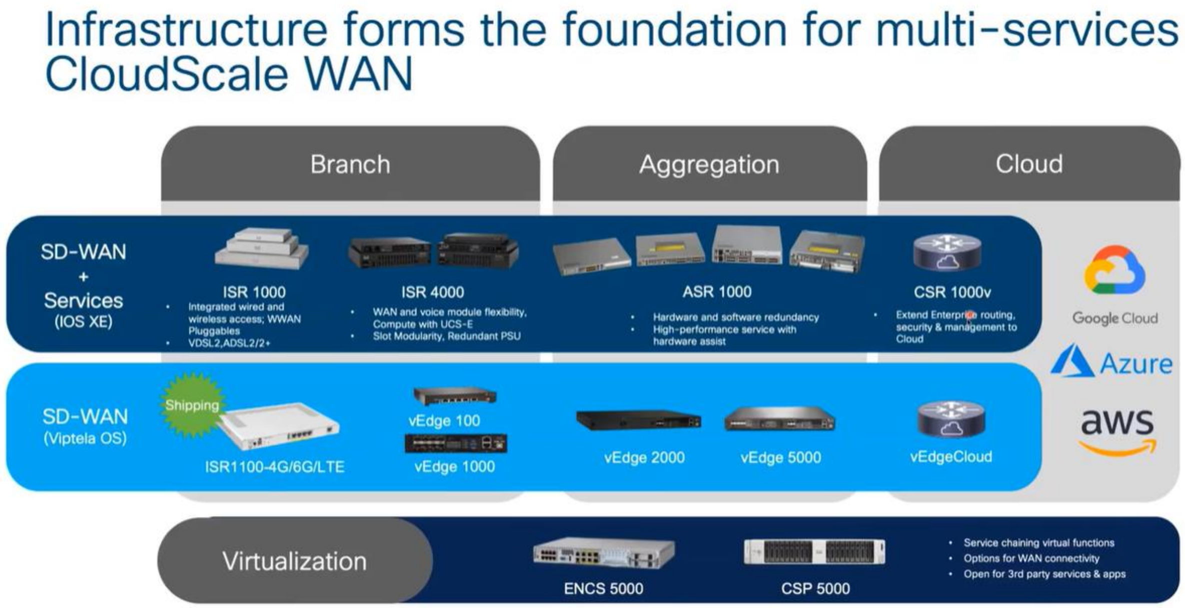
Router and ISR Training

Created by Lance Loftin, SYNNEX Comstor TSE



Infrastructure forms the foundation for multi-services CloudScale WAN

Branch | Aggregation | Cloud

SD-WAN + Services (IOS XE)

ISR 1000
- Integrated wired and wireless access; WWAN Pluggables
- VDSL2,ADSL2/2+

ISR 4000
- WAN and voice module flexibility, Compute with UCS-E
- Slot Modularity, Redundant PSU

ASR 1000
- Hardware and software redundancy
- High-performance service with hardware assist

CSR 1000v
- Extend Enterprise routing, security & management to Cloud

SD-WAN (Viptela OS)

Shipping

ISR1100-4G/6G/LTE

vEdge 100

vEdge 1000

vEdge 2000

vEdge 5000

vEdgeCloud

Google Cloud

Azure

aws

Virtualization

ENCS 5000

CSP 5000

- Service chaining virtual functions
- Options for WAN connectivity
- Open for 3rd party services & apps

- Model breakout, why you'd choose one over the other
    - Branch router vs Edge router
        - Routers are named based on where their location in the network is
        - Branch routers are deployed at ROBO locations while the term Edge router usually refers to the connection to the ISP from a larger location, like the HQ
        - Since there are fewer devices in a branch, routers typically support many features (hence the ISR name). Edge routers may focus more on throughput than features because these larger environments can afford to have more devices/roles
    - **Throughput**
        - Main consideration when choosing a router. Must account for services being turned on since this can influence the performance of a router. Depends on the model. Look for performance whitepapers
        - Remember that ISPs can list their speeds symmetrically. Routers bandwidth requirements are based on the combined total of incoming and outgoing throughput. The sum of the upstream + downstream bandwidth should be used to size the router
        - Different vendors report their "bidirectional" throughput differently. Cisco uses the total performance capacity, regardless of direction; for example, someone might say an ISR 4331 is 2Gbps "bidirectional" when that means it supports 1Gbps UP + 1Gbps DOWN. Another vendor might say that they support 2Gbps "bidirectional" and they mean 2Gbps UP + 2Gbps DOWN. It depends on the vendor and it's important to compare apple to apples
    - **Features**
        - The features that are required influence the licensing and memory utilization.
    - Number of NIM and SM slots
        - Differing models support varying numbers of slots for modules. A higher model may need to be chosen regardless of throughput, though this isn't typical

        - Modules can include small compute blades, switches, additional routed ports, wireless WAN interfaces, voice interface cards, etc
        - NIMs can support up to 2Gbps, Services Modules can support up to 10Gbps toward system or 1Gbps toward other modules (specific to ISR 4K)
    - **Number of ports**
        - The data sheet and hardware installation guide show this best, but keep in mind that some interfaces are listed twice. These are combo ports. They are essentially a single port that has two options, an SFP and a copper option. The hardware installation guide shows interface IDs that I reference at times. Two ports that are combo ports will share the same interface ID
    - PSU redundancy
        - Only available on the 4400 series.
    - E-Series
        - Since a branch office is a small deployment, if a server is needed it could be added into the ISR router itself. This would be added into vCenter and managed just like a traditional server.
- Security features
    - Snort (IDS/IPS)
        - Requires SEC license and 4GB additional memory plus Snort subscription (L-SNT4431-S=, for example)
        - Supported on ISR 4k, ISRv, CSR, ISR 1K
        - Monitoring via a third-party app, Splunk is recommended
        - Cannot use Boost mode/license with Snort IPS because Boost is using the extra CPU cores required for IPS. WAAS also requires the extra CPU cores
    - Umbrella
        - Requires SEC license and per device subscription (UMBRELLA-SUB + UMB-BRAN-4451, for example)
    - ZBFW
        - Requires SEC license
        - App Aware requires AppX (which comes with SEC)
    - VPN
        - Requires the SEC license
        - Certain options may require AnyConnect licensing on top of the SEC license
        - Supports IPsec, DMVPN, FlexVPN, and GET VPN (no SSL)
    - URL Filtering
        - Requires SEC license plus an additional 4GB memory
    - SIG (Secure Internet Gateway)
        - Included in DNA Premier for SD-WAN or in Umbrella subscription (UMB-SEC-SUB + UMB-SIG-ESS-K9)
        - Licensed by number of users
- Licensing
    - Performance vs Boost
        - Previously with the boost license, ISRs limited their bandwidth so that adding additional services would not degrade performance much, if at all. The Boost license removes that software cap and now the only limit is what the physical hardware is capable of. This means adding services will definitely reduce performance
        - Examples of typical services that may reduce performance
            - QoS
            - NAT
            - Firewall
            - IPSec
        - Boost license does not require the Performance license. They are mutually exclusive
    - Feature Sets
        - APPX

      - Includes SEC license
      - Adds features like NBAR, AVC, MPLS, VRFs, VXLAN, WAAS, Akamai
    - SEC
      - Required for pretty much all Security features; ZBFW, IPSec, EZVPN, DMVPN, FlexVPN
      - Most require a fairly recent version of software
      - When selecting an image, unless requested, don't add one with NPE in the description. It stands for No Payload Encryption and will not include features like VPN Ipsec if added. This has to do with export restriction requirements for various countries
    - HSEC
      - Allows MACsec
      - Removes the crypto and VPN throughput cap and 1000 tunnel cap
      - Requires the SEC license for it to function
    - UC
      - CME, SRST, CUBE
- SD-WAN
  - Why?
  - **Cheaper, Faster/Better Performance, Integration with Cloud**
    - Apps moving to the cloud
      - Apps used to be housed at HQ, but are now hairpinning through HQ to get to the internet
    - Wasting bandwidth from unused circuits
    - Intelligence on which circuit to use (performance + latency tracking)
    - Difficult to manage large deployments
    - New security requirements
      - Each branch internet connection is, in essence, a new possible security hole
  - Overview
    - Consists of multiple different pieces
      - vBond (Orchestration), vManage (Management), vSmart (Control Plane), Edge Devices (Data Plane)
      - vBond helps each edge device authenticate and discover connectivity between the planes
      - vManage is the interface (GUI) that is used for mgmt. Sends policies to vSmart
      - vSmart is the controller for the environment, responsible for all configuration that is pushed out to edge devices. Receives configuration from vManage and pushes it out to edge devices
      - Edge devices receive configuration from vSmart
  - Choosing the components
    - Licensing
      - DNA Essentials, Advantage, or Premier
        - Most customers should choose Advantage because of access to vAnalytics, Cloud On-Ramp, and AMP. Premier primarily adds SEC features like SIG and Threat Grid
        - Essentials has a limit on segmentation but would be suitable for small deployments (SD-WAN segmentation = a VRF in concept)
      - Also licensed based on throughput. Keep in mind the aggregate bandwidth is double what the SKU shows. If the SKU shows 10Mbps the actual capacity is 20Mbps. It does NOT have to be equal 10M each way… it can be 5Mbps UP + 15Mbps DOWN (any combination below the max threshold)
      - If an SD-WAN license is higher than what the default throughput on the platform is, a Performance or Boost license is automatically included. HSEC is also automatically included above 250Mbps.
    - Viptela mgmt
      - Cloud or On-Prem

- Cloud should be used unless specifically stated otherwise. Cisco provisions the mgmt infrastructure in the cloud (included in cost). That means that vBond, vManage, and vSmart are provisioned by Cisco for the customer. On-prem leaves all this to the customer to deploy on their own infrastructure

- Devices
  - ISR, vEdge, or Cloud vEdge
    - ISR
      - Are there existing platforms available? May be able to upgrade/add memory and repurpose them if so
      - More physical connectivity options
      - More robust security options
      - Ensure that any additional module/interfaces are compatible with SD-WAN. The Ordering Guide linked below lists these. Don't assume that any module/interface is compatible
    - vEdge
      - Basic connectivity for copper and fiber
      - Basic security features
      - Lower cost

Useful Links -

ISR 4K Performance White Paper

Interfaces and Modules

Branch Router Security CL Session

DNA for SD-WAN Ordering Guide

DNA for SD-WAN Licensing Blog

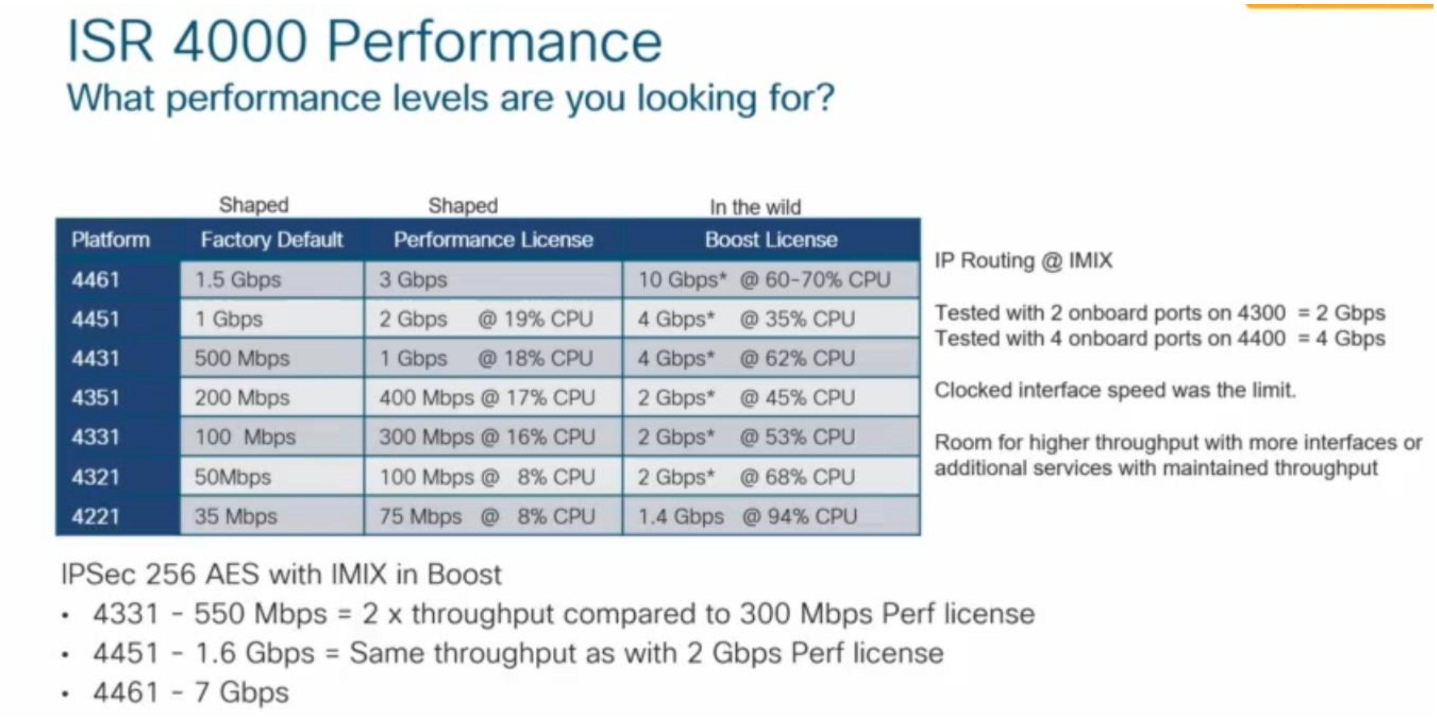
How to Choose the Correct Branch Device CL Session

Cisco 1100 Series Integrated Services Router Product Overview and Architecture CL Session

SalesConnect

Umbrella SIG Essentials (VoE Session)

Useful Slides -



ISR 4000 Performance

What performance levels are you looking for?

	Shaped	Shaped	In the wild
Platform	Factory Default	Performance License	Boost License
4461	1.5 Gbps	3 Gbps	10 Gbps* @ 60-70% CPU
4451	1 Gbps	2 Gbps @ 19% CPU	4 Gbps* @ 35% CPU
4431	500 Mbps	1 Gbps @ 18% CPU	4 Gbps* @ 62% CPU
4351	200 Mbps	400 Mbps @ 17% CPU	2 Gbps* @ 45% CPU
4331	100 Mbps	300 Mbps @ 16% CPU	2 Gbps* @ 53% CPU
4321	50Mbps	100 Mbps @ 8% CPU	2 Gbps* @ 68% CPU
4221	35 Mbps	75 Mbps @ 8% CPU	1.4 Gbps @ 94% CPU

IP Routing @ IMIX

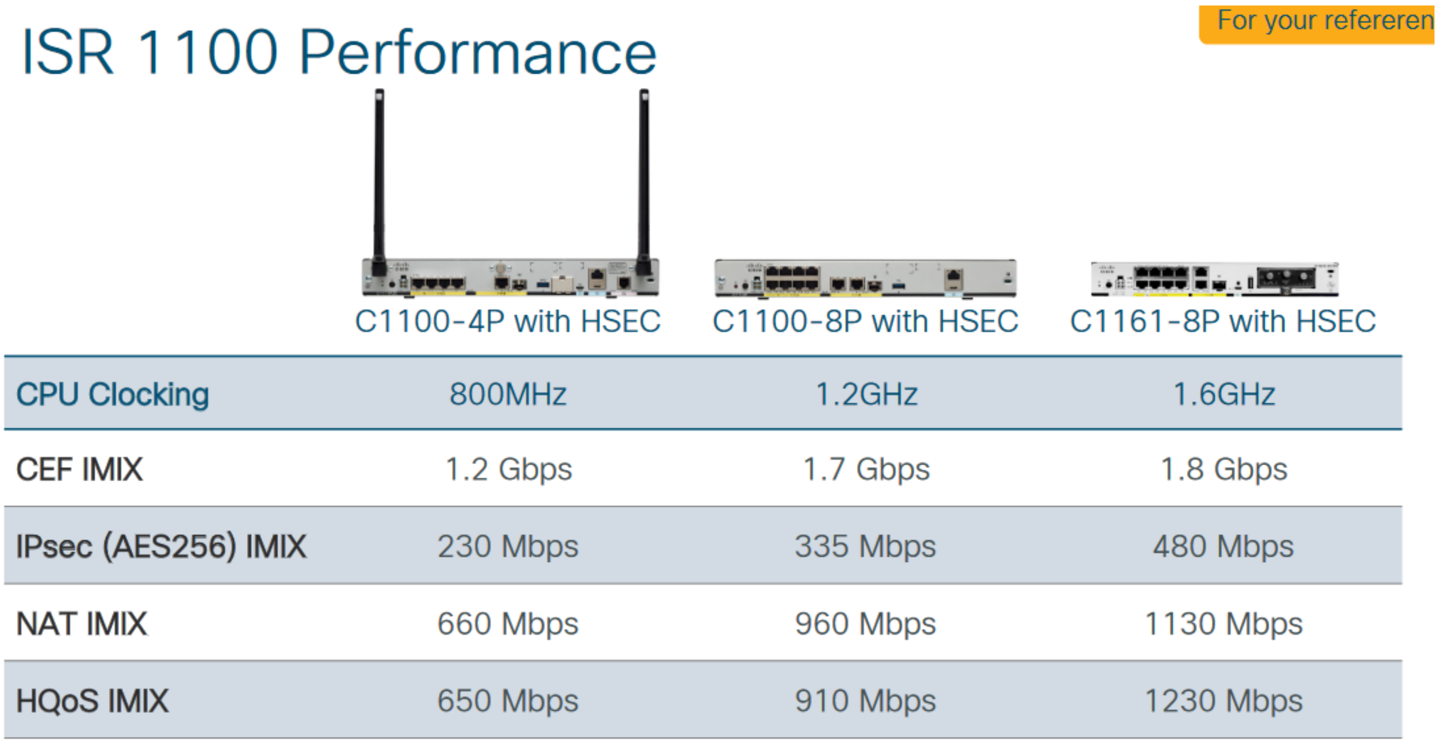
Tested with 2 onboard ports on 4300 = 2 Gbps
Tested with 4 onboard ports on 4400 = 4 Gbps

Clocked interface speed was the limit.

Room for higher throughput with more interfaces or additional services with maintained throughput

IPSec 256 AES with IMIX in Boost

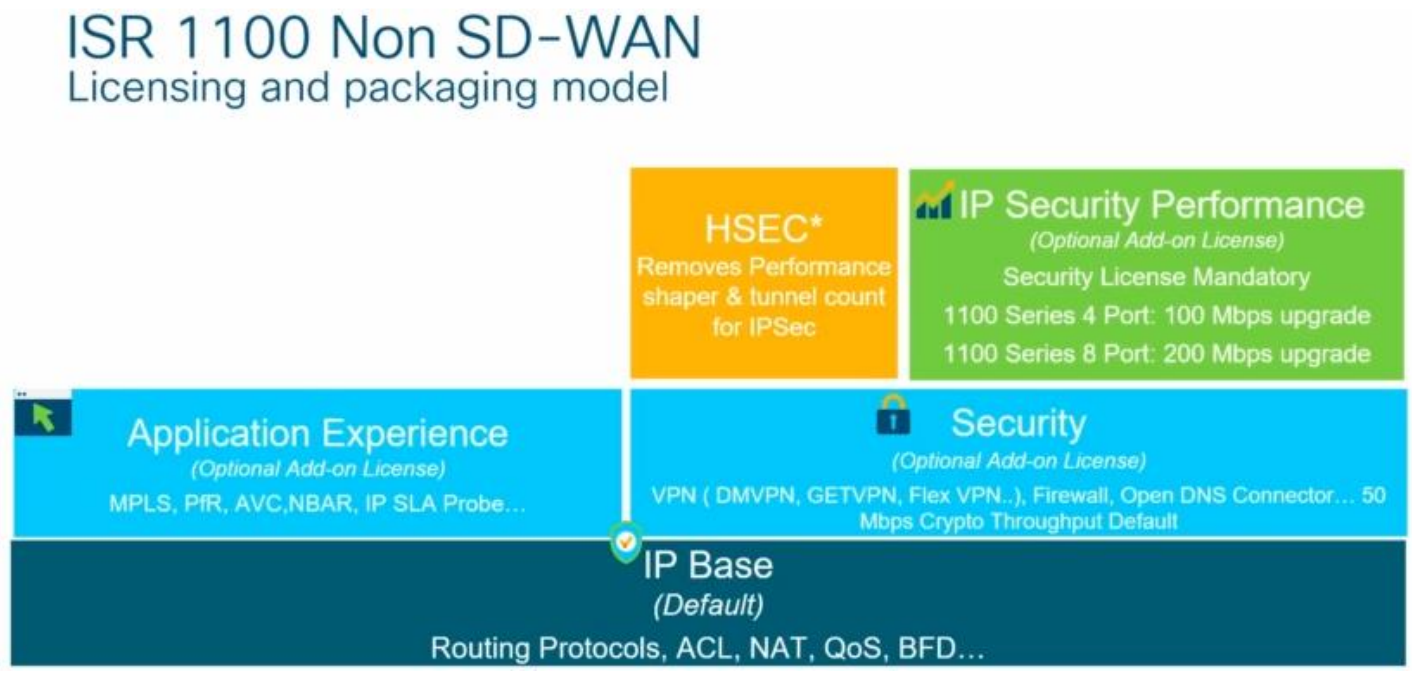
- 4331 - 550 Mbps = 2 x throughput compared to 300 Mbps Perf license
- 4451 - 1.6 Gbps = Same throughput as with 2 Gbps Perf license
- 4461 - 7 Gbps



ISR 1100 Performance

For your refereren

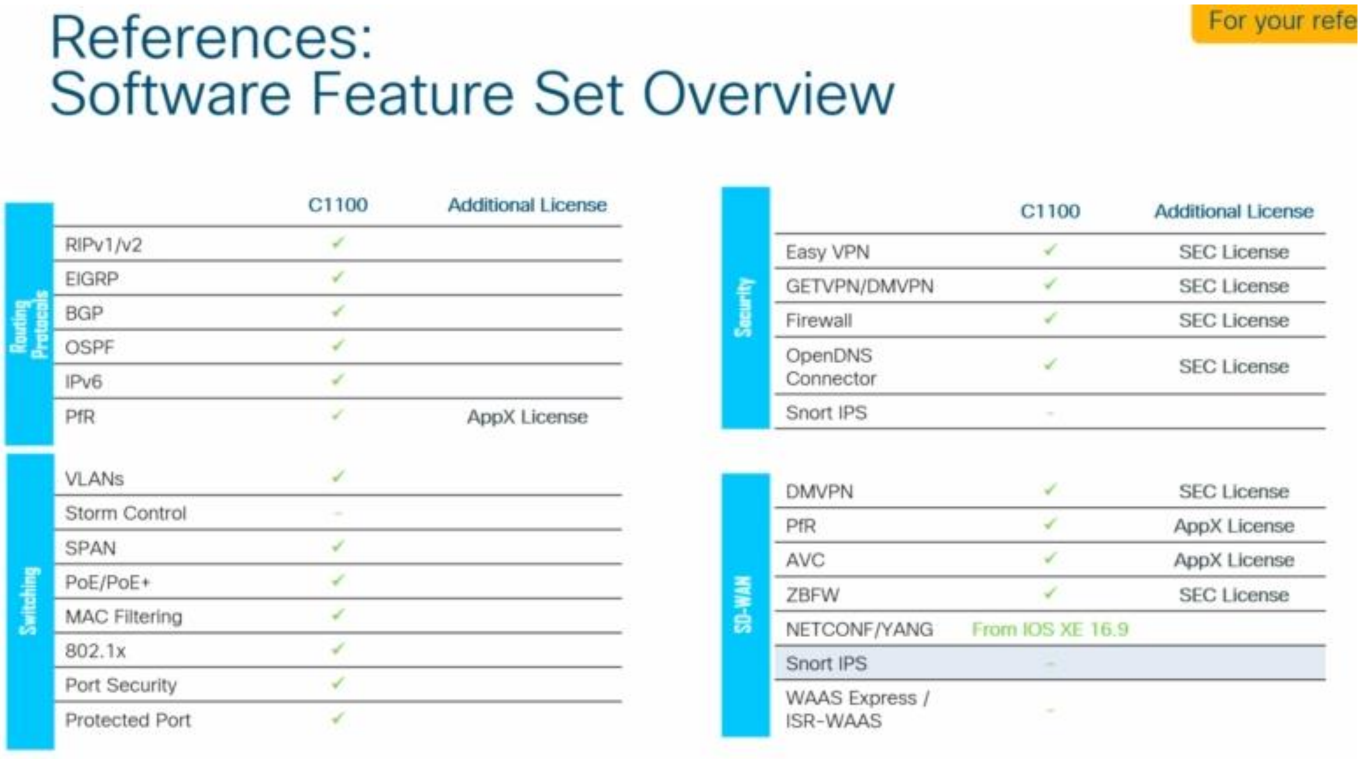
	C1100-4P with HSEC	C1100-8P with HSEC	C1161-8P with HSEC
CPU Clocking	800MHz	1.2GHz	1.6GHz
CEF IMIX	1.2 Gbps	1.7 Gbps	1.8 Gbps
IPsec (AES256) IMIX	230 Mbps	335 Mbps	480 Mbps
NAT IMIX	660 Mbps	960 Mbps	1130 Mbps
HQoS IMIX	650 Mbps	910 Mbps	1230 Mbps



ISR 1100 Non SD-WAN

Licensing and packaging model

HSEC*
Removes Performance shaper & tunnel count for IPSec
IP Security Performance
(Optional Add-on License)
Security License Mandatory
1100 Series 4 Port: 100 Mbps upgrade
1100 Series 8 Port: 200 Mbps upgrade
Application Experience
(Optional Add-on License)
MPLS, PfR, AVC,NBAR, IP SLA Probe…
Security
(Optional Add-on License)
VPN (DMVPN, GETVPN, Flex VPN..), Firewall, Open DNS Connector… 50 Mbps Crypto Throughput Default
IP Base
(Default)
Routing Protocols, ACL, NAT, QoS, BFD…

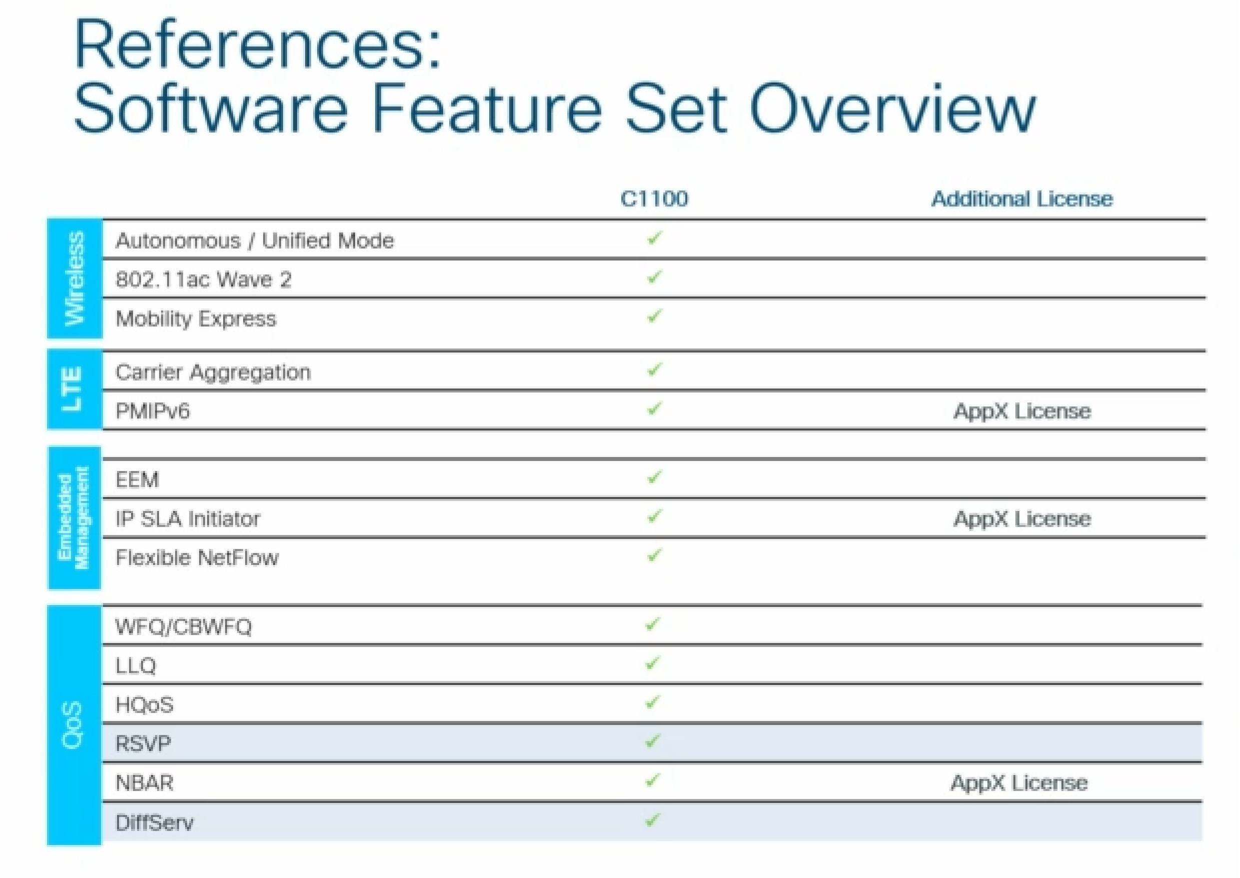


References: Software Feature Set Overview

For your refe

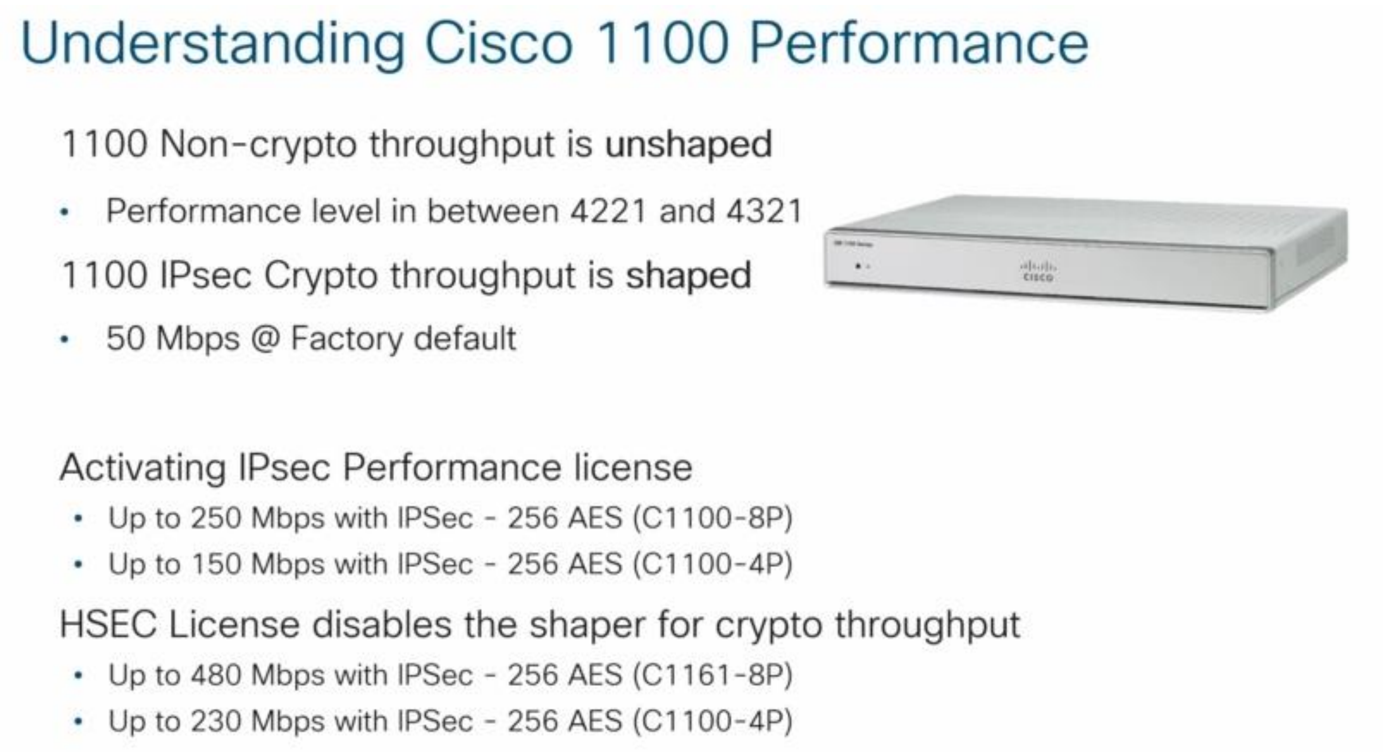
		C1100	Additional License
Routing Protocols	RIPv1/v2	✓	
	EIGRP	✓	
	BGP	✓	
	OSPF	✓	
	IPv6	✓	
	PfR	✓	AppX License
Switching	VLANs	✓	
	Storm Control	-	
	SPAN	✓	
	PoE/PoE+	✓	
	MAC Filtering	✓	
	802.1x	✓	
	Port Security	✓	
	Protected Port	✓	

		C1100	Additional License
Security	Easy VPN	✓	SEC License
	GETVPN/DMVPN	✓	SEC License
	Firewall	✓	SEC License
	OpenDNS Connector	✓	SEC License
	Snort IPS	-	
SD-WAN	DMVPN	✓	SEC License
	PfR	✓	AppX License
	AVC	✓	AppX License
	ZBFW	✓	SEC License
	NETCONF/YANG	From IOS XE 16.9	
	Snort IPS	-	
	WAAS Express / ISR-WAAS	-	



References:
Software Feature Set Overview

		C1100	Additional License
Wireless	Autonomous / Unified Mode	✓	
	802.11ac Wave 2	✓	
	Mobility Express	✓	
LTE	Carrier Aggregation	✓	
	PMIPv6	✓	AppX License
Embedded Management	EEM	✓	
	IP SLA Initiator	✓	AppX License
	Flexible NetFlow	✓	
QoS	WFQ/CBWFQ	✓	
	LLQ	✓	
	HQoS	✓	
	RSVP	✓	
	NBAR	✓	AppX License
	DiffServ	✓	



Understanding Cisco 1100 Performance

1100 Non-crypto throughput is **unshaped**

- Performance level in between 4221 and 4321

1100 IPsec Crypto throughput is **shaped**

- 50 Mbps @ Factory default

Activating IPsec Performance license

- Up to 250 Mbps with IPSec - 256 AES (C1100-8P)
- Up to 150 Mbps with IPSec - 256 AES (C1100-4P)

HSEC License disables the shaper for crypto throughput

- Up to 480 Mbps with IPSec - 256 AES (C1161-8P)
- Up to 230 Mbps with IPSec - 256 AES (C1100-4P)