CCNA Exam: Cisco Certified Network Associate

Exam Description

The Cisco Certified Network Associate v1.0 (CCNA 200-301) exam is a 120-minute exam associated with the CCNA certification. This exam tests a candidate's knowledge and skills related to network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability. The course, Implementing and Administering Cisco Solutions (CCNA), helps candidates prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

1.0 Network Fundamentals

- 1.1 Explain the role and function of network components
    - 1.1.a Routers
    - 1.1.b L2 and L3 switches
    - 1.1.c Next-generation firewalls and IPS
    - 1.1.d Access points
    - 1.1.e Controllers (Cisco DNA Center and WLC)
    - 1.1.f Endpoints
    - 1.1.g Servers
- 1.2 Describe characteristics of network topology architectures
    - 1.2.a 2 tier
    - 1.2.b 3 tier
    - 1.2.c Spine-leaf
    - 1.2.d WAN
    - 1.2.e Small office/home office (SOHO)
    - 1.2.f On-premises and cloud
- 1.3 Compare physical interface and cabling types
    - 1.3.a Single-mode fiber, multimode fiber, copper
    - 1.3.b Connections (Ethernet shared media and point-to-point)
    - 1.3.c Concepts of PoE
- 1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)

1.5 Compare TCP to UDP

1.6 Configure and verify IPv4 addressing and subnetting

1.7 Describe the need for private IPv4 addressing

1.8 Configure and verify IPv6 addressing and prefix

1.9 Compare IPv6 address types

- 1.9.a Global unicast
- 1.9.b Unique local
- 1.9.c Link local
- 1.9.d Anycast
- 1.9.e Multicast
- 1.9.f Modified EUI 64

- 1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)

1.11 Describe wireless principles

- 1.11.a Nonoverlapping Wi-Fi channels
- 1.11.b SSID
- 1.11.c RF
- 1.11.d Encryption

- 1.12 Explain virtualization fundamentals (virtual machines)

1.13 Describe switching concepts

- 1.13.a MAC learning and aging
- 1.13.b Frame switching
- 1.13.c Frame flooding
- 1.13.d MAC address table

2.0 Network Access

- 2.1 Configure and verify VLANs (normal range) spanning multiple switches

- 2.1.a Access ports (data and voice)
- 2.1.b Default VLAN
- 2.1.c Connectivity

- 2.2 Configure and verify interswitch connectivity

- 2.2.a Trunk ports
- 2.2.b 802.1Q
- 2.2.c Native VLAN

- 2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)

2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)

2.5 Describe the need for and basic operations of Rapid PVST+ Spanning Tree Protocol and identify basic operations

- 2.5.a Root port, root bridge (primary/secondary), and other port names
- 2.5.b Port states (forwarding/blocking)
- 2.5.c PortFast benefits

- 2.6 Compare Cisco Wireless Architectures and AP modes

2.7 Describe physical infrastructure connections of WLAN components (AP,WLC, access/trunk ports, and LAG)

2.8 Describe AP and WLC management access connections (Telnet, SSH, HTTP,HTTPS, console, and TACACS+/RADIUS)

2.9 Configure the components of a wireless LAN access for client connectivity using GUI only such as WLAN creation, security settings, QoS profiles, and advanced WLAN settings

3.0 IP Connectivity

- 3.1 Interpret the components of routing table

  - 3.1.a Routing protocol code
  - 3.1.b Prefix
  - 3.1.c Network mask
  - 3.1.d Next hop
  - 3.1.e Administrative distance
  - 3.1.f Metric
  - 3.1.g Gateway of last resort
- 3.2 Determine how a router makes a forwarding decision by default

  - 3.2.a Longest match
  - 3.2.b Administrative distance
  - 3.2.c Routing protocol metric
- 3.3 Configure and verify IPv4 and IPv6 static routing

- 3.3.a Default route
- 3.3.b Network route
- 3.3.c Host route
- 3.3.d Floating static

- 3.4 Configure and verify single area OSPFv2
    - 3.4.a Neighbor adjacencies
    - 3.4.b Point-to-point
    - 3.4.c Broadcast (DR/BDR selection)
    - 3.4.d Router ID
- 3.5 Describe the purpose of first hop redundancy protocol

4.0 IP Services

- 4.1 Configure and verify inside source NAT using static and pools

4.2 Configure and verify NTP operating in a client and server mode

4.3 Explain the role of DHCP and DNS within the network

4.4 Explain the function of SNMP in network operations

4.5 Describe the use of syslog features including facilities and levels

4.6 Configure and verify DHCP client and relay

4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, shaping

4.8 Configure network devices for remote access using SSH

4.9 Describe the capabilities and function of TFTP/FTP in the network

5.0 Security Fundamentals

- 5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)

5.2 Describe security program elements (user awareness, training, and physical access control)

5.3 Configure device access control using local passwords

5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)

5.5. Describe remote access and site-to-site VPNs

5.6 Configure and verify access control lists

5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)

5.8 Differentiate authentication, authorization, and accounting concepts

5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)

5.10 Configure WLAN using WPA2 PSK using the GUI

6.0 Automation and Programmability

- 6.1 Explain how automation impacts network management

  6.2 Compare traditional networks with controller-based networking

  6.3 Describe controller-based and software defined architectures (overlay, underlay, and fabric)

  - 6.3.a Separation of control plane and data plane
  - 6.3.b North-bound and south-bound APIs
- 6.4 Compare traditional campus device management with Cisco DNA Center enabled device management

  6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)

  6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible

  6.7 Interpret JSON encoded data

The 10 Day Advantage

From beginner to expert. Here is a way to build on what you have learnt in CCNA. **The biggest challenge a learner faces is the practical exposure, a platform where you can design networks, work out topologies and configure devices.** After all it needs the hardware (routers and switches) to keep practicing and exploring what Cisco has to offer.

Here is a chance to learn, discover and troubleshoot using powerful networking simulation tools like Cisco packet tracer, GNS3 and EVE which you learn in this course along with CCNA enterprise. Using all these powerful simulators you can continue practicing and learning even after your training is complete without worrying about the hardware needed.

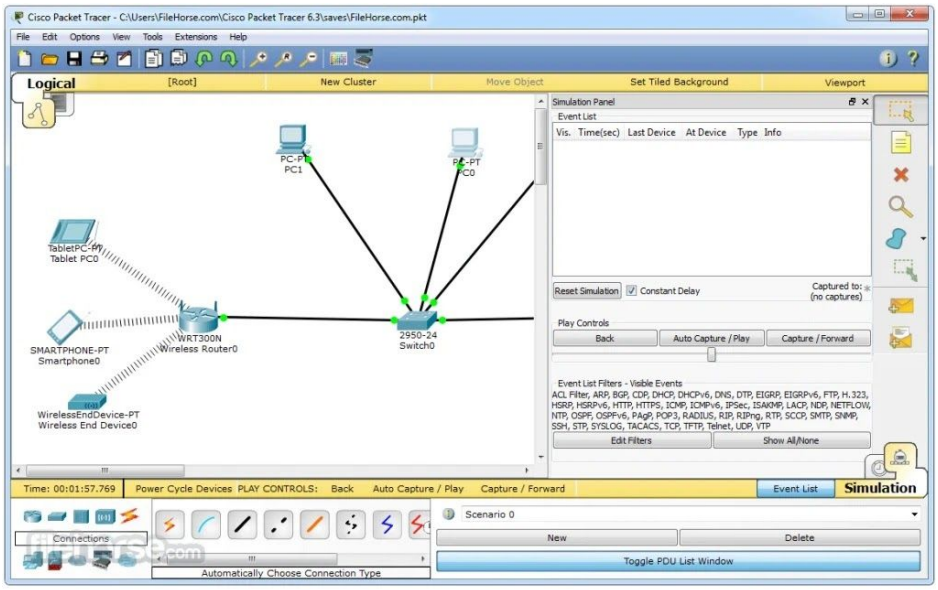
Cisco Packet tracer

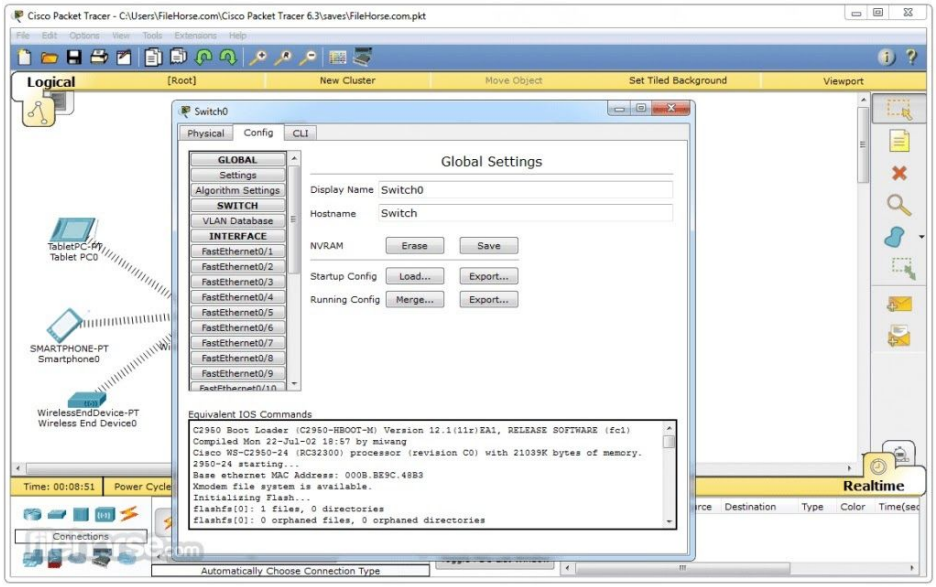
Cisco Packet Tracer is a tool for simulating network configurations. This program is comprehensive and multi-faceted. The software is excellent for students. It is free to download for students. Packet Tracer is a **simulation, visualization, collaboration, and assessment tool** for teaching networking.

It allows students to construct their own model or virtual networks, obtain access to important graphical representations of those networks, animate those networks by adding their own data packets, ask questions about those networks, and finally annotate and save their creations.

Packet Tracer can be used in a variety of ways:

- Class work, Homework, and Distance Learning
- Formative assessment
- Hands-on lab reinforcement
- Lecture demonstrations
- Modeling and visualization of networking device algorithms and networking protocols
- Case studies
- Problem-solving activities in concept-building, skill-building, design, and troubleshooting





GNS3: The software that empowers network professionals.

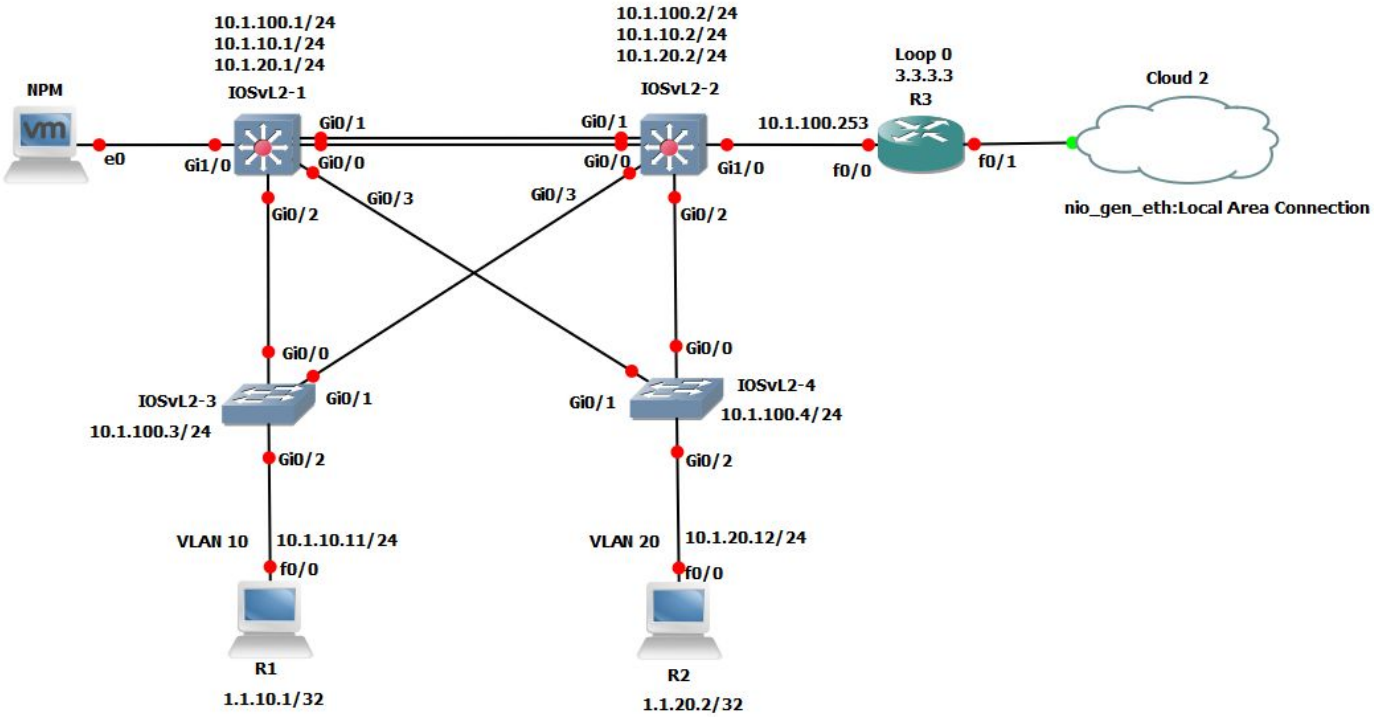
GNS3 is used by hundreds of thousands of network engineers worldwide to emulate, configure, test and troubleshoot virtual and real networks. GNS3 allows you to run topology consisting of only a few

devices on your laptop, to those that have many devices hosted on multiple servers or even hosted in the cloud.

GNS3 is open source, free software that you can download.

It is actively developed and supported and has a growing community of over 800,000 members. GNS3 can help you prepare for certification exams such as the Cisco CCNA, CCNP and some other advanced protocols and technologies.

GNS3 has allowed network engineers to virtualize real hardware devices for over 10 years. Originally only emulating Cisco devices using software called Dynamips, GNS3 has now evolved and supports many devices from multiple network vendors including Cisco virtual switches, Cisco ASAs, Brocade vRouters, Cumulus Linux switches, Docker instances, HPE VSRs, multiple Linux appliances and many others.

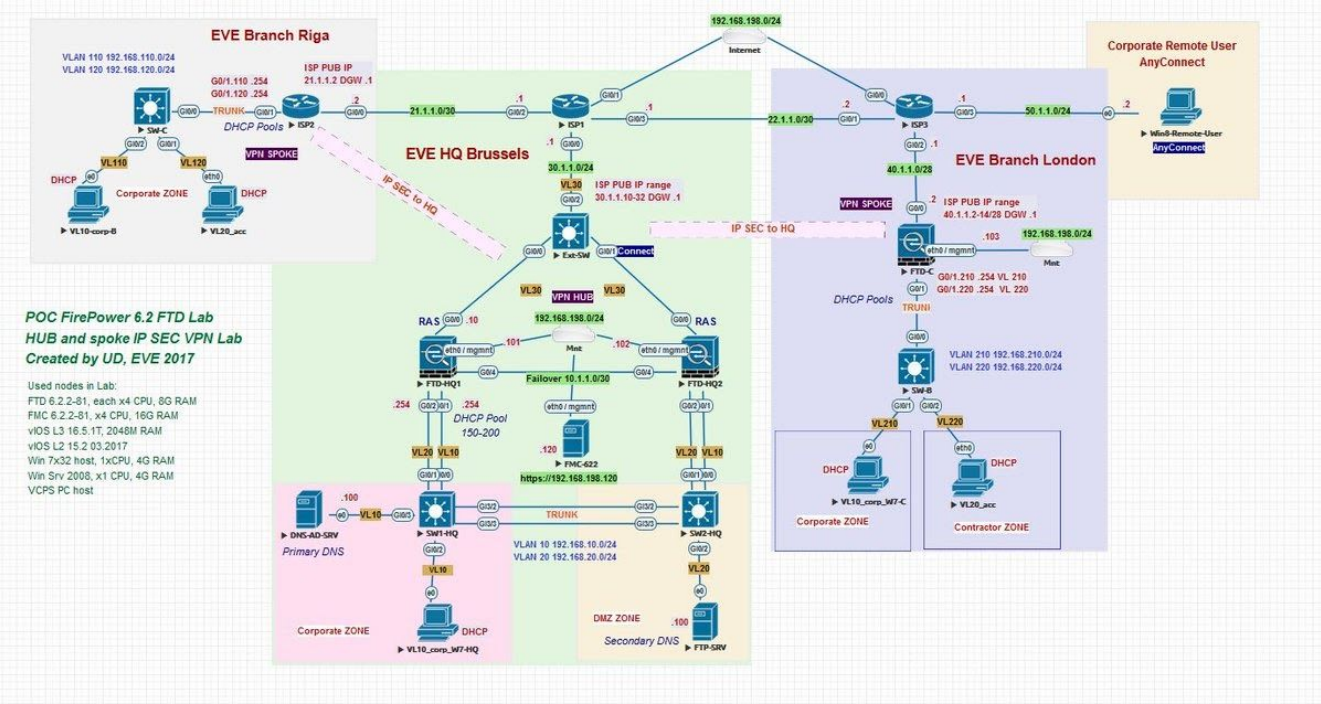


EVE-NG

EVE-NG PRO platform is ready for today's IT-world requirements. It allows enterprises, e-learning providers/centers, individuals and group collaborators to create virtual proof of concepts, solutions and training environments.

EVE-NG PRO is the first clientless multivendor network emulation software that empowers network and security professionals with huge opportunities in the networking world. Clientless management options will allow EVE-NG PRO to be the best choice for Enterprise engineers without influence of corporate security policies as it can be run in a completely isolated environment.

Since it runs in a virtual machine, EVE-NG may be set up on any operating system such as Windows, Linux, or Mac OS.



Introduction to Cisco Data Centers

At its simplest, a data center is a physical facility that organizations use to house their critical applications and data. A data center's design is based on a network of computing and storage resources that enable the delivery of shared applications and data.

Here you get a chance to get introduced to data centers and see how they are different from enterprise networks. You get an introduction to Cisco Nexus, and Data Center technologies.

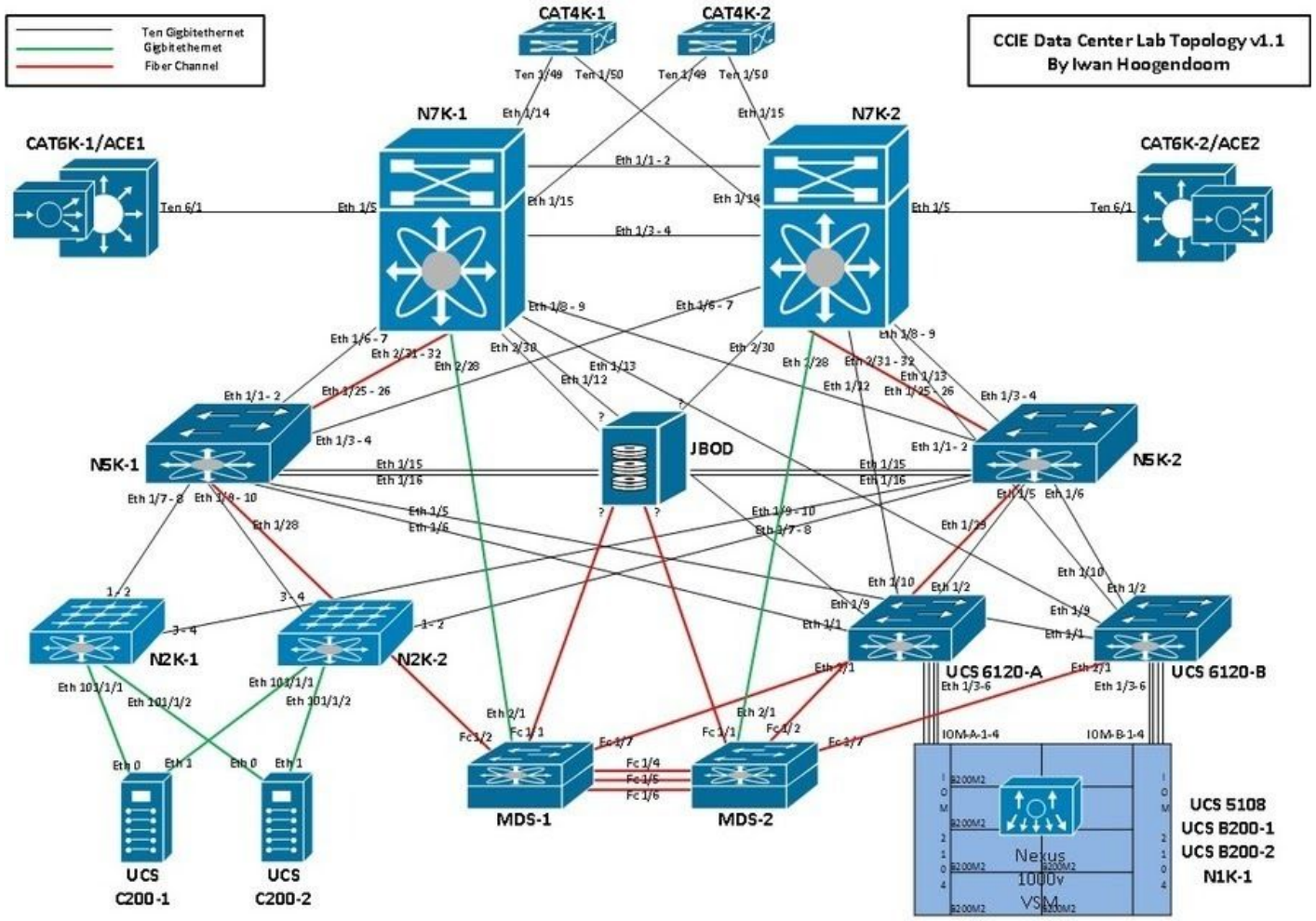
What are the core components of a data center?

Data center design includes routers, switches, firewalls, storage systems, servers, and application delivery controllers. Because these components store and manage business-critical data and applications, data center security is critical in data center design. Together, they provide:

Network infrastructure. This connects servers (physical and virtualized), data center services, storage, and external connectivity to end-user locations.

Storage infrastructure. Data is the fuel of the modern data center. Storage systems are used to hold this valuable commodity.

Computing resources. Applications are the engines of a data center. These servers provide the processing, memory, local storage, and network connectivity that drive applications.



CCNA being a 5 day course from Cisco does not cover the following topics and are marked for self study. Students are supposed to be self-studying these after 5 days and prepare for exam. It may be difficult if you are new to the networking world. If you choose 10 days of training following topics are also covered by the instructor.

Self Study topics that get covered in 10 Days duration.

Building Redundant Switched Topologies
Exploring Layer 3 Redundancy
Introducing WAN Technologies
Introducing QoS
Explaining Wireless Fundamentals
Introducing Architectures and Virtualization
Examining the Security Threat Landscape