchNetworks
Security and Networking Innovation

RANCH NETWORKS PRODUCTS
BENEFITS SUMMARY

Ranch Networks products consolidate an unprecedented set of security and data networking capabilities into a single device. The table below summarizes the capabilities contained in each of our products. (For additional details see our Product Line Data Sheet.) The sections below the table describe the primary benefits of each function.

CAPABILITY	RN40/41	RN20	RN5A	RN5B	RN5C	RN300
Physical Interfaces	10x 10/100/1000	12x 10/100	12x 10/100	12x 10/100	12x 10/100	3x 10/100
Segmented Network Security	✓	✓	✓	✓	✓	✓
Multiple Secure Zones (Total physical and virtual)	**30**	**12**	**5**	**5**	**5**	**3**
LAN Overlay	✓	✓	✓	✓	✓	✓
Physical Zones	**10**	**12**	**5**	**5**	**5**	**3**
Virtual Zones	**30**	**30**	**5**	**5**	**5**	**5**
Special support for Voice-over-IP	✓	✓	✓	✓	✓	✓
Role-Based Authentication and Authorization	✓	✓	✓	✓	✓	✓
User Authentication based on LDAP, RADIUS, Microsoft Active Dir., Local Data Base	✓	✓	✓	✓	✓	✓
Policy-driven Security-On-Demand	✓	✓	✓	✓	✓	✓
Security based on MAC address	✓	✓	✓	✓	✓	✓
Deny outgoing connections	✓	✓	✓	✓	✓	✓
Port mirroring and Rate Limiting	✓	✓	✓	✓	✓	✓
Consolidation of multiple devices	✓	✓	✓	✓	✓	✓
Bandwidth Management	✓	✓	✓	-	✓	✓
Load Balancing	✓	✓	-	✓	✓	-
Server Health Monitoring	✓	✓	-	✓	✓	-
Multicasting	✓	✓	-	-	-	-
Layer 2-4 Switching	✓	✓	✓	✓	✓	**L3-4**
Static Routing	✓	✓	✓	✓	✓	✓
Accounting	✓	✓	✓	✓	✓	✓
Remote Management (GUI, SNMP)	✓	✓	✓	✓	✓	✓

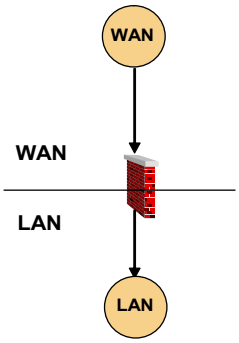
Segmented Network Security
Multiple Secure Zones

Segmenting a network into Secure Zones can achieve a number of important objectives:

- Special security for sensitive application servers
- Separate Secure Zones for multiple customers sharing a Data Center or a LAN
- Allowing only users within a given "area of trust" to have access to restricted information. So for instance, only the Accounting people will have access to the financial applications and data. Only the R&D people will have access to their Intellectual Property.
- Preventing unauthorized access to sensitive areas of the LAN
- Limiting the spread of viruses
- Keeping Operating Systems from being scanned or hacked, even if their latest patches have not yet been installed, by stopping intruders before they get to the server.
- Limiting access to the network from Guest Cubicles, Conference Rooms, and Wireless LAN Access Points.
- Meeting regulatory requirements for privacy and access control to data
- Decreasing the risk of theft or financial fraud

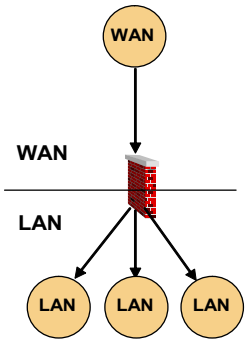
Ranch Networks' products provide Virtual Firewalls with full stateful capability between each pair of Secure Zones.

Traditional Network Security vs. Segmented Network Security



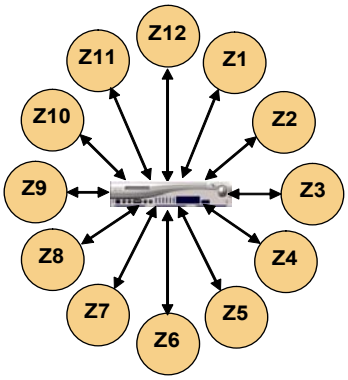
Traditional Firewall:

- "Outside" and "Inside"
  - 1 stateful firewall
  - Unidirectional



Partial Segmentation:

- 3 "zones"
  - 3 stateful firewalls
  - Unidirectional
  - No security policies between zones



Ranch LAN Segmentation:

- Up to 30 zones
  - Virtual Stateful Firewalls between each pair of Zones in both directions (any-to-any)
- Multiple layers of security for each zone
- Many additional data networking functions

LAN Overlay Installation

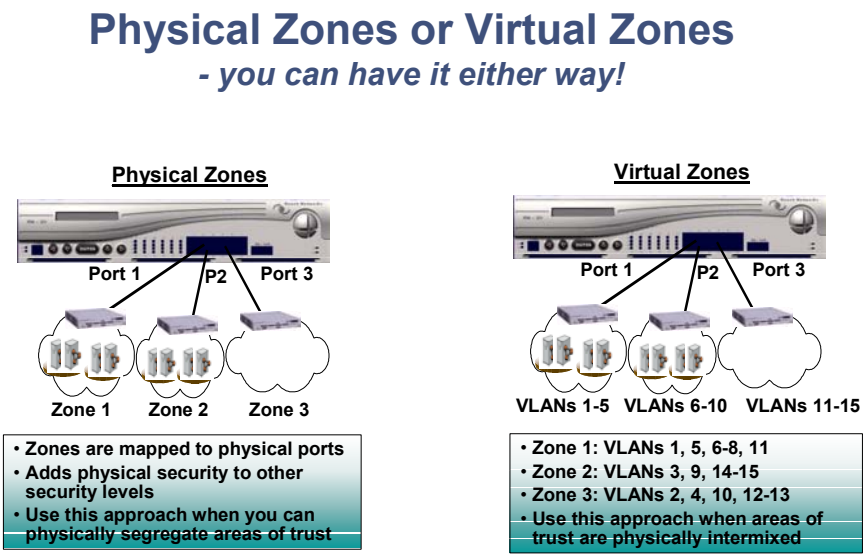
Segmenting a network into separate secure zones normally requires creating new sub-nets and reconfiguring Host IP addresses. By using Ranch Networks Patent Pending "Split-Subnetting" multiple secure zones can be created without significant rewiring or the need to reconfigure Host IP addresses.

Full Stateful Virtual Firewalls

Some other methods for LAN security include Access Control Lists or VLANs. Ranch Products incorporate these capabilities but also include Full Stateful Firewalls between each pair of Secure Zones, in both directions.

Physical Zones
Virtual Zones

Ranch Products offer two basic methods for defining Secure Zones. One method is using Physical Zones, where a Zone is defined as one or more physical ports on the RN device. Thus the Zone consists of the entire network segment connected to the physical port(s). The other method is Virtual Zones, where a Zone is defined as one or more VLANs. The VLANs in a Secure Zone can be associated with any of the physical ports. The Physical Zones approach is best when the network topology corresponds well to the desired "areas of trust" where as Virtual Zones are preferable when people and servers from various organizations in a company are interspersed throughout the network. Both Physical Zones and Virtual Zones can be used in the same device at the same time.



Special Support for Voice-over-IP

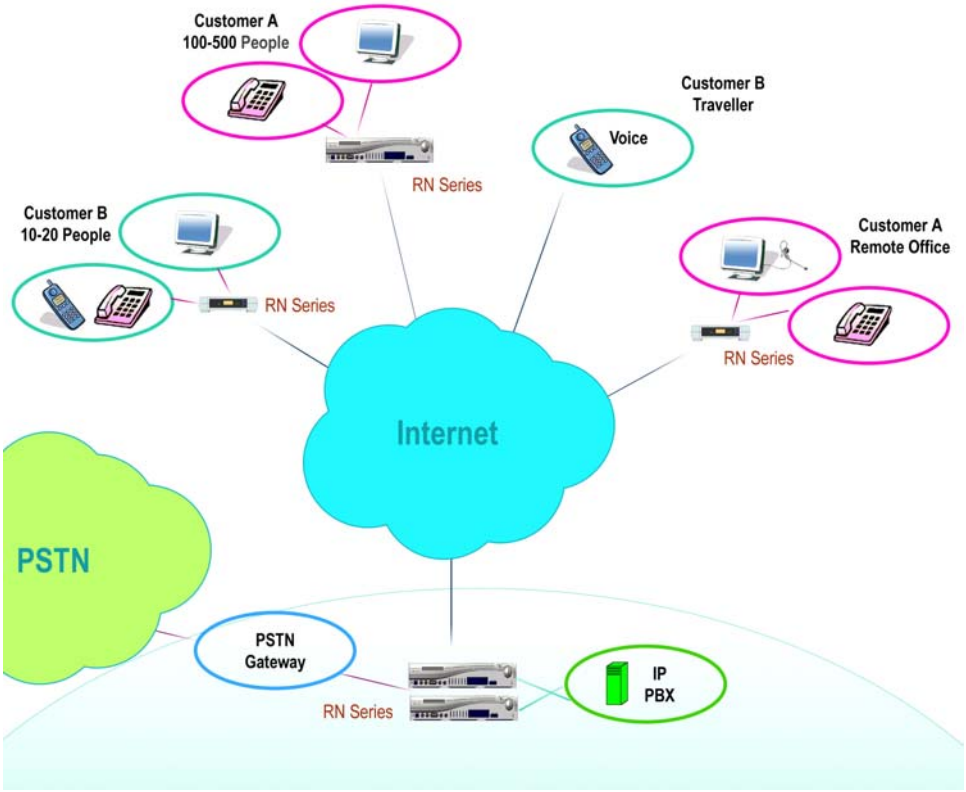
RN devices provide dynamic security, NAT traversal, and bandwidth management for VoIP – regardless of the signalling protocol used and whether or not the signalling or media traffic is encrypted. This allows Ranch solutions to negate many of the network issues typically encountered when delivering VoIP services - issues involving security, performance, NAT traversal and network re-architecting. The Ranch architecture is perfectly suited for a variety of IP Telephony applications.

Unlike Application Layer Gateway (ALG) or Session Border Controller (SBC) approaches, Ranch does not need to interpret signalling protocols or track call states. Instead it receives call set-up and teardown information directly from the Softswitch or IP PBX using an IETF-specified protocol. This approach avoids the security issues inherent with ALGs and SBCs. Most Ranch devices incorporate a dedicated CPU and internal back plane for dynamic VoIP control, allowing them to scale up for very large service provider networks.

VoIP Feature Set Overview

- Dynamic per-call firewall control
- Dynamic per-call bandwidth control
- NAT traversal
- Universal signalling protocol compatibility (SIP, H.323, MGCP, etc.)
- Ability to handle encrypted VoIP Traffic
- WAN failover to back-up gateway for local survivability
- Adjunct Systems Health Monitoring
- Protecting the IP PBX and Adjunct Systems (Denial of Service, Firewall, etc.)
- Endpoint-to-endpoint media traffic
- Preservation of location-specific IP addresses
- Network Call Usage Reporting
- VoIP Overlay Installation
- CALEA support
- Video, IM, Wireless, and other support
- Solutions for a full range of VoIP deployment types
- Redundancy

VoIP Solution for Network-Hosted IP PBX



Role-Based Authentication and Authorization

When enabled, this feature denies network access until a user has been authenticated and once authenticated, allows the user access only to permitted areas of the network. This capability is particularly useful for selectively controlling access from Wireless LAN Access Points. For example, guests entering the network through a Wireless LAN can be allowed access to the Internet but not to the rest of the LAN, whereas employees entering through the Wireless LAN can be authenticated and access those portions of the network where they would normally be allowed. Access within a Secure Zone can be constrained to specific IP addresses, port numbers, or MAC addresses. Other features include authorization profiles for groups or individual users and classification of users into categories for simple moves/adds/changes.

Policy-driven Security-on-Demand

This refers to the ability for new security policies to be dynamically added to the Ranch device using SNMP via the Management Port. This can be useful for integration with Security Policy Management Systems, Intrusion Detection Systems, IP PBXs, and other systems.

Security based on MAC address

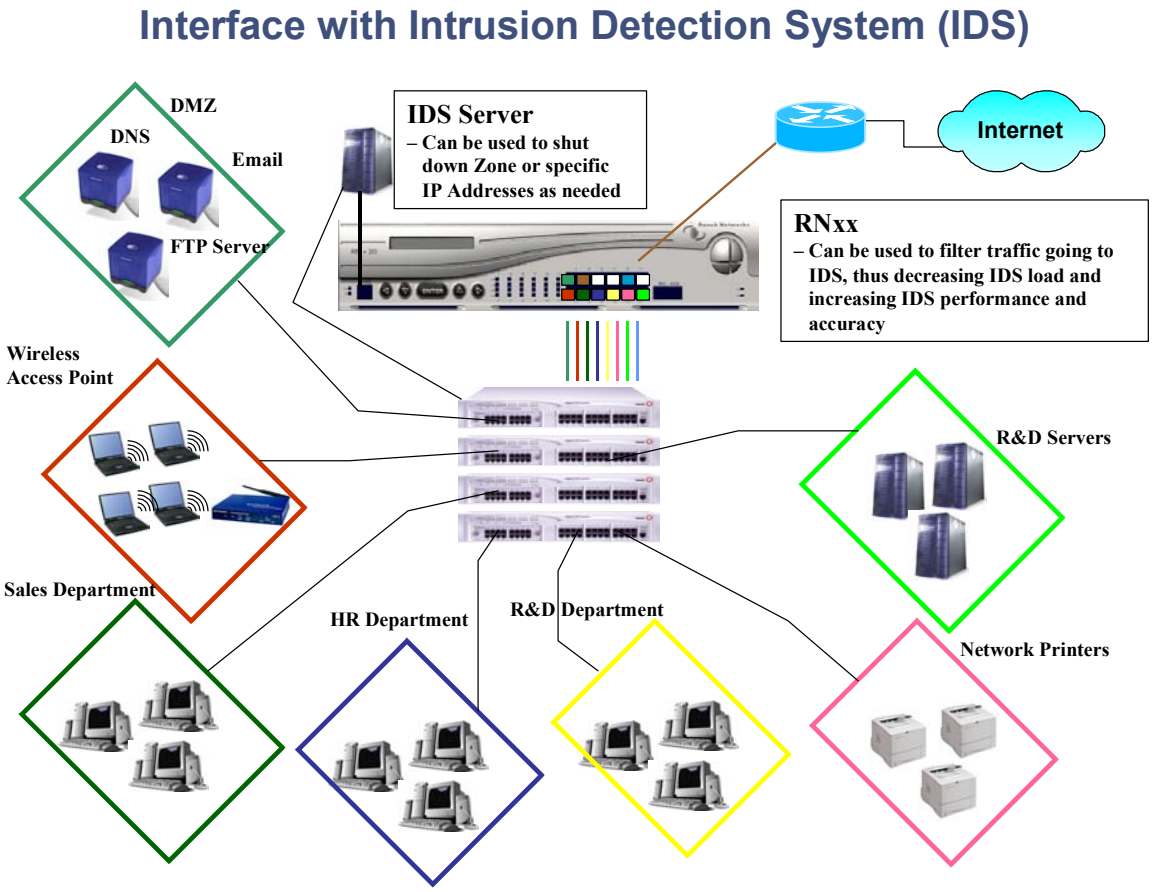
Firewall rules can be configured based on MAC addresses.

Deny outgoing connections

In many cases server applications are configured to respond to client requests but under normal circumstances they do not initiate new connections. However if the server or application is infected by a virus it may initiate new connections in order to spread itself to other servers. Ranch devices can be configured to deny any type of outgoing connections from a Zone, so that if the virus is attempting to spread through this means it is prevented.

Interface to Security Event Management (SEM) or Intrusion Detection Systems (IDS)

Ranch products can interface to SEM/IDS systems in two important ways. First, the Ranch device can be used to filter traffic going to the SEM/IDS, so that only specific traffic can be analyzed and those systems not overloaded. If desired, a company could periodically sample traffic from various sources by changing the configuration of the Ranch device. Second, if the SEM/IDS detects an intrusion, it can send a secure message to the Ranch device instructing it to close off a Zone or a specific IP address.

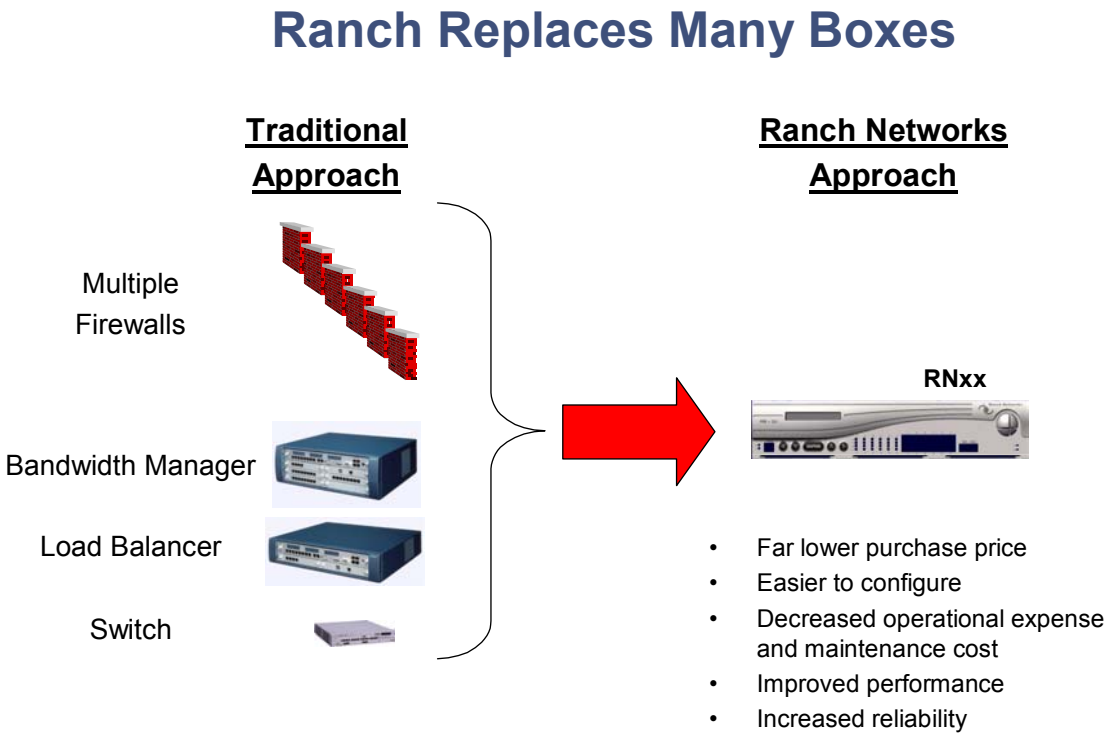


Port Mirroring and Rate Limiting

Rules can be configured to mirror specified traffic to another port, or to limit the rate at which specific traffic can be sent through the Ranch device. Port mirroring is useful for traffic monitoring in conjunction with systems such as Intrusion Detection Systems. Rate limiting is useful in defeating Denial of Service attacks.

Consolidation of multiple devices

One of the important benefits of the Ranch Networks products is that they allow the customer to avoid having to purchase and maintain many separate devices. Depending upon the specific network requirements, this can save the customer tens of thousands of dollars in the initial purchase price alone. In addition to CapEx and OpEx savings, consolidating multiple boxes into one device improves performance and reliability. From a performance perspective, instead of multiple boxes each having to open and inspect a packet and forward it on, this now needs to only occur once. Ranch's patent pending Single Pass Packet Scan algorithm performs this function. From a reliability perspective, going from multiple boxes to a single device decreases the total number of power supplies, fans, and electronic and mechanical components. Thus overall system reliability is increased. Ranch products have been designed to meet rigid NEBS Level 3 compliance – tough Telco-grade Central Office standards.



Bandwidth Management

Ranch products contain most of the functionality typically found in dedicated, single-function Bandwidth Managers or Traffic Shapers. This includes:

- Contracts can be set to permanently allocate bandwidth
- Subcontracts can be set to guarantee bandwidth when it is needed, but if not needed it will be shared with other applications

- Traffic can be classified into Contracts or Subcontracts (or no prioritization) based on Source or Destination Zone, Source or Destination IP Address, Source or Destination Protocol Port, or other Protocol information
- TOS or DiffServ bits can be set
- Prioritization (classification) can be made based on TOS and DiffServ bits

Some of the important benefits of Bandwidth Management are:

- Provide Quality of Service for time-sensitive (real-time) traffic such as Voice-over-IP and Video-over-IP
- Provide prioritization for mission-critical applications
- Provide prioritization for specific groups of users
- Limit the bandwidth used for applications such as file transfers and downloads
- Avoid the cost of expensive WAN upgrades through more efficient utilization of existing bandwidth
- In an environment where a single Ranch device is supporting multiple customers, each customer can have their own guaranteed bandwidth

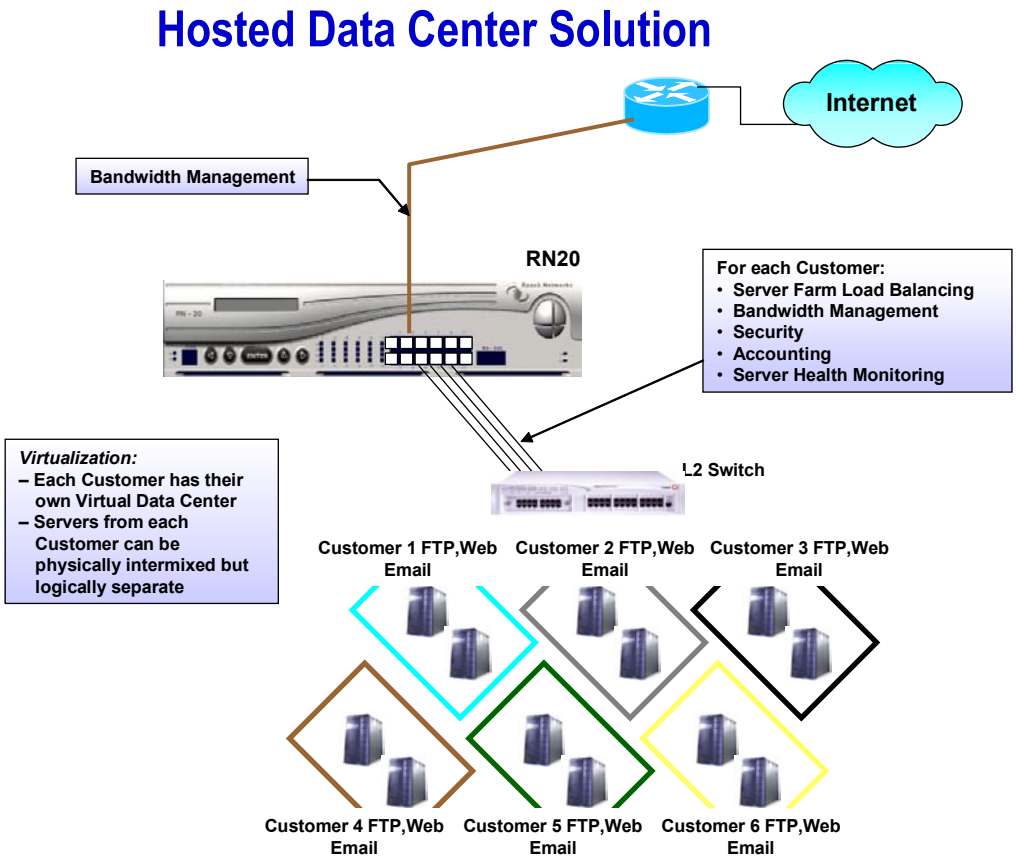
Load Balancing

Ranch products that include the Load Balancing feature contain most of the functionality typically found in dedicated, single-function Load Balancers. This includes:

- Load Balancing for up to 1024 logical servers (server clusters) which can be located in any of the Ranch devices' Zones
- Common Load balancing algorithms such as Round Robin, Weighted Round Robin, and Least Connections
- Persistency can be provided via: Cookie, SSL, Client IP HTTP, HTTPS, FTP (active and passive)
- Support for RFC-822, TCP, and UDP applications
- Data Center Virtualization

Some of the important benefits of Load Balancing are:

- Improve Data Center utilization and performance
- Improve application performance
- Avoid having to add additional servers through more efficient utilization of existing servers
- Avoid having to purchase a separate box for Load Balancing
- In an environment where a single Ranch device is supporting multiple customers, such as Hosting Center, each customer can have their own private Load Balancing among their own servers. Multiple Load Balancing clusters can be supported per customer up to a total of 1024 Load Balancing clusters per Ranch device.
- Due to Virtualization it is not necessary for all servers within a Load Balancing cluster or Secure Zone to be physically segregated. They can be anywhere within the RN's network that is reachable by VLAN.



Server Health Monitoring

Ranch products provide the ability to monitor servers and desktops to ensure they are working properly. If a problem is identified an alarm can be sent via SNMP. The following types of monitoring are provided:

- Link monitoring (Layer 2)
- ICMP ping verification (Layer 3)
- TCP connection verification (Layer 4)
- Active content verification for HTTP, HTTPS, and FTP
    - 5 URLs per logical server cluster for active content verification monitoring
    - Configurable login ID for FTP
    - Client/server hello test for HTTP, HTTPS

Some of the important benefits of Health Monitoring are:

- Improve the availability of resources by knowing instantly when a problem occurs
- Active content verification means that the web server can be forced to access a database server behind it, so that the proper operation of both servers is verified
- Have confidence that resources are up and running properly
- Monitor the network and resources at multiple levels
- Avoid the cost of other network monitoring system

Multicasting

Some of the Ranch's products provide Multicasting with the following capabilities:

- Based on RFC 1112/2236/2933
- Hardware assisted; up to 10 Gbps of Multicast traffic
- Multicast traffic can be limited to only portions of the network based on firewall-like rules. Multicast distribution can also vary depending upon the source of the multicast traffic.

Some of the important benefits of Multicasting are:

- Multicasting decreases the overall level of traffic on the network for broadcast-like applications such as video streaming
- Because of fine-grained control of multicast traffic, streams can be directed only to those recipients that are permitted to receive multicast traffic from specific sources

Switching

Layer 2-4 Switching is provided with VLAN support.

Static Routing

Ranch devices contain static routing tables.

Accounting

All Ranch devices have the ability to count packets and bytes so that network usage can be monitored or charged back to users. As with Bandwidth Management, traffic can be classified for Accounting purposes based on Source or Destination Zone, Source or Destination IP Address, Source or Destination Protocol Port, or other Protocol information. The number of packets (or bytes) corresponding to the classification specification is counted. An external Accounting, Billing, or Network Management System can query the Ranch device periodically in order to read the counters and bill (or measure) users accordingly. Over a thousand Classification Categories can be defined.

Some of the important benefits of the Accounting function are:

- Monitoring network usage by application, user (or group of users), server (or group of servers), or network segment
- Charging back network expenses to departments based on their usage
- In environments where a Ranch device is being used to serve multiple customers, usage by each customer can be tracked so that each can be charged depending on usage.

Remote Management

The primary methods of Remote Management are a Web-based GUI (Graphical User Interface) and SNMP. The Web-based GUI can be accessed through either HTTP or HTTPS. All features of the Ranch products can be configured through this interface. A demonstration of the GUI interface for the RN20 can be found at www.ranchnetworks.com. Ranch devices support Versions 1, 2C, and 3 of SNMP. Ranch devices support the following SNMP MIBs:

- RN Enterprise Configuration MIB
- RN Enterprise Auto-Discovery MIB
- RN Enterprise Statistics MIB
- RFC 1213 MIB-II
- RFC 1493 Bridge MIB
- RFC 1573 Interface Extensions MIB
- RFC 1643 Etherlike MIB
- RFC 1757 RMON1 MIB: Etherstats

In addition to the GUI and SNMP interfaces, RN devices also support email alerts and Syslog.

The benefits of these Remote Management tools are:

- easy configuration
- automatic monitoring of deployed devices from a central location
- compatibility with leading network monitoring systems
- the use of standard tools familiar to security and networking professionals
- convenient storage of primary and secondary Configuration Files
- convenient storage of primary and secondary Images