[MS-SRTP]:
Secure Real-time Transport Protocol (SRTP) Extensions

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft Open Specification Promise or the Community Promise. If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Preliminary Documentation. This Open Specification provides documentation for past and current releases and/or for the pre-release (beta) version of this technology. This Open Specification is final

Preliminary

Copyright © 2012 Microsoft Corporation.

documentation for past or current releases as specifically noted in the document, as applicable; it is preliminary documentation for the pre-release (beta) versions. Microsoft will release final documentation in connection with the commercial release of the updated or new version of this technology. As the documentation may change between this preliminary version and the final version of this technology, there are risks in relying on preliminary documentation. To the extent that you incur additional development obligations or any other costs as a result of relying on this preliminary documentation, you do so at your own risk.

Revision Summary

Date	Revision History	Revision Class	Comments
04/04/2008	0.1		Initial version
04/25/2008	0.2		Revised and edited technical content
06/27/2008	1.0		Revised and edited technical content
08/15/2008	1.01		Revised and edited technical content
12/12/2008	2.0		Revised and edited technical content
02/13/2009	2.01		Revised and edited technical content
03/13/2009	2.02		Revised and edited technical content
07/13/2009	2.03	Major	Revised and edited the technical content
08/28/2009	2.04	Editorial	Revised and edited the technical content
11/06/2009	2.05	Editorial	Revised and edited the technical content
02/19/2010	2.06	Editorial	Revised and edited the technical content
03/31/2010	2.07	Major	Updated and revised the technical content
04/30/2010	2.08	Editorial	Revised and edited the technical content
06/07/2010	2.09	Editorial	Revised and edited the technical content
06/29/2010	2.10	Editorial	Changed language and formatting in the technical content.
07/23/2010	2.10	No change	No changes to the meaning, language, or formatting of the technical content.
09/27/2010	3.0	Major	Significantly changed the technical content.
11/15/2010	3.0	No change	No changes to the meaning, language, or formatting of the technical content.
12/17/2010	3.0	No change	No changes to the meaning, language, or formatting of the technical content.
03/18/2011	3.0	No change	No changes to the meaning, language, or formatting of

Preliminary

Copyright © 2012 Microsoft Corporation.

Date	Revision History	Revision Class	Comments
			the technical content.
06/10/2011	3.0	No change	No changes to the meaning, language, or formatting of the technical content.
01/20/2012	4.0	Major	Significantly changed the technical content.

Preliminary

Copyright © 2012 Microsoft Corporation.

Table of Contents

Preliminary

Copyright © 2012 Microsoft Corporation.

Preliminary

Copyright © 2012 Microsoft Corporation.

1 Introduction

This document specifies a proprietary extension to the Secure Real-time Transport Protocol (SRTP).

This protocol provides the same functional capabilities as SRTP, which include providing confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP.

This protocol is a strict subset of SRTP and differs from it in two key aspects:

- The first key difference is that this protocol supports a strict subset of the SRTP default cryptographic transform algorithms and requires that some parameters of the encryption and authentication algorithms described in [RFC3711] be of specific values. These requirements are specified in section 3.
- The second key difference is that there is a set of "MAY, SHOULD, MUST, SHOULD NOT, MUST NOT" protocol behaviors that differ between this protocol and [RFC3711]. Section 3 enumerates these behavioral differences.

Unless explicitly noted in this document, this protocol follows standard SRTP.

Sections 1.8, 2, and 3 of this specification are normative and contain RFC 2119 language. Sections 1.5 and 1.9 are also normative but cannot contain RFC 2119 language. All other sections and examples in this specification are informative.

1.1 Glossary

The following terms are defined in [MS-GLOS]:

Hash-based Message Authentication Code (HMAC)
salt
SHA-1 hash

The following terms are defined in [MS-OFCGLOS]:

Advanced Encryption Standard (AES)
AES Counter Mode
dual-tone multi-frequency (DTMF)
endpoint
master key
Real-Time Transport Control Protocol (RTCP)
Real-Time Transport Protocol (RTP)
RTCP packet
RTP packet
RTP profile
Secure Real-Time Transport Protocol (SRTP)
Session Description Protocol (SDP)
session key
SHA-1
Synchronization Source (SSRC)

The following terms are specific to this document:

cryptographic context: A set of cryptographic state information that is maintained in a Secure Real-Time Transport Protocol (SRTP) stream.

Preliminary

Copyright © 2012 Microsoft Corporation.

NULL cipher: A cipher that does not modify a Real-Time Transport Protocol (RTP) payload and is defined in the Secure Real-Time Transport Protocol (SRTP) protocol. It is used when RTP packet encryption is not necessary, but packet authentication (1) is necessary.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

References to Microsoft Open Specification documents do not include a publishing year because links are to the latest version of the documents, which are updated frequently. References to other documents include a publishing year when one is available.

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[MS-RTP] Microsoft Corporation, "Real-time Transport Protocol (RTP) Extensions".

[RFC2104] Krawczyk, H., Bellare, M., and Canetti, R., "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997, http://www.ietf.org/rfc/rfc2104.txt

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.rfc-editor.org/rfc/rfc2119.txt

[RFC3711] Baugher, M., McGrew, D., Naslund, M., et al., "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004, http://www.rfc-editor.org/rfc/rfc3711.txt

1.2.2 Informative References

[MS-DTMF] Microsoft Corporation, "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals Extensions".

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary".

[MS-OFCGLOS] Microsoft Corporation, "Microsoft Office Master Glossary".

[MS-SDPEXT] Microsoft Corporation, "Session Description Protocol (SDP) Version 2.0 Extensions".

1.3 Protocol Overview (Synopsis)

This protocol provides the same functionality as the **Secure Real-Time Transport Protocol (SRTP)** by providing confidentiality, message authentication, and replay protection to **Real-Time Transport Protocol (RTP)** traffic and to the control traffic for RTP, the **Real-Time Transport Control Protocol (RTCP)**.

This protocol is a strict subset of SRTP and differs from it in the following two key aspects. In all other cases, this protocol follows standard SRTP.

Preliminary

Copyright © 2012 Microsoft Corporation.

- The first key difference is that this protocol supports a subset of the SRTP default cryptographic transform algorithms, and it requires certain encryption and authentication algorithm parameters to be fixed values. For example, the **NULL cipher** transform is not supported.
- The second key difference is that there is a set of "MAY, SHOULD, MUST, SHOULD NOT, MUST NOT" protocol behaviors where this protocol differs in behavior from [RFC3711]. Section 3 enumerates these behavioral differences.

1.4 Relationship to Other Protocols

This protocol relies on **Session Description Protocol (SDP)** to exchange **master key**s and key parameters. Refer to [MS-SDPEXT] for SDP information pertinent to this protocol.

This protocol works with other **RTP profile**s; for example, **dual-tone multi-frequency (DTMF)**, as described in [MS-DTMF]. This protocol treats all other RTP profile outputs the same as audio or video data. It encrypts and authenticates after processing is performed on the sending side and authenticates and decrypts before passing **RTP packet**s and **RTCP packet**s on the receiving side.

The Secure Real-time Transport Control Protocol (SRTCP) is considered a subprotocol to SRTP, and they are described together in [RFC3711]. The proprietary implementation of SRTCP is specified in this document in a similar way.

1.5 Prerequisites/Preconditions

This protocol has the following prerequisites:

- This protocol requires that encryption and authentication algorithms are negotiated using SDP, as described in [MS-SDPEXT] section 3.1.5.8.
- This protocol requires that the master keys are exchanged using SDP, as described in [MS-SDPEXT] section 3.1.5.8, and the keys are configured properly.
- This protocol only provides message confidentiality, authentication, and replay protection for RTP packets and RTCP packets.

1.6 Applicability Statement

This protocol is used where users require secure RTP traffic. This protocol is required to be used with the SDP extension described in [MS-SDPEXT] section 3.1.5.8 to set up the shared master key securely.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

Preliminary

Copyright © 2012 Microsoft Corporation.

2 Messages

2.1 Transport

This protocol transforms RTP/RTCP packets only. Refer to [MS-RTP] section 2.1 for transports that the RTP protocol uses.

2.2 Message Syntax

This protocol uses the message syntax specified in [RFC3711].

- For the SRTP message syntax, see [RFC3711] section 3.1.
- For the SRTCP message syntax, see [RFC3711] section 3.4.

Preliminary

Copyright © 2012 Microsoft Corporation.

3 Protocol Details

3.1 Endpoint Details

This protocol can be used to secure any RTP traffic. All behavior described here applies to both protocol client and server roles.

The following sections specify the differences between this protocol and SRTP, as specified in [RFC3711].

3.1.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

This protocol requires that each **endpoint (5)** in an SRTP session maintains **cryptographic context**s. A cryptographic context has two categories of parameters:

- Transform independent parameters
- Transform dependent parameters

3.1.1.1 Transform Independent Parameters

Transform independent parameters are parameters independent of what encryption and authentication algorithms are used. For example, regardless of which authentication algorithm is used, the replay checklist size is fixed to 64 entries in this protocol. For details, see [RFC3711] section 3.2.1.

This protocol does not introduce new states, but does require some states to be specific values. For details, see section 3.1.3.2.

3.1.1.2 Transform Dependent Parameters

Transform dependent parameters are parameters for specific encryption or authentication algorithms. This protocol implements the default cryptographic transform specified in [RFC3711] section 4, with exceptions specified in section 3.1.3.3. No new states are introduced.

3.1.2 Timers

None.

3.1.3 Initialization

3.1.3.1 Cryptographic Contexts

SRTP requires that each endpoint in an SRTP session maintain cryptographic contexts. For more information, see [RFC3711] section 3.2.3. This protocol maintains cryptographic contexts differently from SRTP [RFC3711].

This protocol maintains two cryptographic contexts per SRTP session:

Preliminary

Copyright © 2012 Microsoft Corporation.

- One for all media streams on the send direction.
- One for all media streams on the receive direction.

This protocol supports multiple media streams sharing the same SRTP session. Each media stream MUST be uniquely identified by one **Synchronization Source (SSRC)**. This protocol maintains per SSRC transform independent parameters in cryptographic contexts, as specified in section 3.1.3.2.

When sending or receiving an SRTP packet, this protocol first uses the SRTP session and direction to identify the cryptographic context, then uses the Synchronization Source (SSRC) in the packet to decide the per SSRC transform independent parameters in the cryptographic context.

3.1.3.2 SRTP Parameter Settings

For information regarding SRTP transform independent parameters and transform dependent parameters, see [RFC3711] sections 3.2.1 and 3.2.2.

This protocol requires the following parameter settings for transform independent parameters:

- The encryption algorithm MUST be **AES Counter Mode** and encryption MUST be used.
- The authentication algorithm MUST be **Hash-based Message Authentication Code (HMAC)-SHA-1 hash** and authentication MUST be used.
- The replay list size MUST be 64 entries.
- The master key indicator MUST be used.
- The master key indicator length MUST be 1 byte.
- The key derivation rate MUST be 0.
- The master key length MUST be 128-bit.
- The master **salt** key length MUST be 112-bit.
- The encryption **session key** length MUST be 128-bit.
- The encryption session salt length MUST be 112-bit.
- The authentication session key length MUST be 160-bit.
- The master key lifetime MUST be 2^{48} -1 packets for RTP and 2^{31} -1 for RTCP.
- SRTCP and SRTP MUST have the same parameter settings with the exceptions specified in [RFC3711] section 3.2.1.

This protocol maintains the following transform independent parameters per Synchronization Source (SSRC).

- The rollover counter
- The highest received RTP sequence number
- The replay list

For information regarding transform dependent parameters, see sections 3.1.3.3.1 and 3.1.3.3.2.

Preliminary

Copyright © 2012 Microsoft Corporation.

Unless explicitly noted, this protocol follows SRTP, as specified in [RFC3711], to set other mandatory parameters.

3.1.3.3 SRTP Default Cryptographic Transform

This protocol implements a subset of the default SRTP algorithms.

3.1.3.3.1 Message Encryption

The SRTP default encryption algorithms are specified in [RFC3711] section 4.1.

This protocol MUST use AES Counter Mode. AES in f8 mode or NULL cipher mode MUST NOT be used.

This protocol requires that the encryption algorithm MUST be AES Counter Mode with the following parameters. For parameter details, see [RFC3711] section 4.1.

- n_b (block cipher size) MUST be 128-bit (AES algorithm's fixed cipher block size).
- n_e (encryption key size) MUST be 128-bit.
- The Session salt key MUST be used and n_s MUST be 112-bit.
- SRTP_PREFIX_LENGTH MUST be 0.

3.1.3.3.2 Message Authentication and Integrity

The SRTP default authentication algorithm is Hash-based Message Authentication Code (HMAC)-**SHA-1** [RFC2104], as specified in [RFC3711] section 4.2. This protocol implements HMAC-SHA-1 and requires the following parameters:

- n_a (authentication key size) MUST be 160-bit.
- n_tag (authentication tag size) MUST be 80-bit.

3.1.3.4 Session Key Derivation

This protocol implements the session key derivation algorithm specified in [RFC3711] section 4.3.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

3.1.5.1 SRTP Packet Processing

3.1.5.1.1 Sending an SRTP Packet

This protocol implements the steps specified in [RFC3711] section 3.3, with the exception of the method used to identify the appropriate cryptographic context and the per Synchronization Source (SSRC) transform independent parameters. This protocol uses the method specified in section 3.1.3.1.

This protocol requires that RTP packets MUST be encrypted and authenticated.

Copyright © 2012 Microsoft Corporation.

Preliminary

3.1.5.1.2 Receiving an SRTP Packet

This protocol implements the steps specified in [RFC3711] section 3.3, with the following exceptions:

- This protocol uses the method specified in section 3.1.3.1 to identify the cryptographic context and this protocol uses the Synchronization Source (SSRC) to identify the transform independent parameters in the cryptographic context.
- The replay checklist size MUST be 64 entries.
- This protocol logs the number of SRTP failures. Individual replay check failures or authentication failures are not logged.

3.1.5.2 SRTCP Packet Processing

3.1.5.2.1 Sending an SRTCP Packet

This protocol implements the steps specified in [RFC3711] section 3.4. RTCP packets MUST be encrypted and authenticated.

This protocol can adjust avg_rtcp_size or packet_size, as specified in [RFC3711] section 3.4.

The SRTCP index counter is shared by all media streams on the same direction in the SRTP session.

3.1.5.2.2 Receiving an SRTCP Packet

This protocol implements the steps specified in [RFC3711] section 3.4, with the following exceptions:

- This protocol does not honor the e-bit. All incoming RTCP packets MUST be encrypted regardless of the e-bit setting.
- This protocol uses the method specified in section 3.1.3.1 to identify the cryptographic context to use.
- SRTCP index counter is shared by all media streams
- The replay checklist size MUST be 64 entries.
- This protocol logs the number of SRTCP failures. Individual replay check failures or authentication failures are not logged.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

Preliminary

Copyright © 2012 Microsoft Corporation.

4 Protocol Examples

This protocol does not introduce new protocol behaviors. The test vectors in [RFC3711] apply to this protocol. For more information, see [RFC3711] Appendix B.

Preliminary

Copyright © 2012 Microsoft Corporation.

5 Security

5.1 Security Considerations for Implementers

- Master keys are randomly generated. The send and receive directions in the same SRTP session do not use the same master key.
- Master key exchange is done through external mechanisms in Session Description Protocol (SDP). SDP is transferred on a secure transport, for instance Transport Layer Security TLS.
- The Initial RTP sequence number is randomly generated. But it cannot use a value close to 65535, because this could cause a rollover counter mismatch if there is packet loss at the beginning of session startup. For example, the server products supported by this protocol use a random value between 0 and 32767.
- SRTP cannot terminate the connection when a replay attack is detected. Some RTP profiles intentionally send the same packet multiple times, and the duplicated packets fail replay check. For example, DTMF as described in [MS-DTMF].

5.2 Index of Security Parameters

Security parameter	Section
Encryption algorithm	3.1.3.2
Authentication algorithm	3.1.3.2
Replay list size	3.1.3.2
Master key indicator length	3.1.3.2
Session key derivation rate	3.1.3.2
Master key length	3.1.3.2
Master salt length	3.1.3.2
Encryption session key length	3.1.3.2
Encryption session salt length	3.1.3.2
Authentication session key length	3.1.3.2
Master key lifetime	3.1.3.2
Advanced Encryption Standard (AES) cipher block size	3.1.3.3.1
SRTP cipher prefix size	3.1.3.3.1
Authentication tag size	3.1.3.3.2

Preliminary

Copyright © 2012 Microsoft Corporation.

6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Microsoft® Office Communications Server 2007
- Microsoft® Office Communications Server 2007 R2
- Microsoft® Office Communicator 2007
- Microsoft® Office Communicator 2007 R2
- Microsoft® Lync™ Server 2010
- Microsoft® Lync™ 2010
- Microsoft® Lync Server 15 Technical Preview
- Microsoft® Lync 15 Technical Preview

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

Preliminary

Copyright © 2012 Microsoft Corporation.

7 Change Tracking

This section identifies changes that were made to the [MS-SRTP] protocol document between the June 2011 and January 2012 releases. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.
- An extensive rewrite, addition, or deletion of major portions of content.
- The removal of a document from the documentation set.
- Changes made for template compliance.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the language and formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical or language changes were introduced. The technical content of the document is identical to the last released version, but minor editorial and formatting changes, as well as updates to the header and footer information, and to the revision summary, may have been made.

Major and minor changes can be described further using the following change types:

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.

Preliminary

Copyright © 2012 Microsoft Corporation.

- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.
- New content added for template compliance.
- Content updated for template compliance.
- Content removed for template compliance.
- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated.**

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact protocol@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
1 Introduction	Added content for Office 15 Technical Preview.	N	New content added.
1.2 References	Added content for Office 15 Technical Preview.	N	New content added.
3.1.3.1 Cryptographic Contexts	15327: Updated document to reflect protocol behavior change, adding multiple SSRC support.	Y	Content updated.
3.1.3.2 SRTP Parameter Settings	15327: Updated document to reflect protocol behavior change, adding per SSRC transform independent parameters.	Y	Content updated.
3.1.3.2 SRTP Parameter Settings	Updated content for Office 15 Technical Preview.	N	Content updated.
3.1.5.1.1 Sending an SRTP Packet	15327: Updated document to reflect protocol behavior change in the SRTP packet send process.	Y	Content updated.
3.1.5.1.2 Receiving an SRTP Packet	15327: Updated document to reflect protocol behavior change in the SRTP packet receive process to support multiple media streams in the same SRTP session.	Y	Content updated.
3.1.5.2.1 Sending an SRTCP	15327: Clarified the SRTCP behavior when there are multiple media streams sharing the same SRTP session.	Y	Content updated.

Preliminary

Copyright © 2012 Microsoft Corporation.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
Packet			
3.1.5.2.2 Receiving an SRTCP Packet	15327: Clarified the SRTCP behavior when there are multiple media streams sharing the same SRTP session.	Y	Content updated.
6 Appendix A: Product Behavior	Updated product names for Office 15 Technical Preview.	N	New content added.

Preliminary

Copyright © 2012 Microsoft Corporation.

8 Index

Preliminary

Copyright © 2012 Microsoft Corporation.

T

V

Preliminary

Copyright © 2012 Microsoft Corporation.