CompTIA i-Net+ Certification Exam Objectives
(http://www.comptia.org/certification/i-net/objectives.asp)

The skills and knowledge measured by this exam are derived from an industry-wide and worldwide job task analysis and a survey to validate the job task analysis. The survey results were used to weight the test domains and ensure that the weightings are representative of the job requirements.

This exam blueprint includes the test objectives and the relative weightings. The table below lists the domains measured by this examination and the extent to which they are represented in the examination. Example topics and concepts are included to clarify the test objectives and should not be construed as a comprehensive list of all the content of this exam.

Domain	% of Exam
1.0 Internet Basics & Clients	30%
2.0 Development	20%
3.0 Networking	20%
4.0 Internet Security	20%
5.0 Business Concepts	10%
Total	100%

DOMAIN 1.0 Internet Basics and Clients

This domain requires that the candidate have the knowledge of a wide range of Internet basics, including: site functionality, caching, indexes, searching, and Internet infrastructure. In addition candidates should have the knowledge and skills required to use and update client software, and to assist in the administration of Internet/intranet sites.

1.1. Identify the issues that affect Internet site functionality.
Content may include the following:
- Performance, including:
  - Bandwidth (both client and server)
  - Internet connection types (both client and server)

  - Pages taking too long to load
  - Resolution and size of graphics
- Security, including:
  - Authentication
  - Permissions
  - Data encryption

1.2. Understand and be able to describe the concept of caching and its implications.
Content may include the following:
- Web caching
- File caching
- Proxy caching
- Client side caching versus server side caching

1.3. Use different types of search indexes - static index/site map, keyword index, full text index.
Content may include the following:
- Index your site for a search
- Use Internet and Intranet search engines
- Differences between search engines and directories
- Meta search engines
- Spider search engines

1.4. Understand and be able to describe the infrastructure neede d to support an Internet client.
Content may include the following:
- Knowledge of client operating systems
- Knowledge of web server platforms
- Operating system TCP/IP stack configuration
- Network connection
- Web browser
- E-mail client
- Hardware platform
- DHCP
- Client software configuration

1.5. Use/configure Web browsers and other Internet/intranet clients, and be able to describe their use to others.
Content may include the following:
- Web browsers
- FTP clients
- Telnet clients

E-mail clients
All-in-one/universal clients
When to use each type of client
The basic commands (e.g., get and put) for each type of client (e.g., FTP, Telnet. POP3)

1.6. Update client software.

Content may include the following:

Performing routine maintenance on client applications (e.g. updating virus data files)
Applying service packs and maintenance patches
Upgrading to newer versions of client software, or replacing existing client software with versions from a different software vendor

1.7. Assist in the administration of Internet/intranet sites.

Content may include the following:

Reset passwords
Configure permissions
Post content to server

DOMAIN 2.0 Development

This domain requires that the candidate have the knowledge of programming related terms and the differences between popular client and server programming languages. The candidate should also have the ability to create HTML pages, identify when to use multimedia extensions and plug-ins, understand when to use various image and multimedia file formats, identify the common formats used to deliver content to wireless devices, understand when to use popular tools to connect anWeb server to a database, and test pre-production Web and e-Commerce servers.

2.1. Understand and be able to describe programming-related terms.

Content may include the following:

API
CGI script
SQL
Client -side scripting
Server-side scripting

Server-side includes

2.2. Understand and be able to describe differences between popular client-side and server-side programming languages.

Content may include the following:

When to use the languages
When they are executed

Examples may include the following:

Java
JavaScript
XML
ASP
Extensible Stylesheet Language-XSL
Document Type definitions-DTD
JSP
CGI script
Perl
Java Servlets
VBScript
PHP

2.3. Create HTML pages. Content may include the following:

Cascading Style Sheets - CSS
Etensible Stylesheet Language - XSL
DHTML
XHTML
HTML document structure
Understand and use MetaTags properly
Use page layout principles
Coding simple tables, headings, forms
Compatibility between different browsers
Importance of creating cross-browser coding in HTML 3 tier models

2.4. Identify when to use various multimedia extensions or plug-ins. Content may include the following:

QTVR (quick time)
Flash
Shockwave
RealPlayer
Windows Media Player

2.5. Identify when to use various image and multimedia file

formats.
Content may include the following:

- GIF
- GIF89a
- JPEG
- PNG
- PDF
- TIFF
- BMP
- MOV
- MPEG
- AVI

2.6. Identify the common formats used to deliver content to wireless devices. Content may include the following:

- XML
- WML

2.7. Understand when to use popular tools to connect a Web server to a database. Content may include the following:

- PHP
- PERL
- ASP
- ODBC
- JDBC

2.8. Test pre-production Web and e-commerce servers. Content may include the following:

- View web content in various browsers and at various screen resolutions
- Stress test a server
- Stress test the servers' Internet connection
- Create sample transactions with an e-commerce server

DOMAIN 3.0 Networking

This domain requires that the candidate have the knowledge and skills to understand and be able to describe the core components of the Internet infrastructure; identify problems with Internet connectivity; understand how to use Internet domain names and DNS; understand the capabilities of popular remote access protocols; understand how various protocols or services apply to the function of their corresponding server;

identify when to use various diagnostic tools for resolving Internet problems; create a logic diagram of Internet components; describe various hardware and software connection devices; understand when to use various site monitoring procedures; understand how common networking topologies are used; and understand the capabilities of application server providers.

3.1. Understand and be able to describe the core components of the Internet infrastructure. Content may include the following:

- Network access points
- Backbone
- Hardware/software infrastructure knowledge
- Internetworking devices such as routers, switches and bridges

3.2. Identify problems with Internet connectivity from source to destination for various types of servers. Content may include the following:

- E-mail server
- Web server
- FTP server
- News server
- Proxy server
- Caching server
- Media server
- DNS server
- Certificate server
- Directory (LDAP) server
- Connecting through a firewall

3.3. Understand and be able to describe the use of Internet domain names and DNS. Content may include the following:

- DNS entry types
- Hierarchical structure
- Role of root domain servers
- Top level or original domains
- NSlookup.

3.4. Understand and be able to describe the capabilities of popular remote access protocols. Content may include the following:

SLIP
PPP
PPTP
L2TP
PPPOE
Point-to-point multi-point

3.5. Understand how various protocols or services apply to the function of their corresponding server, such as a mail server, a web server or a file transfer server. Content may include the following:

POP3
SMTP
HTTP
FTP
NNTP
LDAP
Telnet

3.6. Identify when to use various diagnostic tools for resolving Internet problems. Content may include the following:

Ping
WinIPcfg
IPconfig
ifconfig
ARP
TraceRT
Network Analyzer

3.7. Create a logic diagram of Internet components from the client to the server. Content may include the following:

Bridge
Brouter
Router
Switch
Hub
Repeater
Network adapter
Cable modem
xDSL modem
Modem
WAN Link
CSU/DSU

FireWall
Network Address Translation (NAT) server
Proxy server

3.8. Describe various hardware and software connection devices and when to use them. Content may include the following:

Network adapter
Bridge
Brouter
Router
Switch
Repeater
Hub
Network adapter
Cable modem
xDSL modem
Modem
CSU/DSU
FireWall
Network Address Translation (NAT) server
Proxy server

3.9. Understand when to use various site monitoring procedures. Content may include the following:

Viewing server log files
Monitoring network traffic
Monitoring server utilization
Monitoring server network bandwidth utilization

3.10. Understand and be able to describe how common networking topologies are used. Content may include the following:

Star
Bus
Mesh
Ring

3.11. Understand and be able to describe the capabilities of application server providers. Content may include the following:

Providing Internet based services on an as needed basis, such as:

Custom Web hosting

Providing e-mail services
Providing fax services
Providing access to an application over the web
Providing shared access to expensive hardware, such as a mainframe computer.

DOMAIN 4.0: Security

This domain requires that the candidate have the knowledge and skills to understand and be able to understand various Internet security concepts; identify suspicious network activities; identify various methods for performing intrusion detection; identify appropriate access-control security features for an Internet server; describe the uses and proper instances to use anti-virus software; describe the uses and proper instances to use various client security add-ons; describe how firewalls are used to protect private networks; understand when to use various DMZ configurations; and describe various authentication/encryption technologies.

4.1. Understand and be able to describe various Internet security concepts. Content may include the following:
- Access control
- Authentication
- Encryption-PKI
- Secure socket layers (SSL)
- Access security tools
- Auditing
- Secure Electronic Transactions (SET)

4.2. Identify suspicious network activities. Content may include the following:
- Multiple login failures
- Ping floods
- Denial of service attacks
- Mail flooding
- Syn floods
- Spoofing
- Repudiation

4.3. Identify various methods for performing intrusion detection. Content may include the following:

- Configure auditing on servers and firewalls
- Review audit logs
- Configure network monitoring software to alert you when suspicious types of traffic occur
- Configure servers to notify you when unauthorized accesses are attempted.

4.4. Identify appropriate access-control security features for an Internet server. Content may include the following:
- E-mail server
- Web server
- APACHE
- NES
- IIS

4.5. Be able to describe the uses and proper instances to use anti-virus software. Content may include the following:
- Server anti-virus protection
- Client computer anti-virus protection
- Network anti-virus protection, such as on a firewall

4.6. Be able to describe the uses and proper instances to use various client security add-ons. Content may include the following:
- Encryption software
- Personal digital identification, such as a digital certificate
- Personal firewall software

4.7. Describe how firewalls are used to protect private networks. Content may include the following:
- Port filtering
- Packet filtering
- Application filtering
- Intrusion detection filtering

4.8. Identify when to use various DMZ configurations. Content may include the following:
- Bastion Host
- Three-homed firewall
- Back-to-back firewalls

4.9. Understand and be able to describe various authentication/encryption technologies. Content may include the following:
- Username/password authentication

Smart card authentication
SSL
Authentication versus encryption
PKI
Asymmetric encryption, including blowfish, RC2, RC4 and RC5
Symmetric encryption, including DES, triple DES and skipjack
One way encryption, including MD5 and SHA

DOMAIN 5.0: Business Concepts

This domain requires the candidate to be able to identify and or describe various e-Business and e-commerce concepts and when they are used, including term definitions, e-Business related network concepts, e-Business models, strategic marketing considerations, and legal/regulatory considerations.

5.1. Understand and be able to describe e-Commerce terms and concepts.
Content may include the following:
Information Service Providers (ISPs)
Portals
SET (Secure Electronic Transactions)
EFT (Electronic Funds Transfer)
EBT (Electronic Benefits Transfer)
EDI (Electronic Data Interchange)
OBI (Open Buying on the Internet)
OTP (Open Trading Protocol)

5.2. Understand and be able to describe the differences between the following from a business standpoint. Content may include the following:
Private Network
Intranet
Extranet
Internet

5.3. Recognize and explain the current types of e-Business models being applied today. Content may include the following:

Business-to-business models
Business-to-consumer models
Business-to-employee models
Business-to-government
Consumer-to-business
Consumer-to-consumer
Storefront (bricks & mortar) vs. e-Business
New and changing customer expectations
e-business and the Internet
Aggregator

5.4. Identify key factors relating to strategic marketing considerations as they relate to launching an e-business initiative. Content may include the following:
Geographic/Localization considerations (local customs/criteria, etc.)
Public relations; impact/risks of site failure

5.5. Identify key factors relating to legal and regulatory considerations when planning ebusiness solutions. Content may include the following:
Knowledge ownership / Intellectual property rights
Privacy
Jurisdiction