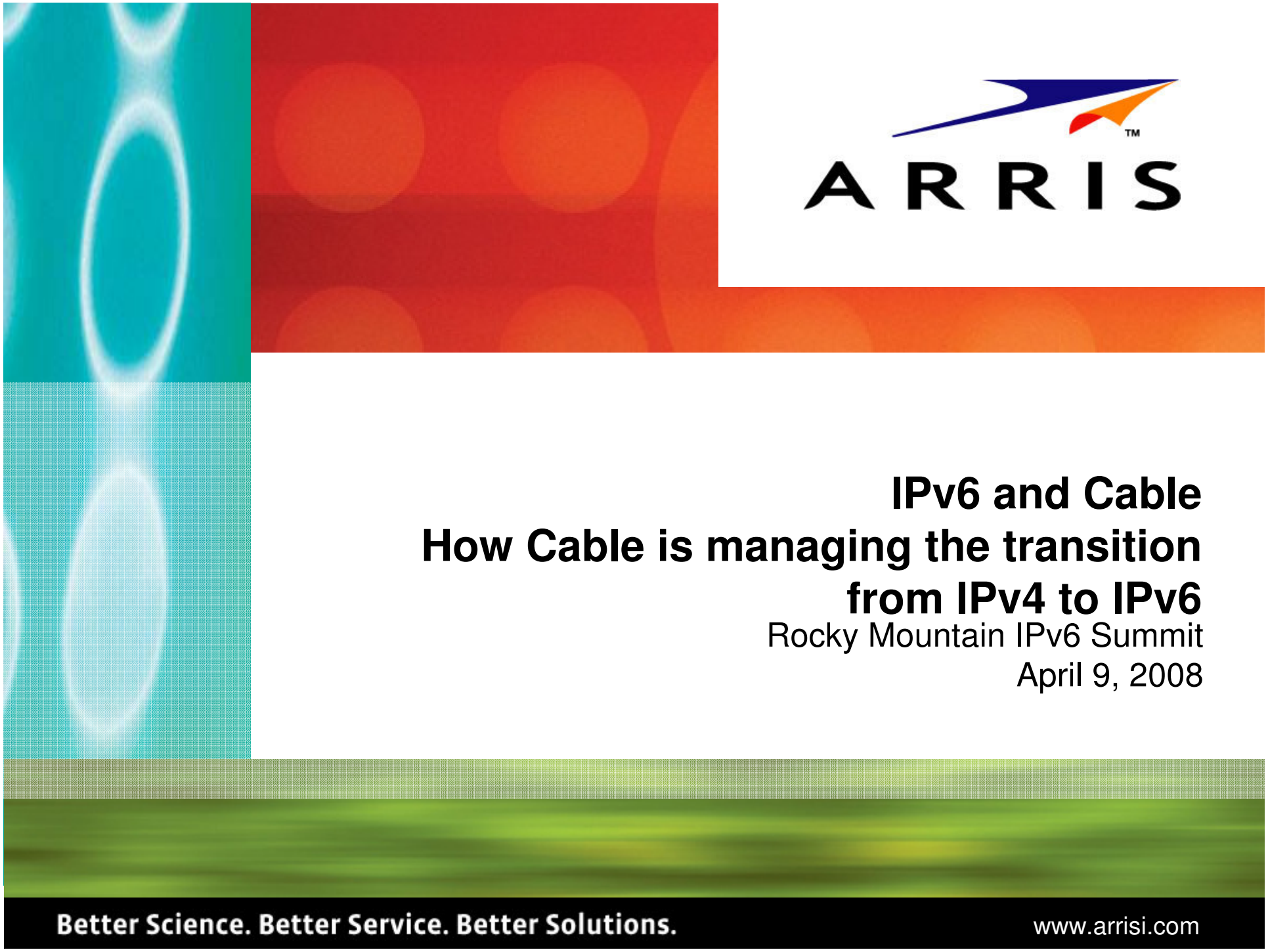


IPv6 and Cable
How Cable is managing the transition from IPv4 to IPv6

Rocky Mountain IPv6 Summit

April 9, 2008

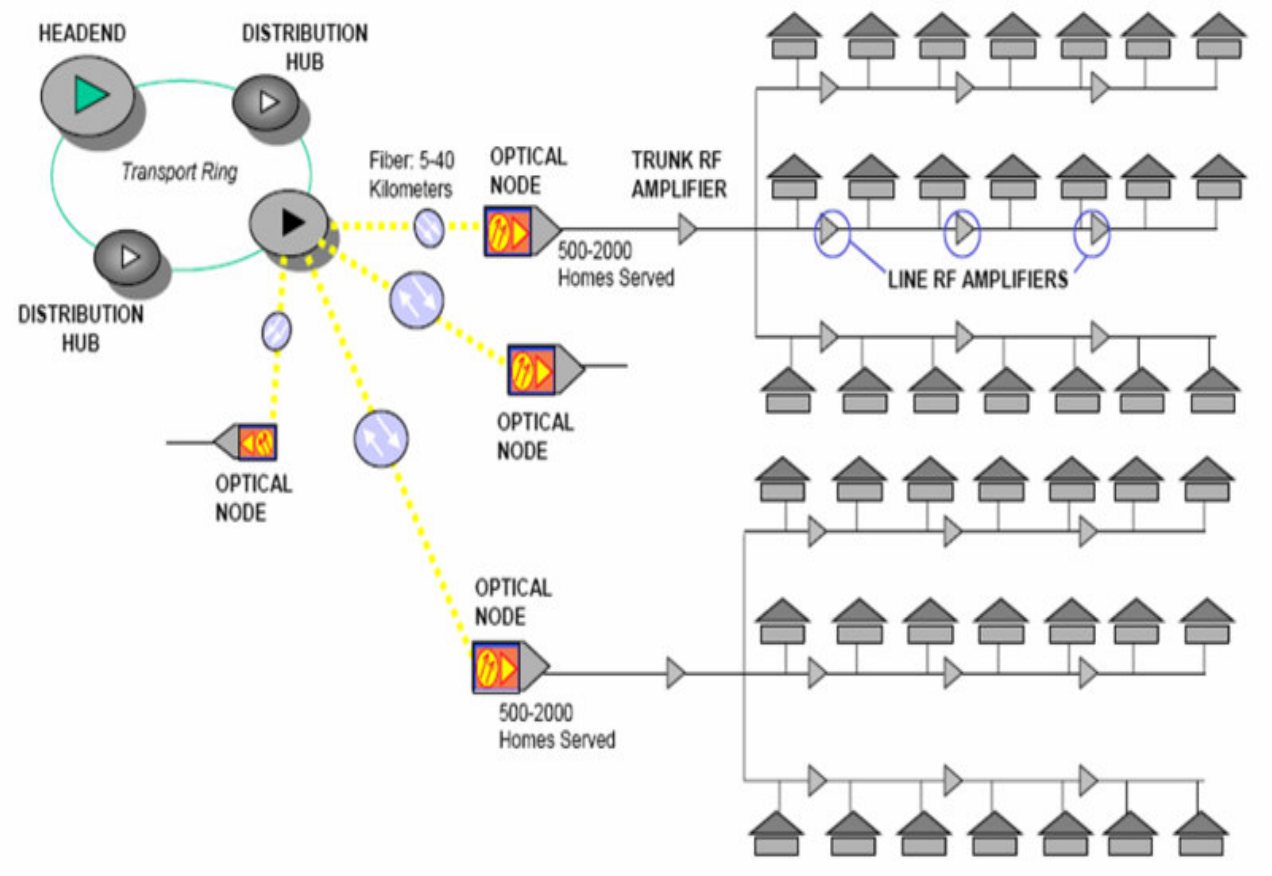
Agenda

- Cable 101
- How Cable is adopting IPv6
- Cable's migration to IPv6 and IPv4 coexistence
- Questions

Terms

- Headend: A location from which all cabling and programming originates in a cable system. This is analogous to a central office in a Telco world
- HFC: Hybrid Fiber Coax – Term that defines the type of distribution network between the headend and the customer home or business
- CMTS: A Cable Modem Termination System
- CM: Cable modem
- DOCSIS: Data over Cable System Interface Specification. A set of industry specifications that define the MAC Layer protocols and operation between a CMTS and CM

Sample Cable TV Distribution Architecture



HOW CABLE IS ADOPTING IPV6

DOCSIS Specifications

- The Cable industry early on adopted a requirement to develop and use a standard architecture and set of specifications
- This effort resulted in a set of specifications called DOCSIS – Data over Cable System Interface Specification.
- The first DOCSIS specifications were released in 199x and have been upgraded over time.

IPv6 and DOCSIS

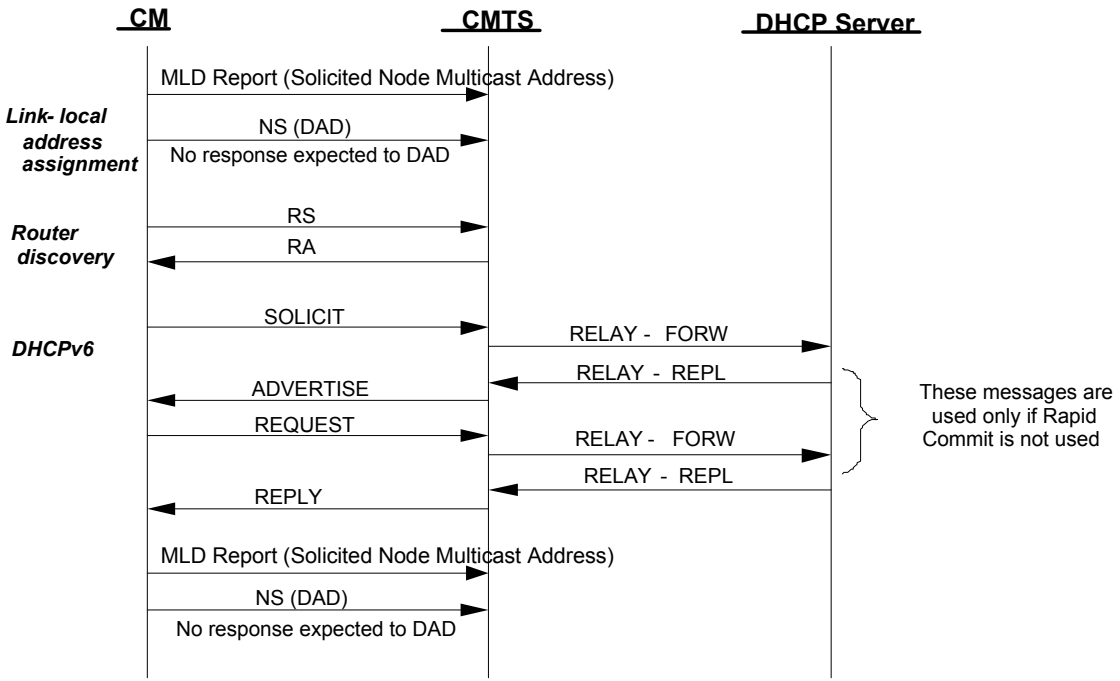
- Until very recently, DOCSIS only defined the use of IPv4 protocols for management and data forwarding by DOCSIS devices.
- The latest generation of DOCSIS Specifications, DOCSIS 3.0, includes support for IPv6.
- IPv6 may be used by the operator for both the CM management stack and customer equipment in the home.

IPv6 and DOCSIS

- Provisioning
  - DOCSIS now defines that a CM can operate in single stack IPv6 or IPv4, Dual Stack or a hybrid mode called Alternative Provisioning mode where the CM attempts IPv6 first and if unsuccessful, falls back to IPv4 operation
  - All forms of provisioning make use of DHCP in order to provide operators with a higher degree of control over their allocation of addresses and allows for multiple prefixes to be used for different classes of devices
  - DOCSIS has also defined the use of DHCPv6 Rapid Commit and DHCP Reconfigure for CMs as well as several Vendor Specific Information options to carry required and optional CM configuration information

IPv6 Provisioning Flows

- The CM first looks for MAC management messages from the CMTS to determine the provisioning mode.
- The CM the looks for Routing Advertisement (RA) Messages from the CMTS to determine the prefix(es) assigned to this link.
- The CM then builds a Link-Local address, and then attempts DHCPv6 to obtain a management address.



- Management
  - A few changes were needed to support an IPv6 address for management purposes on the CM.
    - Previous versions of DOCSIS defined the use of NmAccess (RFC2669) and SNMP Coexistence (RFC 3410-3415, 3484)
    - DOCSIS also defined that RFC 3419 be implemented to allow for IPv6 addresses to be used in the SNMP Coexistence configuration.
    - These parameters are established through the configuration file received by the CM during the registration process

Additional IPv6 impacts in DOCSIS

- Packet Classification
  - DOCSIS has always had a rich set of packet classification capabilities.
    - Classification of packets via individual L2, L3 and L4 criteria, or criterion ranges
    - For IPv6 this is challenging due to the format of the IPv6 packet with the potential for multiple headers
- Filtering
  - In earlier versions of DOCSIS, filtering and classification were separate, but each could filter on L2, L3 and L4 attributes of an IPv4 packet
  - In DOCSIS 3.0, the industry moved to a model where the rich packet classification mechanism is used for filtering packets coming from the CM
    - The CMTS polices the packets forwarded to the CM and beyond
  - The older model is still supported for IPv4 and operation in legacy environments
- Source Address Verification
  - DOCISS and Cable In general have always been concerned about theft of service and making sure a device is authorized for access
    - DOCSIS has defined a set of requirements that include the use of DHCP Lease Query (RFC RFC 4994 DHCP v4 lease Query, and RFC 5007 – DHCPv6 Lease Query and draft-ietf-dhc-dhcpv6-bulk-leasequery-00.txt) as a methods for the CMTS to get information regarding a device's ability to use a specific IP address

New DOCSIS Device - eRouter

- A new lightweight dual stack routing device called an eRouter has been specified, replacing the more complex CableHome specification and adding support for IPv6
  - IPv4 or IPv6 or Dual Stack operation on WAN interface
  - Can NAT (RFC 1918) for IPv4 and route (static routing only in spec) IPv6 with Prefix Delegation (via DHCP)
  - Customer LAN can be configured via DHCPv6 or SLAAC
  - Support for IPv4/v6 Multicast and IGMPv2/v3- MLDv1 and MLDv2

HOW CABLE IS MIGRATING TO IPV6

“Typical Cable System”

- 1-4 CMTS in a headend
  - Each CMTS services between 5000 and 18,000 subscribers.
  - Each subscriber takes up
    - One private IPv4 address for the Cable Modem (management) and one or more public IPv4 addresses for the CPE devices in the customer’s home or office
    - If the CM has a Telephony Adapter, the MTA will take a public IPv4 address, acting as an embedded CPE
    - Many homes have a retail-purchased gateway router which will take a public IPv4 address that will be shared amongst the CPEs attached to the router via NAPT, or one-way NAT

Scale

- In our example, each CMTS provides connectivity for 13k to 40k IPv4 addresses
- In some headends, this equates to close to 160k or more IPv4 addresses.
- Most of the major MSOs have hundreds of headends where CMTS' provide service

Some Realities

- Not all devices will be able to support IPv6 addresses due to several design imposed limitations
  - Not enough memory to support the IPv6 protocol and management stack
  - Not enough processor to handle line rate IPv6 classification and filtering
- The number of IPv6 addresses will only expand
  - This is due to new devices being deployed that support IPv6 from the start – IP Set Top Boxes, new customer devices in the home/office
- IPv4 will exist in these networks for many years, but represent a smaller and smaller total of the population

More Realities

- Drive to IPv6 not based on “Killer Application”
  - The industry is driven to IPv6 by IPv4 address exhaustion
- Significant IPv6 work needs to be done for basic services – email, web, gaming, etc
  - Chicken and egg dilemma
    - Industry needs IPv6 devices to generate the need to migrate content to IPv6 based servers. IPv6 Servers won’t happen quickly if no IPv6 hosts out there to request services….

Current CMTS IPv4 Configurations

- In most cases today, several different IPv4 subnets are used by different devices on the network
  - Cable Modems (CMs) normally get a 10.x address from RFC 1918, at times, this space has run out and ARIN allocated public space is used instead
  - CPE devices in the customer home get 1-5 public addresses
    - Many homes have a gateway that uses NAT for the internal PCs so only one Public IPv4 address is needed
  - Telephony Modems require 1 additional Public IPv4 address for operation

Current CMTS Configuration

- At an interface level we have:
  - Primary addresses/subnet for use on the CM
  - Secondary addresses/subnets for use on the CPE and telephony adapters
- Using a technology referred to as “IP Bundling,” multiple Layer 2 MAC Domains on the CMTS share a common L3 IP space to help simplify configuration and management, while reducing IP address fragmentation

CMTS Configuration

- With IPv6, comes major changes
  - Some populations of new DOCSIS 3.0 CMs and certain DOCSIS 2.0 CMs will migrate to IPv6 management very early, the DOCSIS 2.0 CMs will require a firmware upgrade
  - CPE will continue to be heavily biased towards IPv4, slowly migrating to IPv6 over time
  - MTAs or Telephony modems will get an IPv6 address for the CM management and either IPv4 or IPv6 for the Telephony portion, again, this will require firmware upgrade
  - New Set Top Boxes (STBs) are being designed for IPv6 and IPv4 management

IPv6 Deployment Strategy

- For cable, several questions need to be asked and answered – each has an impact on the IPv6 network design and allocations
  - How many and how large are the prefixes assigned to each CMTS/Headend/Regional Aggregation Center
  - Will the CMTS use one or more prefixes to separate DOCSIS devices from CPE? Will one prefix be used and carved into smaller pieces for different device classes and customers (residential vs Business)
  - How soon will IPv6 support for CPE in the home be turned on? What Operating Systems will be supported?
    - Vista, XP – DHCP Client, SLAAC
    - MAC OS – no DHCP Client SLAAC only now

IPv6 Depoyment

- Some Cable Operators manage their own Nationwide backbone and others choose to pier at a regional level. These different architectures place different requirements on the planning for IPv6 deployments

IPv6 Deployment Strategy

- Develop firm plan
  - Routing and connectivity, routing protocols
  - Prefix allocations for Headend, CMTS etc.
- Back Office Servers and equipment
  - DHCP, DNS, NMS, DPI, and related equipment first
  - Customer services next – email, web, gaming, etc
- Testing
- Trial and pre-production verification – Partial IPv6 deployment
- Production – Full deployment to a given headend, region, aggregation center.

IPv6 Deployment Tasks

- Routers and routing software needs to be upgraded and verified for IPv6 operation
  - OS upgrades and memory and processor upgrades may be needed.
  - Switches and other network equipment needs to be verified to work properly with IPv6 and Multicast protocols (MLDv1)
- Management platforms need to be upgraded to Dual Stack to manage both IPv4 and IPv6 devices

IPv6 Deployment Tasks

- For Cable, nearly all IP addresses are assigned by DHCP.
  - For IPv4 and IPv6 this means significant work to upgrade and scale the needed infrastructure to support the huge volume of devices needing IP addresses.
  - An open question will be the use of Stateless Autonomous Auto Configuration (SLAAC) for CPE
  - Prefix Delegation and dynamic updating of routing tables also needs to be worked out and verified

IPv6 Deployment Tasks

- DNS and other Back Office systems need to be deployed or upgraded to handle traffic from both IPv4 and IPv6 devices.
  - For DOCSIS this includes time of day servers, configuration file servers, firmware management systems, trap and syslog servers, and DPI and firewalls.

IPv6 Deployment Tasks

- Training
  - By far and away, this is the part that scares people the most
    - Many customer support folks understand – or have good scripts for – IPv4 configuration and troubleshooting. This needs to be replicated for IPv6
    - IPv6 in some ways is very similar, but in many ways is very different
    - IPv6 in the home also may require some additional training for customer and support folks

Summary

- Cable Operators face many of the same issues any business faces when adopting IPv6
  - Planning, verification, upgrades
  - Training of staff and customers
- However, Cable networks often come with issues of scale and volume
- Cable operators are forced not by application demand, but by address exhaustion to deploy IPv6

Questions?

My Contact Info

Dan Torbet
Sr. Staff System Architect
Office of the CSO

9600 E. Geddes Avenue
Centennial, CO 80112
1.720.895.7130
dan.torbet@arrisi.com

www.arrisi.com