

Machete Embedded Router

ATCorp's Machete embedded router delivers advanced networking that enables effective and timely dissemination of mission critical information among tactical edge users.

Hardware Systems

Machete is part of the OnTime Networks Routing Solutions, optimized for networks that require IP routing and services. The flexible, compact form factor of the OnTime Networks CR-4000, CR-6000 and CR-7000 routers, complemented by **Machete**, provides highly secure NIAP certified data, voice, and video communications to stationary and mobile network nodes across wired and wireless links.

Virtual Systems

The **Machete** virtual appliance, deployed on VMWare ESXi 7 and higher, complements the OnTime Networks rugged hardware routers to provide integrators with a cost-effective solution for addressing smaller applications where a fully rugged OnTime Networks Ethernet switch or Time Server is not required. The **Machete** virtual appliance can be combined with system-specific applications onto a single, small, low-power hardware solution.

Tactical Communication

Machete enables air-to-air and air-to-ground communications over a variety of radio waveforms such as 4G/5G, ANW2, CDL, SATCOM, Streamcaster, TSM-X, TTNT, WiFi, and more.

Advanced Tactical Networking

DoD tactical networks present unique routing challenges because of node mobility, changing data-link capacities, and crypto separation. Machete was designed to address these challenges through a number of optimizations that are specific to tactical environments, including:

- Bandwidth/loss/latency sensing between routers to dynamically adjust to the best available path
- Optimized multicast operation that tolerates RP failure and minimizes flooding
- Enhanced multicast emulation across NBMA links
- Advanced compression of routing-control data across low-bandwidth SATCOM links

Key Features and Benefits

Machete provides optimal performance in the most demanding environments without the EOL timeline found in other commercial routers.

- Cost-effective retrofit of existing airborne networks for mission-assured multicast applications
- Timely and secure dissemination of multicast data among tactical edge users (ISR and C2 video, voice and data)
- Resilient and efficient multicast operations for mobile users, multiple COIs



- Backward compatibility with existing COTS applications and existing network infrastructure. No changes to existing network applications facilitates rapid and cost-effective deployment of the solution. Similarly, no changes to existing COTS network elements such as routers or WAN accelerators are needed
- **Modular and Open Systems Architecture (MOSA)**, fostering multi-vendor interoperability and extensibility and lowering acquisition and operating costs

Router / Firewall protocols	
IPv4/IPv6 routing	BGP, BMP OSPFv2, OSPFv3 RIP, RIPng ISIS, ISIS v6 EIGRP NHRP BFD LDP Static routes Policy-based routing
VPN	FIPS-certified IPsec VPN Site-to-site VPN (IPSec for IPv4 and IPv6) Supports road warrior remote VPNs
Tunnels	GRE, IPIP, SIT, VXLAN
IP address management	Static DHCP server, DHCP client, DHCP relay DHCPv6 Server, DHCPv6 Client, DHCPv6 Relay
Firewall	Stateful inspection firewall IPv6 firewalling (planned 2023) Time-based firewall rules Rate limiting ICMP Type filtering
Management	Integrated CLI accessible by serial or ssh SNMP Configuration file
Radio Aware Networking	Automated GRE tunnel establishment Dynamic link sensing of end-to-end bandwidth/latency/loss DLEP (planned 2023)
Multicast	IGMP v2/v3 PIM-SM, PIMv6 PIM-DM (planned 2023) SMF (planned 2023)
NAT	Source/Destination NAT Port forwarding One-to-one, one-to-many and many-to-many translations