DTLink Inc

White Paper

Fixed Wireless Architecture
Wireless Star Topology

January, 2006

Notice

The information in this document is subject to change without prior notice. All statements, information and recommendations in this document are believed to be accurate, but are presented without warranty of any kind, expressed or implied. Users should take full responsibility for their use of any products.

DTLink Inc
2, place de la Taconnerie
1204 Geneva
Switzerland

Preface

In many regions of the world, municipalities are faced with the dilemma of providing a digital network for a cost effective voice and last-mile data access to the residential and business customers in the absence of suitable existing wireline infrastructure. In the past, choices have been limited to running costly wires or fibers to the residents.

With the emergence of Wifi and broadband wireless technology a third solution presents itself that solves the access problem in a future-proof cost-effective manner. DTLink Inc **Wireless Star Topology** addresses the need for wireless access by offering a proven wireless network solution that combines toll-quality voice with always-on broadband packet data services.

Municipalities planning broadband wireless data deployments for residential and business customers must carefully consider issues related to network architecture. To avoid becoming trapped by constraints imposed by untried and unworkable implementation, issues related to scaling the network and support for future data services should be seriously considered.

Among the key questions are whether the architecture supports an addressing plan that is manageable and scalable considering the current tight availability of globally-unique IP addresses. The network should be able to support a broad range of customer requirements. The network should be able to support a broad range of customer requirements. For instance, business customers typically require unchanging presence on the Internet for Web and remote access servers, while residential customers normal do not. The data architecture should support customer Local Area Networks (LANs) without restrictions on type of equipment applications or operating systems.

Customers should expect to be able to use the network with minimum configuration for their data equipment. The data network should also be able to efficiently and transparently support the complete range of today's Internet Protocol-based (IP) data applications while providing an expandable architecture framework for the emerging services of tomorrow. As with any new technology, municipalities should expect that solutions providers be able to support their claims with field experience not just from small-scale trials but from real large scale-deployed operational networks.

DTLink Inc **Wireless Star Topology** provides an efficient, scalable, flexible framework for operators to implement broadband wireless data networks for municipalities.

Advantages

- Excellent performance

- Easy to setup and expand

- Any non-centralized failure will have little effect on the network

- Easy to detect faults

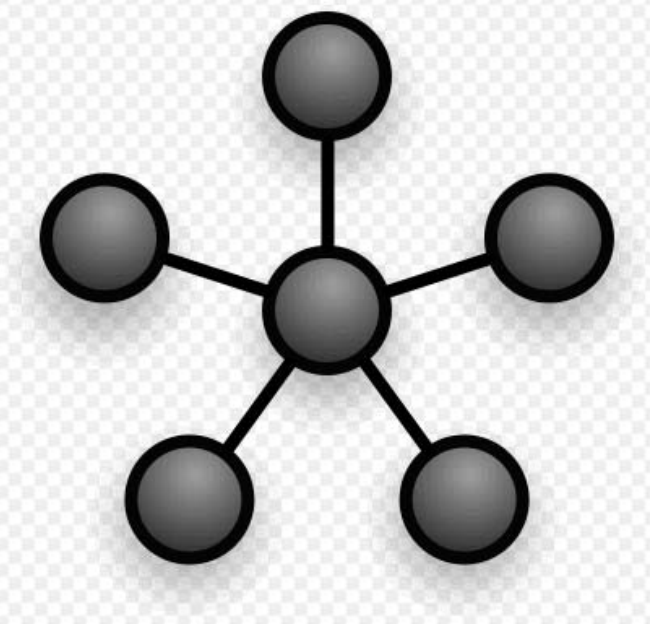
- Data packets are sent quickly as they do not have to travel through any unnecessary nodes

- Multiple stars can be connected together in a larger star topology

- Every star node can expand to cover a specific number of users

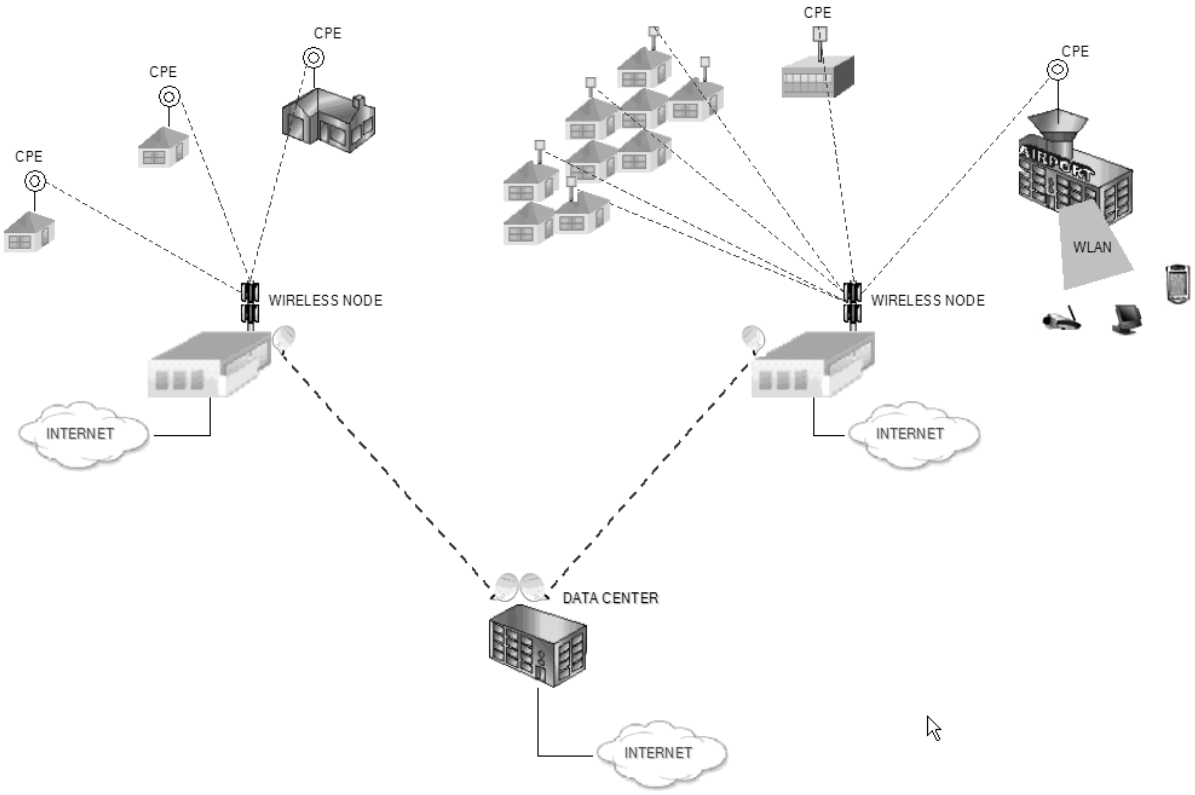
- Every star node may have its own access to the Internet

- Operation may concentrate to specific wireless nodes



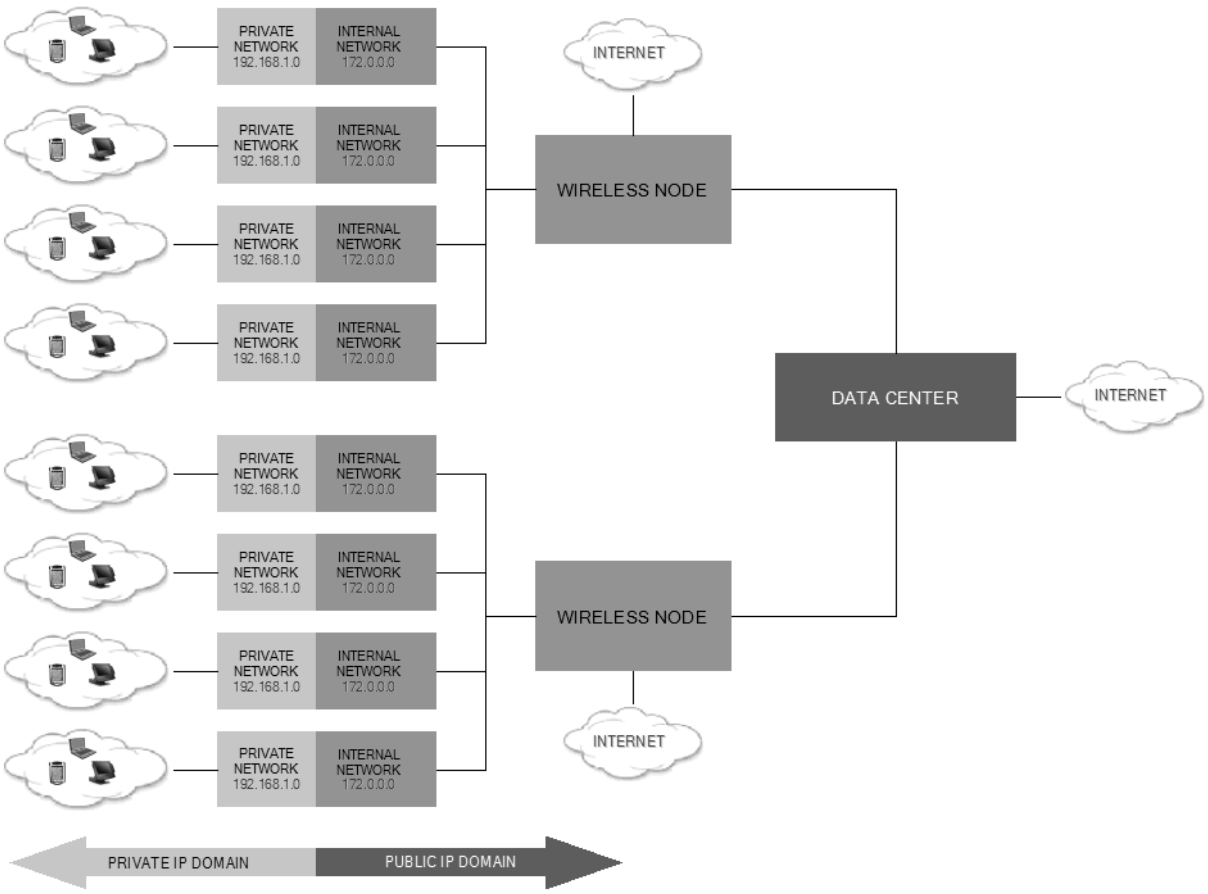
Data Network Architecture Overview

The basic design philosophy of the DTLink Inc **Wireless Star Topology** is to provide a simple, scalable, transparent access network for passing IP packets between the customer and external networks such as the Internet. The network architecture accomplishes this goal and features a reliable wireless channel for transporting IP packets with minimal overhead and low-latency between the **CPE** devices, **Wireless Nodes** and the **Data Center** interfacing to external networks.



The DTLink Inc **Wireless Star Topology** network as shown above offers to municipalities and residents the following features:

- Fixed wireless network featuring broadband packet-switched data with minimal latency and dedicated connection to the Data Center
- Field-proven design deployed and operated multiple metropolitan networks.
- Distributed access to the Internet from the Wireless Nodes for a minimal traffic between the Wireless Nodes and the Data Center
- Seamless integration with Internet and public/private IP carrier data networks
- Low-latency, transport-layer-aware wireless link
- Architecture flexibility for large-scale deployments

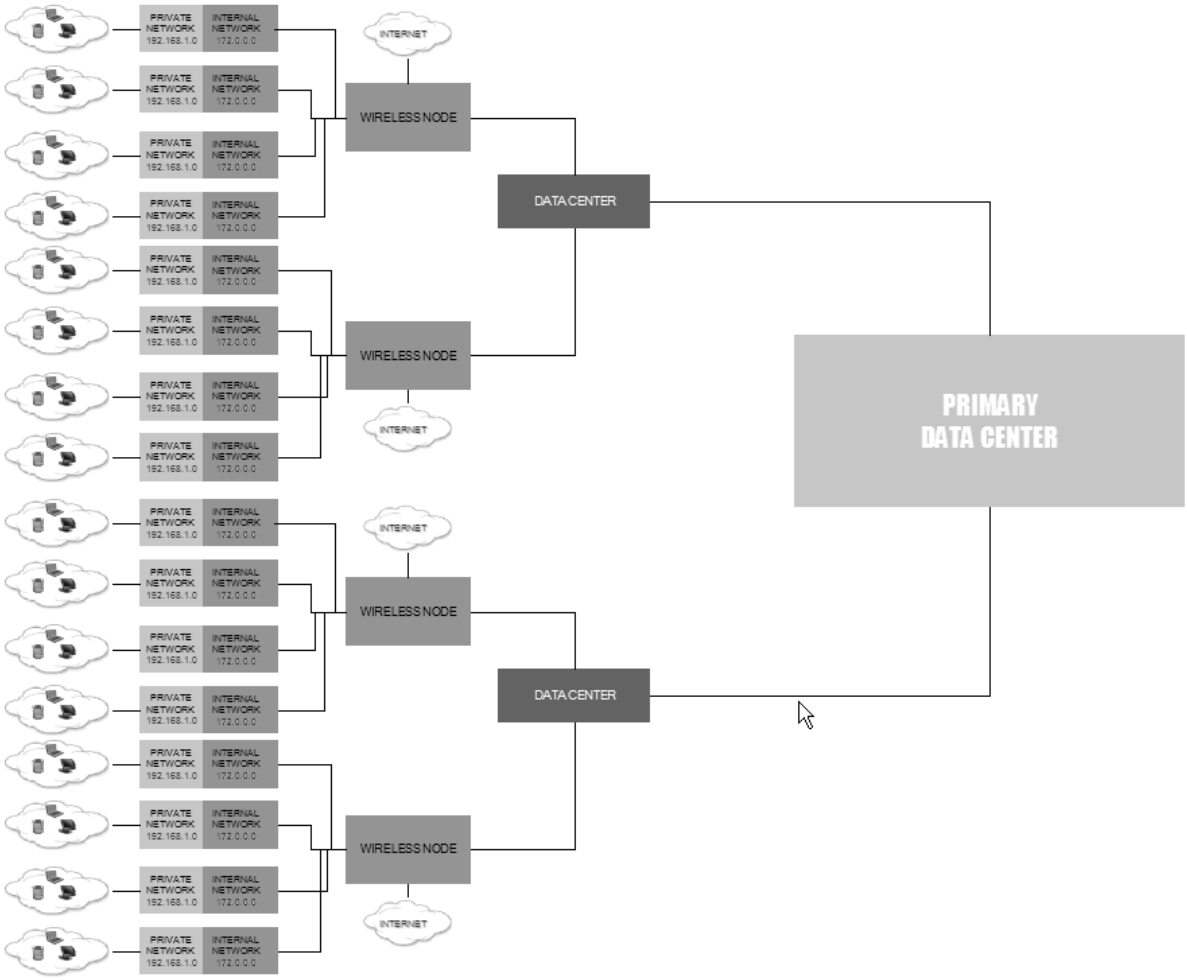


The previous schema illustrates the principle components of the data network including the subscriber unit (**CPE**) residing at the customer premises, the **Wireless Node**, which provides wireless coverage for a cell serving a collection of subscriber units, and the **Data Center**, which contains the data service and the operator's control center.

Each Wireless Node attaches to the Data Center via dedicated private network link.

Large-scale Deployments

Multiple star topologies may connect to a **Primary Data Center** in order to proceed to large-scale deployments.



In this case, the Data Centers will be connected to the Primary Data Center through dedicated wired or wireless connections.

Network Elements

Subscriber Unit

A subscriber unit, located at each residence, serves to interface the CPE on the data LAN to the wireless air interface. From a data network perspective the primary functionality of the subscriber unit includes:

- Forwarding between the local LAN and the wireless bridge
- Firewalled local LAN
- Bandwidth management
- QoS and packet filtering
- CPE gateway for valid external and internal addresses

Wireless Node

The subscriber unit's wireless interface terminates at the serving antenna of the wireless node, which provides coverage for a community of customers in a local coverage are. The wireless node provides data network functionality including:

- Forwarding of all IP traffic from the CPE
- Routing of all IP traffic according to topologically summarized address masks received from the network side
- Filtering of I{ data packets based on configurable ACL and header checksum (security and fraud prevention)
- Extensive OSS link and equipment monitoring including alarms, probes, and configuration control.

Data Center

Each wireless node maintains dedicated Point-to-Point links with the regional Data Center. The link may be a either wireless or wireline depending on the administrator's preference and available local infrastructure. In fact, the network architecture allows any reliable method of connection. The Data Center functionality includes:

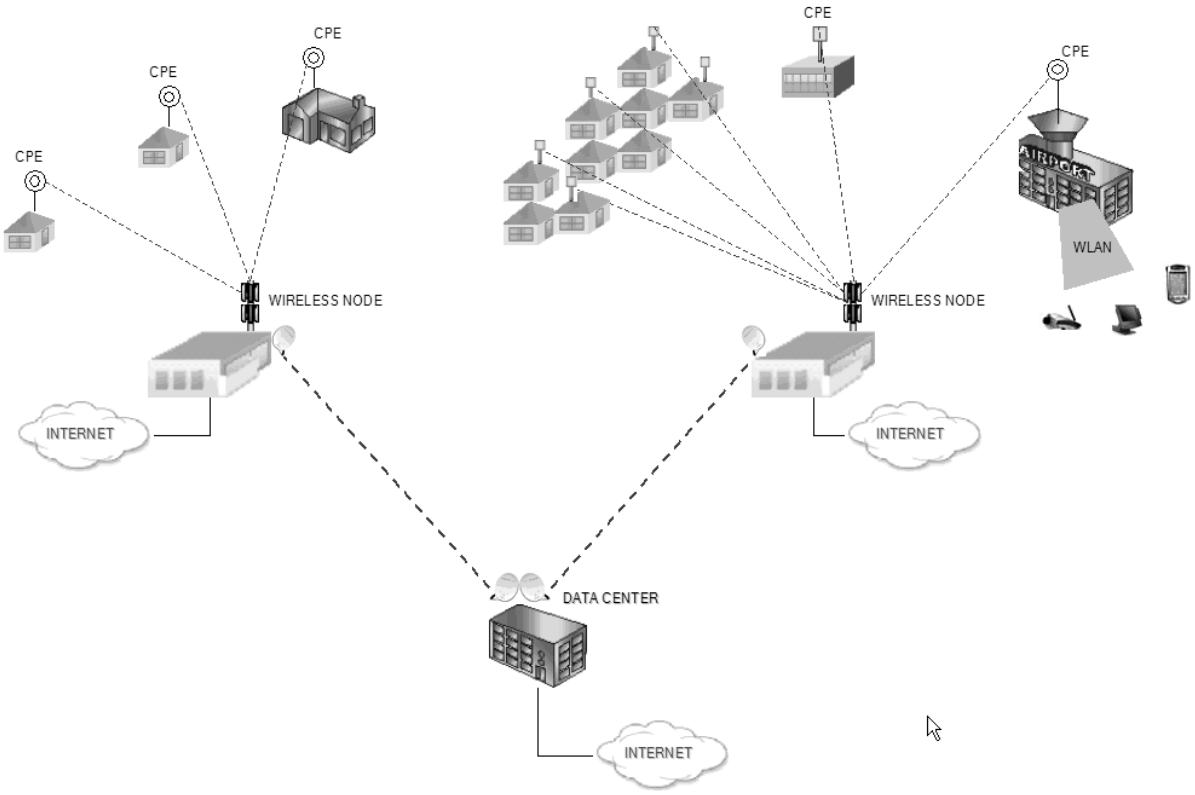
- Validation, filtering, translation, and routing of all IP traffic coming from external networks (in case of global Internet access)
- Policy-based routing of all IP traffic coming from the wireless nodes to either internal FWS server destinations, or out to the external networks after translation
- For private address CPE implementation plans, a Network Address Translation (NAT) server maintains a table including the public/private IP address aliases and translates between aliases for inbound and outbound data packets
- Extensive OSS link and equipment monitoring including alarms, probes, and configuration control

Primary Data Center (PDC) (optional only for large-scale networks)

Each Data Center maintains dedicated Point-to-Point links with the global PDC. The link may be a either wireless or wireline depending on the administrator's preference and available local infrastructure. In fact, the network architecture allows any reliable method of connection. In this case, the main server/router will be placed at the PDC location.

Distributed Internet Access

Internet access represents more than 90% of the traffic between the CPE devices and the external networks. For this reason, the DTLink Inc **Wireless Star Topology** allows a flexible Internet access from every Wireless Node eliminating intranet traffic between the wireless nodes and the regional Data Center.



This unique feature, allowing an unlimited number of gateways at the Wireless Node level, will provide a flexible gateway design especially for very large networks.

Flexible IP Network Architecture

The following sections describe the IP architectures that are used to support the residential and business requirements.

Address Plans

There are three basic CPE addressing plans that can be selected. They include:

- Public
- Private
- A combination of both public and private

Due to the relative scarcity of globally unique public Internet Protocol version four (IPv4) addresses, operators will often want to conserve the public address blocks allocated to customer data equipment. By default, each subscriber unit is allocated a DHCP configured address with an unlimited number of virtual addresses that can be assigned to the device. This means that an unlimited number of public IP addresses can be directed to a specific CPE without compromising the overall security.

Private Address Plan

In the current IPv4 standard there are several blocks of addresses reserved for private networks. One of these class-A block, net-10, spans approximately 16 million host addresses which is sufficient for very large municipal deployments. The advantage of access to such large contiguous address blocks is that the network can be laid out based on data center, which simplifies routing of IP packets resulting in lower operations and maintenance costs.

Every CPE device receives an internal IP address from the Data Center main server/router allowing the configuration of the gateway and DNS server at the CPE level.

However, the private address blocks are not transportable across public networks and must be used in conjuction with NAT for communicating with external public networks such as Internet.

Large corporate data network operators have used this familiar protocol for many years. NAT works by dynamically translating between public and private address aliases when IP packets pas through a NAT gateway. From the customer's perspective, NAT is a transparent operation that requires no configuration or intervention to function.

There are various flavours of NAT, but best protocol behaviour results from using one-to-one NAT, meaning, each active CPE consumes a unique public address. The NAT gateway is located at the main server/router and is provisioned with pools of public addresses for address translations. The NAT gateway functions by translating outgoing (customer-to-Internet) source addresses from private-to-public and incoming destination addresses back from public to private for delivery to the CPE within the municipality network. This means that the public address pool can be substantially smaller than the total number of customer CPE data devices thus conserving the public address space. Another advantage is that customer privacy and security are enhanced since a particular public address cannot be used to identify a customer.

Public Address Plan

Some customers, particularly small to medium enterprises, may require dedicated public addresses for their CPE. In contrast to residential service, they expect to be able to maintain a constant Internet presence to operate local servers for important business applications, such as Web, FTP, mail and VPN services.

For businesses or certain high-end residential customers, this requirement is best satisfied by provisioning each subscriber unit with a static block of public IP addresses used for the customer's IP devices. Each gateway server placed at a wireless node or the data center can be preprovisioned with blocks of public addresses. As with the private address architecture, the number of addresses allocated to a given subscriber unit (CPE) is flexible and depends only on the size of the public address block(s) available to the server. A particularly efficient use of the public address pool would be to allocate each CPE unit with one or more IP addresses, one for the CPE and the others for a local customer or gateway/firewall servicing a local business private network. In contrast to private addressing, public addresses are static

and bound to a particular CPE device. DHCP is used to automatically configure a particular data CPE with an address, which is the released when the device is taken off-line. The public addresses are globally unique and NAT is therefore not required.

The public and private address architecture are disjoint and do not interfere with each other. Operators are free to configure deployments with a combination of private and public addresses to support residential and business requirements.

IPv6

In the future, Internet Protocol version six (IPv6) with its expanded address space will gradually reduce the need for using private addresses, allowing the option o CPE deployments with all-public IPv6 address configurations. The DTLink Inc **Wireless Star Topology** is ready to support next-generation IP protocol when carried Wide Area Network (WAN) backbones make transparent transport of IPv6 reality.

Customer LANs

At the customer premises the CPE device acts as the data LAN gateway for local IP data equipment. There are a variety of LAN formats that can be supported directly to through customer provided equipment. The default CPE supports data networking using TV cable adapters or HomePNA adapters. The advantage of these inexpensive and reliable technologies is that new premises wiring is not required and simultaneous voice and data services are supported on the same existing inside wiring.

The requirements on the customer data equipment are minimal; only basic support of IP and DHCP are required. There is no software connectivity client required on the device, which eliminates configuration issues for both the customer and network operator. The network therefore accepts all types of CPE operating systems.